Panda Adaptive Defense 360

Guía de administración de Panda Adaptive Defense 360 sobre Aether

Versión: 3.40.00-00a

Autor: Panda Security

Fecha: 27/8/2018

Tabla de contenidos

1. Prólogo

¿A quién está dedicada esta guía?
¿Qué es Panda Adaptive Defense 360 sobre Aether?
Iconos

1.1. Introducción

Esta guía contiene información básica y procedimientos de uso para obtener el máximo beneficio del producto **Panda Adaptive Defense 360 sobre Aether**.

1.2. ¿A quién está dirigida esta guía?

Esta documentación está dirigida a los administradores de red que gestionan la seguridad informática de su empresa.

Para sacar el máximo provecho del producto, **Panda Adaptive Defense 360 sobre Aether** requiere conocimientos técnicos en entornos Windows a nivel de procesos, sistema de ficheros y registro, así como entender los protocolos de red utilizados con mayor frecuencia. De esta manera, el administrador podrá interpretar correctamente la información ofrecida por el producto y extraer conclusiones que ayuden a fortalecer la seguridad de su empresa.

1.3. ¿Qué es Panda Adaptive Defense 360 sobre Aether?

Panda Adaptive Defense 360 sobre Aether es un servicio gestionado que protege los equipos informáticos de la empresa, ayuda a determinar el alcance de los problemas de seguridad detectados y permite establecer planes de respuesta y prevención frente a las amenazas desconocidas y a los ataques dirigidos avanzados (APTs).

Panda Adaptive Defense 360 sobre Aether está dividido en dos áreas funcionales bien diferenciadas:

- Panda Adaptive Defense 360
- Plataforma Aether

Panda Adaptive Defense 360

Es el módulo que implementa todas las características orientadas a garantizar la seguridad de los puestos de usuario y servidores, sin requerir la intervención del administrador de la red.

Plataforma Aether

Es una plataforma eficiente, extensible y escalable para gestionar centralizadamente los productos de Panda Security. **Aether** permite presentar la información generada por **Panda Adaptive Defense 360** sobre los procesos, los programas ejecutados por los usuarios y los dispositivos instalados en la empresa, todo ello en tiempo real, de forma ordenada y con un alto nivel de detalle.

Aether es una plataforma diseñada para cubrir las necesidades de la gran cuenta y de MSPs.

1.4. Iconos

En esta guía se utilizan los siguientes iconos:

Aclaraciones e información adicional, como, por ejemplo, un método alternativo para realizar una determinada tarea.

Sugerencias y recomendaciones.

Consejo importante de cara a un uso correcto de las opciones de **Panda Adaptive Defense 360.**

Consulta en otro capítulo o punto del manual.

2. Introducción

Características principales del producto
Características principales de la plataforma
Componentes principales de la arquitectura
Servicios
Perfil de usuario del producto
Dispositivos e idiomas soportados
Recursos y documentación

2.1. Introducción

Panda Adaptive Defense 360 sobre Aether es una solución basada en múltiples tecnologías de protección que permite sustituir el producto de antivirus tradicional por un completo servicio de seguridad gestionada.

Ejecución de software lícito

Panda Adaptive Defense 360 supervisa y clasifica todos los procesos ejecutados en el parque informático en base a su comportamiento y naturaleza. Gracias a este servicio los puestos de usuario y servidores son protegidos limitando la ejecución de los programas instalados a aquellos que han sido previamente certificados como seguros.

Adaptación al entorno de la empresa

A diferencia de los antivirus tradicionales, **Panda Adaptive Defense 360 sobre Aether** utiliza un nuevo concepto de seguridad que le permite adaptarse con precisión al entorno particular de cada empresa. Para ello supervisa la ejecución de todas las aplicaciones y aprende constantemente de las acciones desencadenadas por los procesos lanzados en los puestos de usuario y servidores.

Tras un breve periodo de aprendizaje, **Panda Adaptive Defense 360 sobre Aether** es capaz de ofrecer un nivel de protección muy superior al de un antivirus tradicional.

Alcance y solución de problemas de seguridad

La oferta de seguridad se completa con herramientas monitorización, análisis forense y resolución, que determinan el alcance de los problemas detectados y los solucionan.

La monitorización aporta datos valiosos sobre el contexto en el que se sucedieron los problemas de seguridad. Con esta información, el administrador podrá determinar el alcance de los incidentes e implantar las medidas necesarias para evitar que se vuelvan a producir.

Multiplataforma

Panda Adaptive Defense 360 sobre Aether es un servicio multiplataforma alojado en la nube y compatible con Windows, macOS, Linux y Android; por esta razón, solo es necesaria una única herramienta para cubrir la seguridad de todos los equipos de la empresa.

Panda Adaptive Defense 360 no necesita nueva infraestructura IT en la empresa para su gestión y mantenimiento, y por esta razón reduce el TCO de la solución a niveles muy bajos.

2.2. Características principales de Panda Adaptive Defense 360 sobre Aether.

Panda Adaptive Defense 360 ofrece un servicio de seguridad garantizada frente a amenazas y ataques avanzados y dirigidos a las empresas a través de cuatro pilares:

- **Visibilidad**: trazabilidad de cada acción realizada por las aplicaciones en ejecución.
- **Detección**: monitorización constante de los procesos en ejecución y bloqueo en tiempo real de ataques *Zero-day*, ataques dirigidos y otras amenazas avanzadas, diseñadas para pasar desapercibidas a los antivirus tradicionales.
- **Resolución y Respuesta:** información forense para investigar en profundidad cada intento de ataque, y herramientas de resolución.
- **Prevención**: evita futuros ataques modificando la configuración de los distintos módulos de protección y parcheando las vulnerabilidades de los sistemas operativos y de las aplicaciones instaladas.

*Figura 1: los cuatro pilares de la protección avanzada de **Panda Adaptive Defense 360***

2.3. Características principales de la plataforma Aether

Aether es la nueva plataforma de gestión, comunicación y tratamiento de la información desarrollada por Panda Security, encargada de agrupar y centralizar los servicios comunes a todos sus productos.

La plataforma **Aether** gestiona las comunicaciones con los agentes desplegados y presenta en la consola de administración, de forma ordenada y comprensible, toda la información recogida por **Panda Adaptive Defense 360** para su posterior análisis por parte del administrador de la red.

Por su parte**, Panda Adaptive Defense 360** ha sido desarrollado para sacar partido de los servicios suministrados por la plataforma **Aether.** De esta manera, permite focalizar todos los esfuerzos invertidos en el desarrollo del producto en mejorar la seguridad de los clientes.

Este diseño modular de la solución evita la instalación de nuevos agentes o productos en los equipos del cliente por cada módulo adicional contratado. Todos los productos de Panda Security que funcionen sobre la plataforma **Aether** comparten un mismo agente en el equipo del cliente y una misma consola web de administración, facilitando su gestión y minimizando los recursos de los equipos.

2.3.1 Principales beneficios de Aether

A continuación, se presentan los principales servicios ofrecidos por **Aether** para todos los productos de Panda Security que sean compatibles con la plataforma:

- **Plataforma de gestión Cloud**

Aether es una plataforma que reside en la nube de Panda Security, lo cual incorpora importantes ventajas de cara a su manejo, funcionalidad y accesibilidad:

- No requiere servidores de gestión que alojen la consola de administración en las instalaciones del cliente: al funcionar desde la nube, es directamente accesible por todos los equipos suscritos al servicio, desde cualquier lugar y en cualquier momento, sin importar si están dentro de la oficina o desplazados.
- El administrador de la red puede acceder a la consola de administración desde cualquier momento y en cualquier lugar, simplemente con un navegador compatible desde un equipo portátil, un equipo de sobremesa o incluso un dispositivo móvil como una tablet o un smartphone.
- Es una plataforma ofrecida en régimen de alta disponibilidad, operativa el 99'99% del tiempo. El administrador de la red queda liberado de diseñar y desplegar costosos sistemas en redundancia para alojar las herramientas de gestión.

- **Comunicación con la plataforma en tiempo real**

El envío de configuraciones y tareas programas desde y hacia los equipos de la red se realiza en tiempo real, en el momento en que el administrador aplica la nueva configuración a los dispositivos seleccionados. El administrador puede ajustar los parámetros de la seguridad de forma casi instantánea para solucionar posibles brechas de seguridad o adaptar el servicio de seguridad al constante cambio de la infraestructura informática de las empresas.

- **Multi producto y Multiplataforma**

La integración de los productos de Panda Security en una misma plataforma ofrece las siguientes ventajas al administrador:

- **Minimiza la curva de aprendizaje**: todos los productos comparten una misma consola, de esta forma se minimiza el tiempo que el administrador requiere para aprender el manejo de una nueva herramienta, redundando en menores costes de TCO.
- **Único despliegue para múltiples productos**: solo es necesario un único programa instalado en cada equipo para ofrecer la funcionalidad de todos los productos compatibles con **Aether Platform**. De esta forma se minimizan los recursos utilizados en los equipos de los usuarios en comparación con la utilización de productos independientes.
- **Mayores sinergias entre productos**: todos los productos reportan en una misma consola y en una única plataforma: el administrador dispone de un único panel de control donde puede observar toda la información generada, minimizando el tiempo y el esfuerzo

invertido en mantener varios repositorios de información independientes y en consolidar la información generada en un único formato.

- **Compatible con múltiples plataformas**: ya no es necesario contratar distintos productos para cubrir todo el espectro de dispositivos de la compañía: **Aether Platform** funciona para Windows, Linux, macOS y Android.

- **Configuraciones flexibles y granulares**

El nuevo modelo de configuración permite acelerar la gestión de los equipos mediante la reutilización de configuraciones, haciendo uso de mecanismos específicos como la herencia y la asignación de configuraciones a equipos individuales. El administrador de la red podrá asignar configuraciones mucho más específicas y con menor esfuerzo.

- **Información completa y a medida**

Aether Platform implementa mecanismos que permiten configurar la cantidad de datos mostrados a lo largo de una amplia selección de informes, según las necesidades del administrador o del consumidor final de la información.

La información de producto se completa además con datos sobre los equipos, hardware y software instalado, así como un registro de cambios, que ayudarán al administrador a determinar de forma precisa el estado de la seguridad del parque informático administrado.

2.3.2 Arquitectura de Aether

La arquitectura de **Aether** está diseñada de forma escalable para ofrecer un servicio flexible y eficiente. La información se envía y se recibe en tiempo real desde / hacia múltiples fuentes y destinos de forma simultánea. Los orígenes y destinos pueden ser equipos vinculados al servicio, consumidores externos de información como sistemas SIEM o servidores de correo, instancias web para las peticiones de cambios de configuración y presentación de información de los administradores de red, entre otros.

Además, **Aether** implementa un backed y una capa de almacenamiento que utiliza una amplia variedad de tecnologías que le permite manipular los múltiples tipos de datos de forma ágil.

En la Figura 2 se presenta un diagrama a alto nivel de **Aether Platform**.

2.3.3 Aether en los equipos de usuario

Los equipos de la red protegidos con **Panda Adaptive Defense 360 sobre Aether** llevan instalado un software, formado por dos módulos independientes pero relacionados, que aportan toda la funcionalidad de protección y gestión:

- **Módulo Agente de comunicaciones Panda (agente Panda)**: es el encargado de servir de puente entre el módulo de protección y la nube, gestionando las comunicaciones,

eventos y configuraciones de seguridad implementadas por el administrador desde la consola de administración.

- **Módulo Protección Panda Adaptive Defense 360**: es el encargado de proteger de forma efectiva el equipo del usuario. Para ello se sirve del agente de comunicaciones para recibir las configuraciones y emite estadísticas y datos de las detecciones y elementos analizados.

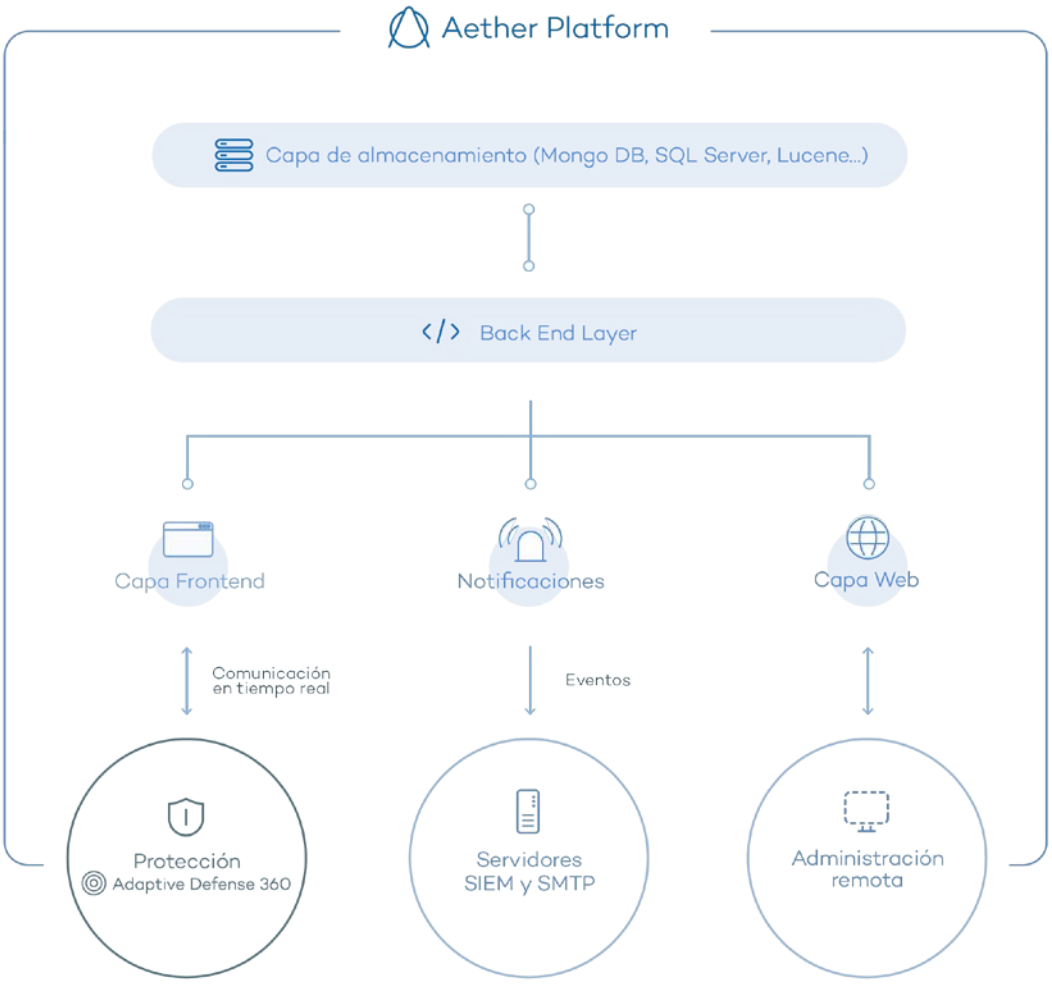


*Figura 2: estructura lógica de la **plataforma Aether***

- **Agente de comunicaciones en tiempo real Panda**

El agente Panda se encarga de las comunicaciones, tanto entre los equipos administrados y el servidor de **Panda Adaptive Defense 360** como de establecer un diálogo entre los equipos que pertenecen a una misma red del cliente.

Este módulo, además ser el encargado de la gestión de los procesos de la solución de seguridad, recoge los cambios de configuración que el administrador haya realizado a través de la consola Web, y los aplica sobre el módulo de protección **Panda Adaptive Defense 360**.

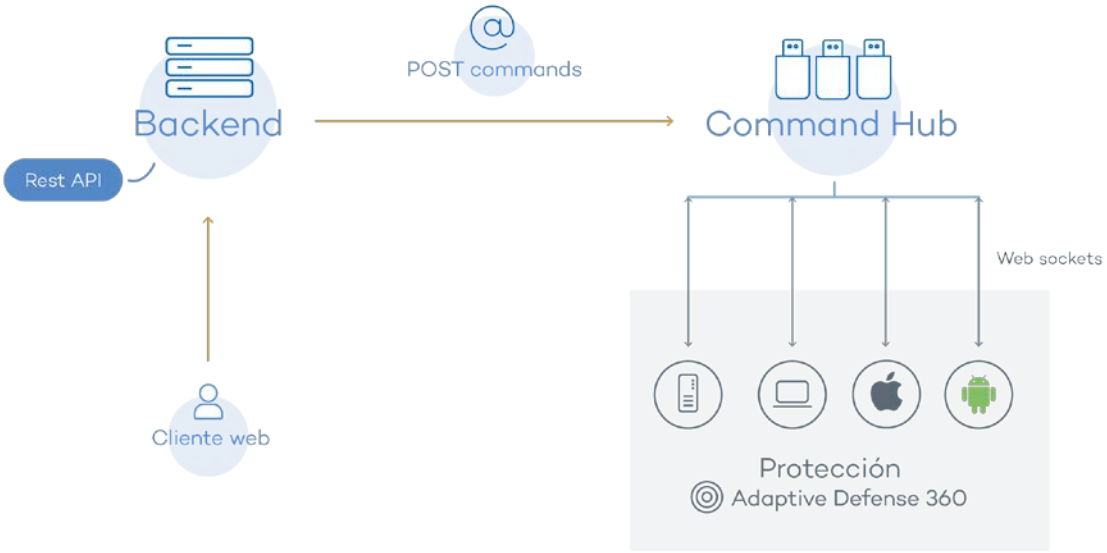


Figura 3: recorrido de los comandos introducidos con la consola de administración

La comunicación entre los dispositivos y el Command Hub se implementa mediante conexiones websockets persistentes y en tiempo real, estableciendo una conexión por cada uno de los equipos para el envío y recepción de datos. Para evitar que dispositivos intermedios provoquen el cierre de las conexiones, se genera un flujo de keepalives constante.

Las configuraciones establecidas por el administrador de la red mediante la consola de administración **Panda Adaptive Defense 360** se envían mediante una API REST al backend; éste las reenvía al Command hub generando un comando POST, el cual finalmente ejecuta un push de la información a todos los dispositivos suscritos. En ausencia de congestión en las líneas de comunicación y con un buen funcionamiento de elementos intermedios, los equipos recibirán la configuración en tiempo real.

2.4. Componentes principales de la arquitectura Panda Adaptive Defense 360

Panda Adaptive Defense 360 se apoya en el análisis del comportamiento de los procesos ejecutados en el parque de cada cliente. Este análisis aplica técnicas de Machine Learning en infraestructuras Big Data alojadas en la nube.

En la Figura 4 se muestra el esquema general de **Panda Adaptive Defense 360** y los componentes que lo forman:

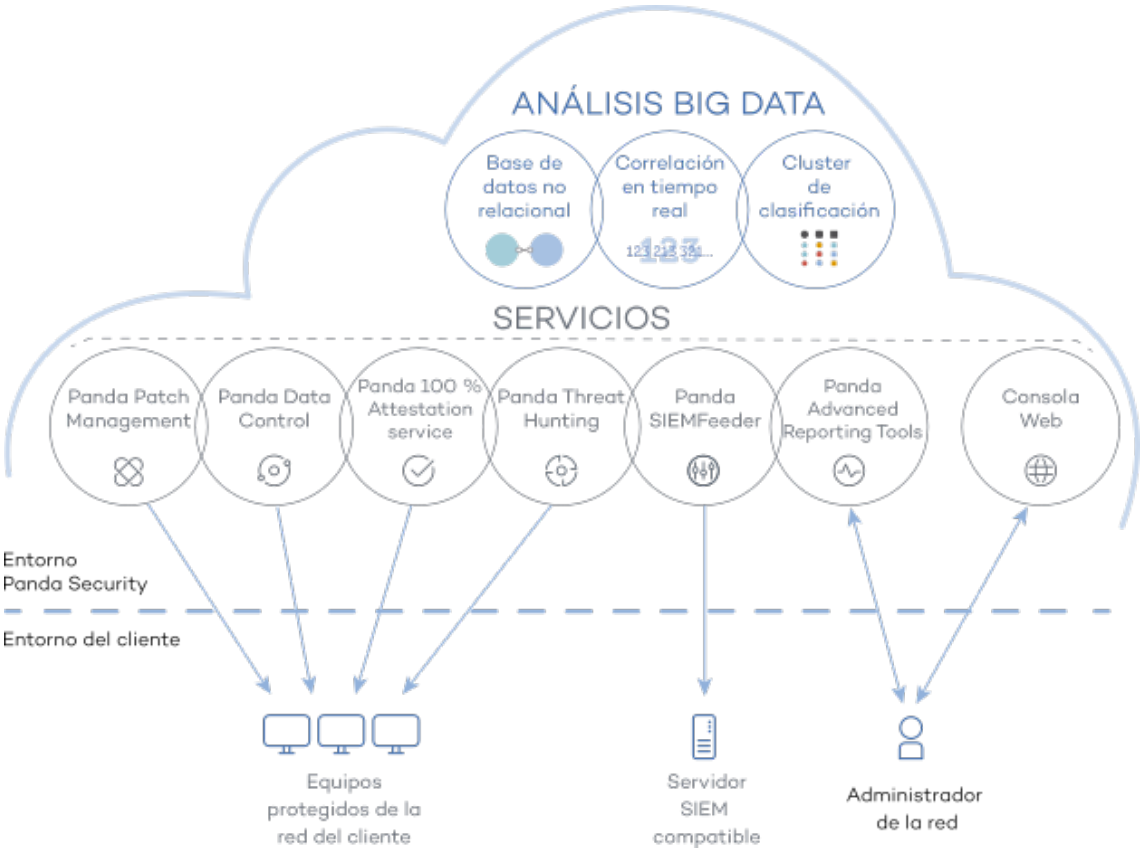


Figura 4: esquema general ***Panda Adaptive Defense 360***

Panda Adaptive Defense 360 está formado por los elementos mostrados a continuación:

- **Infraestructura de análisis big data**, formada por bases de datos no relacionales, servicios de correlación de eventos monitorizados en tiempo real y un cluster de clasificación de los procesos monitorizados.
- **Servicio 100% Attestation**: clasifica todos los procesos ejecutados sin ambigüedades ni falsos positivos ni negativos.
- **Servicio Threat Hunting**: relaciona de forma horizontal toda la telemetría recogida de la ejecución de procesos en todos los clientes para detectar amenazas avanzadas.
- **Panda SIEMFeeder** (opcional): integra **Panda Adaptive Defense 360** con soluciones SIEM de proveedores externos.
- **Servicio Panda Data Control** (opcional): servicio de visibilidad y supervisión de la información personal que almacenan los ficheros PII.
- **Servicio Advanced Reporting Tool** (opcional)**:** servicio de informes para generar inteligencia de seguridad avanzada.
- **Servicio Panda Patch Management** (opcional): parcheo de sistemas operativos Windows y aplicaciones de terceros.
- **Consola web**: servidor de la consola de administración.
- **Servidor SIEM** de la empresa (opcional).
- Equipos protegidos mediante el software **Panda Adaptive Defense 360** instalado.

- Equipo del administrador de red que accede a la consola Web.

A continuación, se detallan los diferentes roles de la arquitectura mostrada.

2.4.1 Infraestructura de análisis big data

El clúster de servidores en la nube recibe todas las acciones realizadas por los programas del usuario y monitorizadas por el módulo de protección instalados en los equipos del cliente. Mediante técnicas de inteligencia artificial, la granja de servidores **Panda Adaptive Defense 360** evalúa el comportamiento de dichos programas y dicta una clasificación por cada proceso en ejecución. Esta clasificación se devolverá al módulo de protección en el equipo, y será tomada como base para ejecutar las acciones pertinentes con el objetivo de mantenerlo el equipo protegido.

El clúster de **Panda Adaptive Defense 360** está formado por una granja de servidores alojada en la nube que forma un entorno de explotación Big Data. En este entorno se aplican de forma continua una mezcla de tecnologías basadas en algoritmos Machine Learning. Estos algoritmos clasifican los programas ejecutados tomando sus atributos estáticos, su información de contexto de ejecución y las acciones de los procesos monitorizados ejecutados en los equipos de los usuarios.

Las ventajas de este nuevo modelo de análisis de procesos en la nube frente al adoptado por los antivirus tradicionales basados en el envío de muestras al proveedor y análisis manual son:

- Todos los procesos de los equipos protegidos son monitorizados y analizados. De esta forma se elimina la incertidumbre de los antivirus tradicionales, capaces únicamente de reconocer el malware sin considerar el resto de aplicaciones.
- El retraso en la clasificación de los procesos vistos por primera vez (ventana de oportunidad) es mínimo ya que **Panda Adaptive Defense 360** envía las acciones en tiempo real que ejecuta cada proceso. Los servidores en la nube trabajan de forma continuada sobre estas acciones recogidas, de forma que se disminuye de manera sustancial el retraso en emitir una clasificación y por tanto el tiempo de exposición a las amenazas.
- La monitorización continúa de cada proceso permite a **Panda Adaptive Defense 360** clasificar como malware elementos que inicialmente tenían un comportamiento de goodware. Este patrón de actuación es muy habitual en los ataques dirigidos y otras amenazas avanzadas diseñadas para operar por debajo del radar.
- El análisis en la nube libera al cliente de instalar y mantener infraestructura de hardware y software junto al pago de licencias y la gestión de garantías del hardware, con lo que el TCO de la solución desciende significativamente.

2.4.2 Servidor Web de la consola de administración

Toda la gestión de **Panda Adaptive Defense 360** se realiza a través de la consola Web accesible para el administrador desde la URL https://www.pandacloudsecurity.com/PandaLogin/

La consola Web es compatible con los navegadores más comunes y es accesible desde cualquier lugar y en cualquier momento utilizando cualquier dispositivo que tenga instalado un navegador compatible.

Consulta el capítulo 4 La consola de administración para verificar si tu navegador es compatible con el servicio.

La consola Web es "responsive", de modo que se puede utilizar sin problemas desde móviles y tablets.

2.4.3 Equipos protegidos con Panda Adaptive Defense 360

Panda Adaptive Defense 360 requiere de la instalación de un componente software en todas las máquinas del parque informático susceptibles de sufrir problemas de seguridad. Este componente está formado por dos módulos: el agente de comunicaciones Panda y el módulo de la protección **Panda Adaptive Defense 360**.

El módulo de la protección **Panda Adaptive Defense 360** contiene las tecnologías encargadas de proteger los equipos del cliente. **Panda Adaptive Defense 360** reúne en un mismo producto todos los recursos necesarios para detectar el malware de nueva generación y ataques dirigidos (APT), al tiempo que incorpora herramientas de resolución para desinfectar los equipos comprometidos y determinar el alcance de los intentos de intrusión en la red del cliente.

Panda Adaptive Defense 360 se instala sin problemas en máquinas con otras soluciones de seguridad de la competencia.

2.5. Servicios Panda Adaptive Defense 360

Panda Security ofrece otros servicios, algunos de carácter opcional, que le permiten al cliente integrar la solución con su infraestructura IT ya desplegada, y obtener de forma directa la inteligencia de seguridad desarrollada en los laboratorios de Panda Security.

2.5.1 Servicio 100% Attestation

Este servicio incluido por defecto en el producto tiene como objetivo permitir la ejecución únicamente de los programas certificados por Panda Security. Para conseguirlo, se utiliza una mezcla de tecnologías locales en el equipo del usuario y en la infraestructura de análisis big data que clasifican de forma automática el 99'08 % de los procesos ejecutados. Para el resto de procesos se aplican clasificaciones manuales ejecutadas por expertos en malware. Con este enfoque se consiguen clasificar el 100% de los binarios ejecutados en los equipos de los clientes sin falsos positivos ni negativos.

Los ficheros ejecutables encontrados en el equipo del usuario y desconocidos para la plataforma se envían de forma automática a la infraestructura de análisis big data para su análisis.

Los ficheros desconocidos se envían una sola vez para todos los clientes que usan Panda Adaptive Defense 360, por lo tanto, el impacto en el rendimiento de la red del cliente es prácticamente nulo. Además, se han implementado mecanismos de gestión del ancho de banda y limites por equipo y hora.

2.5.2 Servicio Panda Threat Hunting

Este servicio incluido por defecto en el producto detecta malwares sin fichero (malwareless / fileless) y los movimientos laterales de las amenazas avanzadas, previos a la ejecución de acciones dañinas para las empresas.

Mediante la monitorización continua de los equipos, Panda Threat Hunting es capaz de detectar atacantes que no utilizan malware conocido e incluso empleados maliciosos.

2.5.3 Servicio Panda Advanced Reporting Tool (opcional)

Panda Adaptive Defense 360 envía de forma automática y transparente toda la información recogida de los equipos de usuario al servicio **Panda Advanced Reporting Tool**, un sistema de almacenamiento y explotación del conocimiento generado en la red del cliente.

Las acciones de los procesos ejecutados en el parque de IT se envían a **Panda Advanced Reporting Tool** para su estudio y correlación, con el objetivo de extraer inteligencia de seguridad. El administrador dispondrá de información adicional sobre las amenazas y sobre el uso que los usuarios dan a los equipos de la empresa. Esta nueva información se presenta de forma flexible y visual para favorecer su comprensión.

El servicio **Panda Advanced Reporting Tool** es accesible directamente desde el panel de control de la propia consola Web de **Panda Adaptive Defense 360**.

Consulta la Guía de usuario Advanced Reporting Tool accesible desde la web de producto para configurar y sacar provecho del servicio de análisis de conocimiento y búsquedas avanzadas.

2.5.4 Servicio Panda SIEMFeeder (opcional)

Panda Adaptive Defense 360 se integra con las soluciones SIEM de proveedores externos implementadas por los clientes en sus infraestructuras de IT. La actividad de las aplicaciones que se ejecutan en el parque informático se entrega al servidor al SIEM, ampliada con todo el conocimiento ofrecido por **Panda Adaptive Defense 360,** y lista para ser utilizada.

A continuación, se listan los sistemas SIEM compatibles con **Panda Adaptive Defense 360**:

- QRadar
- AlienVault
- ArcSight

- LookWise
- Bitacora

Consulta la Guía de usuario SIEMFeeder para una descripción detallada de la información recogida por Panda Adaptive Defense 360 y enviada al sistema SIEM del cliente.

2.5.5 Servicio Panda Data Control (opcional)

Es un módulo de seguridad integrado en la plataforma **Panda Adaptive Defense** que ayuda a cumplir con las regulaciones en materia de retención de datos personales (PII) almacenados en la infraestructura IT de las empresas.

Panda Data Control descubre, audita y monitoriza en tiempo real el ciclo de vida completo de los ficheros PII: desde datos en reposo, las operaciones efectuadas sobre ellos y su transferencia al exterior.

Consulta la Guía para el administrador de Panda Data Control para una descripción detallada del servicio.

2.5.6 Servicio Panda Patch Management (opcional)

Este servicio reduce la superficie de ataque de los puestos de usuario y servidores Windows actualizando el software vulnerable (sistemas operativos y aplicaciones de terceros) con los parches publicados por los proveedores correspondientes.

Además, permite localizar los programas que han entrado en EoL considerados peligrosos por no tener mantenimiento de su proveedor original y ser el blanco de los hackers que aprovechan las vulnerabilidades conocidas y sin corregir. El administrador puede localizar con facilidad todos los programas en EoL y planificar una sustitución controlada de los mismos.

2.6. Perfil de usuario de Panda Adaptive Defense 360 sobre Aether

Aunque **Panda Adaptive Defense 360** es un servicio gestionado que ofrece seguridad sin intervención del administrador de la red, también provee información muy detallada y comprensible sobre la actividad de los procesos ejecutados por los usuarios en toda la infraestructura de IT de la empresa. Esta información puede ser utilizada por el administrador para precisar el impacto de problemas de seguridad y adaptar sus protocolos, evitando así la repetición de situaciones similares en el futuro.

2.7. Dispositivos e idiomas soportados en Panda Adaptive Defense 360 sobre Aether

Para una descripción detallada de las plataformas y requisitos consulta el Apéndice I: Requisitos de Panda Adaptive Defense 360

Panda Adaptive Defense 360 es compatible con los siguientes sistemas operativos:

- Windows Workstation
- Windows Server
- macOS
- Linux
- Tablets y móviles Android

La consola de administración se encuentra disponible en varios idiomas y es compatible con los navegadores mostrados a continuación:

- Chrome
- Internet Explorer
- Microsoft Edge
- Firefox
- Opera

Los idiomas soportados en la consola de administración son:

- Español
- Inglés
- Sueco
- Francés
- Italiano
- Alemán
- Portugués
- Húngaro
- Ruso
- Japonés
- Finlandés (consola local)

2.8. Recursos y documentación disponible

A continuación, se detalla una relación de recursos disponibles sobre **Panda Adaptive Defense 360 sobre Aether**

Guía de administración de Panda Adaptive Defense 360

http://resources.pandasecurity.com/enterprise/solutions/adaptivedefense/ADAPTIVEDEFENSE360oAP-guia-3.40.0-ES.pdf

Guía de administración de Advanced Reporting Tool

http://resources.pandasecurity.com/enterprise/solutions/adaptivedefense/ADVANCEDREPORTINGTOOL-Guia-ES.pdf

Guía de administración de Panda Data Control

https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/DATACONTROL-Guia-ES.pdf

Página de soporte de producto.

http://www.pandasecurity.com/spain/support/adaptive-defense-360-aether.htm

Página de producto

http://www.pandasecurity.com/spain/intelligence-platform/solutions.htm

3. El ciclo completo de protección adaptativa

3.1. Introducción

Este capítulo ofrece una visión de la estrategia general adoptada por **Panda Adaptive Defense 360** para gestionar la seguridad de la red de la empresa.

En la actualidad se generan más de 200.000 nuevos virus diariamente, y una parte muy sustancial de este nuevo malware está diseñado para ejecutarse en los equipos de los usuarios durante largos periodos de tiempo y en segundo plano, sin dar muestras de su existencia.

Por esta razón, el enfoque tradicional de protección mediante archivos de identificadores locales o en la nube ha demostrado ser gradualmente ineficiente: debido al creciente número de malware desarrollado, su ventana de oportunidad es cada vez mayor, entendida ésta como el tiempo que transcurre desde que el primer equipo es infectado a nivel mundial, hasta que los proveedores de seguridad identifican ese nuevo malware y alimentan sus archivos de identificadores con la información necesaria para detectarlo.

De esta manera, toda estrategia de seguridad pasa por minimizar el tiempo de exposición al malware, exposición estimada actualmente en 259 días para ataques dirigidos, cada vez más frecuentes y que tienen como principales objetivos el robo de datos y el espionaje industrial.

Debido a este cambio drástico en el panorama del malware, **Panda Adaptive Defense 360 sobre Aether** propone un nuevo enfoque de seguridad basado en el **ciclo de protección adaptativa**: un conjunto de servicios de protección, detección, monitorización, análisis forense y resolución. Todos los servicios están integrados y centralizadas en una única consola Web de administración para mostrar el ciclo completo de la seguridad de la red en tiempo real.

Con este nuevo enfoque se evitan o minimizan al máximo las brechas de seguridad, reduciendo de forma drástica las pérdidas de productividad y el riesgo de robo de información confidencial en las empresas; el administrador es liberando de la compleja tarea de determinar qué es peligroso y por qué razón, recuperando espacio y recursos para gestionar y vigilar el estado de la seguridad.

El departamento de IT podrá tomar decisiones que permitan adaptar la política de seguridad de la empresa con la misma agilidad que mutan los patrones de ataque del malware avanzado.

3.2. El ciclo de protección adaptativa

El objetivo de **Panda Adaptive Defense 360** es el de facilitar al departamento de IT crear un espacio donde definir y establecer las políticas de seguridad de la empresa que respondan rápida y adecuadamente a los nuevos tipos de amenazas.

Este espacio es producto, por una parte, de la liberación de responsabilidades del equipo técnico en la compañía a la hora de decidir qué ficheros son seguros y cuales son peligrosos, y por qué motivo: con **Panda Adaptive Defense 360** el departamento técnico de la empresa recibirá una

clasificación sin ambigüedades de absolutamente todos los programas ejecutados en el parque informático gestionado.

Por otra parte, el departamento de IT también recibirá un conjunto de herramientas para la visualización del estado de la seguridad, la resolución de los problemas ocasionados por el malware avanzado y el estudio de forma detallada del comportamiento de APTs y otras amenazas.

Con toda esta información y herramientas, el administrador podrá cerrar el ciclo completo de la seguridad en la empresa: monitorizar el estado del parque informático gestionado, revertir el sistema a la situación previa a las brechas de seguridad en caso de producirse, y conocer su alcance para poder implementar las medidas de contingencia apropiadas. Todo este ciclo se encaja dentro de un proceso de refinamiento contante, que resultará en un entorno informático seguro, flexible y productivo para los usuarios de la empresa.

Este ciclo constante de protección adaptativa implementado por las empresas con ayuda de **Panda Adaptive Defense 360** se puede resumir en la Figura 5.

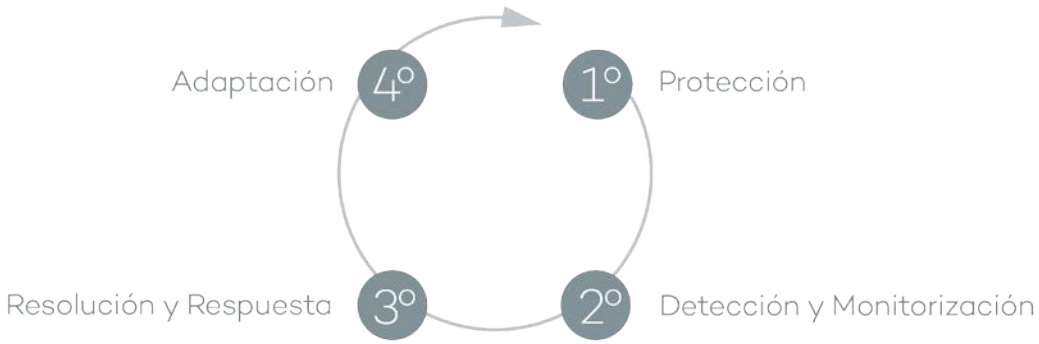


Figura 5: el ciclo de protección adaptativa

3.3. Fase I: Protección completa del parque informático

La primera fase del ciclo de protección adaptativa incluye las herramientas necesarias para proteger y defender de forma efectiva el parque informático de ataques e intentos de infección.

3.3.1 Protección antivirus permanente e inteligencia colectiva.

La protección antivirus permanente es el módulo de seguridad tradicional que cubre los vectores de infección más utilizados por los hackers. Se alimenta tanto del archivo de identificadores publicado por Panda Security para su descarga en local como del acceso en tiempo real a la Inteligencia Colectiva.

En el contexto actual de crecimiento continuo del malware, los servicios alojados en la nube han cobrado especial importancia frente a las actualizaciones del fichero de firmas local. Por esta

razón, la protección de antivirus de **Panda Adaptive Defense 360** se basa fundamentalmente en la Inteligencia Colectiva, una plataforma de conocimiento en la nube que aumenta exponencialmente la capacidad de detección.

Esta plataforma consta de servidores que clasifican y procesan de forma automática toda la información que la comunidad de usuarios proporciona sobre las detecciones que se han producido en sus equipos. La protección **Panda Adaptive Defense 360** instalada en los equipos consulta a la Inteligencia Colectiva cuando lo necesita, consiguiendo así maximizar su capacidad de detección y sin afectar negativamente al consumo de recursos.

Cuando se detecta un nuevo ejemplar de malware en el equipo de un miembro de la comunidad de usuarios, **Panda Adaptive Defense 360** envía la información a los servidores de Inteligencia Colectiva alojados en la nube, de forma automática y anónima. Esta información es procesada para generar una solución no sólo al usuario afectado, sino también al resto de usuarios de la comunidad, en tiempo real.

Panda Adaptive Defense 360 utiliza la Inteligencia Colectiva para aumentar la capacidad de detección y evitar penalizaciones en el rendimiento del equipo del cliente. Todo el conocimiento está en la nube y, gracias a **Panda Adaptive Defense 360**, todos los usuarios pueden beneficiarse de ello.

Consulta el capítulo 10 y 11 para más información sobre el servicio de antivirus de Panda Adaptive Defense 360 en las distintas plataformas soportadas

3.3.2 Protección contra técnicas avanzadas de ocultación y virus de macro

Al margen de la estrategia tradicional de detección que compara el payload del fichero objeto de estudio con el contenido en el fichero de firmas, **Panda Adaptive Defense 360** implementa varios motores de detección que analizan el comportamiento de los procesos de forma local.

De esta manera, se detectan comportamientos extraños en los principales motores de scripting (Visual basic Script, Javascript y Powershell) incorporados en todos los sistemas Windows actuales y utilizados como extensión de la línea de comandos, y en macros maliciosas embebidas en ficheros ofimáticos como Word, Excel, PowerPoint etc.

Como complemento, se incorporan además los tradicionales motores heurísticos y de detección de ficheros maliciosos por características estáticas.

3.3.3 Protección del correo y la Web

Panda Adaptive Defense 360 se aleja del tradicional enfoque de seguridad basado en plugins que añaden la funcionalidad de protección a determinados clientes de correo o navegadores. En su lugar, la protección intercepta a bajo nivel de todas las comunicaciones que usan protocolos comunes como HTTP, HTTPS o POP3. De esta manera, se ofrece una protección homogénea y

permanente para todas las aplicaciones de correo y Web pasadas presentes y futuras: no se necesitan configuraciones específicas ni actualizaciones cuando los proveedores de los programas de correo y navegación publiquen nuevas versiones incompatibles con plugins anteriores.

3.3.4 Protección de la red por cortafuegos y sistema de detección de intrusos (IDS)

Panda Adaptive Defense 360 ofrece tres herramientas básicas para filtrar el tráfico de red que recibe o envía el equipo protegido:

- **Protección mediante reglas de sistema**: son reglas que describen las características de una comunicación entre dos equipos: puertos, IPs, protocolos etc. con el objetivo de permitir o denegar los flujos de datos que coincidan con las reglas establecidas.
- **Protección de programas**: establece un conjunto de reglas que permitan o denieguen la comunicación a determinados programas instalados en el equipo de usuario.
- **Sistema de detección de intrusos**: detecta patrones de tráfico malformado que afecten a la seguridad o al rendimiento del equipo protegido, rechazando dicho tráfico.

3.3.5 Control de dispositivos

Dispositivos de uso común como las llaves USB, las unidades de CD/DVD, dispositivos de imágenes, bluetooth, módems o teléfonos móviles también pueden constituir una vía de infección para los equipos.

Panda Adaptive Defense 360 permite establecer el comportamiento del dispositivo en los equipos protegidos, bloqueando su acceso o permitiendo su uso de forma parcial (solo lectura) o completa.

3.3.6 Filtrado de Spam, Virus y contenidos en servidores Exchange

Panda Adaptive Defense 360 analiza los servidores Exchange en busca de virus, herramientas de hacking y programas potencialmente no deseados, con destino los buzones de los usuarios de la red.

Eliminar el correo basura -spam- es una labor que requiere mucho tiempo y supone un peligro de estafa. Para solucionar esta situación **Panda Adaptive Defense 360** implementa una protección anti-spam para servidores Exchange. De esta forma se consigue optimizar el tiempo de trabajo de los usuarios y aumentar la seguridad de los equipos de la red.

Panda Adaptive Defense 360 protege los servidores de correo Exchange mediante dos tecnologías:

- **Protección de buzones**

Se utiliza en los servidores Exchange con el rol de Mailbox, y analiza las carpetas / buzones en background o cuando el mensaje es recibido y almacenado en la carpeta del usuario.

La protección de buzones manipula los diferentes elementos del cuerpo del mensaje analizado para sustituir los elementos peligrosos encontrados por otros seguros, introducir únicamente los elementos peligrosos en cuarentena etc.

Además, la protección de buzones analiza las carpetas de usuario del servidor Exchange en segundo plano, aprovechando los tiempos de menor carga del servidor. Este análisis se ejecuta de forma inteligente, evitando volver a analizar los mensajes ya examinados. Con cada nuevo archivo de identificadores publicado se analizarán los buzones y la cuarentena en segundo plano.

- **Protección de transporte**

Se utiliza en servidores Exchange con el rol de Acceso de clientes, Edge Transport y Mailbox. Analiza el tráfico que atraviesa el servidor Exchange.

En la protección de transporte no se permite la manipulación del cuerpo de los mensajes. De esta forma, el cuerpo de un mensaje peligroso se trata como un único bloque y las acciones que **Panda Adaptive Defense 360** permite ejecutar aplican al mensaje por completo: borrar el mensaje, meterlo en cuarentena, dejar pasar sin modificar etc.

3.3.7 Control de acceso a páginas Web

Panda Adaptive Defense 360 agrupa las páginas web en 64 categorías para que el administrador de la red pueda restringir el acceso a las que considere oportunas, así como a las URLs que especifique de forma manual. Con esta protección se optimiza del ancho de banda de la red y la productividad del negocio, evitando el acceso a recursos web sin relación con la actividad desarrollada en la empresa.

Además, **Panda Adaptive Defense 360** permite definir una configuración de horarios para restringir el acceso a determinadas categorías de páginas Web y listas negras durante las horas de trabajo, y autorizarlo en el horario no laborable o en el fin de semana.

3.4. Fase II: Detección y monitorización

La segunda fase del ciclo de protección adaptativa asume que el malware o el ataque dirigido consiguió sortear las barreras establecidas en la fase de Protección e infectó con éxito una o varias máquinas de la red, pasando esta infección desapercibida para el usuario del equipo.

En esta fase, **Panda Adaptive Defense 360** implementa una serie de tecnologías que permiten al administrador de la red localizar el problema.

3.4.1 Protección permanente avanzada

La protección avanzada de **Panda Adaptive Defense 360** monitoriza de forma continuada todos los procesos que se ejecutan en los equipos Windows de la red del cliente. **Panda Adaptive Defense 360** recoge todas las acciones desencadenadas por los procesos del usuario y los envía a la nube de Panda Security, donde se examinan mediante técnicas automáticas de Machine Learning en entornos Big Data para emitir una clasificación (goodware o malware) con un 99'9991 (menos de 1 error cada 100.000 ficheros analizados) de precisión, evitando de esta manera falsos positivos.

Para los casos más complicados Panda Security cuenta con un laboratorio de expertos especialistas en diseccionar malware, con el único objetivo de clasificar todos los ejecutables localizados en el menor tiempo posible, desde la primera vez que fueron vistos en la red del cliente.

Panda Adaptive Defense 360 admite tres modos de bloqueo para los procesos que todavía no han sido clasificados (desconocidos) y para los ya clasificados como malware:

- **Audit**

En el modo Audit **Panda Adaptive Defense 360** solo informa de las amenazas detectadas, pero no bloquea ni desinfecta el malware encontrado. Este modo es útil para probar la solución de seguridad o para comprobar que la instalación del producto no comprometa el buen funcionamiento del equipo.

- **Hardening**

En aquellos entornos donde se producen cambios constantes del software instalado en los equipos de los usuarios o se ejecutan muchos programas desconocidos (como por ejemplo programas de creación propia) puede no ser viable esperar a que **Panda Adaptive Defense 360** aprenda de ellos para clasificarlos.

El comportamiento del modo Hardening consiste en balancear el riesgo de infección de los equipos y la productividad de los usuarios, limitando el bloqueo de los programas desconocidos a aquellos que se consideran peligrosos a priori. De esta forma se distinguen cuatro escenarios:

- Ficheros ya clasificados por **Panda Adaptive Defense 360** como goodware: se permite su ejecución.
- Ficheros ya clasificados por **Panda Adaptive Defense 360** como malware: son enviados a cuarentena o desinfectados.
- Ficheros sin clasificar que vienen del exterior (Internet, correo y dispositivos USB): se bloquea su ejecución hasta que el sistema emita una clasificación. En función de la clasificación se permitirá su ejecución (goodware) o serán movidos a cuarentena (malware).

En muchas ocasiones la clasificación es casi inmediata; un programa descargado de internet y desconocido para Panda Adaptive Defense 360 será bloqueado en un primer momento, pero minutos después podrá ser ejecutado si resultó ser goodware.

- Ficheros sin clasificar ya instalados en el equipo del usuario antes de la implantación de **Panda Adaptive Defense 360**: se permite su ejecución, aunque sus acciones se monitorizan y se envían al servidor para su estudio. Una vez clasificados se permitirá su ejecución (goodware) o serán bloqueados (malware).

- **Lock**

Para entornos donde la seguridad sea la máxima prioridad, y con el objetivo de ofrecer una protección de máximas garantías, **Panda Adaptive Defense 360** incluye el modo Lock. En este modo se bloquea la ejecución del software en proceso de clasificación y todo aquel que ya ha sido clasificado como malware. Únicamente se permite ejecutar el software lícito.

De la misma forma que en el modo Hardening, los programas clasificados como maliciosos se envían a cuarentena, mientras que la ejecución de programas desconocidos se bloquea hasta ser clasificados como goodware o malware.

Más del 99% de los programas encontrados en los equipos de los usuarios ya están clasificados en los sistemas de Panda Adaptive Defense 360. Los bloqueos afectan a una minoría de programas. Consulta el capítulo 10 Configuración de seguridad para estaciones y servidores para más información sobre la configuración de los distintos modos de bloqueo

3.4.2 Detección de exploits

Panda Adaptive Defense 360 implementa tecnologías para proteger los equipos de la red frente a las amenazas que aprovechan vulnerabilidades en el software. Estas vulnerabilidades son utilizadas (explotadas) para provocar comportamientos anómalos en las aplicaciones, produciendo fallos de seguridad.

Las amenazas de tipo exploit utilizan tanto vulnerabilidades conocidas como de día cero (0-day) o desconocidas, como parte de una cadena de eventos (CKC, Cyber Kill Chain), que ejecutan para comprometer los equipos de la red. **Panda Adaptive Defense 360** bloquea de forma efectiva y en tiempo real esta cadena de eventos para impedir que los ataques de tipo exploit prosperen, dejándolos sin efecto.

Para detectar las técnicas de explotación de vulnerabilidades usadas por los hackers, **Panda Adaptive Defense 360** implementa nuevos hooks en el sistema operativo, que utiliza para monitorizar localmente y de forma constante las acciones de los procesos ejecutados en el equipo del usuario. Gracias a este enfoque, **Panda Adaptive Defense 360** se aleja del esquema tradicional

implementado por otros productos de seguridad, que buscan patrones y detecciones estáticas de pares CVE - payload mediante ficheros de firmas.

Panda Adaptive Defense 360 ofrece una protección anti exploit generalista, fruto de algoritmos en constante adaptación por el equipo de expertos en ciberataques de Panda Security para detectar el uso de técnicas avanzadas de explotación de vulnerabilidades como Head Spraying, Anti ROP, desactivación de DEP y ASLR, entre otras.

3.4.3 Detección de amenazas sin fichero (fileless / malwareless)

Algunas amenazas avanzadas sortean las estrategias de detección de malware basadas en archivos de identificadores evitando almacenar ficheros en el disco duro del equipo infectado. Estas amenazas únicamente residen en la memoria RAM del equipo, y con esta estrategia se vuelven muy complicadas de detectar y de cuantificar el alcance de sus acciones mediante procesos de análisis forense estándar.

La protección avanzada de **Panda Adaptive Defense 360** es capaz de evitar esta estrategia monitorizando de forma continuada todos los procesos ejecutados y analizando su comportamiento. Los procesos que muestren una secuencia de acciones declarada como peligrosa serán clasificados como malware, independientemente del número de ficheros que depositen en el sistema de almacenamiento del equipo de usuario o servidor. De esta misma manera, al quedar almacenadas todas las acciones del proceso en la nube de Panda Security, es posible ejecutar un análisis forense completo.

3.4.4 Monitorización de ficheros de datos (Panda Data Control)

Panda Adaptive Defense 360 registra todos los accesos a ficheros de datos del usuario por parte de los procesos ejecutados en el equipo. De esta manera, aunque el malware consiga infectar el equipo, es posible precisar con exactitud qué ficheros modificó y en qué momento. También es posible determinar si envió ficheros fuera de la empresa a través de Internet, las direcciones IP de destino y otra información valiosa que facilita tanto el análisis forense posterior como las acciones de resolución. A continuación, se muestran los tipos de ficheros de datos que se monitorizan:

- Documentos de suites ofimáticas.
- Documentos en formato PDF.
- Documentos de aplicaciones CAD.
- BBDD de escritorio.
- Almacenes de contraseñas de navegadores.
- Almacenes de contraseñas de clientes de correo.
- Almacenes de contraseñas de clientes de FTP.
- Almacenes de contraseñas de Directorio Activo.
- Almacenes de certificados y certificados de usuario.
- Almacenes de Digital Wallet.

- Configuración de navegadores.
- Configuración de firewall.
- Configuración de GPO.

3.4.5 Parcheo de vulnerabilidades (Panda Patch Management)

Panda Patch Management mantiene de forma automática una base de datos de los parches y actualizaciones publicadas por los proveedores del software para los sistemas operativos Windows instalados en el parque informático. Comparando esta base de datos con los parches ya instalados en los equipos se muestran aquellos que contienen software vulnerable, y que por lo tanto son susceptibles de recibir ataques de programas maliciosos para infectar la red de la empresa.

Para evitar esto, **Panda Patch Management** permite crear tareas programadas e inmediatas de parcheo de los equipos, reduciendo de esta forma la superficie de ataque de puestos de usuario y servidores,

3.4.6 Visibilidad del estado de la red

Panda Adaptive Defense 360 ofrece recursos para poder valorar el estado de la seguridad de la red en un solo vistazo, a través de un panel de control (dashboard) formado por diferentes widgets y de los informes.

Lo importante en esta etapa no solo es determinar si la red del cliente está siendo atacada y en qué grado o forma, sino contar con la información necesaria para poder valorar una probabilidad de infección.

En los paneles de **Panda Adaptive Defense 360** se incluye información clave en este sentido:

- Cuáles son los procesos desconocidos para **Panda Adaptive Defense 360** encontrados en los equipos de la red, y que están siendo investigados para su posterior clasificación en Panda Security, junto con una valoración preliminar de su peligrosidad.
- Actividad detallada en forma de listados de acciones de aquellos programas desconocidos que finalmente resultaron ser malware.
- Detecciones realizadas en los diferentes vectores de infección protegidos.

Con este módulo el administrador tiene una visión global de los procesos que se ejecutan en su red: por el lado del malware ya conocido que intentó infectar algún equipo y fue detenido en el módulo de protección; y por el lado del malware desconocido y diseñado para pasar inadvertido por las tecnologías de detección tradicionales, y que consiguió sortear los sistemas de detección configurados.

El administrador tendrá la posibilidad de reforzar la seguridad de su red impidiendo toda ejecución de software desconocido o, por el contrario, balancear el nivel de bloqueo en favor de una mayor flexibilidad a la hora de ejecutar ciertos programas no conocidos.

Consulta el capítulo 16 Visibilidad del malware y del parque informático para más información sobre Visibilidad y monitorización de equipos y procesos

3.5. Fase III: Resolución y respuesta

En caso de producirse una brecha de seguridad, el administrador tiene que ser capaz de actuar en dos líneas: revertir de forma rápida el estado de los equipos afectados previo a la infección, y poder calcular el impacto del ataque: si hubo fuga de datos, hasta donde consiguió penetrar el ataque, qué equipos resultaron comprometidos etc. La fase resolución y respuesta ofrece herramientas para estos dos escenarios.

- **Respuesta**

Mediante la herramienta de análisis forense el administrador puede ver todas las acciones ejecutadas por el malware en el equipo infectado, así como información fundamental a la hora de valorar la peligrosidad de la amenaza: vector de infección (como llegó el malware a la red de la organización), patrón de propagación a otros equipos y accesos al disco duro en busca de información confidencial, entre otros.

Panda Adaptive Defense 360 genera un entorno seguro para que el administrador ejecute el análisis forense, aislando los equipos afectados de la red. De esta manera, se impiden las comunicaciones con el exterior para evitar la fuga de información, pero se mantiene la conexión con la nube de Panda Security para poder investigar el suceso sin desplazarse físicamente al equipo afectado.

Además, **Panda Advanced Reporting Tool** y **Panda Data Control** extienden y ayudan a interpretar los datos recogidos por **Panda Adaptive Defense 360**. De esta manera, el administrador tiene acceso a información representada gráficamente de todos los procesos ejecutados por el usuario, y no solo de los clasificados como malware. También se identifican los ficheros que contienen datos personales (PII) y los procesos que acceden a ellos y los envían fuera de la red de la organización.

- **Resolución**

Panda Adaptive Defense 360 cuenta con herramientas de desinfección propias de un antivirus, tradicional junto a la cuarentena, que almacena los elementos sospechosos o eliminados.

Consulta el capítulo 19 Herramientas de resolución para más información

3.6. Fase IV: Adaptación / Prevención

Una vez realizado el estudio con las herramientas de Resolución y respuesta de la fase III y localizadas las causas que propiciaron la infección, el administrador deberá de ajustar la política de seguridad de la empresa para que no se vuelvan a producir situaciones equivalentes en el futuro.

La fase de Adaptación puede reunir una gran cantidad de iniciativas en función de los resultados revelados por el análisis forense: desde cursos de educación y sensibilización en el correcto uso de Internet para los empleados de la empresa, hasta la reconfiguración de los routers corporativos o de los permisos de los usuarios en sus máquinas personales.

Desde el punto de vista del equipo, **Panda Adaptive Defense 360** puede reforzar la seguridad de múltiples maneras:

- **Cambio en la configuración de la protección avanzada.**

Si los usuarios de la empresa tienden a utilizar siempre el mismo software, o algunos de ellos suelen instalar programas de dudosa procedencia, una opción para minimizar el riesgo de estos equipos es implementar el modo Lock de la protección avanzada. De esta forma se limita la exposición al malware en los equipos más problemáticos y se impide la ejecución de los programas que no sean legítimos.

- **Cambio de la configuración de la protección antivirus**

Cambiar la frecuencia de los análisis bajo demanda o activar la protección de vectores de infección como Web o correo ayudarán a proteger los equipos que reciban malware por estas dos vías.

- **Limitación de la navegación Web a categorías concretas**

Reconfigurar las categorías accesibles a la navegación para limitar el acceso a páginas de origen dudoso, cargadas de publicidad y propensas a ofrecer descargas en apariencia inocentes (descarga de libros, programas piratas etc.) pero que pueden infectar de malware los equipos.

- **Filtrado de la llegada de correo con Phising o Spam**

Un vector muy utilizado para ataques de tipo phising es el correo. Refuerza la configuración del filtrado de contenidos y del filtro antiSpam para limitar la cantidad de correo no solicitado que llega a los buzones de los usuarios, reduciendo la superficie de ataque.

- **Bloqueo parcial o total de pen drives y otros dispositivos externos**

Otro de los vectores de infección más típicos son las memorias y los módems USB que los usuarios traen de sus casas. Limita o bloquea completamente su uso para evitar la infección por estas vías.

- **Limitación la comunicación de los programas instalados con el Firewall y el Sistema de detección de intrusos (IDS)**

El firewall es una herramienta orientada a reducir la superficie de exposición de los equipos y evita la comunicación de programas que, de por sí, no son malware pero que pueden suponer una ventana abierta a la entrada del mismo. Si se ha detectado una intrusión de malware por programas de tipo chat o P2P, una correcta configuración de las reglas del firewall evitará la comunicación de estos programas con el exterior.

El firewall y el IDS también pueden ser utilizados para minimizar la propagación del malware una vez ha infectado al primero de los equipos de la red. Examina las acciones que desencadenó con la herramienta de análisis forense para generar nuevas reglas de cortafuegos que limiten la comunicación entre equipos o los protejan de ataques de red.

- **Cambio de la configuración de Panda Patch Management**

Cambiar la configuración de las tareas de parcheo permite minimizar el tiempo que los programas instalados incorporan vulnerabilidades aprovechables por el malware. Ampliar el número de tipos de parches a instalar incrementa la seguridad de la red, garantizando que todo el software instalado incorpora las últimas actualizaciones publicadas por los proveedores.

Desinstalar o actualizar los programas que han entrado en EoL minimiza la superficie de ataque de los equipos: se retira el software que ya no recibe actualizaciones de los proveedores, y por lo tanto tiene una mayor probabilidad de incorporar fallos y vulnerabilidades no resueltas y aprovechables por el malware.

4. La consola de administración

Características generales de la consola
Estructura general de la consola web de administración

4.1. Introducción

La consola Web es la herramienta principal del administrador para la gestión de la seguridad. Al tratarse de un servicio Web centralizado, hereda una serie de características que influirán de manera positiva en la forma de trabajo del departamento de IT:

- **Única herramienta para la gestión completa de la seguridad.**

Con la consola Web el administrador podrá distribuir el paquete de instalación **Panda Adaptive Defense 360** en los equipos de la red, establecer las configuraciones de seguridad, monitorizar el estado de la protección de los equipos y disponer de herramientas de resolución y análisis forense en caso de problemas. Toda la funcionalidad se ofrece desde una única consola Web, favoreciendo la integración de las distintas herramientas y minimizando la complejidad de utilizar varios productos de distintos proveedores.

- **Gestión centralizada de la seguridad para todas las oficinas y usuarios desplazados**

La consola Web está alojada en la nube de forma que no es necesario instalar nueva infraestructura en las oficinas del cliente ni configuraciones de VPNs o redirecciones de puertos en los routers corporativos. Tampoco serán necesarias inversiones en hardware, licencias de sistemas operativos o bases de datos, ni gestión de mantenimientos / garantías para asegurar el funcionamiento del servicio.

- **Gestión de la seguridad desde cualquier lugar y en cualquier momento**

La consola Web de administración es de tipo “responsive / adaptable” con lo que se ajusta al tamaño del dispositivo utilizado para la gestión de la seguridad. De esta manera el administrador de la red podrá gestionar la seguridad desde cualquier lugar y en cualquier momento mediante un smartphone, un notebook o un PC de escritorio.

4.1.1 Requisitos de la consola Web

La consola Web es accesible a través de la siguiente URL

https://www.pandacloudsecurity.com/PandaLogin/

Para acceder a la consola Web de administración es necesario cumplir con el siguiente listado de requisitos:

- Contar con unas credenciales validas (usuario y contraseña).

Consulta el Apéndice II: Creación y gestión de cuentas Panda para más información sobre cómo crear una Cuenta Panda de acceso a la consola Web.

- Un navegador compatible certificado
- Conexión a internet y comunicación por el puerto 443

4.1.2 Federación con IDP

Panda Adaptive Defense 360 delega la gestión de las credenciales en un Proveedor de Identidades (Identity Provider, IDP), una aplicación centralizada responsable de gestionar las identidades de los usuarios.

De esta forma con una única Cuenta Panda el administrador de la red tendrá acceso a todos los productos contratados con Panda Security de forma segura y sencilla.

4.2. Características generales de la consola

Panda Adaptive Defense 360 utiliza la consola de administración para interactuar con el servicio, aplicando los siguientes beneficios:

- **Diseño responsive / adaptativo**: la consola web se adapta al dispositivo utilizado para el acceso y a su tamaño, ocultando y recolocando dinámicamente elementos.
- **Sin recarga de páginas**: se utiliza tecnología Ajax para navegar y mostrar los listados de manera que se evitan las recargas de páginas completas.
- **Flexible**: se ofrece una interface fácilmente adaptable a las necesidades del administrador, permitiendo almacenar los ajustes realizados para los posteriores accesos.
- **Homogénea**: los recursos implementados en la consola de administración siguen unos patrones de usabilidad bien definidos que permiten minimizar la curva de aprendizaje del administrador.
- **Exportación de listados**: todos los listados son exportables en formato csv con campos extendidos para su posterior consulta.

4.3. Estructura general de la consola Web de administración

La consola Web de administración cuenta con recursos que facilitan al administrador una experiencia de gestión homogénea y coherente, tanto en la administración de la seguridad de la red como en las tareas de resolución y análisis forense.

El objetivo de la consola de administración es entregar una herramienta sencilla, pero a la vez flexible y potente, que permita al equipo técnico empezar a gestionar la seguridad de la red de forma productiva en el menor período de tiempo posible.

A continuación, se incluye una descripción de los elementos de la consola y su modo de utilización.

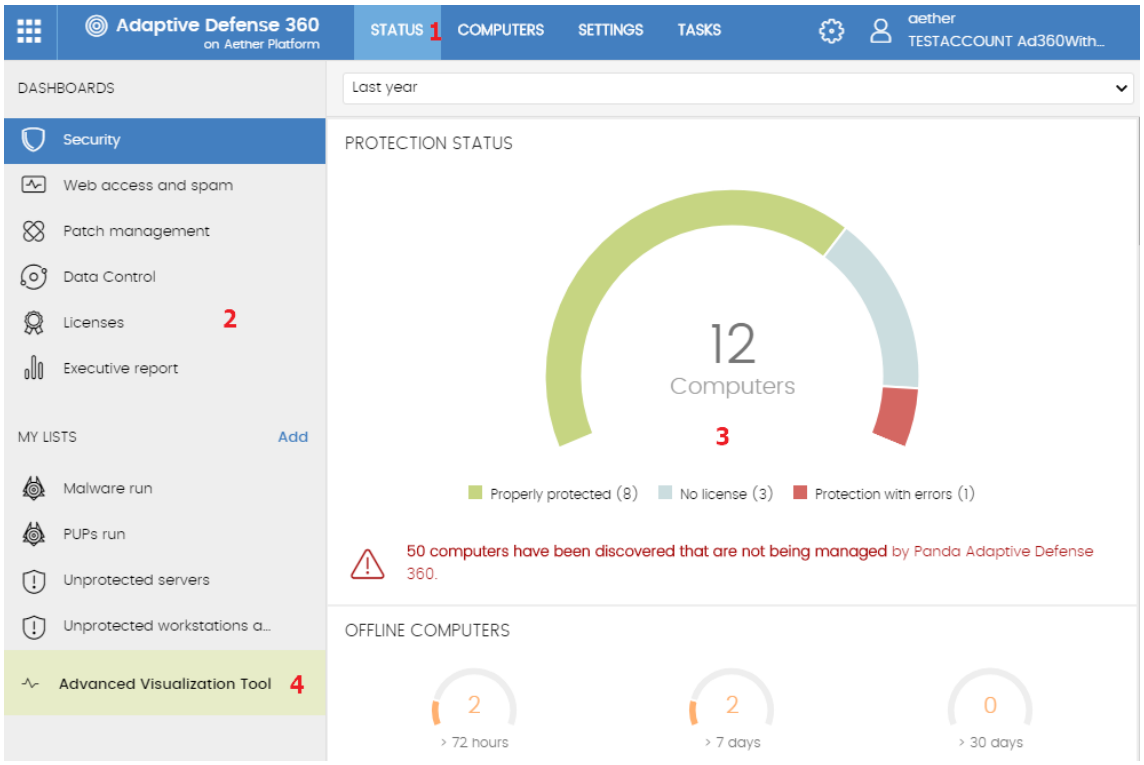


Figura 6: vista general de la consola de administración ***Panda Adaptive Defense 360***

4.3.1 Menú superior (1)

Muestra las 7 zonas de la consola en las que la consola de administración divide toda su funcionalidad:

- Botón Panda Cloud
- Estado
- Equipos
- Configuración
- Tareas
- Configuración general
- Cuenta de usuario

Botón Panda Cloud

Haz clic en el botón  situado en el lateral izquierdo del menú superior. Desde aquí puedes elegir el producto de seguridad contratado para gestionarlo, así como modificar la configuración de tu Cuenta Panda.

Menú superior Estado

El menú superior **Estado** muestra el panel de control de la consola, desde la cual el administrador tiene acceso de un vistazo a toda la información de seguridad, tanto en forma gráfica mediante widgets como mediante los listados situados en el menú lateral.

Consulta el capítulo 7 Gestión de equipos y dispositivos para obtener más información.

Menú superior Equipos

El menú superior **Equipos** ofrece las herramientas básicas para que el administrador de la red pueda definir la estructura de los equipos de la red que mejor se ajuste a la configuración de la seguridad del parque informático.

Elegir una correcta estructura de dispositivos es fundamental a la hora de asignar configuradores de seguridad de forma fácil y sencilla.

Consulta el capítulo 8 Gestión de configuraciones para obtener más información.

Menú superior Configuración

Permite crear configuraciones de varios tipos:

- **Usuarios**: permite gestionar los usuarios que podrán acceder a la consola de administración, así como las acciones que podrá realizar dentro de la misma

Consulta el capítulo 22 Control y supervisión de la consola de administración para obtener más información.

- **Ajustes por equipos**: permite definir las actualizaciones del software Panda Adaptive Defense 360 y su contraseña de administración.
- **Proxy e idioma**: permite crear la configuración de salida a internet y de idioma del software instalado en los equipos de la red.
- **Estaciones y servidores**: permite crear los perfiles de configuraciones que serán asignados a los dispositivos en el Menú superior **Equipos**.

Consulta el capítulo 10 Gestión de configuraciones para estaciones y servidores para obtener más información.

- **Dispositivos Android**: permite crear los perfiles de configuraciones que serán asignados a tablets y teléfonos móviles Android en el Menú Superior **Equipos**.

Consulta el capítulo 11 Configuración de seguridad Android para obtener más información.

- **Alertas**: establece el tipo de alertas que el administrador recibirá en su buzón.

Consulta el capítulo 20 Alertas para obtener más información.

Menú superior Tareas

Permite la gestión de tareas de seguridad programadas para su ejecución en los intervalos de tiempo designados por el administrador.

Consulta el capítulo 15 Tareas para obtener más información.

Menú superior Configuración General

Muestra un menú desplegable que permite el acceso a la documentación del producto, cambio de idioma de la consola y otras herramientas.

- **Guía de administración de Panda Adaptive Defense 360**
- **Guía de administración de Panda Advanced Reporting Tool**
- **Guía de administración de Panda Data Control**
- **Soporte técnico**: lanza el navegador con la dirección de la web de soporte técnico de Panda Security para **Panda Adaptive Defense 360 sobre Aether.**
- **Buzón de sugerencias**: lanza la herramienta de correo local instalada en equipo para mandar un mensaje de correo al departamento de soporte técnico de Panda Security.
- **Acuerdo de licencia**: Muestra el EULA (End User License Agreement)
- **Idioma**: permite seleccionar el idioma en que se mostrara la consola de administración
- **Acerca de...:** muestra la versión de los diferentes elementos de **Panda Adaptive Defense 360**
  - **Versión**: versión del producto.
  - **Versión de la protección:** Versión interna del módulo de protección instalado en los equipos.
  - **Versión del agente:** Versión interna del módulo de comunicaciones instalado en los equipos.

Menú superior Cuenta de usuario

Muestra un menú desplegable con las siguientes entradas de configuración:

- **Configurar mi perfil**: permite cambiar la información de la cuenta principal del producto.
- **Cambiar de cuenta**: lista las cuentas accesibles por el administrador y permite seleccionar

una nueva cuenta para operar con la consola.

- **Cerrar sesión**: hace logout de la consola de administración y devuelve al usuario a la pantalla de IdP.

4.3.2 Menú lateral (2)

El menú lateral permite la selección de las diferentes subzonas dentro de la zona elegida, actuando como un selector de segundo nivel con respecto al menú superior.

El menú lateral varía en función de la zona presentada, adaptándose al tipo de información que se muestra.

4.3.3 Widgets (3)

Los widgets son representaciones gráficas de datos que permiten interpretar de un vistazo la información recogida relativa a un determinado aspecto de la seguridad de la red. Los widgets son accesibles, mostrando pequeños tooltips al pasar el rato por sus zonas activas y permiten ampliar la información al hacer clic, mostrando desgloses completos de la información mostrada.

Consulta el capítulo 16 Visibilidad del malware y del parque informático para obtener más información.

4.3.4 Acceso a Advanced Visualization Tool (4)

Advanced Visualization Tool es el punto de entrada para la consola de gestión de los módulos **Panda Data Control** y **Panda Advanced Reporting Tool**. Ambos módulos comparten una consola especialmente diseñada para mostrar gráficas avanzadas y tablas con información relevante sobre la actividad de los todos procesos ejecutados en los puestos de usuario y servidores.

4.3.5 Menú de pestañas superior

En las zonas de la consola más complejas se muestra un selector de tercer nivel en forma de pestañas que mantiene la información ordenada por categorías.

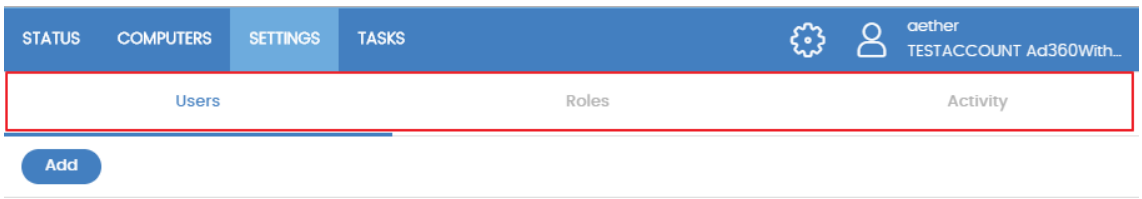


Figura 7: menú de pestañas

4.3.6 Barra de acciones

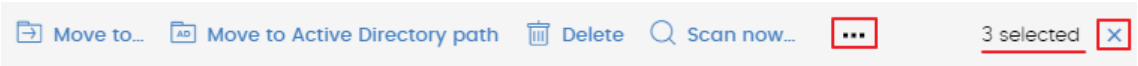


Figura 8: barra de acciones

Para facilitar la navegación de la consola y el acceso a algunas operaciones comunes sobre los puestos y servidores administrados, se incorpora una barra de acciones en la parte superior de los listados que incluyan casilla de selección de equipos.

El número de botones mostrados se adapta al tamaño de la ventana, y los botones que queden fuera se añaden al icono ··· situado a la derecha de la barra de acciones.

En la esquina derecha de la barra de acciones se muestra el número total de equipos seleccionados. Haz clic en el icono del aspa para deshacer la selección.

4.3.7 Herramientas de filtrado y búsqueda

Las herramientas de filtrado y búsqueda muestran los subconjuntos de información de interés para el administrador. Algunas herramientas de filtrado son generales y aplican a toda la zona de la consola mostrada, como por ejemplo en el Menú superior **Estado** o Menú superior **Equipos**.

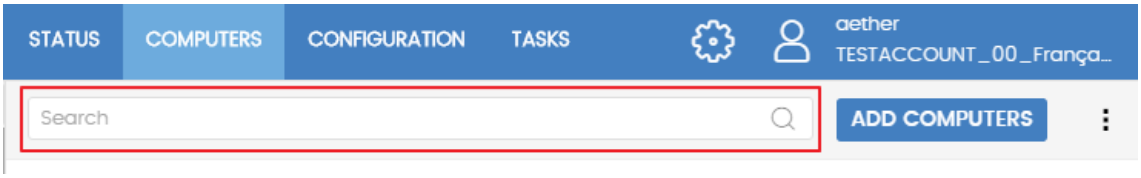


Figura 9: herramienta de búsqueda

Las herramientas de filtrado completas se ocultan por defecto bajo el desplegable **Filtros** y permiten definir búsquedas por categorías, rangos y otros parámetros dependientes del tipo de información mostrada.

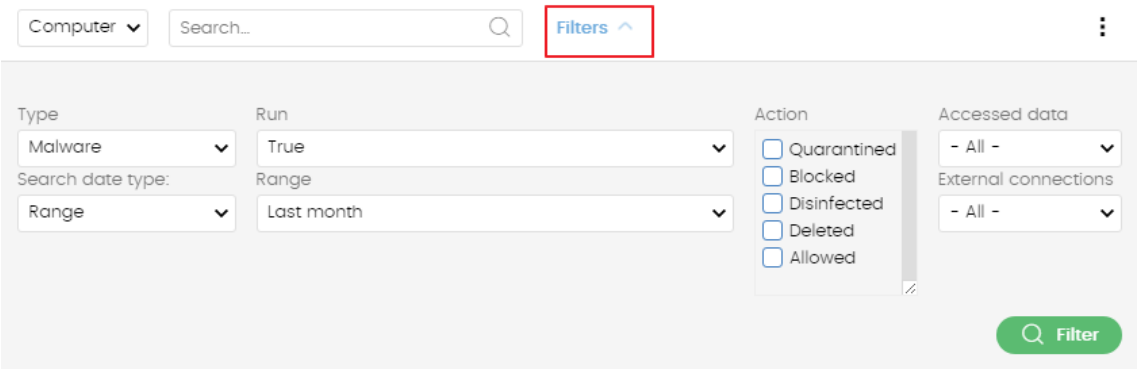


Figura 10: sistema de filtrado de información en listados

4.3.8 Elementos de configuración (8)

La consola Web **Panda Adaptive Defense 360** utiliza controles estándar para introducir configuraciones, como son:

- Botones **(1)**
- Links **(2)**
- Casillas de activación y desactivación **(3)**
- Desplegables de selección **(4)**
- Combos de selección **(5)**
- Cuadros de texto **(6)**

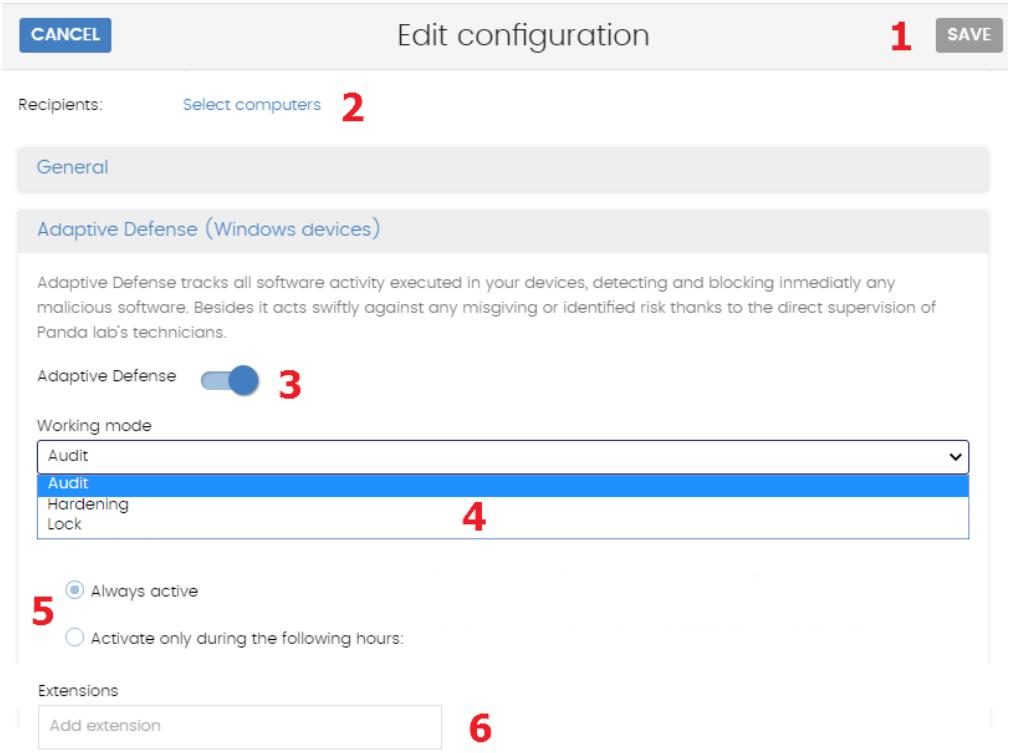


Figura 11: controles para el manejo de la consola de administración

4.3.9 Menús de contexto

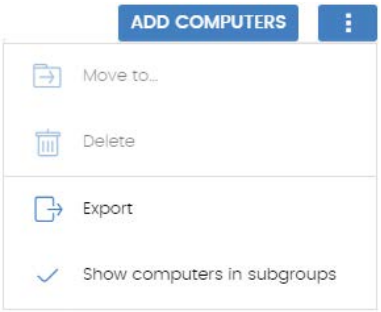


Figura 12: menús de contexto

Son menús desplegables que se muestran al hacer clic en el icono ⋮, con opciones que afectan al ámbito al que pertenecen según su posición.

4.3.10 Listados

Los listados presentan la información en forma de tabla y están acompañados de un conjunto de herramientas comunes que facilitan su navegación.

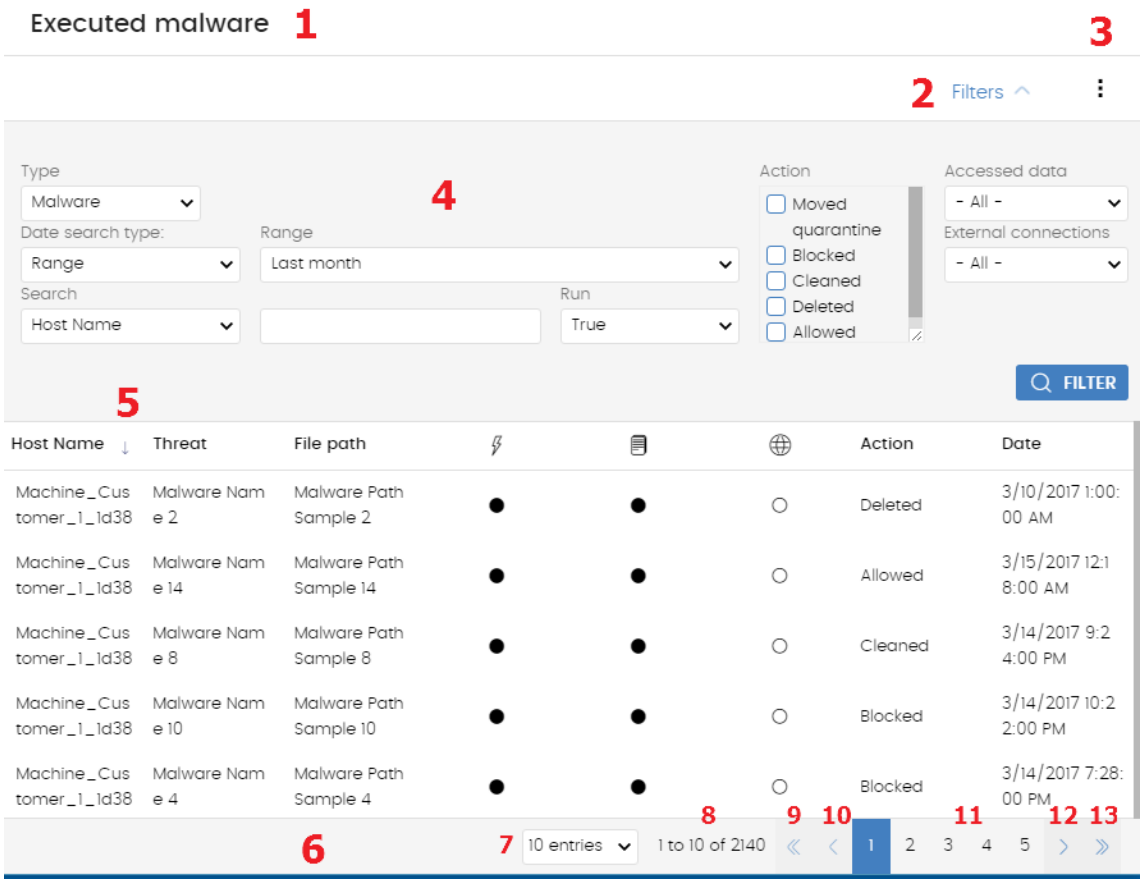


Figura 13: elementos de las pantallas de listados

- **Nombre del listado (1)**: permite identificar el tipo de datos que se muestran en el listado.
- **Link de herramientas de filtrado y búsqueda (2)**: al hacer clic se despliega un panel con los controles de búsqueda y filtrado.
- **Menú de contexto (3):** muestra un menú desplegable con las opciones de exportación.
- **Bloque de controles de filtrado y búsqueda (4):** permiten refinar los datos mostrados en el listado.
- **Criterio de ordenación (5)**: haciendo clic en el nombre de las columnas se permite la ordenación de la información mostrada, tomando como referente esa columna. Haciendo clic varias veces en el nombre de la columna se cambia el sentido de la ordenación (ascendente o descendente). El sentido de ordenación se muestra mediante una fecha ascendente ↑ o descendente ↓.
- **Paginación (6)**: en el pie de la página se incluyen una serie de controles que permiten navegar la información mostrada.

- Selector del número de filas mostradas por página **(7)**
- Intervalo de registros mostrados del total disponible **(8)**
- Retroceso a la primera página **(9)**
- Retroceso a la página anterior a la actual **(10)**
- Acceso directo a las 5 páginas posteriores a la visualizada **(11)**
- Avance a la siguiente página **(12)**
- Avance a la última página **(13)**

5. Licencias

Definiciones y conceptos clave
Licencias contratadas
Licencias caducadas
Licencias de prueba (trial)
Búsqueda de equipos según el estado de licencia

5.1. Introducción

Para beneficiarse de los servicios de seguridad avanzada de **Panda Adaptive Defense 360** es necesario adquirir y asignar licencias del producto a los diferentes equipos de la red a proteger, de acuerdo con las necesidades de seguridad en la empresa.

En este capítulo se tratará la gestión de licencias de **Panda Adaptive Defense 360**, cómo asignarlas a los equipos de la red, liberarlas y comprobar su estado.

Para la puesta en marcha del servicio **Panda Adaptive Defense 360** es necesaria la contratación de licencias en un número igual o superior a los equipos que se quieran proteger. Una licencia de **Panda Adaptive Defense 360** es asignada a un único equipo (estación de trabajo, dispositivo móvil o servidor).

Para contratar y/o renovar licencias consulta con tu partner asignado

5.2. Definiciones y conceptos clave para la gestión de licencias

A continuación, se describen los términos necesarios para interpretar las gráficas y la información suministrada por **Panda Adaptive Defense 360** que refleja el estado de las licencias de los equipos.

5.2.1 Mantenimientos

Las licencias contratadas se agrupan en mantenimientos. Un mantenimiento es un conjunto de licencias con las características comunes, mostradas a continuación:

- **Tipo de Producto**: Panda Adaptive Defense 360, Panda Adaptive Defense 360 con Advanced Reporting Tools, Panda Adaptive Defense 360 con Data Control, Panda Adaptive Defense 360 con Advanced Reporting Tools y Data Control, Patch Management.
- **Licencias contratadas**: número de licencias contratadas en el mantenimiento
- **Tipo de licencias**: NFR, Trial, Comercial, Suscripción.
- **Caducidad**: Fecha en la que las licencias caducan y los equipos dejarán de estar protegidos.

5.2.2 Estado de los equipos

Desde el punto de vista de las licencias, **Panda Adaptive Defense 360** distingue tres estados en los equipos de la red:

- **Equipos con licencia**: el equipo tiene una licencia válida en uso.
- **Equipos sin licencia**: el equipo no tiene una licencia en uso, pero es candidato a tenerla.
- **Excluidos**: equipos a los que se ha decidido no aplicarles la licencia. Estos equipos no serán protegidos por **Panda Adaptive Defense 360** aunque se mostrarán en la consola y se podrá

utilizar algunas funcionalidades de gestión. Para excluir un equipo es necesario liberar su licencia de forma manual.

Es importante distinguir entre el número de equipos sin licencia asignada (candidatos a tenerla en caso de haber licencias sin asignar) y el número de equipos excluidos (sin posibilidad de tener una licencia asignada, aunque haya licencias disponibles).

5.2.3 Estado de las licencias y grupos

Las licencias contratadas pueden tener dos estados:

- **Asignada**: es una licencia usada por un equipo de la red.
- **Sin asignar**: es una licencia que no está siendo usada por ningún equipo de la red.

Las licencias se agrupan por su estado en dos grupos:

- **Grupo de licencias usadas**: formado por todas las licencias asignadas a equipos.
- **Grupo de licencias sin usar**: formado por las licencias sin asignar.

5.2.4 Tipos de licencias

- **Licencias comerciales**: son las licencias estándar de **Panda Adaptive Defense 360**. Un equipo con una licencia comercial asignada tiene acceso a toda la funcionalidad del producto licenciado.
- **Licencias de prueba (Trial)**: son licencias gratuitas de prueba, válidas por un periodo limitado de 30 días. Un equipo con una licencia de prueba asignada tiene acceso de prueba a toda la funcionalidad del producto.
- **Licencias NFR**: licencias *Not For Resale*, destinadas a personal interno y partners de Panda Security. No está permitida su venta ni uso por personal o partners ajenos a Panda Security.
- **Licencias de tipo suscripción**: licencias que no tienen fecha de caducidad. El servicio es de tipo "pago por uso".

5.2.5 Asignación de licencias

La asignación de licencias se puede realizar de dos maneras: automática o manualmente.

Asignación automática

Al instalar el software **Panda Adaptive Defense 360** en un equipo de la red, y siempre que existan licencias sin utilizar, el sistema asignará de forma automática una licencia libre.

Asignación manual

Para asignar manualmente una licencia de **Panda Adaptive Defense 360** a un equipo de la red sigue los pasos mostrados a continuación.

- En el menú superior **Equipos** localiza el dispositivo a asignar la licencia mediante el árbol de carpetas, el árbol de filtros o la herramienta de búsqueda.

- Haz clic en el equipo para mostrar la ventana de detalle.
- En la pestaña **Detalles** se muestra el apartado **Licencias,** donde se mostrará el **estado Sin licencias**. Haciendo clic en el icono  se asignará de forma automática una licencia libre.

5.2.6 Liberación de licencias

De forma equivalente a la asignación de licencias, la liberación de licencias se puede realizar de dos maneras: automática o manual.

Liberación automática

Al desinstalar el software **Panda Adaptive Defense 360** de un equipo de la red el sistema recuperará de forma automática una licencia y la devolverá al grupo de licencias sin usar.

Igualmente, al caducar un mantenimiento se desasignarán automáticamente licencias de los equipos siguiendo la lógica de licencias caducadas explicadas más adelante en este capítulo.

Liberación manual

La liberación manual de una licencia asignada previamente a un equipo lo convertirá en un equipo excluido. De esta forma, aunque existan licencias libres, estas no serán asignadas al equipo de forma automática.

Para liberar manualmente una licencia de **Panda Adaptive Defense 360** de un equipo de la red sigue los pasos mostrados a continuación.

- En el menú superior **Equipos** localiza el dispositivo a liberar la licencia mediante el árbol de carpetas, el árbol de filtros o la herramienta de búsqueda.
- Haz clic en el equipo para mostrar su información.
- En la pestaña **Detalles** se muestra el apartado **Licencias,** donde se mostrará el estado. **Panda Adaptive Defense 360**. Haciendo clic en el icono  se liberará la licencia y se devolverá al pool de licencias sin utilizar.

5.2.7 Procesos de asignación y liberación de licencias

Caso I: Equipos con licencia asignada y equipos excluidos

Por defecto, a cada nuevo equipo integrado en la plataforma **Aether** se le asigna una licencia de producto **Panda Adaptive Defense 360** de forma automática, pasando a tomar el estado de equipo con licencia asignada. Este proceso se mantiene hasta que el número de licencias contratadas queda reducido a 0.

Los equipos que ven retirada de forma manual su licencia asignada, toman el estado de equipos excluidos, y a partir de ese momento no compiten por la asignación de una licencia de forma automática, en el caso de existir licencias sin usar.

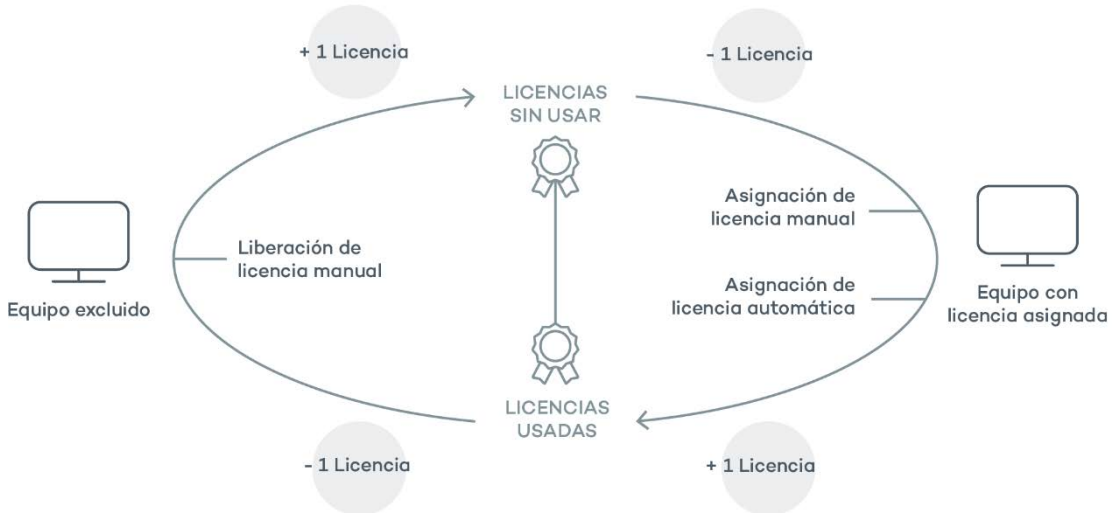


Figura 14: modificación de los grupos de licencias en equipos con licencia asignada y excluidos

Caso II: Equipos sin licencia asignada

En el momento en que nuevos equipos se incorporen a la plataforma **Aether** y el grupo de licencias sin usar este a 0, los equipos pasarán al estado Equipos sin licencia. En el momento en que nuevas licencias estén disponibles estos equipos tomaran una licencia de forma automática.

De la misma forma, en el momento en que una licencia asignada caduque un equipo de la red pasará al estado Sin licencia asignada, siguiendo la lógica de licencias caducadas explicadas más adelante en este capítulo.

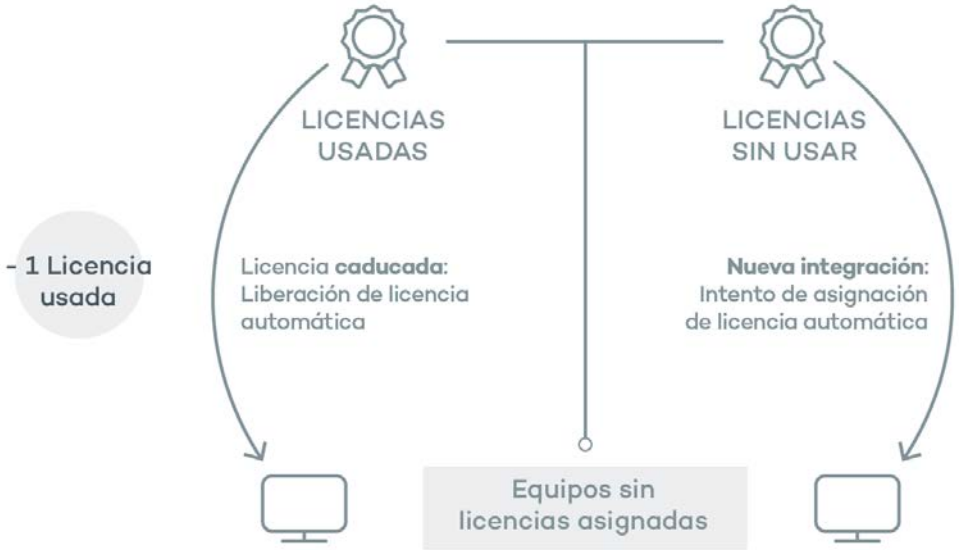


Figura 15: equipos sin licencia asignada por caducidad del mantenimiento y por grupo de licencias sin usar vacio en el momento de la integración

5.3. Licencias contratadas

Para visualizar el detalle de las licencias contratadas haz clic en el menú superior **Estado** y después en el menú lateral **Licencias**. Se mostrará una ventana con dos graficas: **Licencias contratadas** y **Caducidad de licencias.**

5.3.1 Widget

El panel representa como se distribuyen las licencias del producto contratado.

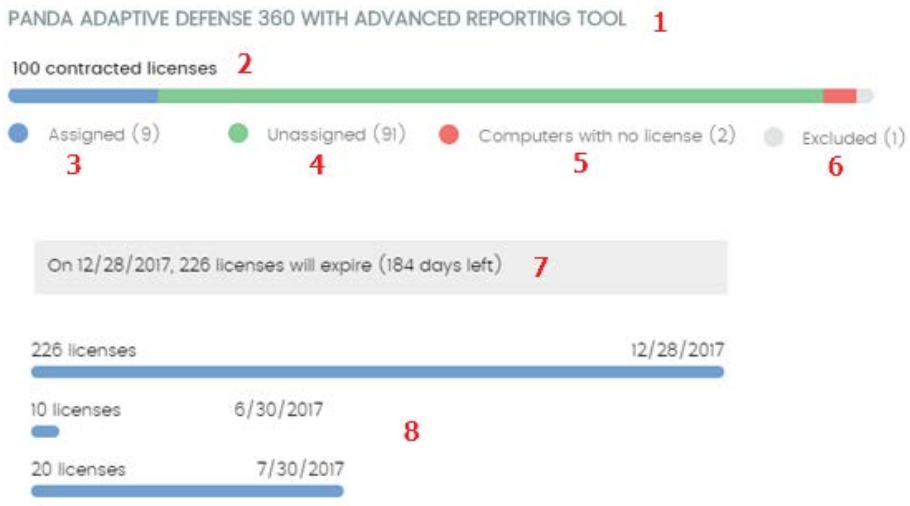


Figura 16: panel de licencias con 3 mantenimientos

- **Nombre del producto contratado (1)**
- **Número de licencias contratadas totales (2)**
- **Número de licencias asignadas (3)**
- **Número de licencias sin asignar (4)**
- **Número de equipos sin licencia (5)**
- **Número de equipos excluidos (6)**
- **Caducidad de las licencias (7)**
- **Caducidad por mantenimiento (8)**

Nombre del producto contratado (1)

Indica el producto y los servicios contratados. Cada producto diferente se muestra de forma independiente. Si se ha contratado el mismo producto varias veces (varios mantenimientos de un mismo producto) se mostrarán de forma agrupada, indicando las diferentes fechas de caducidad de las licencias mediante un diagrama de barras horizontales.

Número de licencias contratadas totales (2)

Representa el número máximo de equipos que se pueden proteger, en el caso de que todas las licencias contratadas sean asignadas.

Asignadas (3)

Es el número de equipos protegidos con una licencia asignada.

Sin asignar (4)

Es el número de licencias contratadas pero que no se han asignado a ningún equipo y por lo tanto no se están utilizando.

Equipos sin licencia (5)

Equipos no protegidos por no disponer de licencias suficientes. Se les asignará licencia de forma automática si se adquieren nuevas licencias.

Equipos excluidos (6)

Equipos sin licencia asignada que no son candidatos a tenerla.

Caducidad de las licencias (7)

Si existe un único mantenimiento contratado, todas las licencias caducaran a la vez, en la fecha indicada.

Caducidad de los mantenimientos (8)

Si un mismo producto ha sido contratado varias veces a lo largo del tiempo se mostrará una gráfica de barras horizontales con las licencias asociadas a cada contrato / mantenimiento y su fecha de caducidad independiente.

5.3.2 Listado de Licencias

Este listado muestra en detalle el estado de las licencias de los equipos de la red, incorporando filtros que permiten localizar aquellos puestos de trabajo o dispositivos móviles según su estado de licenciamiento.

Campo	Comentario	Valores
Equipo	Nombre del equipo	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo	Cadena de caracteres
Estado de licencia		'Licencia asignada Equipo sin licencia Equipo excluido

Campo	Comentario	Valores
Ultima conexión	Fecha del ultimo envío del estado del equipo a la nube de Panda Security	Fecha

Tabla 1: campos del listado Equipos protegidos

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el producto	Cadena de caracteres
Tipo de equipo		Estación Portátil Dispositivo móvil Servidor
Equipo	Nombre del equipo	Cadena de caracteres
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de par-che aplicado	Cadena de caracteres
Plataforma	Sistema operativo instalado en el equipo	Windows Linux macOS Android
Directorio Activo	Ruta dentro del árbol de directorio activo de la empresa donde se encuentra el equipo	Cadena de caracteres
Servidor Exchange	Versión del servidor de correo instalada en el servidor	Cadena de caracteres
Máquina virtual	Indica si el equipo es físico o esta virtualizado	Booleano
Versión del agente		Cadena de caracteres
Versión de la protección		Cadena de caracteres
Fecha de arranque del sistema		Fecha
Fecha instalación	Fecha en la que el software Panda Adaptive Defense 360 se instaló con éxito en el equipo	Fecha
Fecha de la última conexión	Fecha del último envío del estado del equipo a la nube de Panda Security	Fecha
Estado de licencia		Asignada No asignada Excluido
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que	Cadena de caracteres

Campo	Comentario	Valores
	pertenece el equipo	
Dirección IP	Dirección IP principal del equipo	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo	Cadena de caracteres
Descripción		Cadena de caracteres

Tabla 2: campos del fichero exportado Licencias

Herramienta de filtrado

Campo	Comentario	Valores
Buscar equipo	Nombre del equipo	Cadena de caracteres
Tipo de equipo		Estación Portátil Dispositivo móvil Servidor
Plataforma	Sistema operativo instalado en el equipo	Todos Windows Linux macOS Android
Ultima conexión	Fecha del último envío del estado del equipo a la nube de Panda Security	Todos Más de 72 horas Más de 7 días Más de 30 días
Estado de licencia		Asignada Sin licencia Excluido

Tabla 3: campos de filtrado para el listado Licencias

Filtros pre establecidos desde el panel

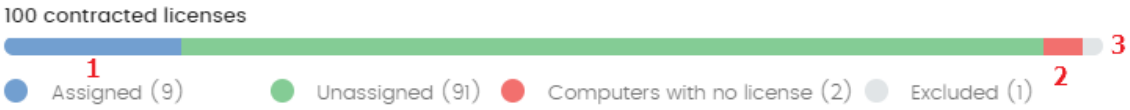


Figura 17: zonas activas del panel licencias contratadas

El listado se muestra con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

- **(1)** Filtra por **Estado de licencia** = Asignada
- **(2)** Filtra por **Estado de licencia** = No Asignada
- **(3)** Filtra por **Estado de licencia** = Excluido

5.4. Licencias caducadas

Excepto los mantenimientos de tipo suscripción, todos los demás tienen asignada una fecha de caducidad, pasada la cual los equipos de la red dejarán de están protegidos.

5.4.1 Mensajes de caducidad próxima y vencida

A los 30 días de vencer el mantenimiento, el panel Licencias contratadas mostrará un mensaje con los días que quedan para finalizar el mantenimiento y el número de licencias que se verán afectadas.

Adicionalmente, se mostrará un mensaje por cada mantenimiento caducado, avisando en el plazo de los 30 últimos días del número de licencias que ya no son funcionales.

Si todos los productos y mantenimientos están caducados se denegará el acceso a la consola de administración.

5.4.2 Lógica de liberación de licencias caducadas

Panda Adaptive Defense 360 no mantiene una relación de pertenencia estricta entre mantenimientos de licencias y equipos. Los equipos con licencias asignadas no pertenecen a un mantenimiento concreto u otro; en su lugar todas las licencias de todos los mantenimientos se suman en un único grupo de licencias disponibles, que se reparten posteriormente entre los equipos de la red.

En el momento en que un mantenimiento caduca, **Panda Adaptive Defense 360** determina el número de licencias asignadas a ese mantenimiento. Acto seguido, se ordenan los equipos de la red con licencia asignada utilizando como criterio de ordenación el campo Ultima conexión, que contiene la fecha en la que el equipo se conectó por última vez a la nube de Panda Security.

Los equipos candidatos a retirar su licencia de protección son aquellos no vistos en el periodo de tiempo más grande. Así, se establece un sistema de prioridades donde la mayor probabilidad de retirar una licencia se asigna a los equipos que no han sido utilizados recientemente.

La lógica de liberación de licencias caducadas afecta a todos los dispositivos compatibles con Panda Adaptive Defense 360 que tengan licencias asignadas.

5.5. Licencias de prueba (trial) sobre licencias comerciales

En el caso de tener licencias comerciales de **Panda Endpoint Protection**, **Panda Endpoint Protection Plus** o **Fusion** sobre la plataforma **Aether** y obtener una trial de **Panda Adaptive Defense 360**, se

producirán una serie de ajustes, tanto en la consola de administración como en el software instalado en los equipos de la red:

- Se creará un mantenimiento nuevo de tipo trial, con la duración contratada para la prueba y un número de licencias igual a la suma de las licencias disponibles previamente y las licencias contratadas para la trial.
- Los mantenimientos comerciales aparecen desactivados temporalmente mientras dure el periodo de trial, pero el ciclo de caducidad y renovación se mantiene intacto.
- Se habilitará la funcionalidad asociada al producto en pruebas sin necesidad de actualizar los equipos de la red.
- **Panda Adaptive Defense 360** por defecto, se activará en todos los equipos con el modo de protección Audit. En caso de no querer activar **Panda Adaptive Defense 360** en todos los puestos o en caso de querer establecer un modo de protección distinto se podrá hacer estableciendo la configuración oportuna.
- Una vez terminado el periodo de prueba el mantenimiento creado para la trial se elimina, el mantenimiento comercial se reactivará y los equipos de la red sufrirán un downgrade automático, manteniendo las configuraciones previas.

5.6. Búsqueda de equipos según el estado de la licencia asignada

Panda Adaptive Defense 360 incluye la categoría "licencia" en el árbol de filtros, que permite localizar los equipos de la red que tengan un determinado estado de licencia.

Consulta el capítulo 7 Gestión de equipos y dispositivos para obtener más información acerca de cómo crear un filtro en Panda Adaptive Defense 360.

A continuación, se muestran las propiedades de la categoría **Licencias** para crear filtros que generen listados de equipos con información relevante sobre licencias.

- **Propiedad – Estado de la licencia**: permite establecer un filtro según el estado de la licencia.
  - **Asignada**: lista los equipos con una licencia **Panda Adaptive Defense 360** asignada.
  - **Sin asignar**: lista los equipos que no tiene una licencia **Panda Adaptive Defense 360** asignada
  - **Desasignada manualmente**: el administrador de la red liberó la licencia **Panda Adaptive Defense 360** previamente asignada al equipo.
  - **Desasignada automáticamente**: el sistema liberó al equipo la licencia **Panda Adaptive Defense 360** asignada previamente.
- **Propiedad - Nombre de la licencia**: muestra a todos los equipos con una licencia **Panda Adaptive Defense 360** asignada.

- **Propiedad – Tipo**: lista los equipos con licencia **Panda Adaptive Defense 360** según su tipo.
  - **Release**: lista los equipos con licencias **Panda Adaptive Defense 360** comerciales.
  - **Trial**: lista los equipos con licencias **Panda Adaptive Defense 360** de prueba.

6. Instalación del software Panda Adaptive Defense 360

6.1. Introducción

La instalación es el proceso que distribuye **Panda Adaptive Defense 360** en los equipos de la red del cliente. Todo el software necesario para activar el servicio de protección avanzado, la monitorización y la visibilidad del estado de la seguridad de la red se encuentra en el interior del paquete de instalación: no se requiere la instalación de ningún otro programa en la red del cliente.

Es importante instalar el software **Panda Adaptive Defense 360** en todos los equipos de la red del cliente para evitar brechas de seguridad que puedan ser aprovechadas por los atacantes mediante malware dirigido específicamente a equipos vulnerables.

Panda Adaptive Defense 360 ofrece varias herramientas que facilitan la instalación de la protección, que se mostrarán a lo largo de este capítulo.

6.2. Visión general del despliegue de la protección

El proceso de instalación comprende una serie de pasos a seguir, dependiendo del estado de la red en el momento del despliegue y del número de equipos a proteger. Para desarrollar un despliegue con garantías de éxito es necesario elaborar una plantificación que comprenda los puntos enumerados a continuación:

Localizar los equipos desprotegidos en la red

El administrador deberá de localizar los equipos que no tienen instalada protección en la red del cliente o que tienen un producto de terceros que sea necesario sustituir o complementar con **Panda Adaptive Defense 360**.

Una vez localizados, se deberá de comprobar que el número de licencias contratadas es suficiente.

Panda Adaptive Defense 360 permite la instalación del software sin tener contratadas licencias suficientes. Estos equipos serán visibles en la consola de administración y mostrarán el software instalado, hardware y otras características, pero no estarán protegidos frente al malware de nueva generación.

Determinar si se cumplen los requisitos mínimos de la plataforma destino

Los requisitos mínimos de cada plataforma se describen más adelante en este capítulo, en su sección correspondiente.

Determinar el procedimiento de instalación

Dependiendo del número total de equipos Windows a proteger, los puestos y servidores con un agente Panda ya instalado y la arquitectura de red de la empresa, será preferible utilizar un procedimiento u otro de los cuatro disponibles:

- Herramienta de despliegue centralizado.
- Instalación manual utilizando la herramienta **Enviar URL por mail**.
- Programa de instalación compartido en una carpeta accesible por los usuarios de la red.
- Instalación remota desde la consola de administración.

Determinar si es necesario un reinicio para completar la instalación

Todos los servicios de protección de **Panda Adaptive Defense 360** comenzarán a funcionar sin necesidad de reiniciar los equipos en el caso de equipos sin antivirus previamente instalado.

Es posible que se requiera un reinicio del cliente o se produzca un pequeño micro corte en la conexión con algunas versiones anteriores de Citrix.

Si deseas instalar **Panda Adaptive Defense 360** en un equipo en el que ya se encuentra instalada alguna otra solución de seguridad ajena a Panda Security, puedes elegir entre instalarlo sin desinstalar la otra protección, de tal manera que ambas soluciones de seguridad convivan en el mismo equipo o, por el contrario, desinstalar la otra solución de seguridad y funcionar exclusivamente con **Panda Adaptive Defense 360**.

Para completar la desinstalación del antivirus de terceros es posible que se requiera un reinicio de la máquina.

En función del tipo de versión de **Panda Adaptive Defense 360** que desees instalar, el comportamiento por defecto varía tal y como se muestra a continuación.

- **Versiones Trials**

En la instalación de versiones de evaluación, por defecto **Panda Adaptive Defense 360** no desinstalará las soluciones de seguridad de terceros. De esta forma, podrás evaluar **Panda Adaptive Defense 360** comprobando cómo registra amenazas avanzadas que pasan inadvertidas para el antivirus tradicional instalado.

- **Versiones comerciales**

En este caso, por defecto **Panda Adaptive Defense 360** no se instalará en un equipo que ya dispone de otra solución ajena a Panda Security. Si **Panda Adaptive Defense 360** dispone del desinstalador de dicho producto, previamente lo desinstalará y a continuación se lanzará la instalación de **Panda Adaptive Defense 360**. En caso contrario, se detendrá la instalación.

Puedes consultar una lista de los antivirus que Panda Adaptive Defense 360 desinstala automáticamente en el Apéndice III: Listado de des instaladores. Si la solución a desinstalar no está en la lista, será necesaria su desinstalación manual.

El comportamiento por defecto es configurable tanto en versiones trial como en versiones comerciales asignando una configuración de Estaciones y servidores donde esté habilitada la opción **Desinstalar otros productos de seguridad.**

Consulta el capítulo 10 Configuración de seguridad para estaciones y servidores si quieres diseñar una configuración de seguridad. Consulta el capítulo 8 Gestión de configuraciones para asignar configuraciones a los equipos de la red.

- **Productos de protección antivirus de Panda Security**

Si el equipo está protegido previamente con Panda Endpoint Protection, Panda Endpoint Protection Plus o Panda Fusion se procederá a la desinstalación automática del agente de comunicaciones para instalar el agente Panda y, posteriormente, el sistema comprobará si es necesaria una actualización de la protección. En caso de ser necesaria se requerirá un reinicio del equipo.

En la Tabla 4 se resumen las condiciones necesarias para que se produzca un reinicio.

Producto Anterior	Panda Adaptive Defense 360 sobre Aether	Reinicio
Ninguno	**Trial o comercial**	NO
Panda Endpoint Protection Legacy, Panda Endpoint Protection Plus Legacy, Panda Adaptive Defense 360 Legacy, Panda Adaptive Defense Legacy, Panda Fusion Legacy	**Comercial**	PROBABLE (solo si requiere actualización de la protección)
Antivirus de terceros	**Trial**	NO (por defecto los dos productos conviven)
Antivirus de terceros	**Comercial**	POSIBLE (se puede requerir un reinicio para completar la desinstalación del producto de terceros)
Sistemas Citrix	**Trial o comercial**	POSIBLE (en versiones anteriores)

Tabla 4: probabilidad de reinicio al cambiar de producto de protección

Establecer si es necesario la instalación en horario no laboral

Adicionalmente a la necesidad de reinicio del equipo de usuario descrita en el punto anterior, la instalación de **Panda Adaptive Defense 360** provoca un micro corte de menos de 4 segundos de duración sobre las conexiones establecidas por los programas en funcionamiento. Las aplicaciones que no implementen mecanismos para detectar cortes de conexión requerirán un reinicio. Si no es posible este reinicio y además la aplicación no se comporta adecuadamente tras el micro corte, se recomienda la instalación del software **Panda Adaptive Defense 360** fuera del horario laboral.

Determinar la configuración por defecto de los equipos

Con el objeto de proteger a los equipos de la red desde el primer momento, **Panda Adaptive Defense 360** obliga a seleccionar por una parte el grupo de destino en la que el equipo se integrará dentro del árbol de grupos, y por otra la configuración de Proxy e idioma de forma independiente. Esta selección se realiza al generar el instalador, consulta el punto Descarga del software **Panda Adaptive Defense 360** para más información.

Una vez instalado el software en el equipo, **Panda Adaptive Defense 360** aplicará las configuraciones establecidas en el grupo al que pertenece el equipo y, posteriormente, si la configuración de proxy e idioma del grupo seleccionado difiere de la indicada al generar el instalador, se generará una asignación manual de forma que sea esta configuración de proxy e idioma la que prevalezca, antes que la asignada en el grupo del árbol de grupos.

6.3. Requisitos de instalación

Para una descripción completa de los requisitos por plataforma consulta el capítulo 23 Apéndice I: Requisitos de Panda Adaptive Defense 360.

6.3.1 Requisitos por plataforma

Requisitos plataformas Windows

- **Estaciones de trabajo**: Windows XP SP3 y superiores, Windows Vista, Windows 7, Windows 8 y superiores, y Windows 10.
- **Servidores**: Windows 2003 SP2 y superiores, Windows 2008, Windows Small Business Server 2011 y superiores, Windows Server 2012 R2, Windows Server 2016, Windows Server Core 2008 y superiores.
- **Servidores Exchange**: 2003 al 2016.
- **Espacio para la instalación**: 650 Mbytes.

Requisitos plataformas macOS

- **Sistemas operativos**: macOS 10.10 Yosemite y superiores.
- **Espacio para la instalación**: 400 Mbytes.

- **Puertos:** se requieren los puertos 3127, 3128, 3129 y 8310 libres para el funcionamiento del filtrado web y la detección web de malware.

Requisitos plataformas Linux

- **Sistemas operativos 64 bits**: Ubuntu 14.04 LTS y superiores, Fedora 23 y superiores.
- **Kernel soportado**: hasta la versión 4.10 64 bits.
- **Espacio para la instalación**: 100 Mbytes.
- **Puertos:** se requieren los puertos 3127, 3128, 3129 y 8310 libres para el funcionamiento del filtrado web y la detección web de malware.

Consulta la web de soporte para comprobar la última versión del kernel de Linux soportada por Panda Adaptive Defense 360. Versiones superiores del kernel no funcionarán.

Requisitos plataformas Android

- **Sistemas operativos**: Android 4.0 y superiores.
- **Espacio para la instalación**: 10 Mbytes (dependiendo del modelo de dispositivo se requerirá espacio adicional).

6.3.2 Requisitos de red

Panda Adaptive Defense 360 accede a varios recursos alojados en internet. De forma general se requiere acceso a los puertos 80 y 443. Para un listado completo de las URLs que se acceden desde los equipos con el software **Panda Adaptive Defense 360** instalado consulta el Apéndice I: Requisitos de Panda Adaptive Defense 360.

6.4. Descarga e instalación manual del software Panda Adaptive Defense 360

6.4.1 Descarga del paquete de instalación desde la consola Web

Consulta el capítulo 7 para más información sobre los diferentes tipos de grupos, el capítulo 8 para asignar configuraciones a equipos y ramas del árbol, y el capítulo 9 para crear nuevas configuraciones de Proxy e idioma.

Consiste en descargar el paquete de instalación directamente desde la consola de administración. Para ello sigue los pasos mostrados a continuación:

- En la ventana **Equipos** haz clic en el botón **Añadir equipo** y elige la plataforma a proteger: Windows, Linux, Android o macOS (Figura 18).

- Selecciona donde será integrado el equipo en el árbol de carpetas (Figura 19):
  - Para integrar el equipo en un grupo nativo haz clic en **Añadir los equipos al siguiente grupo (1)** y selecciona el destino en el árbol de carpetas mostrado.
  - Para integrar el equipo en un grupo Directorio Activo haz clic en **Añadir los equipos en su ruta de Directorio Activo (2)**.
- Selecciona la configuración de proxy e idioma **(3)** que se aplicará al equipo a instalar. Si quieres integrar el puesto en un grupo nativo, se seleccionará de forma automática la configuración asignada a la carpeta donde residirá. Si has elegido integrarlo en un grupo Directorio Activo deberás seleccionar de forma manual la configuración de proxy e idioma de entre las mostradas en el desplegable. Si la elección automática no se ajusta a tus necesidades haz clic en el desplegable y elige otra de entre las disponibles.

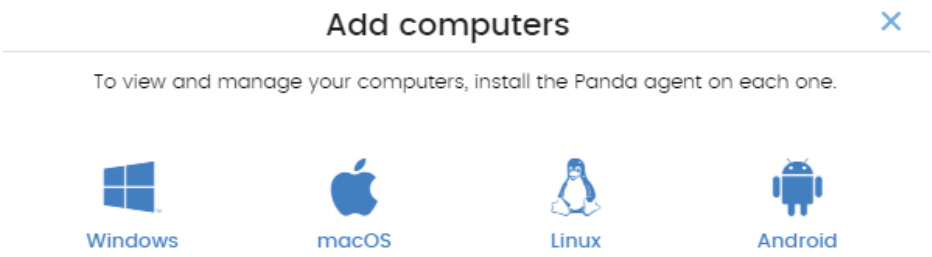


Figura 18: ventana de selección de la plataforma a descargar

- Finalmente haz clic en el botón **Descargar instalador (5)** para iniciar la descarga del paquete apropiado. El instalador contiene un asistente que guiará al usuario en los pasos necesarios para completar la instalación del software.

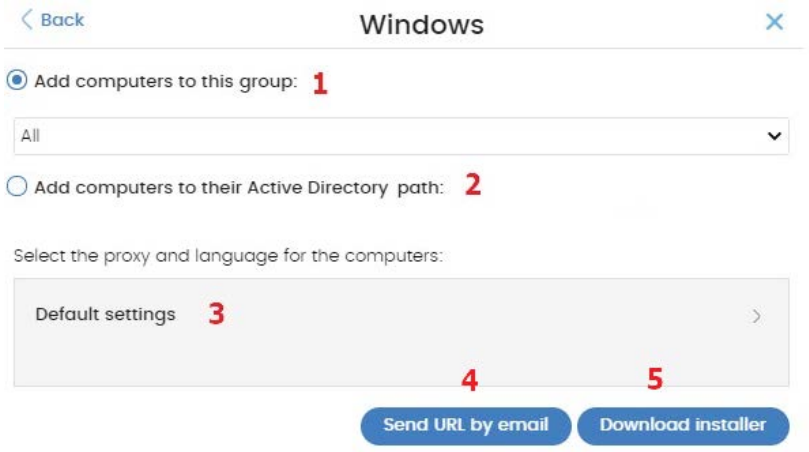


Figura 19: configuarción del paquete de descarga

6.4.2 Generación de URL de descarga

Este método permite la creación de una URL de descarga que podrá ser enviada por correo a los usuarios para iniciar una instalación manual en cada equipo.

El método de distribución de la URL de descarga implementado de forma directa en **Panda Adaptive Defense 360** es mediante correo, haciendo clic en el botón **Enviar por email (4)**.

De la misma manera que en la descarga desde la consola web, es necesario establecer la pertenencia del equipo a un grupo dentro del árbol de grupos y la asignación de una configuración de Proxy e idioma que prevalecerá por encima de la designada en el grupo.

Los usuarios recibirán un correo electrónico con el enlace de descarga correspondiente a su sistema operativo. Al hacer clic en el enlace, se iniciará la descarga del instalador.

6.4.3 Instalación manual del software Panda Adaptive Defense 360

Para la instalación del software Panda Adaptive Defense 360 en el equipo de usuario se requieren permisos de administrador.

Instalación en plataformas Windows, Linux y macOS

Ejecuta el instalador descargado y sigue el asistente de instalación. Una vez completado, el producto comprobará que tiene la última versión del fichero de firmas y del motor de protección. Si no es así, iniciará una actualización automática.

Instalación en plataformas Android

Al hacer clic en el botón **Añadir equipo** del menú superior **Equipos** y seleccionar el icono de Android, se mostrará una ventana con la información mostrada a continuación:

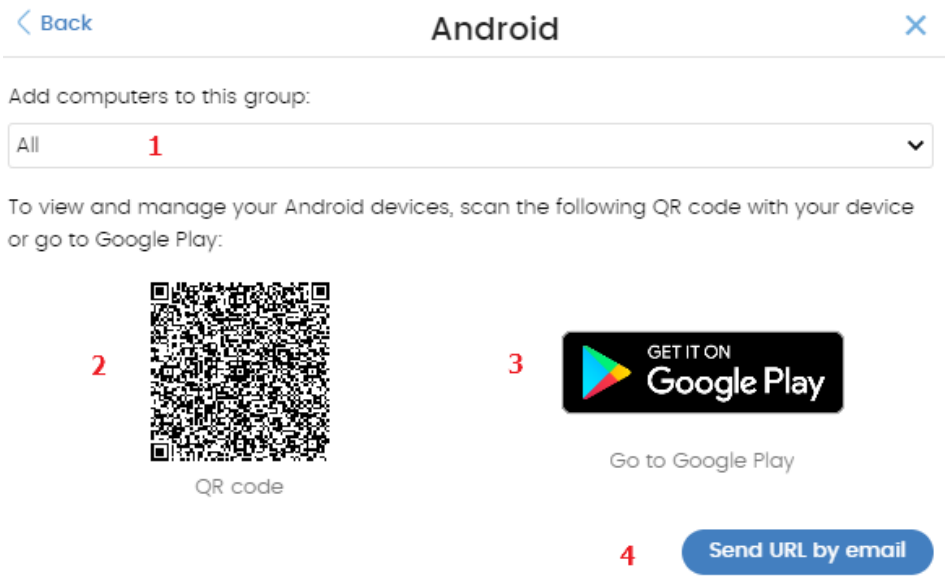


Figura 20: pantalla de selección de plataforma

- **Añadir los equipos al siguiente grupo (1):** permite especificar el grupo dentro del árbol de carpetas en el que se integrará el dispositivo una vez se haya instalado el software Panda Adaptive Defense 360.

- **Código QR (2):** código QR que contiene el link para descargar el software de la Google Play.
- **Acceso a la Google Play (3)**: link directo de descarga del software Panda Adaptive Defense 360 de la Google Play.
- **Enviar URL por mail (4):** mensaje de correo con el link de descarga listo para enviar al usuario del dispositivo a proteger con **Panda Adaptive Defense 360.**

Para instalar el software en el dispositivo del usuario sigue los pasos mostrados a continuación:

- Selecciona el grupo dentro del árbol de carpetas donde se integrará el dispositivo. El código QR se actualizará de forma automática con la nueva selección.
- Descarga la aplicación Android siguiendo uno de los tres procedimientos descritos a continuación:
  - **Mediante código QR**: haz clic en el código QR para agrandarlo, enfoca la cámara del dispositivo a la pantalla y, mediante una aplicación de lectura de códigos QR, escanéalo. En la pantalla del terminal aparecerá una URL de la Google Play que mostrará la ficha de la aplicación lista para su descarga. Pulsando la URL se mostrará la ficha de la aplicación lista para su descarga.

QR Barcode Scanner y Barcode Scanner son dos aplicaciones para la lectura de códigos QR gratuitas y disponibles en la Google Play

  - **Mediante correo electrónico**: haz clic en el link **Enviar URL por email** para generar un mail con el link correcto al usuario. El usuario deberá de seleccionar el link que le llevará a la Google Play con la ficha de la aplicación lista para su descarga.
  - **Mediante la consola de administración**: si has accedido a la consola de administración desde el propio dispositivo, haz clic en el link **Acceso a la Google Play**. Se mostrará la ficha de la aplicación lista para su descarga.
- Una vez instalada la aplicación se le pedirá al usuario que acepte la concesión de permisos de administrador para la aplicación. Dependiendo de la versión de Android (6.0 en adelante), estos permisos se presentarán de forma progresiva según se vayan necesitando, o por el contrario se mostrará una única ventana la primera vez que se ejecute la aplicación, solicitando todos los permisos necesarios de una sola vez.

Una vez terminado el procedimiento el dispositivo aparecerá en el grupo seleccionado dentro del árbol de carpetas.

6.5. Descubrimiento automático de equipos e instalación remota

Los productos basados en Aether Platform incorporan las herramientas necesarias para localizar los puestos de usuario y servidores sin proteger, e iniciar una instalación remota desatendida desde la consola de administración.

La instalación remota solo es compatible con plataformas Windows.

6.5.1 Requisitos para instalar Panda Adaptive Defense 360 en los equipos

Para poder instalar **Panda Adaptive Defense 360** de forma remota, es necesario que los equipos cumplan con los requisitos indicados a continuación:

- Puertos UDP 21226 y 137 abiertos para el proceso System.
- Puerto TCP 445 abierto para el proceso System.
- Protocolo NetBIOS sobre TCP habilitado.
- Resolución DNS permitida.
- Acceso al recurso de administración Admin$. En las ediciones "Home" de Windows es necesario habilitar este recurso de forma explícita.
- Credenciales de administrador de dominio o de la cuenta de administrador local generada por defecto en la instalación del sistema operativo.
- Administración remota activada.

Para cumplir con estos requisitos de forma rápida sin necesidad de añadir reglas de forma manual en el firewall de Windows, selecciona Activar la detección de redes red y Activar el uso compartido de archivos e impresoras en Centro de redes y recursos compartidos, Configuración de uso compartido avanzado.

6.5.2 Descubrimiento de equipos

El descubrimiento de equipos se efectúa a través de un equipo con el rol de *Descubridor*. Todos los equipos que cumplan los requisitos indicados en el punto anterior se mostrarán en el listado de equipos descubiertos, independientemente de si el sistema operativo o el tipo de dispositivo admite la instalación de **Panda Adaptive Defense 360.**

Requisitos para encontrar equipos desprotegidos en la red

El listado de equipos descubiertos contiene los puestos de usuario y servidores que cumplen con los siguientes requisitos:

- No están ocultos por el administrador
- No están siendo ya administrados por **Panda Adaptive Defense 360 sobre Aether Platform**
- Se encuentran en el mismo segmento de subred al que pertenece el equipo descubridor

Asignación del rol de descubridor a un equipo de la red

- Comprueba que el equipo descubridor tiene instalado **Panda Adaptive Defense 360**.
- Haz clic en el menú superior **Configuración**, panel lateral **Configuración de red** y pestaña **Descubrimiento**.
- Haz clic en el botón **Añadir equipo descubridor** y selecciona del listado los equipos que

lanzarán procesos de descubrimiento en la red.

Características del equipo descubridor

Una vez asignado el rol de descubridor a un equipo, éste se mostrará en la lista de equipos descubridores (menú superior **Configuración**, panel lateral **Configuración de red**, pestaña **Descubrimiento**). Para cada equipo descubridor se muestra la siguiente información:

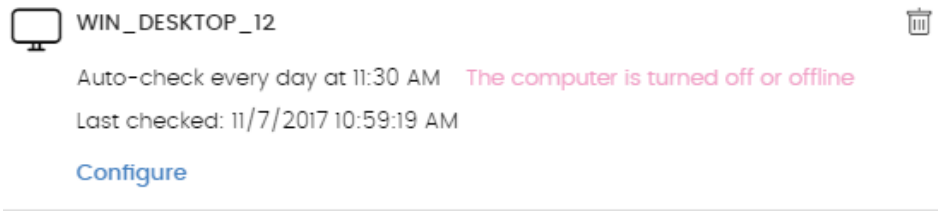


Figura 21: información mostrada en cada equipo descubridor

- **Nombre del equipo**
- **Configuración de la tarea de descubrimiento:** configuración de la tarea automática que se lanza para descubrir equipos en la red, si está configurada.
- **Ultima comprobación**: fecha y hora de la última vez que se lanzó una tarea de descubrimiento.
- **El equipo está apagado o sin conexión: Panda Adaptive Defense 360** no es capaz de conectar con el equipo descubridor.
- **Configurar**: establece el alcance y tipo de descubrimiento (automático o manual). Si es automático, la tarea de descubrimiento se ejecutará una vez al día.

6.5.3 Alcance del descubrimiento

Para limitar el alcance del descubrimiento de equipos en la red sigue los pasos mostrados a continuación:

- En el menú superior **Configuración**, panel lateral **Configuración de red**, pestaña **Descubrimiento**, selecciona el equipo descubridor a configurar el alcance de descubrimiento.
- En la sección **Limitar el alcance del descubrimiento** selecciona un criterio:
  - **Buscar solo en la subred del equipo descubridor**: el equipo descubridor utiliza la máscara configurada en la interface para efectuar un barrido completo de la subred a la que pertenece.
  - **Buscar solo en los siguientes rangos de direcciones IPs**: define varios rangos de búsqueda en la red separados por comas. Separa el inicio y el final del rango mediante el carácter guion '-'.
  - **Buscar sólo equipos de los siguientes dominios**: la búsqueda queda limitada a los dominios Windows indicados separados por comas.

6.5.4 Programación del descubrimiento de equipos

Programación de tareas de descubrimiento

Las tareas de descubrimiento de equipos se pueden programar para ser lanzadas por los equipos descubridores de forma automática cada cierto tiempo.

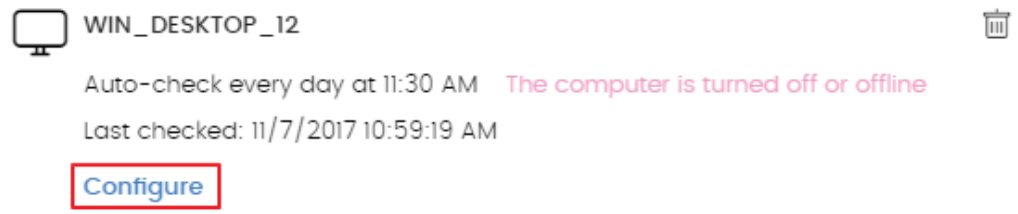


Figura 22: acceso a la ventana de configuración de la tarea de descubrimiento

- **Ejecución automática de la tarea de descubrimiento:**

- En el menú superior **Configuración**, panel lateral **Configuración de red**, pestaña **Descubrimiento**, haz clic en el enlace **Configurar** del equipo descubridor a configurar.
- En el desplegable **Ejecutar automáticamente** elige **Todos los días.**
- Elige la hora a la que se ejecutará la tarea.
- Marca en la casilla para tomar la hora local del equipo o la hora del servidor **Panda Adaptive Defense 360.**
- Haz clic en **Aceptar**. El equipo configurado mostrará en su descripción la programación configurada.

- **Ejecución manual de la tarea de descubrimiento:**

- En el menú superior **Configuración**, panel lateral **Configuración de red**, pestaña **Descubrimiento**, haz clic en el enlace **Configurar** del equipo descubridor a configurar.
- En el desplegable **Ejecutar** automáticamente elige **No.**
- Haz clic en **Aceptar**. El equipo mostrará un enlace **Comprobar ahora** que el administrador podrá utilizar para lanzar una tarea de descubrimiento bajo demanda.

6.5.5 Listado de equipos descubiertos

Contiene los dispositivos encontrados y no administrados por **Panda Adaptive Defense 360**.

Existen dos formas de acceder al listado de equipos descubiertos:

- Desde el widget **Estado de protección**
- Desde **Mis listados**

- **Widget Estado de la protección**

Desde el menú superior **Estado** se accede al panel de control de **Panda Adaptive Defense 360** donde se encuentra el widget **Estado de la protección**. En su parte inferior se mostrará el enlace **Se han descubierto x equipos que no están siendo administrados desde Panda Adaptive Defense 360**.

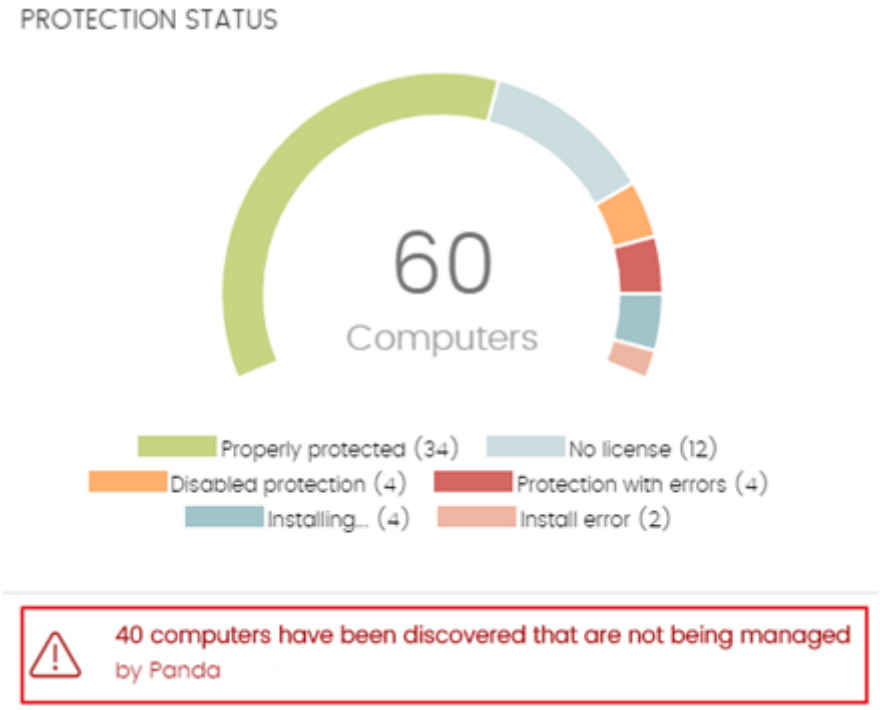


Figura 23: acceso al listado de equipos descubiertos desde el widget Estado de la protección

- **Listado general**

Accede a la sección **Mis listados** desde el menú lateral y haz clic en el enlace **Agregar.** Selecciona en el desplegable el listado **Equipos no administrados descubiertos.**

Descripción de la tabla de equipos descubiertos

Campo	Comentario	Valores
Equipo	Nombre del equipo descubierto	Cadena de caracteres
Estado	Indica el estado en el que se encuentra el equipo con respecto al proceso de instalación	— **Descubierto**: el equipo ha sido localizado como candidato a la instalación, pero ésta aún no se ha iniciado **Instalando**: el proceso de instalación se ha iniciado **Error instalando:** mensaje con el tipo de error producido en la instalación. Consulta más adelante la relación de mensajes de error y una explicación de cada uno de ellos.

Campo	Comentario	Valores
Dirección IP	Dirección IP principal del equipo	Cadena de caracteres
Fabricante NIC	Marca de la tarjeta de red del equipo descubridor	Cadena de caracteres
Descubierto por	Nombre del equipo descubridor	Cadena de caracteres
Ultima vez visto	Fecha en la que el equipo fue descubierto por última vez	Fecha

Tabla 5: campos del listado de equipos descubiertos

A continuación, se muestran los mensajes de error:

- **Credenciales incorrectas:** introduce unas credenciales con permisos para instalar el agente.
- **Equipo descubridor no disponible**:
  - El equipo que descubrió al puesto de usuario o servidor ha sido borrado y por lo tanto la instalación no se puede ejecutar.
- **No es posible conectar con el equipo**:
  - El equipo está apagado
  - El firewall impide la conexión
  - El equipo no tiene un sistema operativo compatible.
- **No es posible descargar el instalador del agente**:
  - El paquete descargado está corrupto
  - No existe un paquete de instalación para el sistema operativo del puesto o servidor
  - No hay espacio suficiente en el equipo para descargar el paquete del agente
  - La descarga del paquete del agente es muy lenta y se ha cancelado.
- **No es posible copiar el agente**.
  - No hay espacio suficiente en el equipo para copiar el paquete del agente
- **No es posible instalar el agente**.
  - No hay espacio suficiente en el equipo para instalar el agente
  - Ya hay un agente instalado en el equipo. Si es la misma versión, se lanza en modo reparación.
- **No es posible registrar el agente**.
  - El equipo esté pendiente de reiniciar para desinstalar el agente
  - **Panda Panda Endpoint Protection** está instalado en el equipo remoto

Campos mostrados en el fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio	Cadena de caracteres
Equipo	Nombre del equipo descubierto	Cadena de caracteres
IP	Dirección IP principal del equipo	Cadena de caracteres
Dirección MAC	Dirección física del equipo	Cadena de caracteres
Fabricante NIC	Marca de la tarjeta de red del equipo descubridor	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo	Cadena de caracteres
Primera vez visto	Fecha en la que el equipo fue descubierto por primera vez	Cadena de caracteres
Primera vez visto por	Nombre del equipo descubridor que vio por primera vez al puesto de usuario	Cadena de caracteres
Ultima vez visto	Fecha en la que el equipo fue descubierto por última vez	Fecha
Ultima vez visto por	Nombre del equipo descubridor que vio por última vez al puesto	Cadena de caracteres

Tabla 6: campos del fichero exportado Listado de equipos descubiertos

Herramienta de búsqueda

Campo	Comentario	Valores
Buscar	Búsqueda por el nombre del equipo, IP, fabricante de la tarjeta de red o equipo descubridor	Cadena de caracteres
Estado	Estado de la instalación de Panda Adaptive Defense 360	**Descubierto**: el equipo ha sido localizado como candidato a la instalación, pero ésta aún no se ha iniciado **Instalando**: el proceso de instalación se ha iniciado **Error instalado**
Ultima vez visto	Fecha en la que el equipo fue descubierto por última vez	Últimas 24 horas Últimos 7 días Último mes

Tabla 7: campos de filtrado para el listado Accesos a páginas web por equipo

Equipos ocultos

Para evitar generar listados de equipos descubiertos muy extensos que incluyan dispositivos sin interés para la instalación de **Panda Adaptive Defense 360**, es posible ocultarlos de forma selectiva siguiendo los pasos mostrados a continuación:

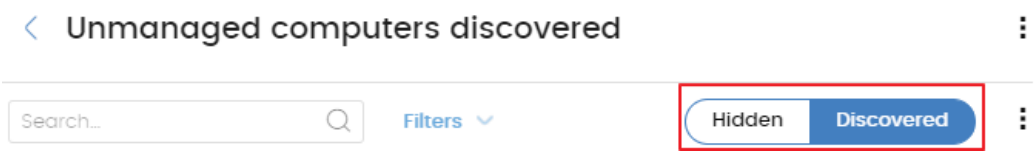


Figura 24: selección del tipo de listado de equipos descubiertos (Ocultos y Descubiertos)

- En el listado de equipos descubiertos selecciona **Descubierto** en el combo **(1)** y haz clic en **Filtrar.**
- Haz clic en las casillas correspondientes a los equipos a ocultar **(2).**
- Para ocultar varios equipos haz clic en el menú de contexto general y en **Ocultar y no volver a descubrir (3).**
- Para ocultar un único equipo haz clic en el menú de contexto del equipo y en **Ocultar y no volver a descubrir (4).**

Equipos borrados

Panda Adaptive Defense 360 no elimina de la lista de equipos descubiertos los dispositivos que una vez fueron detectados, pero ya no están accesibles por haberse retirado, avería, robo o cualquier otra razón.

Para retirar de forma manual estos equipos nunca más accesibles sigue los pasos mostrados a continuación:

- En el listado de equipos descubiertos selecciona **Descubiertos** u **Ocultos** en el combo dependiendo del estado del dispositivo **(1).**
- Haz clic en las casillas correspondientes a los equipos a borrar **(2).**
- Para borrar varios equipos haz clic en el menú de contexto general y en **Borrar (3).**
- Para borrar un único equipo haz clic en el menú de contexto del equipo y en **Borrar (4).**

Un equipo que se elimina de la consola sin desinstalar el software Panda Adaptive Defense 360, y sin retirarse físicamente de la red volverá a aparecer en la siguiente tarea de descubrimiento. Borra únicamente los equipos que nunca más vayan a ser accesibles.

6.5.6 Detalles del equipo descubierto

Haz clic en un equipo descubierto para ver su ventana de detalle dividida en 3 secciones:

- **Alertas de equipo (1)**: muestra potenciales problemas asociados a la instalación del equipo.
- **Detalles del equipo (2)**: muestra un resumen ampliado del hardware, software y seguridad

configurada en el equipo.

- **Descubierto por (3)**: muestra los equipos descubridores que vieron el equipo no administrado.

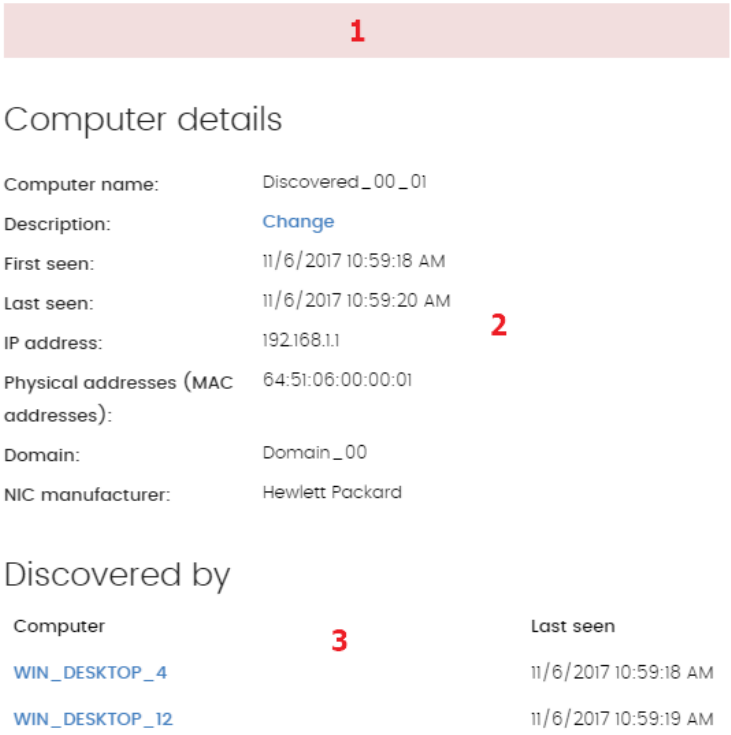


Figura 25: distribución de la información en un equipo descubierto

Alertas de equipo

- **Error instalando el agente de Panda**: indica el motivo del error en la instalación del agente
  - Credenciales incorrectas. Lanza de nuevo la instalación con unas credenciales con suficientes privilegios para realizar la instalación.
  - Equipo descubridor no disponible.
  - No es posible conectar con el equipo. Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
  - No es posible descargar el instalador del agente. Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
  - No es posible copiar el instalador del agente. Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
  - No es posible instalar el agente. Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
  - No es posible registrar el agente. Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
- **Error instalando la protección de Adaptive Defense 360**: indica el motivo del error en la instalación de la protección.
  - No hay suficiente espacio libre en el disco para realizar la instalación.
  - El servicio de Windows Installer no está operativo.
  - El usuario canceló la desinstalación de la protección de otro fabricante.

  - Hay otra instalación en curso.
  - Error desinstalando automáticamente protecciones de otros fabricantes.
  - Desinstalador no disponible para protección de otro fabricante.
- **Instalando agente de Panda**: una vez terminado el proceso de instalación el equipo dejará de aparecer en el listado de equipos descubiertos.
- **Equipo oculto**
- **Equipo no administrado**: el equipo no tiene el agente Panda instalado.

Detalles del equipo

- **Nombre del equipo**
- **Descripción:** permite asignar una descripción al equipo, aunque no esté administrado todavía.
- **Primera vez visto:** fecha y hora de la primera vez que el equipo fue descubierto.
- **Última vez visto:** fecha y hora de la primera vez que el equipo fue descubierto.
- **Dirección IP**
- **Direcciones físicas (MAC)**
- **Dominio:** dominio Windows al que pertenece el equipo.
- **Fabricante NIC:** fabricante de la tarjeta de red instalada en el equipo.

Descubierto por

- **Equipo**: nombre del equipo descubridor que vio al equipo no administrado.
- **Ultima vez visto**: fecha y hora de la primera vez que el equipo fue visto por el equipo descubridor.

6.5.7 Instalación de equipos

Para instalar de forma remota el software **Panda Adaptive Defense 360** en uno o varios equipos distribuidos sigue los pasos mostrados a continuación:

Desde el listado de equipos descubiertos

- Accede al listado de equipos descubiertos.
  - Desde el panel lateral **Mis ficheros**, **Añadir**, selecciona el listado **Equipos no administrados descubiertos.**
  - Desde el menú superior **Estado** en el widget **Estado de la protección,** haz clic en el link **Se han descubierto x equipos que no están siendo administrados desde Panda Adaptive Defense 360.**
  - Desde el menú superior **Equipos** haz clic en **Añadir equipos** y selecciona **Descubrimiento e instalación remota.** Se mostrará una ventana con un asistente. Haz clic en el link **Ver equipos no administrados descubiertos.**
- En el listado de equipos descubiertos selecciona **Descubiertos** u **Ocultos** en el combo, dependiendo del estado del dispositivo **(1).**
- Haz clic en las casillas correspondientes a los equipos a instalar.
- Para instalar varios equipos haz clic en el menú de contexto general y en **Instalar agente de Panda**.

- Para instalar un único equipo haz clic en el menú de contexto del equipo y en **Instalar agente de Panda.**
- Configura la instalación según los pasos descritos en el punto 6.4.3 Instalación manual del software Panda Adaptive Defense 360.
- Introduce una o varias credenciales de instalación. Es necesario utilizar una cuenta de administración local del equipo o del dominio al que pertenece para completar la instalación con éxito.

Desde la pantalla de detalles de equipo

Al hacer clic en un equipo descubierto se mostrará su detalle y en la parte superior el botón **Instalar agente de Panda.** Sigue los pasos descritos en el punto 6.4.3 Instalación manual del software Panda Adaptive Defense 360.

6.6. Instalación con herramientas centralizadas

Con la ayuda de herramientas de terceros, es posible la instalación del software Windows **Panda Adaptive Defense 360** de forma centralizada en redes de tamaño medio o grande.

6.6.1 Línea de comandos del paquete de instalación

Para automatizar la instalación e integración del agente Panda en la consola de administración se implementan los parámetros siguientes de línea de comandos:

- **IGNORE_LEGACY_AGENT=[TRUE|FALSE]**: mantiene el agente **de Panda Endpoint Protection / Pro** de la plataforma tradicional (legacy) en caso de ya estar instalado. El valor por defecto es FALSE: sí el agente legacy se encuentra en el equipo la instalación se interrumpe.
- **GROUPPATH="grupo1\grupo2"**: ruta dentro del árbol de grupos y sin indicar el nodo raíz Todos donde se integrará el equipo. Si el grupo no existe el equipo se integra en el nodo raíz Todos.
- **PRX_SERVER**: dirección IP o nombre del servidor proxy corporativo.
- **PRX_PORT**: puerto del servidor proxy corporativo.
- **PRX_USER**: usuario del servidor proxy corporativo.
- **PRX_PASS**: contraseña del servidor proxy corporativo.

A continuación, se muestra un ejemplo de instalación con parámetros

```
Msiexec /i "PandaAetherAgent.msi" GROUPPATH="Madrid\Contabilidad"
PRX_SERVER="ProxyCorporative" PRX_PORT="3128" PRX_USER="admin" PRX_PASS="panda"
IGNORE_LEGACY_AGENT=TRUE
```

6.6.2 Despliegue de Panda Adaptive Defense 360 desde Panda Systems Management

Para los clientes de **Panda Systems Management** el despliegue de **Panda Adaptive Defense 360** para Windows, macOS y Linux está completamente automatizado a través de los componentes:

- Panda Endpoint Protection on Aether Installer for Windows
- Panda Endpoint Protection Installer on Aether for macOS
- Panda Endpoint Protection Installer on Aether for Linux

Los tres componentes son gratuitos para todos los usuarios de **Panda Systems Management** y están disponibles en la Comstore.

Características y requisitos del componente

Los componentes no tienen ningún requisito más allá de los indicados para **Panda Systems Management** y **Panda Adaptive Defense 360 sobre Aether**.

El tamaño del componente es:

- Panda Endpoint Protection on Aether Installer for Windows: 1.5 Mbytes
- Panda Endpoint Protection Installer on Aether for macOS: 3 Kbytes
- Panda Endpoint Protection Installer on Aether for Linux: 3 Kbytes

Una vez desplegado y ejecutado, el componente descargará el instalador **Panda Adaptive Defense 360 sobre Aether**. Dependiendo de la versión, el tamaño varía entre 6 y 8 Mbytes por cada equipo a instalar.

6.6.3 Despliegue de Panda Adaptive Defense 360 con Microsoft Active Directory

A continuación, se detallan los pasos para el despliegue del software **Panda Adaptive Defense 360** en los equipos de una red Windows con Directorio Activo mediante GPO (Group Policy Object).

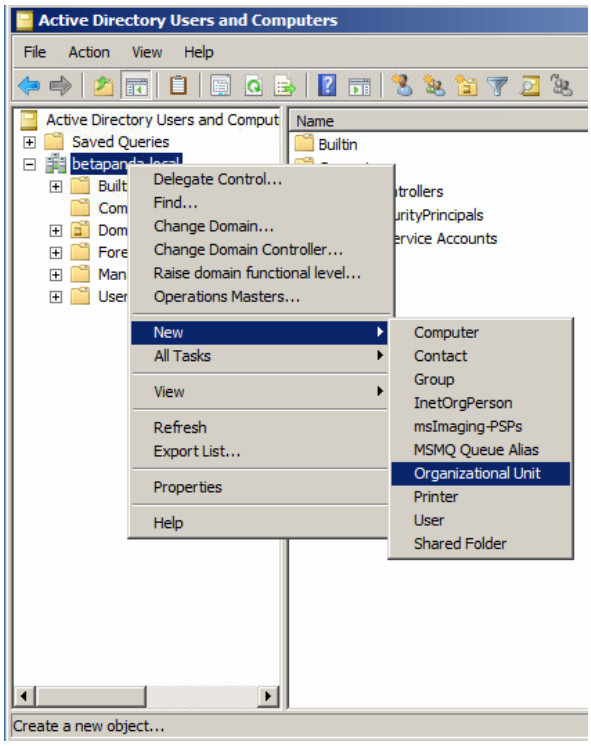


Figura 26: creación de una unidad organizativa

1 Descarga de Panda Adaptive Defense 360 y compartición del instalador en la red

- Coloca el instalador **Panda Adaptive Defense 360** en una carpeta compartida que sea accesible por todos los equipos que vayan a recibir el software.

2 Crea un nueva OU (Organizational Unit) de nombre "Panda Adaptive Defense".

- Abre el applet "Active Directory Users and Computers" en el Directorio Activo de la red.
- Abre el snap-in Group Policy Management y en Domains selecciona la OU recién creada para bloquear la herencia.

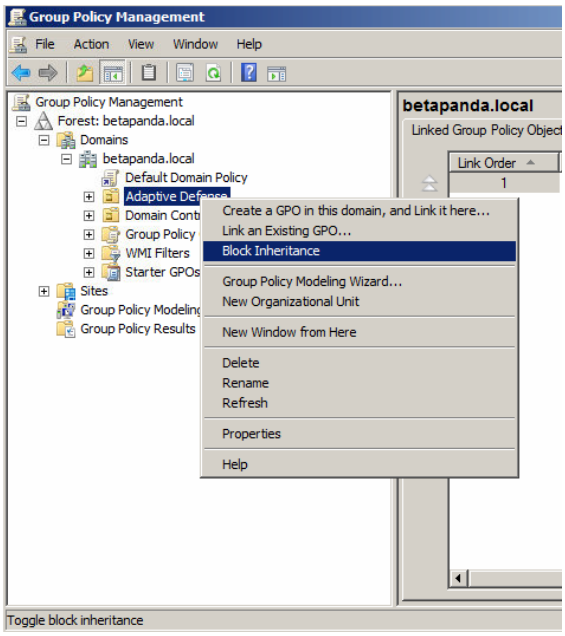


Figura 27: bloqueo de herencia

- Crea una nueva GPO en la OU “Panda Adaptive Defense”.

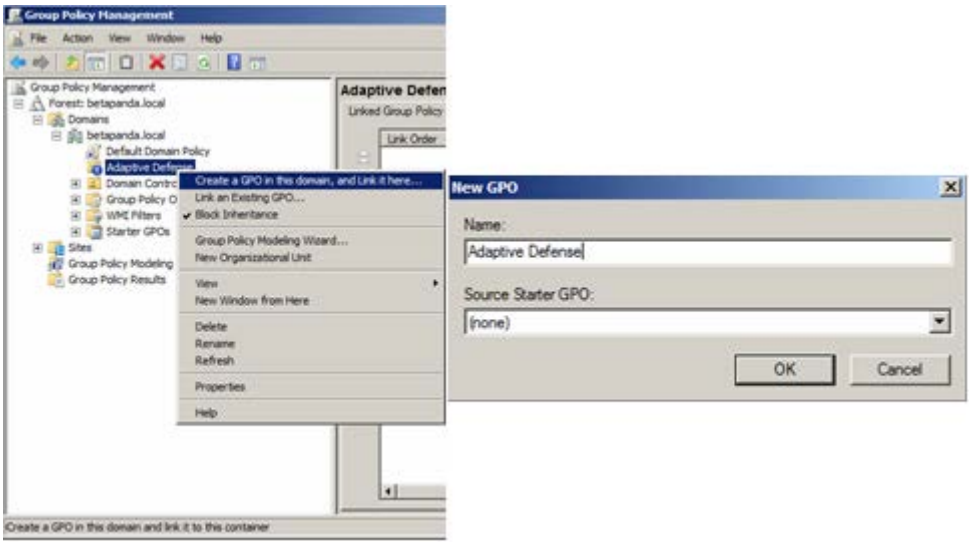


Figura 28: creación de una GPO

3 Añade un nuevo paquete de instalación a la GPO recién creada

- Edita la GPO.

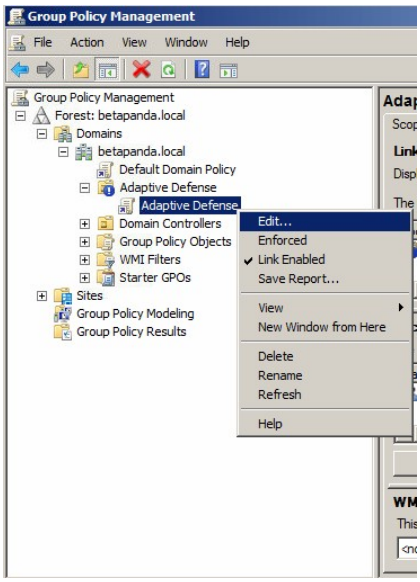


Figura 29: edición de la GPO recien creada

- Añade un nuevo paquete de instalación que contendrá el software **Panda Adaptive Defense 360**. Para ello pedirá añadir el instalador a la GPO.

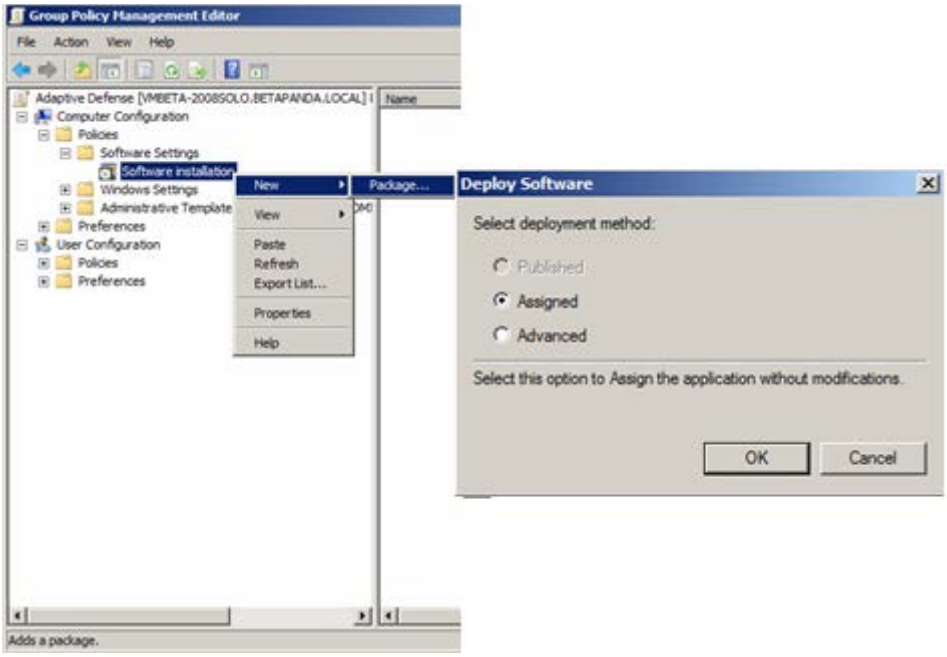


Figura 30: asignación de un nuevo paquete de despliegue

4 Edita las propiedades de despliegue

- En el menú propiedades, pestaña Deployment, Advanced selecciona la casilla que evita la comprobación entre el sistema operativo de destino y el definido en el instalador.

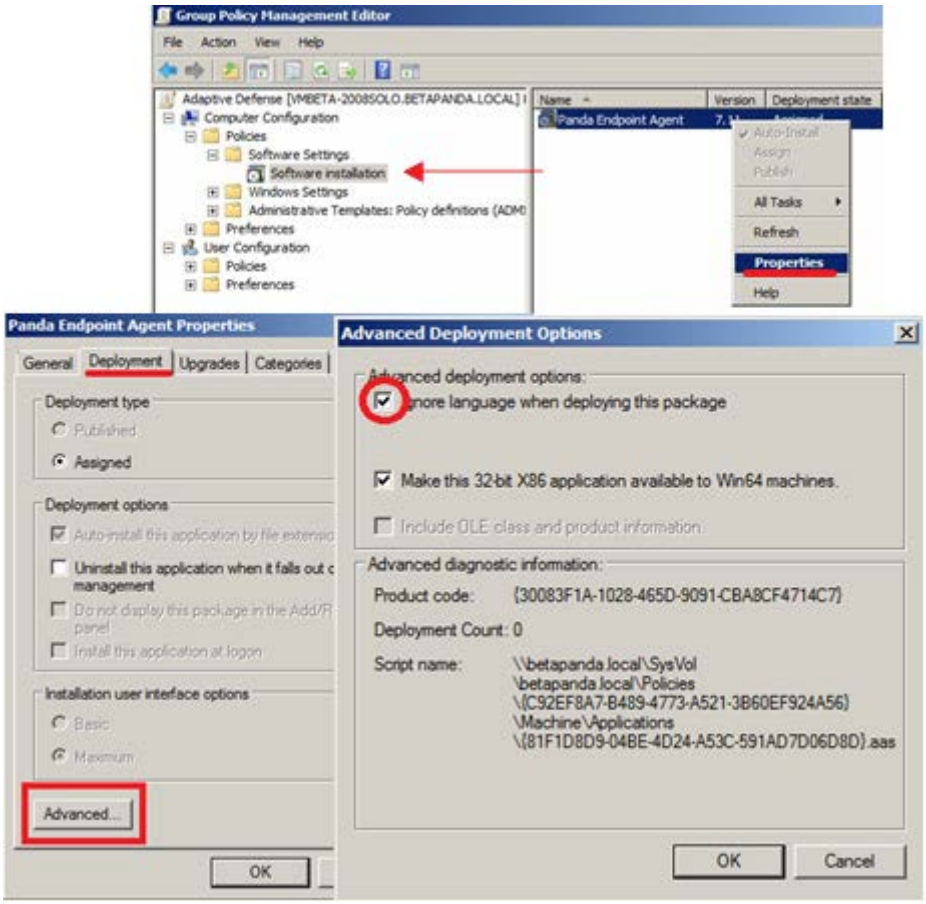


Figura 31: configuración del paquete de despliegue

- Finalmente añade en la OU Panda Adaptive Defense creada anteriormente en Active Directory Users and Computers a todos los equipos de la red que se quiera enviar el agente.

6.7. Desinstalación del software

Puedes desinstalar el software **Panda Adaptive Defense 360** de forma manual desde el panel de control del sistema operativo, o de forma remota desde la zona **Equipos** o desde los listados **Estado de la protección de los equipos** y **Licencias**.

6.7.1 Desinstalación manual

El propio usuario podrá ejecutar una desinstalación manual siempre y cuando el administrador de la protección no haya establecido una contraseña de desinstalación al configurar el perfil de la protección para su PC. Si lo ha hecho, se necesitará autorización o disponer de las credenciales necesarias para poder desinstalar la protección.

La instalación de **Panda Adaptive Defense 360** incluye varios programas independientes, según sea la plataforma de destino:

- **Equipos Windows y macOS**: agente y protección.
- **Equipos Linux**: agente, protección y módulo del kernel.
- **Dispositivos Android**: protección.

Para desinstalar completamente **Panda Adaptive Defense 360** es necesario quitar todos los módulos. Si se desinstala únicamente el módulo de la protección, transcurrido un tiempo el agente la reinstalará de forma automática.

En Windows 8 o superior:

- Panel de Control > Programas > Desinstalar un programa.
- También puedes desinstalar tecleando, en el menú Metro: "desinstalar un programa".

En Windows Vista, Windows 7, Windows Server 2003 y superiores:

- Panel de Control > Programas y características > Desinstalar o cambiar.

En Windows XP:

- Panel de Control > Agregar o quitar programas.

En macOS:

- Finder > Aplicaciones > Arrastra el icono de la protección que deseas desinstalar a la papelera o ejecuta el comando `sudo sh /Applications/Protection-Agent.app/Contents/uninstall.sh`.
- El agente no se desinstala arrastrando el icono a la papelera, en su lugar es necesario ejecutar el comando `sudo sh /Applications/Management-Agent.app/Contents/uninstall.sh`

En dispositivos Android:

- Accede a Configuración de Android. Seguridad > Administradores de dispositivos.
- Desactiva la casilla correspondiente a Panda Adaptive Defense 360. A continuación, Desactivar > Aceptar.
- De nuevo en la pantalla de Configuración de Android selecciona Aplicaciones instaladas. Haz clic en Panda Adaptive Defense 360 > Desinstalar > Aceptar.

En Linux:

En Linux se utiliza el entorno grafico para gestionar paquetes incluido en la distribución.

- **Fedora**: Actividades > Software > Instalado
- **Ubuntu**: Software de Ubuntu > Instaladas

Se recomienda utilizar la línea de comandos para desinstalar el producto:

- Ubuntu
  - **Agente**: `sudo dpkg -r management-agent`
  - **Kernel**: `sudo dpkg -r protection-agent-dkms`
  - **Protección**: `sudo dpkg –r protection-agent-corporate`

- Fedora (sustituye “version” por la build del maquete pulsando la tecla de tabulación)
  - **Agente**: `sudo dnf remove management-agent-“version”`
  - **Kernel**: `sudo dnf remove protection-agent-dkms-“version”`
  - **Protección**: `sudo dnf remove protection-agent-corporate-“version”`

6.7.2 Resultado de la desinstalación manual

Al desinstalar el software **Panda Adaptive Defense 360** (agente Panda y Protección) el equipo desaparecerá completamente de la consola de administración. Todos los contadores, entradas en informes e información de la actividad del equipo y de sus procesos se borrarán.

Si, posteriormente, el mismo equipo vuelve a ser integrado en la consola de administración mediante la reinstalación del software Panda Adaptive Defense 360, se recuperará toda la información previamente eliminada.

6.7.3 Desinstalación remota

Para desinstalar de forma remota un equipo Windows protegido con **Panda Adaptive Defense 360** sigue los pasos mostrados a continuación:

- En la zona **Equipos**, o en los listados **Licencias** y **Estado de la protección de equipos** marca los equipos a desinstalar con las casillas de selección.
- En la barra de acciones haz clic en el botón **Eliminar**. Se mostrará una ventana de confirmación.
- En la ventana de confirmación haz clic en la casilla **Desinstalar el agente de Panda de los equipos seleccionados** para retirar por completo el software Panda Adaptive Defense 360.

Una vez desinstalado, los contadores asociados a los equipos (malware detectado, URLs bloqueadas, correos filtrados, dispositivos bloqueados etc) se eliminarán de la consola de administración. Al reinstalar el software **Panda Adaptive Defense 360** en el equipo, se recuperarán todos los contadores.

La desinstalación remota solo se soporta en plataformas Windows. En plataformas Linux y macOS únicamente se retirará el equipo de la consola junto a todos los contadores, si bien en el próximo descubrimiento de la red el equipo será reincorporado a la consola, junto a toda su información.

7. Gestión de equipos y dispositivos

7.1. Introducción

La consola de administración permite mostrar los equipos administrados de forma ordenada y flexible, aplicando distintas estrategias que ayudan al administrador a localizar rápidamente las máquinas para facilitar su gestión.

7.1.1 Requisitos para la gestión de equipos desde la consola de administración

Para que un equipo de la red sea gestionable por la consola de administración se requiere como mínimo de la instalación del agente Panda en el equipo.

Al igual que otros productos de Panda Security basados en **Aether, Panda Adaptive Defense 360** entrega el agente de comunicaciones Panda en el paquete de instalación para todas las plataformas compatibles.

Los equipos sin licencia **Panda Adaptive Defense 360** pero con el agente Panda instalado aparecerán en la consola de administración, aunque su protección estará desactualizada y no podrán ejecutar tareas, análisis ni otros recursos propios de **Panda Adaptive Defense 360.**

> ***Los equipos con la licencia caducada seguirán analizando en busca de amenazas, pero no actualizarán el fichero de firmas ni utilizarán la protección avanzada. En este estado, Panda Adaptive Defense 360 no será una solución efectiva para la protección frente a amenazas y Panda Security recomienda encarecidamente la renovación de los servicios contratados para mantener el parque IT debidamente protegido.***

7.2. La zona Equipos

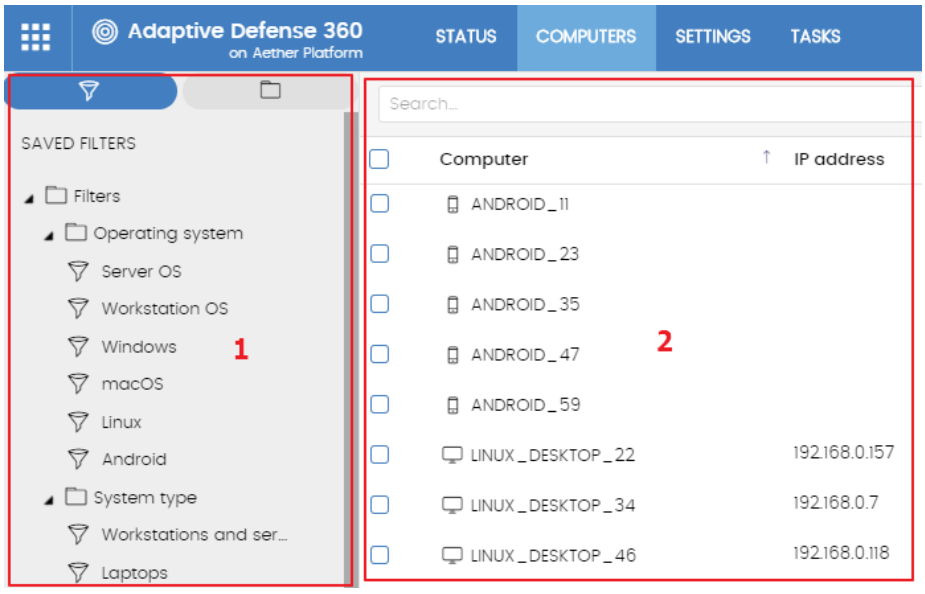


Figura 32: vista general de los paneles en la zona Equipos

Para acceder a la ventana de administración de equipos haz clic en el menú superior **Equipos.** Se mostrarán dos zonas bien diferenciados: el panel lateral con un **Árbol de equipos (1)** y el panel central con un **Listado de equipos (2)**. Ambos paneles trabajan de forma conjunta y su funcionamiento se muestra a lo largo de este capítulo.

Al seleccionar una rama del **Árbol de equipos**, el **Listado de equipos** se actualiza con todos sus equipos asignados.

Mostrar equipos en subgrupos

Es posible limitar el listado de los equipos mostrando únicamente los que pertenecen a la rama del árbol seleccionada, o por el contrario mostrar todos los equipos que cuelgan de la rama seleccionada y de ramas de orden inferior. Para definir este comportamiento haz clic en el menú de contexto y selecciona la opción **Mostrar equipos de los subgrupos**.

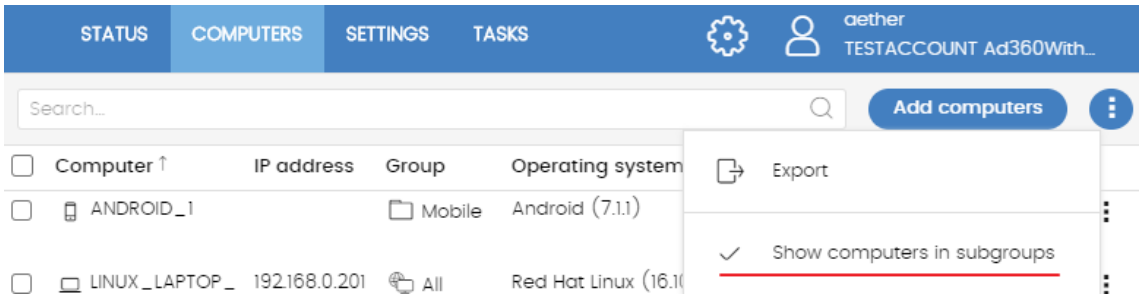


Figura 33: habilitar el listado de equipos pertenecientes a ramas dependientes

7.3. El panel Listado de equipos

El listado de equipos muestra los puestos de usuario y servidores correspondientes al grupo o filtro seleccionado en el árbol de equipos. Además, incluye herramientas de gestión que pueden ser aplicadas a equipos de forma individual o a varios de ellos.

A continuación, se muestra un esquema del panel Listado de equipos:

- **(1)** Listado de equipos que pertenecen a la rama del árbol seleccionada.
- **(2)** Herramienta de búsqueda. Permite localizar equipos por su nombre. Se admiten coincidencias parciales sin tener en cuenta mayúsculas y minúsculas
- **(3)** Menú de contexto que permite aplicar una misma acción a varios equipos.
- **(4)** Casillas de selección de equipos.
- **(5)** Sistema de paginación en la parte inferior del panel.
- **(6)** Menú de contexto

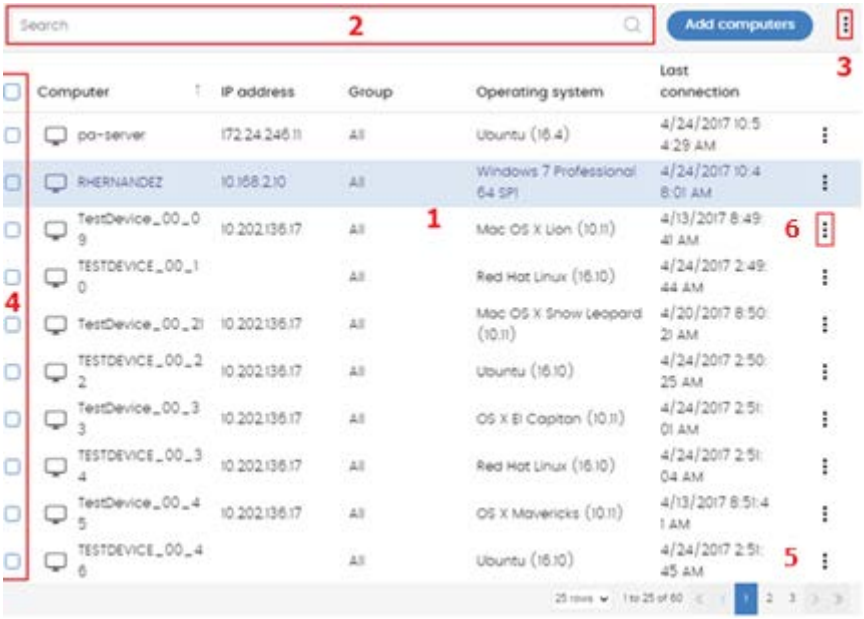


Figura 34: el panel Listado de equipos

Al marcar uno o más equipos con las casillas de selección **(4)**, la herramienta de búsqueda **(2)** se oculta para mostrarse en su lugar la Barra de Acciones **(7)**

Figura 35: barra de acciones solapando a la herramienta de búsqueda

7.3.1 Listado de equipos

Por cada equipo se incluye la información mostrada a continuación

Campo	Comentario	Valores
Equipo	Nombre del equipo y su tipo	Cadena de caracteres Equipo de sobremesa (puesto de trabajo, servidor Windows, Linux o macOS) Equipo portátil Dispositivo móvil (smart-phone o tablet Android)

Campo	Comentario	Valores
Dirección IP	Dirección IP principal del equipo	Cadena de caracteres  Equipo en proceso de entrar en aislamiento  Equipo aislado  Equipo en proceso de salir del aislamiento
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo y su tipo	Cadena de caracteres  Grupo  Dominio AD o raíz del Directorio Activo  Unidad Organizativa  Raíz del árbol de grupos
Sistema operativo		Cadena de caracteres
Ultima conexión	Fecha del ultimo envío del estado del equipo a la nube de Panda Security	Fecha

Tabla 8: campos del Listado de equipos

Campos mostrados en el fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio	Cadena de caracteres
Tipo de equipo	Clase del dispositivo	Estación Portátil Dispositivo móvil Servidor
Equipo	Nombre del equipo	Cadena de caracteres
Direcciones IP	Listado de todas las direcciones IP de las tarjetas instaladas en el equipo	Cadena de caracteres
Direcciones físicas (MAC)	Listado de todas las direcciones físicas de las tarjetas instaladas en el equipo	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo	Cadena de caracteres
Directorio Activo	Ruta dentro del árbol de directorio activo de la empresa donde se encuentra el equipo	Cadena de caracteres

Campo	Comentario	Valores
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo	Cadena de caracteres
Versión del agente		Cadena de caracteres
Fecha arranque del sistema		Fecha
Fecha de instalación	Fecha en la que el Software Panda Adaptive Defense 360 se instaló con éxito en el equipo	Fecha
Fecha de última conexión	Fecha más reciente en la que el equipo contactó con la nube	Fecha
Plataforma	Tipo de sistema operativo instalado	Windows Linux macOS Android
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado	Cadena de caracteres
Máquina virtual	Indica si el equipo es físico o esta virtualizado	Booleano
Servidor Exchange	Versión del servidor de correo instalada en el servidor	Cadena de caracteres
Versión de la protección		Cadena de caracteres
Fecha de última actualización	Fecha de la última actualización de la protección	Fecha
Licencias	Producto licenciado en el equipo	Panda Adaptive Defense 360
Configuración de proxy e idioma	Nombre de la configuración de proxy e idioma que afecta al equipo	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de proxy e idioma	Cadena de caracteres
Configuración de seguridad para estaciones y servidores	Nombre de la configuración de seguridad que afecta al puesto de trabajo o servidor	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de seguridad	Cadena de caracteres
Configuración de seguridad para dispositivos Android	Nombre de la configuración de seguridad que afecta al dispositivo móvil	Cadena de caracteres

Campo	Comentario	Valores
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de seguridad	Cadena de caracteres
Ajustes por equipo	Nombre de la configuración de ajustes que afecta al equipo	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de ajustes	Cadena de caracteres
Configuración de seguimiento de información personal	Nombre de la configuración de seguimiento de información personal (Panda Data Control) que afecta al equipo	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de seguimiento de información personal	Cadena de caracteres
Descripción		Cadena de caracteres

Tabla 9: campos del fichero exportado Listado de equipos

Herramientas de filtrado

Campo	Comentario	Valores
Equipo	Nombre del equipo	Cadena de caracteres

Tabla 10: filtros disponibles en el listado Equipos

7.3.2 Herramientas de gestión

Utiliza las casillas de selección **(4)** para indicar los equipos que recibirán las acciones administrativas.

Al activar una casilla, se mostrará la barra de acciones con las siguientes opciones:

- **Mover a**: muestra una ventana con el árbol de grupos. Elige un grupo como destino de los equipos seleccionados. Los equipos heredarán las configuraciones asignadas al grupo de destino. Consulta el capítulo 8 para definir configuraciones.
- **Mover a su ruta de directorio activo**: mueve los equipos seleccionados al grupo que se corresponde con la unidad organizativa del directorio activo de la empresa.
- **Eliminar**: borra el equipo de la consola y desinstala el software **Panda Adaptive Defense 360**. Consulta el capítulo 6 Instalación del software Panda Adaptive Defense 360 para obtener más información sobre la desinstalación del software **Panda Adaptive Defense 360.**
- **Analizar ahora**: consulta más adelante en este mismo capítulo para una introducción a las tareas de análisis, o el capítulo 15 Tareas para obtener más información sobre tareas de análisis inmediatas.
- **Programar análisis**: consulta más adelante en este mismo capítulo para una introducción a las tareas de análisis o el capítulo 15 Tareas para obtener más información sobre tareas programadas.
- **Reiniciar**: consulta el capítulo 19 Herramientas de resolución para más información sobre el

reinicio remoto de equipos.

- **Aislar equipo**: consulta el capítulo 19 Herramientas de resolución para más información sobre aislar equipos y sus implicaciones.
- **Dejar de aislar equipo**: consulta el capítulo 19 Herramientas de resolución para más información sobre aislar equipos y sus implicaciones.
- **Programar instalación de parches**: consulta el capítulo 13 Panda Patch Management (Actualización de programas vulnerables) para obtener información sobre cómo instalar parches en equipos Windows.
- **X seleccionados**: para anular la selección actual haz clic en el botón **x seleccionados** de la barra de acciones.

7.4. El panel Árbol de equipos

Panda Adaptive Defense 360 representa la estructura de equipos mediante el Árbol de equipos **(1)**, que presenta dos vistas o árboles independientes **(2)**:

- **Árbol de filtros** : permite gestionar los equipos de la red mediante agrupaciones dinámicas. La pertenencia de un equipo a una agrupación de este tipo se establece de forma automática.
- **Árbol de grupos** : gestiona los equipos de la red mediante agrupaciones estáticas. La pertenencia de un equipo a una agrupación de este tipo se establece de forma manual.

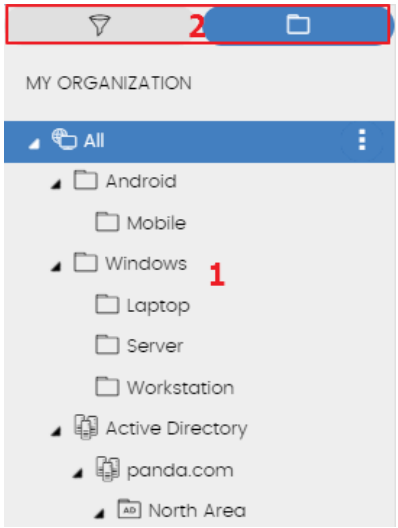


Figura 36: el panel Árbol de equipos

Los dos árboles muestran el parque de equipos y dispositivos Android del cliente de formas alternativas, con el objeto de favorecer la ejecución de tareas de distintos tipos, tales como:

- Localizar equipos que cumplan con características determinadas, relativas al hardware, software o a la seguridad.
- Asignar perfiles de configuración de seguridad de forma ágil.
- Ejecutar acciones de resolución sobre grupos de equipos.

Para localizar equipos desprotegidos o de características determinadas relativas a la seguridad o al estado de la protección consulta el capítulo 16 Visibilidad del malware y del parque informático. Para asignar perfiles de configuración de seguridad consulta el capítulo 8 Gestión de configuraciones. Para ejecutar tareas de resolución de problemas consulta el capítulo 19 Herramientas de resolución

Al pasar el puntero del ratón por las ramas del árbol de filtros y de grupos se muestra el icono de menú de contexto, haciendo clic se desplegará un menú emergente con todas las operaciones disponibles sobre esta rama del árbol en particular.

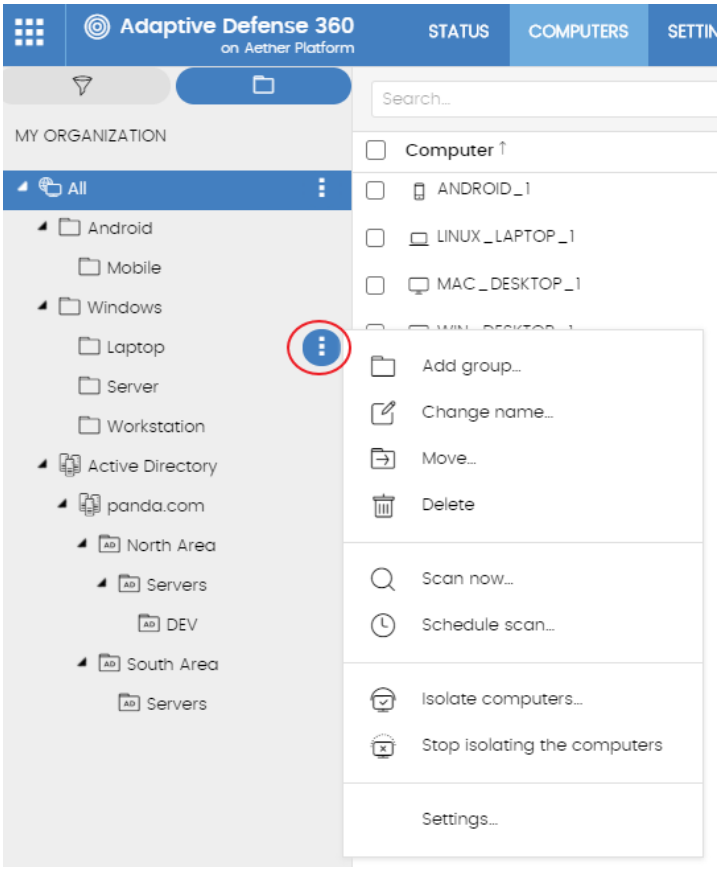


Figura 37: menú emergente con las operaciones disponibles de la rama seleccionada

7.5. Árbol de filtros

El árbol de filtros es una de las dos vistas del árbol de equipos, y permite agrupar de forma dinámica los equipos en la red mediante reglas y condiciones que describen características de los dispositivos. Estas reglas se pueden combinar mediante operaciones lógicas para producir expresiones complejas.

El árbol de filtros es accesible desde el panel de la izquierda, haciendo clic en el icono de filtro.

Al hacer clic en los diferentes elementos del árbol, el panel de la derecha se actualiza, presentando todos los equipos que cumplen con los criterios establecidos en el filtro seleccionado.

7.5.1 ¿Qué es un filtro?

Los filtros son agrupaciones dinámicas de equipos. La pertenencia de un equipo a un filtro se determina de forma automática cuando el equipo en cuestión cumple con las condiciones de pertenencia al filtro que haya configurado el administrador.

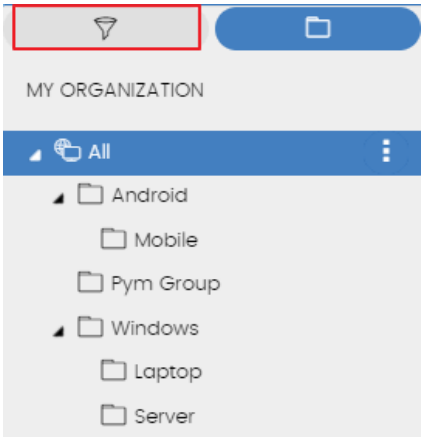


Figura 38: acceso al árbol de filtros

Un equipo puede pertenecer a más de un filtro.

Un filtro está constituido por un conjunto de reglas o condiciones que los equipos tendrán que satisfacer para pertenecer a aquél. En la medida en que el equipo cumpla con las características descritas formará parte del filtro; de la misma forma, cuando un equipo cambie su estado y no cumpla los criterios de pertenencia, automáticamente dejará de formar parte de la agrupación descrita por el filtro.

7.5.2 Agrupaciones de filtros

Los filtros se pueden ordenar de forma manual agrupándolos en carpetas, con el criterio que el administrador considere oportuno.

7.5.3 Filtros predefinidos

Panda Adaptive Defense 360 incorpora filtros de uso muy común que el administrador puede utilizar desde el primer momento para ordenar y localizar equipos en la red. Los filtros predeterminamos se pueden modificar o borrar.

No es posible recuperar un filtro predeterminado que haya sido borrado

Nombre	Grupo	Descripción
Equipos de escritorio y servidores	Tipo de máquina	Lista los equipos físicos de sobremesa o servidores
Móviles y tablets	Tipo de máquina	Lista los dispositivos smartphones y tablets
Máquinas virtuales	Tipo de máquina	Lista los equipos virtualizados
SO de servidores	Sistema operativo	Lista los equipos con un Sistema operativo de tipo Servidor instalado
SO de estaciones	Sistema operativo	Lista los equipos con un Sistema operativo de tipo estación de trabajo
Windows	Sistema operativo	Lista todos los equipos con sistema operativo Windows instalado
macOS	Sistema operativo	Lista todos los equipos con sistema operativo macOS instalado
Android	Sistema operativo	Lista todos los dispositivos equipos con sistema operativo Android instalado
Java	Software	Lista todos los equipos que tiene instalado el SDK JRE Java
Adobe Acrobat Reader	Software	Lista todos los equipos que tiene instalado el software Acrobat Reader
Adobe Flash Player	Software	Lista todos los equipos que tiene instalado el plugin de reproducción Flash
Google Chrome	Software	Lista todos los equipos que tiene instalado el navegador Chrome
Mozilla Firefox	Software	Lista todos los equipos que tiene instalado el navegador Firefox
Servidores Exchage	Software	Lista los equipos que tienen instalado el servidor de correo Microsoft Exchange Server

Tabla 11: listado de filtros predefinidos

7.5.4 Creación y organización de filtros

Todas las operaciones están disponibles haciendo clic en el icono de menú de contexto de las ramas del árbol de filtros. Se mostrará un menú emergente con las opciones permitidas en esa rama en particular.

Creación de filtros

Para crear un filtro es necesario seguir los pasos mostrados a continuación:

- Selecciona el menú de contexto de la carpeta en el árbol donde será creado el filtro.

Los filtros no se pueden anidar si no es utilizando una carpeta contenedora. Si se selecciona un filtro en el árbol, el nuevo filtro que se cree lo hará a su mismo nivel, compartiendo su carpeta contenedora

- Haz clic en **Añadir filtro**
- Indica el nombre del filtro. No es necesario que sea un nombre único. El resto de la configuración de un filtro se detalla más adelante en este capítulo.

Creación de carpetas

Haz clic en el menú de contexto de la rama donde quieras crear la carpeta y haz clic en **Añadir carpeta.** Introduce el nombre de la carpeta y haz clic en **Aceptar.**

Una carpeta no puede colgar de un filtro. Si seleccionas un filtro antes de crear la carpeta, ésta se creará al mismo nivel que el filtro, compartiendo su carpeta padre.

Borrado de filtros y carpetas

Haz clic en el menú de contexto de la rama a borrar y haz clic en **Eliminar.** La rama se borrará junto a todos sus descendientes.

No se permite borrar el nodo raíz Filtros.

Movimiento y copia de filtros y carpetas

Para mover o copiar un filtro o carpeta sigue los pasos mostrados a continuación:

- Haz clic en el menú de contexto de la rama a copiar o mover.
- Haz clic en **Mover** o **Hacer una copia**. Se mostrará una ventana emergente con el árbol de filtros de destino.
- Selecciona la carpeta de destino y pulsa **Aceptar.**

No es posible copiar carpetas de filtros. Únicamente se permite la copia de filtros.

Renombrar filtros y carpetas

Para renombrar un filtro o carpeta sigue los pasos mostrados a continuación:

- Haz clic en el menú de contexto de la rama a renombrar.
- Haz clic en **Renombrar.**
- Introduce el nuevo nombre.

No es posible renombrar la carpeta raíz. Para renombrar un filtro es necesario editarlo.

7.5.5 Configuración de filtros

La ventana de configuración de filtros es accesible al crear un nuevo filtro o editar uno existente.

Un filtro está formado por una o más reglas, relacionados entre sí mediante operadores lógicos **Y** / **O**. Un equipo formará parte de un filtro si cumple con los valores especificados en las reglas del filtro.

El esquema general de un filtro se compone de cuatro bloques:

- **Nombre del filtro (1)**: identifica al filtro.
- **Reglas de filtrado (2)**: permite construir condiciones atómicas de pertenencia al filtro. Una regla de filtrado únicamente comprueba una característica de los equipos de la red.
- **Operadores lógicos (3)**: Permiten combinar dos reglas de filtrado mediante los operadores lógicos **Y** o **O**.
- **Agrupaciones (4)**: permiten variar el orden de evaluación de las reglas de filtrado configuradas y relacionadas mediante operadores lógicos.

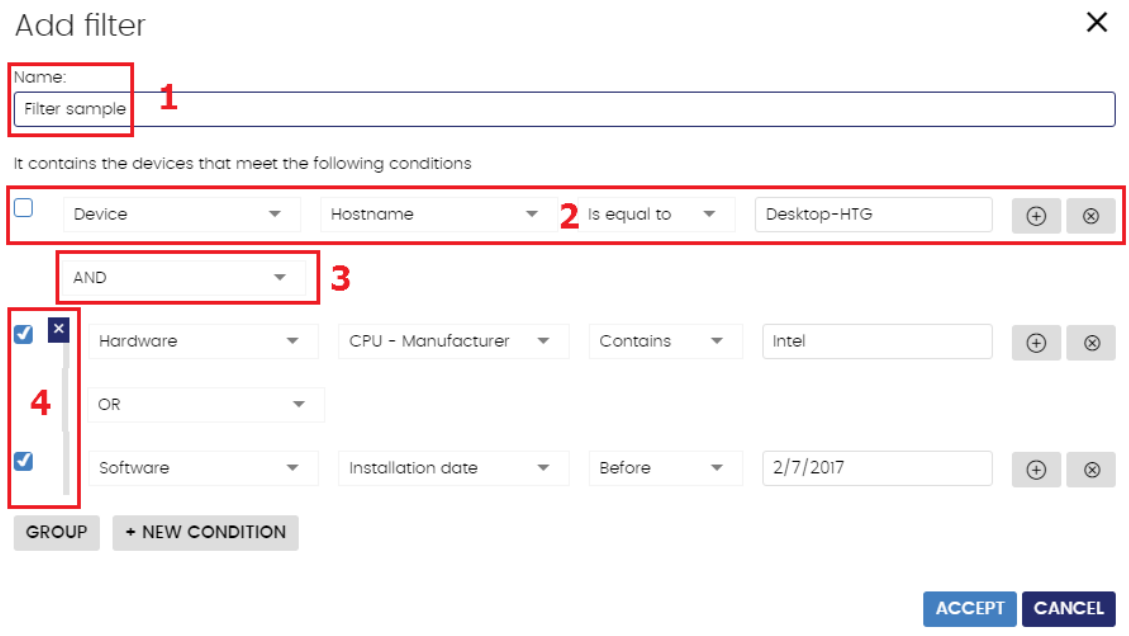


Figura 39:vista general de configuración de un filtro

7.5.6 Reglas de filtrado

Una regla de filtrado se compone de los elementos mostrados a continuación:

- **Categoría (1)**: agrupa las propiedades en secciones para facilitar su localización.
- **Propiedad (2)**: característica del equipo que determinará su pertenencia al filtro.
- **Operador (3)**: establece el modo de comparación del contenido de la propiedad del

equipo con el valor de referencia que establezca el administrador para el filtro.

- **Valor (4)**: contenido de la propiedad. Dependiendo del tipo de propiedad el campo valor cambiará para ajustarse a entradas de tipo fecha, literales etc.

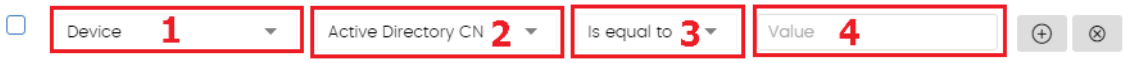


Figura 40: elementos de una regla de filtrado

Para añadir reglas de filtrado a un filtro haz clic en el icono  y para borrarlas en el icono  .

7.5.7 Operadores lógicos

Para combinar dos reglas en un mismo filtro se utilizan los operadores lógicos **Y** y **O**. Es posible encadenar de esta forma varias reglas de filtrado mediante operadores lógicos: de forma automática, al añadir una segunda regla y posteriores se mostrará un desplegable con los operadores lógicos disponibles que se aplicarán a las reglas que lo rodean.

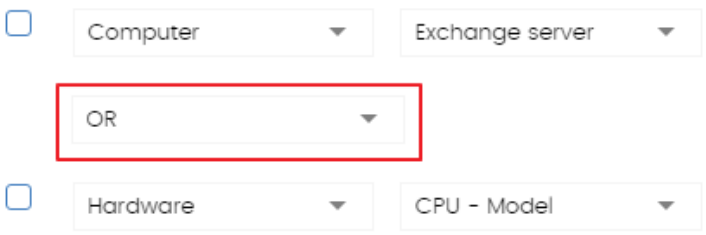


Figura 41: operador lógico O

7.5.8 Agrupaciones de reglas de filtrado

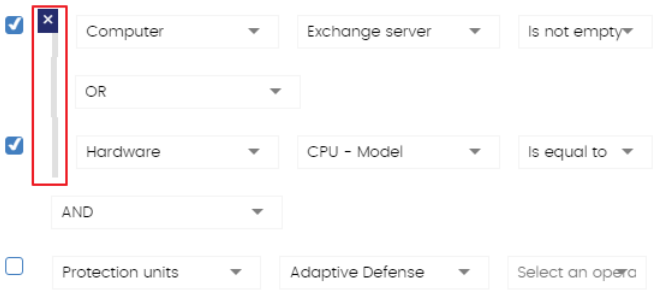


Figura 42: agrupación de reglas equivalente a (Regla 1 O Regla 2) Y Regla 3

Una agrupación equivale al uso de paréntesis en una expresión lógica. Los paréntesis en una expresión lógica se utilizan para variar el orden de evaluación de los operadores, en este caso, de las reglas de filtrado introducidas.

De este modo, para encerrar dos o más reglas en un paréntesis, es necesario crear una agrupación seleccionando con las casillas las reglas que sean necesarias y haciendo clic en el botón **Agrupación**. Se mostrará una línea delgada que abarcará las reglas de filtrado que forman parte de la agrupación.

Se pueden definir agrupaciones de varios niveles de la misma forma que se pueden anidar grupos de operandos en una expresión lógica mediante el uso de paréntesis.

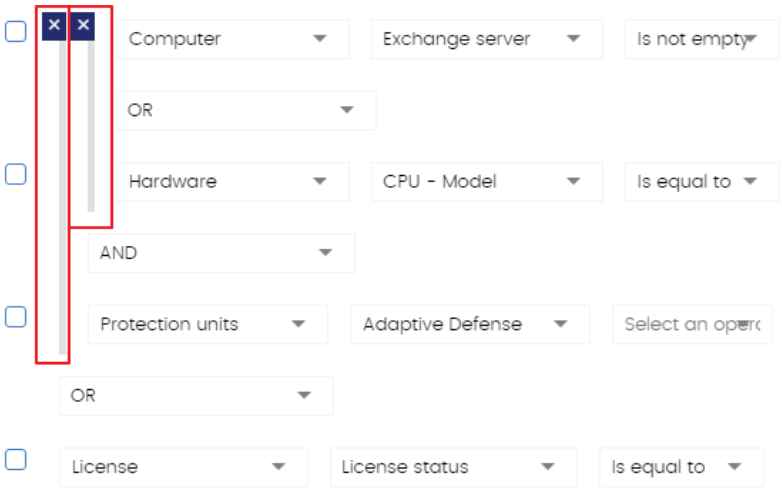


Figura 43: agrupación anidada equivalente a ((Regla 1 Y Regla 2) Y Regla 3) O Regla 4

7.6. Árbol de grupos

El árbol de grupos reúne de forma estática los equipos en la red en las agrupaciones definidas por el administrador.

Para acceder al árbol de grupos haz clic en el icono de carpeta.

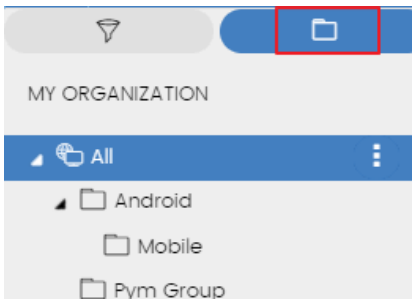


Figura 44: acceso al árbol de grupos

Al hacer clic en las diferentes ramas del árbol, el panel de la derecha se actualiza, presentando todos los equipos que contienen el grupo seleccionado y sus subgrupos.

7.6.1 Definición de grupo

Es un contenedor de equipos asignados de forma manual por el administrador. El árbol de grupos admite crear una estructura de n-niveles compuesta por grupos, subgrupos y equipos.

El máximo nivel de profundidad del árbol es 10.

7.6.2 Tipos de grupos

- **Grupo raíz**  : es el grupo padre del que cuelgan el resto de carpetas.
- **Grupos nativos**  : son los grupos estándar de **Panda Adaptive Defense 360** y soportan todas las operaciones (movimiento, renombrado, borrado etc.) Contiene otros grupos estándar y equipos.
- **Grupos Directorio Activo**  : son grupos que replican la estructura del Directorio Activo instalado en la empresa. Tienen limitadas algunas operaciones. Contiene otros grupos de Directorio Activo y equipos.
- **Grupo raíz del directorio activo**  : abarca todos los dominios del Directorio Activo configurados en la red de la organización. Contiene grupos de dominio Directorio Activo.
- **Grupo de dominio Active Directory**  : ramas del Directorio Activo que representan dominios. Contienen otros grupos de dominio Directorio Activo, grupos Directorio Activo y equipos.

7.6.3 Estructura de grupos

El tamaño de la organización, lo homogéneos que sean los equipos gestionados y la presencia o no de un servidor de Directorio Activo en la red de la empresa determinará la estructura del árbol de grupos. La estructura de grupos podrá variar desde un árbol plano de un único nivel para los casos más sencillos, hasta una estructura compleja con varios niveles, para redes grandes formadas por equipos muy heterogéneos.

A diferencia de los filtros, un equipo solo puede pertenecer a un único grupo.

7.6.4 Grupos de Directorio Activo

Para las organizaciones que tienen instalado un servidor de Directorio Activo en la red, **Panda Adaptive Defense 360** puede obtener de forma automática la estructura configurada y replicarla en el árbol de grupos. De esta manera, bajo la rama  se presentará una distribución de los equipos familiar para el administrador, con el objeto de acelerar la localización de dispositivos y su gestión.

Panda Adaptive Defense 360 replica de forma automática la estructura de Directorio Activo instalada en la organización: los agentes Panda reportan a la consola Web el grupo del Directorio Activo al que pertenecen y, conforme se despliegan los agentes, el árbol se completa con las distintas unidades organizativas.

Por esta razón, el árbol de Directorio Activo es inmutable desde la consola de **Panda Adaptive Defense 360** únicamente cambiará cuando lo haga la estructura de Directorio Activo subyacente. Los cambios se replicarán en la consola Web de **Panda Adaptive Defense 360** transcurrido un máximo de 15 minutos.

7.6.5 Creación y organización de grupos

Todas las operaciones están disponibles haciendo clic en el icono de menú de contexto de las ramas del árbol de grupos. Se mostrará un menú emergente con las opciones permitidas en esa rama en particular.

Creación de grupos

Selecciona el menú de contexto del grupo padre del cual dependerá el grupo a crear, y haz clic en **Añadir grupo.**

No es posible crear grupos de Directorio Activo en el árbol de grupos, Solo se replicarán los grupos y unidades organizativas creadas en el servidor de Directorio Activo de la empresa.

Borrado de grupos

Selecciona el menú de contexto del grupo a borrar. Si el grupo contiene subgrupos o equipos asignados, la consola de administración mostrará un error.

No se permite borrar el nodo raíz Todos.

Para borrar los grupos vacíos de tipo Directorio Activo que cuelgan de uno dado, haz clic en el menú de contexto del grupo y selecciona **Eliminar grupos vacíos.**

Movimiento de grupos

Para mover un grupo es necesario seguir los pasos mostrados a continuación:

- Selecciona el menú de contexto del grupo a mover.
- Haz clic en **Mover**. Se mostrará una ventana emergente con el árbol de grupos de destino.
- Selecciona el grupo de destino y pulsa **Aceptar.**

No se permite el movimiento del nodo raíz Todos ni de grupos Directorio Activo.

Renombrar grupos

Para renombrar un grupo es necesario seguir los pasos mostrados a continuación:

- Selecciona el menú de contexto del grupo a renombrar.
- Haz clic en **Cambiar nombre.**
- Introduce el nuevo nombre.

No es posible renombrar el grupo raíz Todos ni grupos Directorio Activo.

7.6.6 Movimiento de equipos entre grupos

Para mover uno o varios equipos a un grupo, el administrador puede seguir varias estrategias:

Movimiento de conjuntos de equipos a grupos

Para mover varios equipos a la vez a un grupo, sigue los pasos mostrados a continuación:

- Selecciona el grupo **Todos** para listar todos los equipos administrados o utiliza la herramienta de búsqueda para localizar los equipos a mover.
- Selecciona con las casillas los equipos en el panel de listado de equipos.
- Haz clic en el icono situado a la derecha de la barra de búsqueda. Se mostrará un menú desplegable con la opción **Mover a.** Haciendo clic se mostrará el árbol de grupos destino.
- Selecciona el grupo destino del árbol de grupos mostrado.

Movimiento de un único equipo a un grupo

Para asignar un único equipo a un grupo se pueden seguir varias estrategias:

- Seguir el método mostrado más arriba para asignar conjuntos de equipos a grupos, pero seleccionando un único equipo.
- Selecciona con la casilla el equipo dentro del panel de listado de equipos que quieras asignar y haz clic en el icono de menú situado en la parte derecha de la fila de ese equipo.
- Desde la ventana de detalles del propio equipo a mover:
  - Dentro en el panel de listado de equipos haz clic en el equipo que quieras mover para mostrar la ventana de detalles.
  - Localiza el campo **Grupo** y haz clic en el botón **Cambiar**. Se mostrará una ventana con el árbol de grupos de destino.
  - Selecciona el grupo destino y haz clic en **Aceptar**.

Movimiento de equipos desde grupos Active Directory

Un equipo que reside en un grupo Directorio Activo puede moverse a un grupo estándar, pero nunca a otro grupo Directorio Activo.

Movimiento de equipos hacia grupos Active Directory

No es posible mover un equipo desde un grupo nativo a un grupo Directorio Activo en particular, solo puedes devolverlo a su grupo Directorio Activo al que pertenece. Para ello haz clic en el menú de contexto del equipo y selecciona **Mover a su ruta de Active Directory.**

Restaurar la pertenencia de varios equipos a su grupo Active Directory

Para restablecer la pertenencia de equipos a su grupo Directorio Activo original haz clic en el menú de contexto de un grupo de Directorio Activo y selecciona la opción **Recuperar los equipos de esta rama de Active Directory**. Todos los equipos que pertenecen a ese grupo en el Directorio Activo de la empresa y que el administrador movió a otros grupos dentro de la consola **Panda Adaptive Defense 360** serán devueltos a su grupo original.

7.6.7 Tareas de análisis

El árbol de grupos permite asignar tareas de análisis inmediatas o programadas a todos los equipos que pertenecen a un grupo y a sus grupos descendientes.

Análisis inmediato

Haz clic en la entrada **Analizar ahora** para lanzar un análisis inmediato sobre los equipos que pertenecen al grupo o a alguno de los subgrupos. Se mostrará una ventana con el tipo de análisis a ejecutar: **Todo el ordenador** o **Áreas críticas**. Consulta el capítulo 15 Tareas para obtener más información sobre los tipos de análisis disponibles en **Panda Adaptive Defense 360**.

Análisis programado

Haz clic en la entrada **Programar análisis** para crear una tarea programada de análisis. Consulta el capítulo 15 Tareas para obtener más información sobre la configuración de una tarea programada.

7.7. Información de equipo

Al seleccionar un equipo en el panel de listado de equipos se mostrará una ventana con el detalle de la información del hardware y software instalado, así como de la configuración de seguridad asignada.

La ventana de detalle del equipo se divide en 6 secciones:

- **General (1)**: muestra información para ayudar en la identificación del equipo.
- **Alertas de equipo (2)**: muestra potenciales problemas asociados al equipo.

- **Detalles (3)**: muestra un resumen ampliado del hardware, software y seguridad configurada en el equipo.
- **Hardware (4)**: muestra el hardware instalado en el equipo, sus componentes y periféricos conectados, así como su consumo y utilización.
- **Software (5)**: muestra los paquetes de software instalados en el equipo, así como su versión y un registro de cambios.
- **Configuración (6)**: muestra las configuraciones de seguridad y otras asignadas al equipo.

7.7.1 Sección general (1)

Contiene la siguiente información:

- **Nombre del equipo e icono** indicando el tipo de equipo.
- **IP**: Dirección IP del equipo.
- **Ruta del directorio activo**: muestra la ruta completa del equipo en el Directorio Activo de la empresa.
- **Grupo**: carpeta del árbol de grupos a la que pertenece el equipo.
- **Sistema operativo**: versión completa del sistema operativo instalada en la máquina.
- **Rol del equipo**: indica si el equipo hace las funciones de descubridor, cache o proxy.

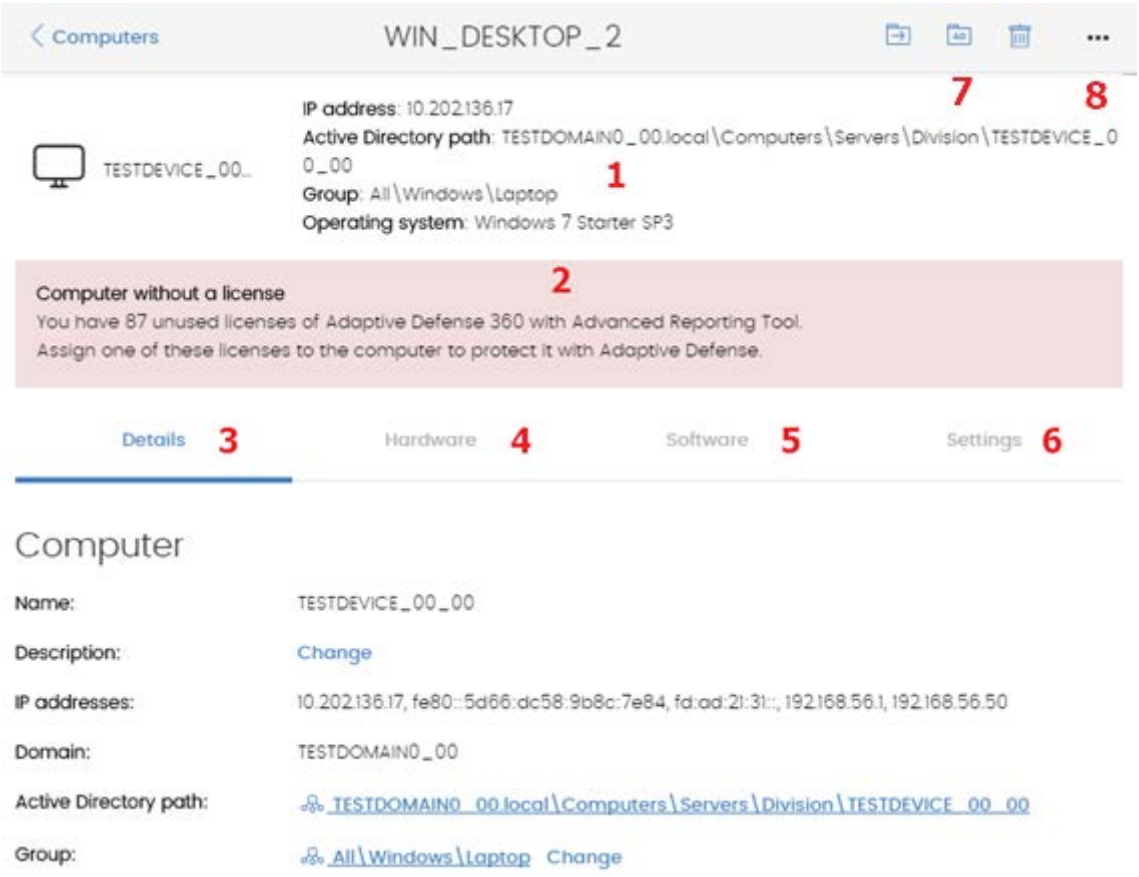


Figura 45: vista general de la información de equipo

7.7.2 Sección alertas de equipo (2)

Las alertas describen los problemas encontrados en los equipos de la red en lo que respecta al funcionamiento de **Panda Adaptive Defense 360** y su motivo, así como indicaciones para solucionarlos. A continuación, se muestra un resumen de los tipos de alertas generadas y las acciones recomendadas para su resolución.

Equipo desprotegido:

- **Protecciones desactivadas**: se mostrará un mensaje indicando que la protección antivirus, la protección Panda Adaptive Defense (avanzada) o la protección Exchange están desactivadas. Se recomienda asignar una configuración de protección al equipo con las protecciones activadas. Consulta el capítulo 8 para asignar una configuración de seguridad y el capítulo 10 para crear configuraciones de seguridad.
- **Protección con error**: se mostrará un mensaje indicando que la protección antivirus, la protección Panda Adaptive Defense (avanzada) o la protección Exchange están en estado erróneo. Reinicia el equipo o reinstala el software. Consulta el capítulo 6 para instalar el software en el equipo y el capítulo 19 para reiniciar el equipo.
- **Error instalando el gestor de parches**: se ha producido un error instalando el gestor de parches en el equipo (**Panda Patch Management**).
  - **Imposible realizar la descarga**: instalador no disponible.
  - **Imposible realizar la descarga**: fichero corrupto.
  - **Espacio insuficiente en disco**.
- **Fallo en la instalación**: el equipo está desprotegido porque la instalación terminó en error. Consulta el capítulo 6 para reinstalar el software en el equipo.
- **Instalación en proceso**: el equipo estará desprotegido hasta que no termine la instalación de **Panda Adaptive Defense 360**. Espera unos minutos hasta que la instalación se haya completado.

Equipo desactualizado:

- **Protección pendiente de reinicio**: la actualización del motor de seguridad se ha descargado, pero es necesario un reinicio para que se aplique en el equipo. Consulta el capítulo 19 para reiniciar el equipo de forma remota.
- **Actualizaciones de la protección desactivadas**: el software no recibirá ninguna mejora y la seguridad puede verse comprometida en un futuro. Consulta el capítulo 8 para crear y asignar una configuración de tipo Ajustes por equipo que permita la actualización del software.
- **Actualizaciones de conocimiento desactivadas:** el software no recibirá ninguna actualización del fichero de firmas y su seguridad puede verse comprometida en el corto plazo. Consulta el capítulo 10 y 11 para crear configuraciones de seguridad que permitan la actualización del fichero de firmas.
- **Error en la actualización del conocimiento**: la descarga del fichero de firmas falló. Consulta este mismo capítulo para comprobar el espacio libre en el disco duro del equipo. Consulta el capítulo 19 para reiniciar el equipo. Consulta el capítulo 6 para reinstalar el software en el equipo.

Archivos bloqueados

El equipo contiene ficheros desconocidos que están en proceso de clasificación y su ejecución está bloqueada. Consulta el panel Programas actualmente bloqueados en el dashboard para comprobar el fichero y añadir una exclusión en caso de ser necesario. Consulta el capítulo 17 para gestionar los elementos en clasificación.

Sin conexión desde…

El equipo no se ha conectado a la nube de Panda Security en varios días. Comprueba la conectividad del equipo y la configuración del cortafuegos de la red. Consulta el capítulo 10 Configuración de seguridad para estaciones y servidores para comprobar si se cumplen los requisitos de conectividad. Consulta el capítulo 6 para reinstalar el software en el equipo.

Pendiente de reinicio

- El administrador ha solicitado un reinicio que todavía no se ha producido.
- Se han instalado parches en el equipo que requieren un reinicio.

7.7.3 Sección Detalles (3)

La información mostrada en esta pestaña se divide en dos apartados: **Equipo** con la información de la configuración del dispositivo ofrecida por el agente Panda, y **Seguridad**, con el estado de las protecciones de **Panda Adaptive Defense 360.**

- **Equipo**
  - **Nombre:** nombre del equipo**.**
  - **Descripción**: texto descriptivo asignado por el administrador.
  - **Direcciones físicas (MAC)**: dirección física de las tarjetas de red instaladas.
  - **Direcciones IP**: listado con todas las direcciones IP (principal y alias).
  - **Dominio**: dominio Windows al que pertenece el equipo. Vacío si no pertenece a un dominio.
  - **Ruta de directorio activo**: ruta dentro del árbol de directorio activo de la empresa donde se encuentra el equipo.
  - **Grupo**: grupo dentro del Árbol de grupos al que pertenece el equipo. Para cambiar el grupo del equipo haz clic en el botón **Cambiar**.
  - **Sistema operativo**
  - **Servidor de correo**: versión del servidor Microsoft Exchange instalada en el equipo.
  - **Máquina virtual**: indica si el equipo es físico o esta virtualizado.
  - **Licencias**: licencias de productos de Panda Security instalados en el equipo. Para obtener más información consulta el capítulo 5.
  - **Versión del agente**
  - **Fecha de arranque del sistema**
  - **Fecha de instalación**
  - **Ultima conexión** del agente con la infraestructura de Panda Security. Como mínimo el

agente de comunicaciones contactará cada 4 horas.

- **Seguridad:** en esta sección se indican el estado (Activado, Desactivado, Error) de las distintas tecnologías de **Panda Adaptive Defense 360.**
  - **Protección avanzada**
  - **Antivirus de archivos**
  - **Antivirus de correo**
  - **Antivirus para navegación web**
  - **Firewall**
  - **Control de dispositivos**
  - **Control de acceso a páginas web**
  - **Gestión de parches**
  - **Versión de la protección**
  - **Versión de actualización del conocimiento:** fecha de la última descarga del fichero de firmas en el equipo.
- **Data Control**: en esta sección se indica el estado y la versión del servicio **Panda Data Control** instalada.
  - **Seguimiento de información personal**.
  - **Permitir búsquedas de información en este equipo:** indica si el equipo tiene asignado un perfil de configuración que le permita recibir búsquedas de ficheros y reportar sus resultados.
- **Estado de indexación:** si se permiten búsquedas de ficheros por contenido, es necesario que **Panda Data Control** examine todos los ficheros de los medios de almacenamiento soportados para recuperar su contenido y generar una base de datos.
- **Versión**: versión interna del motor de indexado.

Para obtener información sobre los datos relativos a la seguridad de los equipos protegidos consulta el capítulo 16 Visibilidad del malware y del parque informático.

7.7.4 Sección Hardware (4)

Contiene la siguiente información:

- **CPU**: información del microprocesador instalado en el equipo y una gráfica de líneas con el consumo de CPU en diferentes periodos e intervalos según la selección:
  - Intervalos de 5 minutos para la última hora.
  - Intervalos de 10 minutos para las 3 últimas horas.
  - Intervalos de 40 minutos para las últimas 24 horas.
- **Memoria**: información sobre las características de los chips de memoria instalados y una gráfica de líneas con el consumo de memoria en diferentes periodos e intervalos según la selección:
  - Intervalos de 5 minutos para la última hora.
  - Intervalos de 10 minutos para las 3 últimas horas.

- Intervalos de 40 minutos para las últimas 24 horas.

- **Disco**: información sobre las características del sistema de almacenamiento masivo y un gráfico de tarta con el porcentaje de espacio libre y ocupado en el momento de la consulta.

7.7.5 Sección Software (5)

Contiene un listado del software instalados en el equipo y de las actualizaciones del sistema operativo Windows y otros programas de Microsoft. El listado contiene la siguiente información:

- **Nombre:** nombre del programa.
- **Editor:** empresa que desarrolló el programa.
- **Fecha de instalación**
- **Tamaño**
- **Versión**

Herramienta de búsqueda

La herramienta que permite localizar paquetes de software instalado mediante coincidencias parciales o completas en todos los campos mostrados anteriormente.

Mediante el control desplegable es posible limitar la búsqueda para localizar únicamente las actualizaciones, el software instalado o ambos conceptos.

Registro de cambios

El registro de cambios es un listado que muestra todos los eventos de instalación y desinstalación de software sucedidos en el intervalo de fechas configurado. Por cada evento se muestra la siguiente información:

- **Evento**: Instalación  o desinstalación  .
- **Nombre**: nombre del paquete de software que provoco el evento.
- **Editor:** empresa que desarrolló el programa.
- **Versión**
- **Fecha**

7.7.6 Sección Configuración (6)

La sección **Configuración** muestra toda la información relevante de la asignación de configuraciones al equipo, y permite su gestión y modificación:

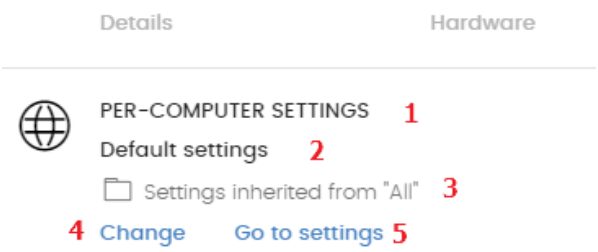


Figura 46: gestión y modificación de configuraciones asignadas

- **(1)** Nombre de la categoría de la configuración: Ajustes por equipo, Proxy e idioma, Configuración para estaciones y servidores, Configuración para dispositivos Android.
- **(2)** Nombre de la configuración asignada.
- **(3)** Método de asignación de la configuración: directamente al equipo o heredada de un grupo superior.
- **(4)** Botón para cambiar la asignación de la configuración.
- **(5)** Botón para editar el contenido de la configuración.

> *La creación, edición y asignación de configuraciones se tratan en el capítulo 8 Gestión de configuraciones.*

7.7.7 Barra de acciones (7)

Agrupa múltiples operaciones sobre el equipo:

- **Mover a**: mueve el equipo a un grupo estándar.
- **Mover a su ruta de Active Directory**: mueve el equipo a su grupo Directorio Activo original.
- **Eliminar**: libera la licencia de **Panda Adaptive Defense 360** y elimina el equipo de la consola Web.
- **Analizar ahora**: programa una tarea de análisis de ejecución inmediata. Consulta el capítulo 19 Herramientas de resolución para más información.
- **Programar análisis**. programa una tarea de análisis. Consulta el capítulo 15 Tareas para más información.
- **Aislar equipo**: impide las comunicaciones con el exterior para facilitar las tareas de análisis forense remoto al administrador, en el caso de que el equipo haya sido comprometido. Consulta el capítulo 19 para obtener más información.
- **Dejar de aislar equipo**: restaura las comunicaciones con el exterior. Consulta el capítulo 19 Herramientas de resolución para más información sobre aislar equipos y sus implicaciones.
- **Programar instalación de parches:** crea una tarea que instalará los parches publicados y no aplicados en el equipo. Consulta el capítulo 13 Panda Patch Management (Actualización de programas vulnerables)para más información.
- **Reiniciar**: reinicia el equipo de forma inmediata. Consulta el capítulo 19 Herramientas de resolución para obtener más información.
- **Notificar un problema**: abre un ticket de mantenimiento con el departamento técnico de

Panda Security. Consulta el capítulo 19 Herramientas de resolución para obtener más información.

7.7.8 Iconos ocultos (8)

Dependiendo del tamaño de la ventana y del número de iconos a mostrar, parte de ellos pueden quedar ocultos bajo el icono  . Haz clic para desplegar el menú con los iconos restantes.

8. Gestión de configuraciones

8.1. Introducción

En este capítulo se tratan los recursos implementados en **Panda Adaptive Defense 360** para la gestión de configuraciones de los equipos de la red.

8.2. ¿Qué es una configuración?

Las configuraciones, también llamados "perfiles de configuración" o simplemente "perfiles", ofrecen a los administradores un modo rápido de establecer los parámetros de seguridad, productividad y conectividad gestionados por **Panda Adaptive Defense 360** en los equipos que administran.

El administrador de la red creará tantos perfiles como variaciones de configuraciones sean necesarias. Una nueva configuración viene dada por la existencia de equipos heterogéneos en la red de la empresa:

- Equipos de usuario manejados por personas con distintos niveles de conocimientos en informática requerirán configuraciones más o menos estrictas frente a la ejecución de software, acceso a internet o a periféricos.
- Usuarios con diferentes tareas a desempeñar y por lo tanto diferentes usos y necesidades, requerirán configuraciones que permitan el acceso a diferentes recursos.
- Usuarios que manejen información confidencial o delicada para la empresa requerirán un nivel de protección superior frente a amenazas e intentos de sustracción de la propiedad intelectual de la compañía.
- Equipos en distintas delegaciones requerirán configuraciones distintas que les permitan conectarse a internet utilizando diferentes infraestructuras de comunicaciones.
- Servidores críticos para el funcionamiento de la empresa requerirán configuraciones de seguridad específicas.

8.3. Visión general de la asignación de configuraciones a equipos

De forma general, la asignación de configuraciones a los equipos de la red es un proceso de cuatro pasos:

1 **Creación de los grupos que reúnan equipos del mismo tipo o con idénticos requisitos de conectividad y seguridad**

2 **Asignación de los equipos a su grupo correspondiente**

3 **Asignación de configuraciones a los grupos**

4 **Difusión inmediata y automática de la configuración a los equipos de la red**

Todas estas operaciones se realizan desde el árbol de grupos, accesible desde el menú superior **Equipos.** El árbol de grupos es la herramienta principal para asignar configuraciones de forma rápida y sobre conjuntos amplios de equipos.

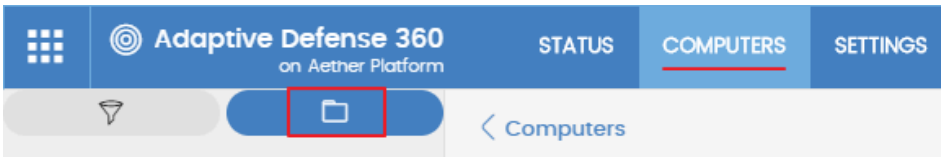


Figura 47: acceso al árbol de grupos

Por lo tanto, la estrategia principal del administrador consiste en reunir todos los equipos similares en un mismo grupo y crear tantos grupos como conjuntos diferentes de equipos existan en la red que gestiona.

> *Para obtener más información sobre el manejo del árbol de grupos y asignación de equipos a grupos consulta el capítulo 7.*

8.3.1 Difusión inmediata de la configuración

Una vez que una configuración es asignada a un grupo, esa configuración se aplicará a los equipos del grupo de forma inmediata y automática, siguiendo las reglas de la herencia mostradas más adelante en este capítulo. La configuración así establecida se aplica a los equipos sin retardos, en cuestión de unos pocos segundos.

> *Para desactivar la difusión inmediata de la configuración consulta el capítulo 9*

8.3.2 Árbol multinivel

En empresas de tamaño mediano y grande, la variedad de configuraciones puede ser muy alta. Para facilitar la gestión de parques informáticos grandes, **Panda Adaptive Defense 360** permite generar árboles de grupos de varios niveles de forma que el administrador pueda gestionar con facilidad los equipos de la red.

8.3.3 Herencia

En redes de tamaño amplio es muy probable que el administrador quiera reutilizar configuraciones ya establecidas en grupos de orden superior dentro del árbol de grupos. El mecanismo de herencia permite asignar una configuración sobre un grupo y, de forma automática, sobre todos los grupos que dependen de éste, ahorrando tiempo de gestión.

8.3.4 Configuraciones manuales

Para evitar la propagación de configuraciones en todos los niveles inferiores de una rama del árbol, o asignar una configuración distinta a la recibida mediante la herencia sobre un determinado equipo dentro de una rama, es posible asignar de forma manual configuraciones a equipos individuales o a grupos.

8.3.5 Configuración por defecto

Inicialmente todos los equipos en el árbol de grupos heredan la configuración establecida en el nodo raíz **Todos**.

El nodo raíz **Todos** tiene asignadas las configuraciones por defecto mostradas a continuación:

- **Configuración de ajustes por equipo**: configuración por defecto.
- **Proxy e idioma**: configuración por defecto.
- **Configuración de seguridad para estaciones y servidores**: configuración por defecto.
- **Configuración de seguridad para dispositivos Android**: configuración por defecto.
- **Gestión de parches**: configuración por defecto.
- **Información sensible**: configuración por defecto.

De esta manera, los equipos estarán protegidos desde el primer momento, incluso antes de que el administrador haya accedido a la consola para establecer una configuración de seguridad.

8.4. Perfiles de configuración modulares vs monolíticos

Panda Adaptive Defense 360 utiliza un enfoque modular a la hora de crear y distribuir las configuraciones a aplicar en los equipos administrados. Para ello utiliza cuatro tipos de perfil independientes, que cubren otras tantas áreas de configuración.

Los tipos de perfiles se muestran a continuación:

- Configuración de ajustes por equipo.
- Proxy e idioma.
- Configuración de seguridad para estaciones y servidores.
- Configuración de seguridad para dispositivos Android.
- Gestión de parches.
- Seguimiento de información personal.

El objetivo de utilizar este enfoque modular y no un único perfil de configuración monolítico que abarque toda la configuración, es el de reducir el número de perfiles creados en la consola de gestión. El enfoque modular permite generar configuraciones lo más pequeñas y ligeras posible, frente a perfiles monolíticos que fomentan la aparición de muchos perfiles de configuración muy largos y redundantes, con muy pocas diferencias entre sí. De esta manera, se minimiza el tiempo que el administrador tendrá que dedicar a gestionar todos los perfiles creados.

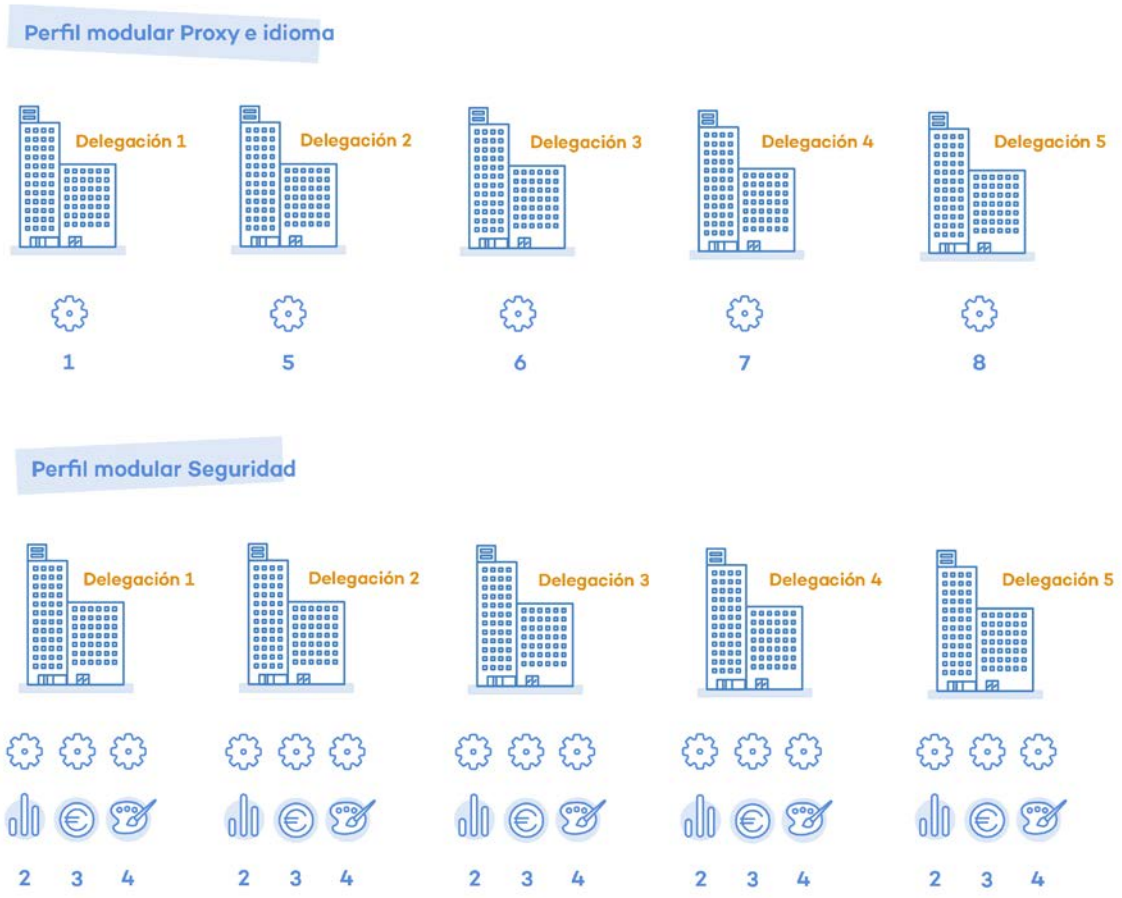
Con perfiles modulares es posible combinar varias configuraciones para construir una única configuración que se ajuste a las necesidades del usuario, con un número de perfiles distintos mínimo.

Caso práctico: Creación de configuraciones para varias delegaciones

En este caso práctico tenemos una empresa con 5 delegaciones, cada una de ellas tiene una infraestructura de comunicaciones distinta y por tanto una configuración de proxy diferente. Además, dentro de cada delegación se requieren 3 configuraciones de seguridad diferentes, una para el departamento de diseño, otro para el departamento de contabilidad y otra para el departamento de marketing.

Si **Panda Adaptive Defense 360** implementara todos los parámetros de configuración en un único perfil monolítico, serían necesarios 15 perfiles de configuración distintos (5 x 3 =15) para dar servicio a todos los departamentos de todas las delegaciones de la empresa.

Como **Panda Adaptive Defense 360** separa la configuración de proxy de la de seguridad, el número de perfiles a crear se reduce (5 perfiles de proxy + 3 perfiles de departamento = 8) ya que los perfiles de seguridad por departamento de una delegación se pueden reutilizar y combinar con los perfiles de proxy en otras delegaciones.



8.5. Introducción a los cinco tipos de configuraciones

Consulta el capítulo 9, 10, y 11 para obtener más información sobre la configuración del agente Panda y sobre las protecciones para las distintas plataformas compatibles.

Proxy e idioma

Define el idioma del agente instalado en el equipo de usuario y configura su forma de conectar con internet para pasar a través de un servidor de proxy.

Ajustes por equipo

Define varios parámetros del agente Panda:

- Intervalo de actualizaciones del software **Panda Adaptive Defense 360** en los equipos. Consulta el capítulo 14 Actualización del Software para obtener más información.
- Contraseña de instalación en los equipos de usuario.
- Protección anti-tamper.

Seguridad para Estaciones y servidores

Define la configuración de seguridad de los equipos de la red Windows, macOS y Linux, tanto de los puestos de trabajo como servidores.

Seguridad para Dispositivos Android

Define la configuración de seguridad de dispositivos Android (tablets y smartphones).

Gestión de parches

Define la configuración de descubrimiento de parches que los proveedores del software instalado en la red de la empresa publican de sus aplicaciones.

Información Sensible

Define el comportamiento del servicio **Panda Data Control** con respecto a la detección y seguimiento de información personal (PII) en ficheros de datos no estructurados.

8.6. Creación y gestión de configuraciones

Haz clic en el menú superior **Configuración** para crear, copiar y borrar configuraciones. En el panel de la izquierda se encuentran las cinco entradas correspondientes a los tipos de perfil de configuración posibles **(1)**, **(2)**, **(3), (4), (5) y (6)**. En el panel de la derecha se muestran los perfiles de configuración ya creados **(9)** del tipo seleccionado y los botones para **Añadir (7)**, copiar **(8)** y eliminar perfiles **(10).**

Creación de configuraciones

Al hacer clic sobre el botón **Añadir** se muestra la ventana de creación de configuraciones. Todos los perfiles tienen un nombre principal y una descripción que son mostradas en los listados de configuraciones.

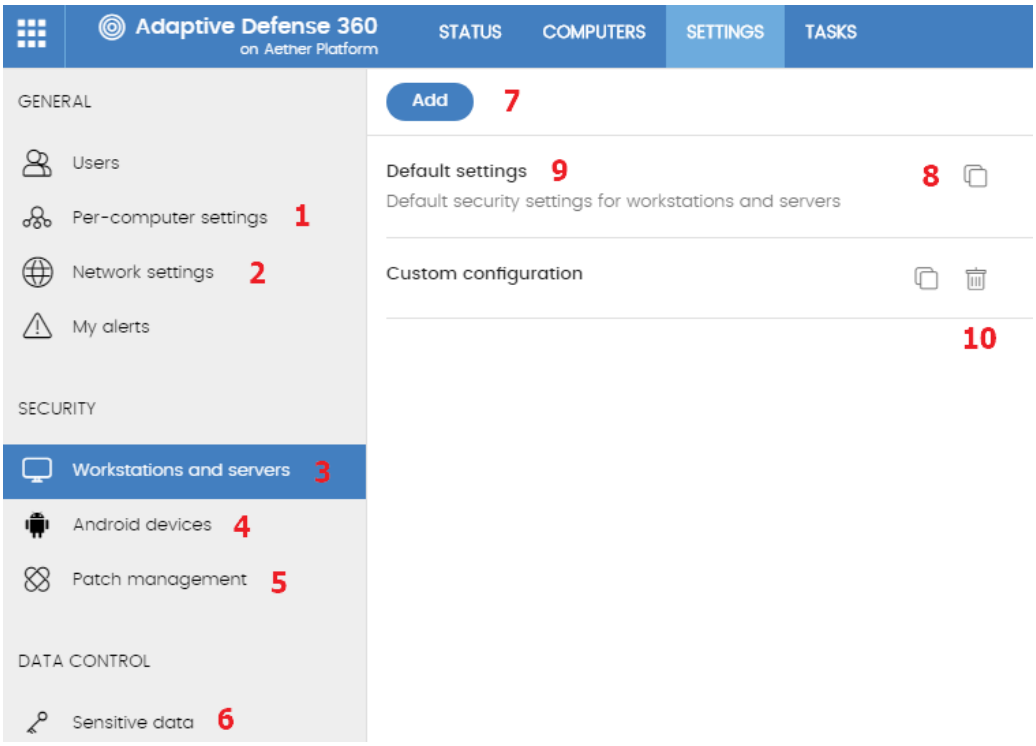


Figura 48: pantalla para crear y gestionar configuraciones

Copia y borrado de configuraciones

Mediante los iconos **(8)** y **(10)** es posible copiar y borrar un perfil de configuración, pero si ha sido asignado a uno o más equipos se impedirá su borrado hasta que sea liberado.

Haciendo clic en el perfil de configuración se permite su edición.

> *Antes de modificar un perfil comprueba que la nueva configuración sea correcta ya que, si el perfil ya está asignado a equipos de la red, esta nueva configuración se propagará y aplicará de forma automática y sin retardos.*

8.7. Asignación manual y automática de configuraciones a grupos de equipos

Una vez creados los perfiles de configuración, éstos pueden ser asignados a los equipos de la red siguiendo dos estrategias diferentes:

- Mediante asignación manual (asignación directa).
- Mediante asignación automática a través de la herencia (asignación indirecta).

Ambas estrategias son complementarias y es muy recomendable que el administrador comprenda las ventajas y limitaciones de cada mecanismo para poder definir una estructura de equipos lo más simple y flexible posible, con el objetivo de minimizar las tareas de mantenimiento diarias.

8.7.1 Asignación directa / manual de configuraciones

La asignación manual consiste en la asignación de forma directa de perfiles de configuración a equipos o grupos. De esta manera es el administrador el que, de forma manual, asigna una configuración a un grupo o equipo.

Una vez creados los perfiles de configuración, estos son asignados de tres maneras posibles:

- Desde el menú superior **Equipos**, en el árbol de grupos mostrado en el panel de la izquierda.
- Desde el detalle del equipo en el panel de listado de equipos, accesible desde el menú superior **Equipos.**
- Desde el propio perfil de configuración creado o editado.

Para obtener más información sobre el árbol de grupos consulta el capítulo 7.

Desde el árbol de grupos

Para asignar un perfil de configuración a un conjunto de equipos que pertenecen a un grupo, haz clic menú superior **Equipos,** selecciona el árbol de grupos en el panel izquierdo y sigue los pasos mostrados a continuación:

- Haz clic en el menú contextual en la rama apropiada del árbol de grupos.
- Haz clic en el menú emergente **Configuraciones**, se mostrará una ventana con los perfiles ya asignados al grupo seleccionado y el tipo de asignación:
  - **Manual / Asignación directa**: mediante la leyenda **Asignada directamente a este grupo.**
  - **Heredada / Asignación indirecta**: mediante la leyenda **Configuración heredada de** y el nombre del grupo junto con la ruta completa para llegar al mismo, y que recibió la configuración manual de la cual se hereda.
- Elige la nueva configuración y haz clic en **Aceptar** para asignar la configuración al grupo.
- La configuración se propagará de forma inmediata a todos los miembros del grupo y sus descendientes.
- Los cambios se aplicarán en los equipos afectados de forma inmediata.

Desde el panel listado de equipos

Para asignar un perfil de configuración a un equipo en concreto sigue los pasos mostrados a continuación:

- En el menú superior **Equipos** haz clic en el grupo o filtro donde reside el equipo a asignar la configuración. Haz clic sobre el equipo en la lista de equipos mostrada en el panel derecho para ver la pantalla detalles de equipo.
- Haz clic en la pestaña **Configuración**. Se mostrarán los perfiles asignados al equipo y el tipo de asignación:
  - **Manual / Asignación directa**: mediante la leyenda **Asignada directamente a este grupo.**
  - **Heredada / Asignación indirecta**: mediante la leyenda **Configuración heredada de** y el nombre del grupo junto con la ruta completa para llegar al mismo, y que recibió la configuración manual de la cual se hereda.

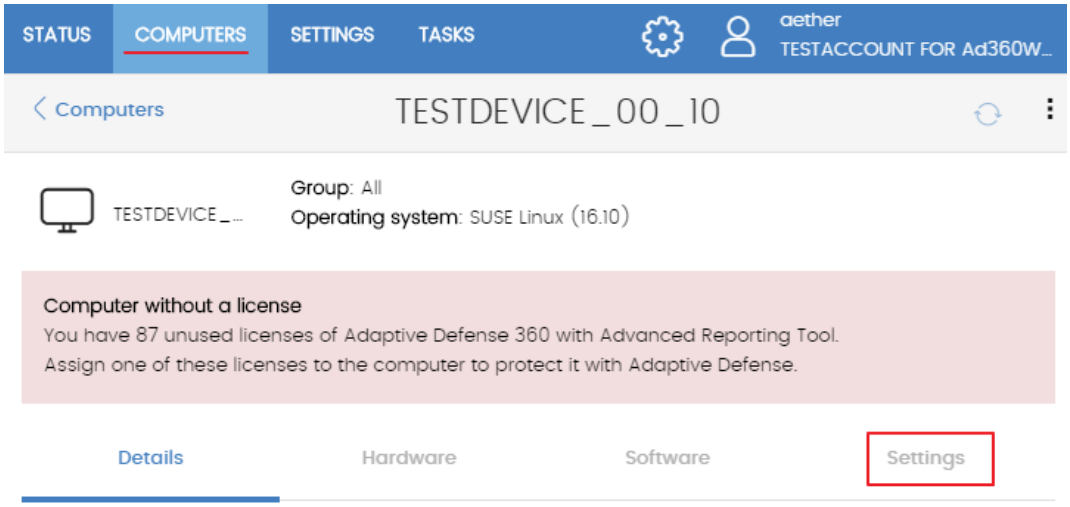


Figura 49: acceso a las configuraciones desde la ficha de equipo

- Selecciona la nueva configuración. Ésta se aplicará de forma automática al equipo.

Desde el propio perfil de configuración

La forma más rápida de asignar una configuración a varios equipos que pertenecen a grupos distintos es a través del propio perfil de configuración.

Para asignar equipos o grupos de equipos a un perfil de configuración sigue los pasos siguientes:

- En el menú superior **Configuración**, panel lateral, haz clic en el tipo de perfil que quieres asignar.
- Selecciona la configuración de entre las disponibles y haz clic en el botón **Destinatarios**. Se mostrará una ventana dividida en dos secciones: **Grupos de equipos** y **Equipos adicionales**.
- Haz clic en el botón ⊕ para añadir equipos o grupos al perfil de configuración.
- Haz clic en el botón **Añadir**. El perfil quedará asignado a los equipos seleccionados y la nueva configuración se aplicará de forma inmediata.

Al retirar un equipo de la lista de equipos asignados a una configuración, el equipo volverá a heredar las configuraciones asignadas al grupo al que pertenece. La consola de administración resaltará este hecho mostrando una ventana de advertencia antes de aplicar los cambios.

8.7.2 Asignación indirecta de configuraciones: las dos reglas de la herencia

La asignación indirecta de configuraciones se realiza a través del mecanismo de la herencia, que permite propagar de forma automática un mismo perfil de configuración a todos los equipos subordinados del nodo sobre el cual se asignó la configuración.

Las reglas que rigen la interacción entre los dos tipos de asignaciones (manuales / directas y automática / herencia) se muestran a continuación por orden de prioridad:

1 **Regla de la herencia automática: un grupo o equipo hereda de forma automática las configuraciones del grupo del cual depende (grupo padre o de orden superior).**

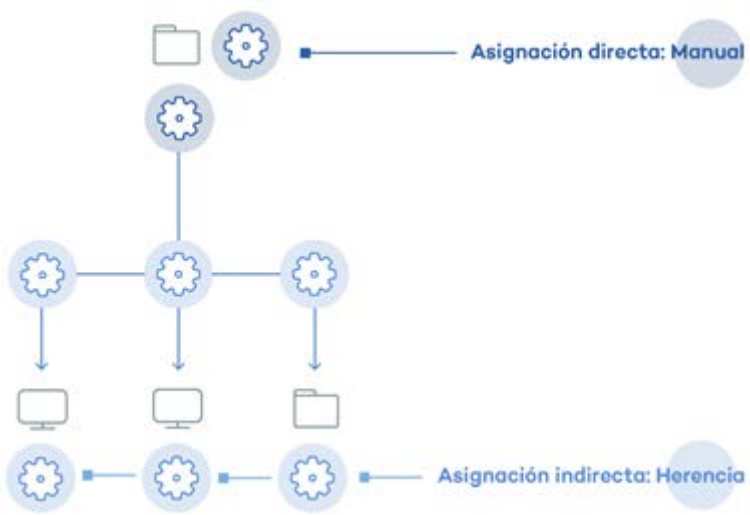


Figura 50: ejemplo de herencia / asignación indirecta. El grupo padre recibe una configuración que se propaga a sus nodos hijos

2 **Regla de la prioridad manual: Una configuración manual prevalece sobre una configuración heredada.**

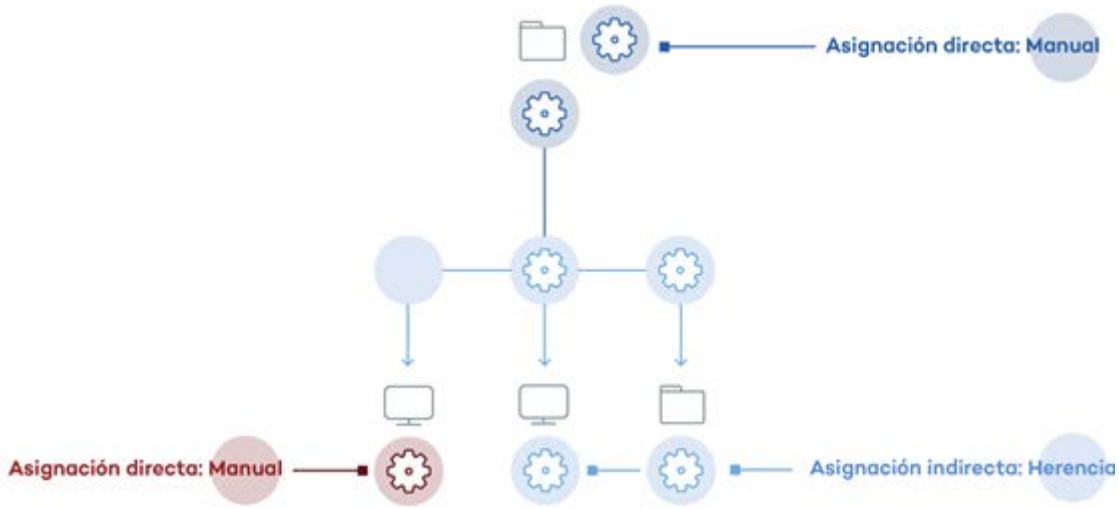


Figura 51: ejemplo de prioridad de la asignación directa sobre indirecta. La configuración heredada se sobrescribe con la configuración manual del nodo.

8.7.3 Límites de la herencia

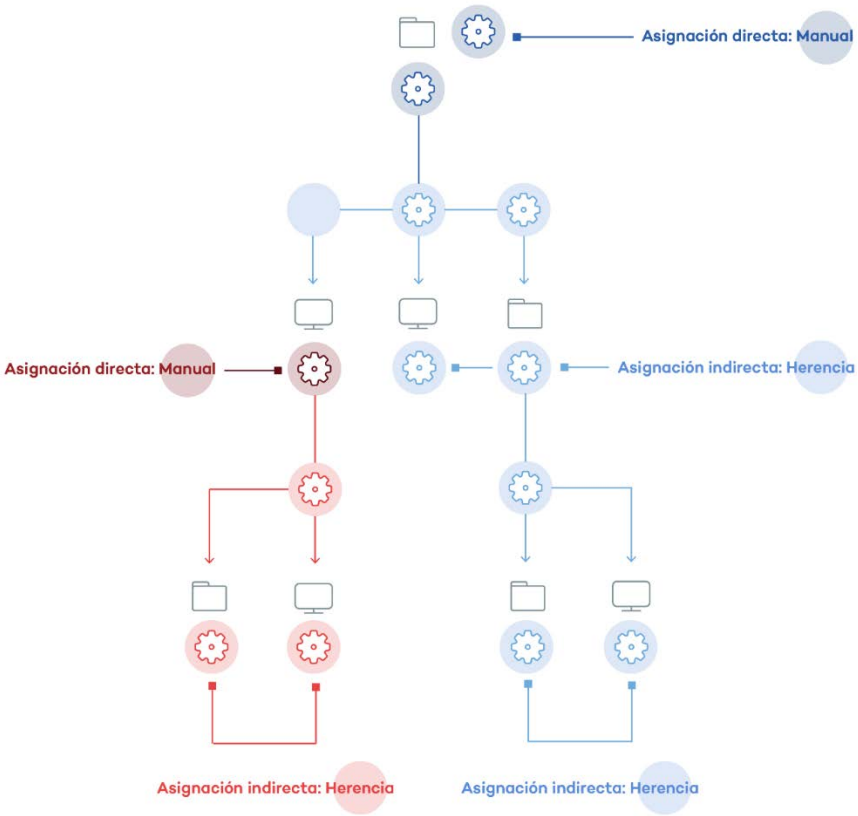


Figura 52: ejemplo de herencia limitada por asignación manual / directa. La configuración del nodo padre se hereda a sus descendientes, pero se detiene ante una configuración manual

La configuración asignada a un grupo (manual o heredada) se heredará a todos los elementos de la rama del árbol sin límite, hasta que se encuentre una asignación manual.

8.7.4 Sobre escritura de configuraciones

Como se ha visto en el punto anterior, la regla 2 (prioridad manual) dicta que las configuraciones manuales prevalecen sobre las configuraciones heredadas. Esto es así en un escenario típico donde primero se establecen las configuraciones heredadas sobre todos los elementos del árbol, y luego se asignan de forma manual aquellas configuraciones especiales sobre ciertos elementos.

Sin embargo, es frecuente que una vez establecidas las configuraciones heredadas y manuales, haya un cambio de configuración heredada en un nodo de orden superior que afecta a la configuración manual de un descendiente.

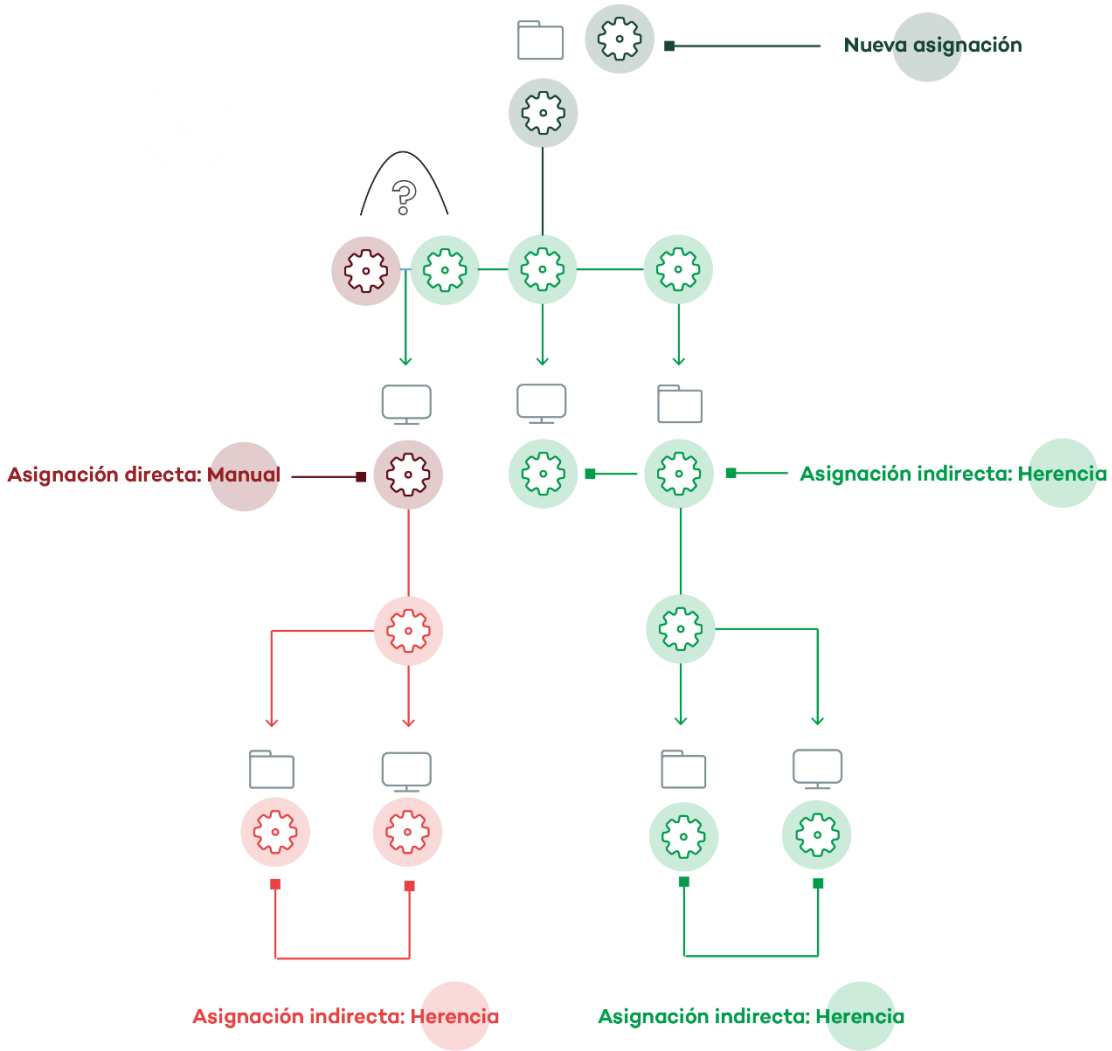


Figura 53: cambio de configuración heredada de nivel superior existiendo previamente una configuración manual en un nodo inferior

En este caso, **Panda Adaptive Defense 360** pregunta al administrador si las configuraciones manuales establecidas previamente se mantendrán o se sobrescribirán mediante la herencia:

- Si las configuraciones heredadas tienen prioridad, la nueva configuración se heredará a todos los elementos subordinados, independientemente de si tienen configuraciones manuales establecidas o no, borrando por lo tanto las configuraciones manuales si las hubiera.
- Si las configuraciones manuales tienen prioridad, la nueva configuración solo se heredará en aquellos grupos donde no se haya establecida ninguna configuración manual previa, conservando las configuraciones manuales existentes.

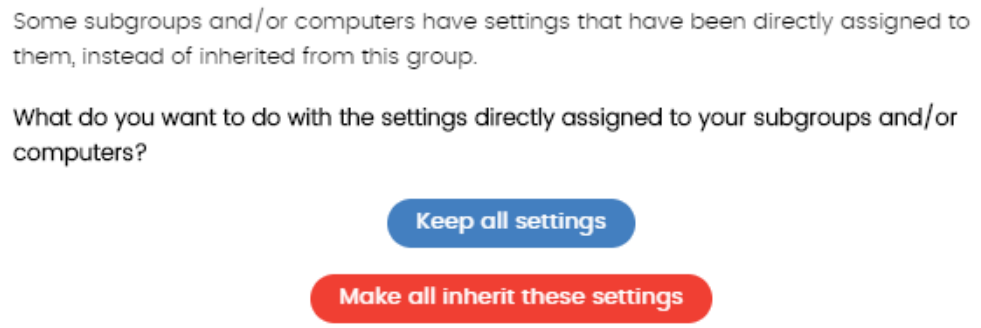


Figura 54: ventana de selección del comportamiento en cambios de configuración que se propagarán sobre una rama con grupos configurados manualmente

De esta manera, cuando el sistema detecte un cambio de configuración que tenga que propagar a los nodos subordinados, y alguno de estos tenga una configuración manual (sin importar el nivel en el que se encuentre) se presentará la pantalla de selección, preguntando al administrador sobre el comportamiento a seguir: **Hacer que todos hereden esta configuración** o **Mantener todas las configuraciones.**

Hacer que todos hereden esta configuración

> ***¡Utiliza esta opción con mucho cuidado, esta acción no tiene vuelta atrás! Todas las configuraciones manuales que cuelguen del nodo se perderán y se aplicará la configuración heredada de forma inmediata en los equipos. El comportamiento de Panda Adaptive Defense 360 podrá cambiar en muchos equipos de la red.***

La nueva asignación directa **(1)** se propagará mediante la herencia a todo el árbol por completo, sobrescribiendo la asignación directa anterior **(2)** y llegando hasta los nodos hijos de ultimo nivel **(3)** y **(4).**

Mantener todas las configuraciones

La nueva configuración solo se propagará a aquellos nodos subordinados que no tengan configuraciones manuales establecidas.

Si eliges la opción de mantener las configuraciones establecidas de forma manual, la propagación de la nueva configuración heredada se detiene en el primer nodo configurado manualmente. Aunque los nodos subordinados a un nodo configurado de forma manual heredan su configuración, la propagación de la nueva configuración se detiene en el primer nodo del árbol que tiene la configuración manual. En la figura, la propagación de la configuración establecida en **(1)** se detiene en el nodo **(2)**, de modo que los nodos **(3)** y **(4)** no reciben esa nueva configuración, aun utilizando el mecanismo de la herencia para recoger su configuración.

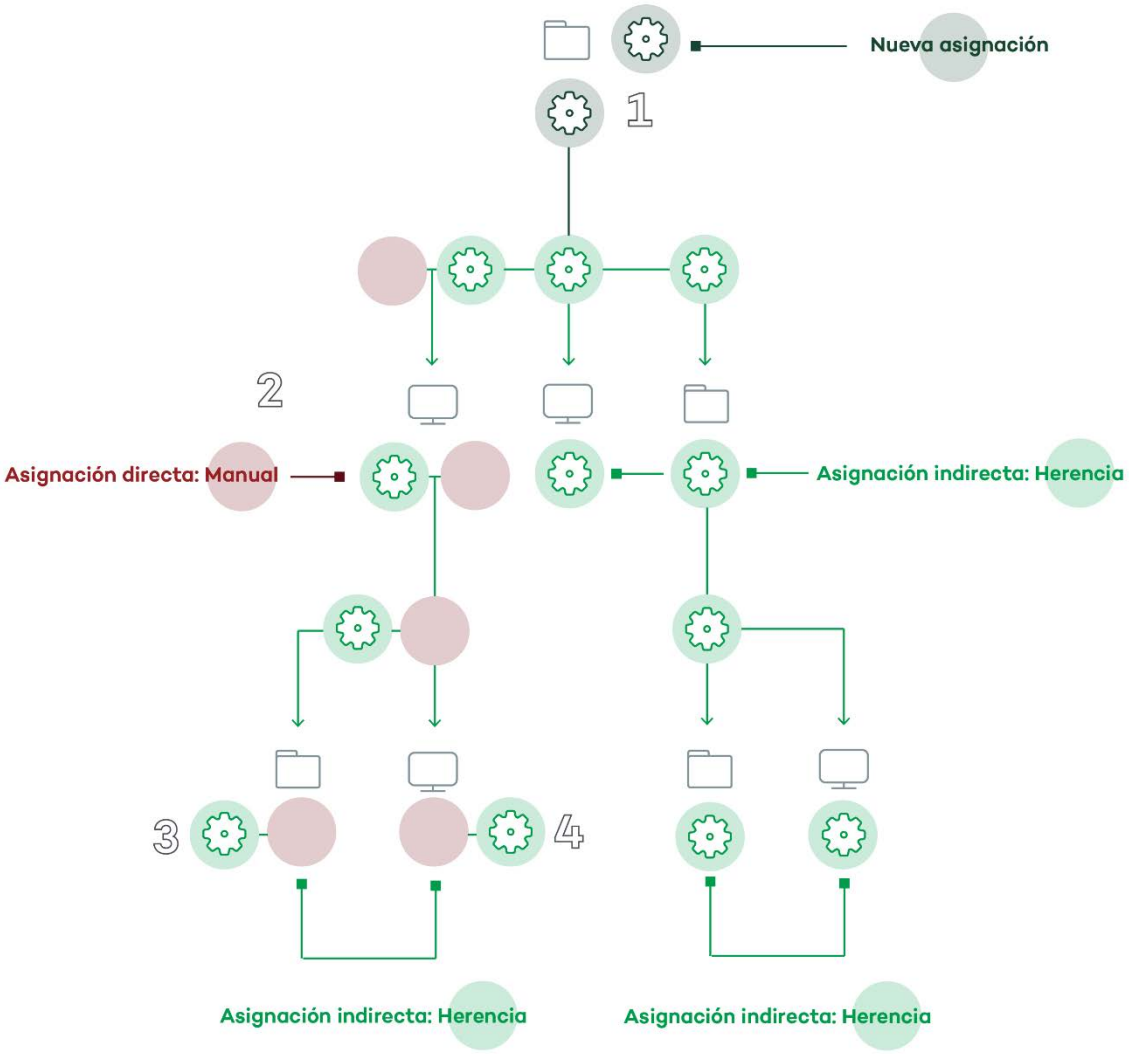


Figura 55: las configuraciones manuales se invalidan y se hereda la configuración establecida en el nodo padre

8.7.5 Eliminación de asignaciones manuales y restauración de la herencia

Para eliminar una asignación manual realizada sobre una carpeta y volver a heredar la configuración de la rama padre, es necesario seguir los pasos mostrados a continuación:

- En el menú superior **Equipos** haz clic en el grupo que tiene la asignación manual a eliminar, en el árbol de grupos situados en el panel izquierdo.
- Haz clic en el icono de menú contextual de la rama apropiada. Se mostrará una ventana emergente con las configuraciones asignadas. Elige el perfil que esté asignado de forma manual y se quiera eliminar.
- Se desplegará un listado con todos los perfiles disponibles para realizar una nueva asignación manual, y al final de la lista se mostrará el botón **Heredar del grupo padre** junto con información de la configuración que se heredaría si se pulsara el botón, y el grupo del cual se heredará.

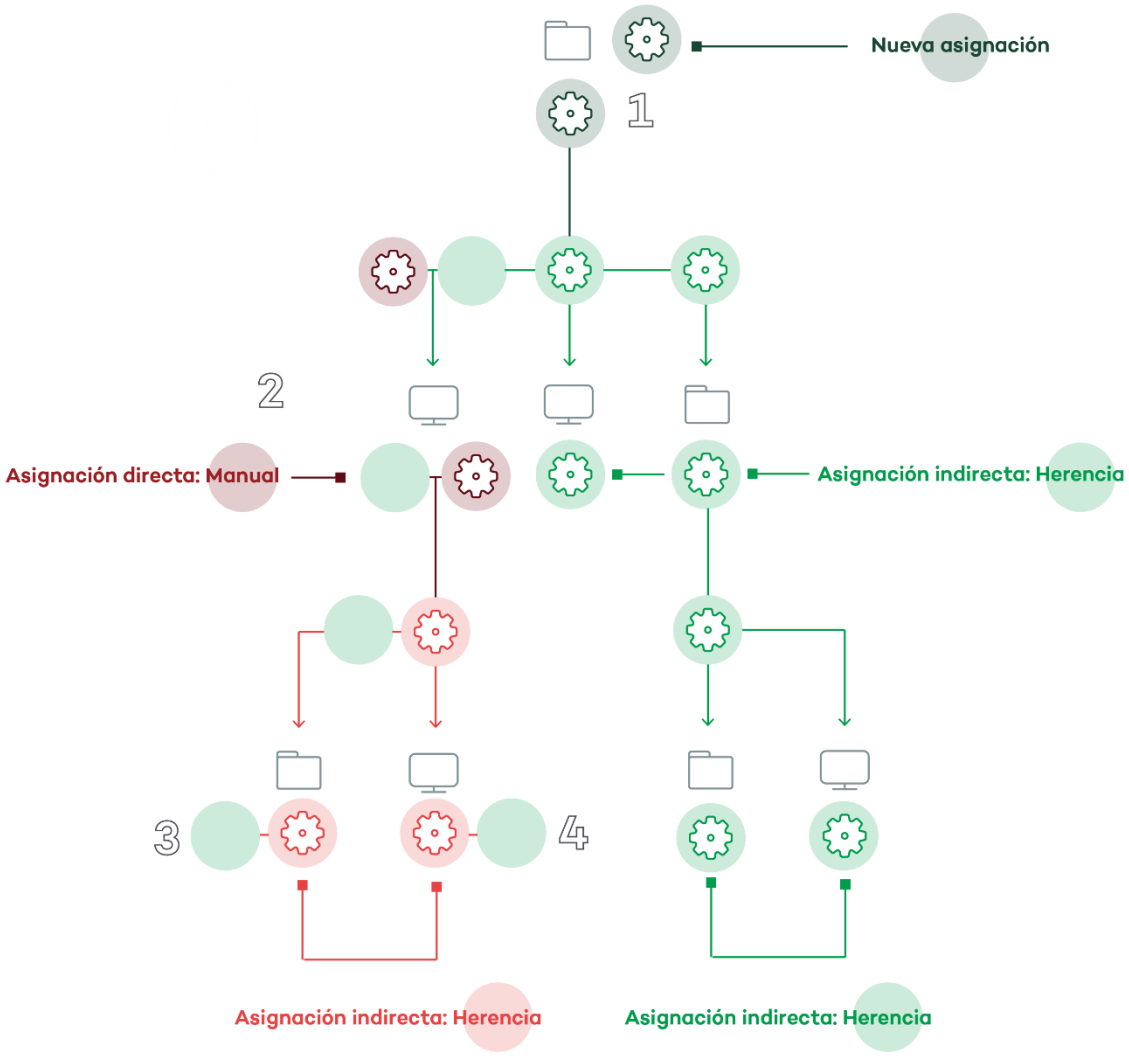


Figura 56: las configuraciones manuales se mantienen

8.7.6 Movimiento de grupos y equipos

Al mover un equipo o grupo de equipos a otra rama del árbol, el comportamiento de **Panda Adaptive Defense 360** con respecto a las configuraciones a aplicar varía en función de si los elementos movidos son grupos completos o equipos individuales.

Movimiento de equipos individuales

En el caso de movimiento de equipos individuales, **Panda Adaptive Defense 360** respeta las configuraciones manuales establecidas sobre los equipos movidos, y sobrescribe de forma automática las configuraciones heredadas con las configuraciones establecidas en el nuevo grupo padre.

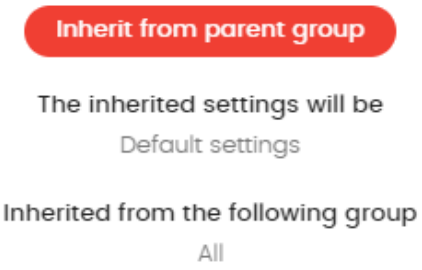


Figura 57: botón para eliminar una configuración manual y restablecer la herencia

Movimiento de grupos

En el caso de movimiento de grupos, Panda Adaptive Defense 360 mostrará una ventana con la pregunta "¿Quieres que las configuraciones asignadas a este grupo mediante herencia, sean sustituidas por las del nuevo grupo padre?".

- En el caso de contestar **SI** el procedimiento será el mismo que en el movimiento de equipos: las configuraciones manuales se respetarán y las heredadas se sobrescribirán con las configuraciones establecidas en el grupo padre.
- En el caso de contestar **NO**, las configuraciones manuales se seguirán respetando, pero las configuraciones heredadas originales del grupo movido prevalecerán, pasando de esta forma a ser configuraciones manuales.

8.8. Visualizar las configuraciones asignadas

La consola de administración implementa hasta cuatro formas de mostrar los perfiles de configuración asignados a un grupo o equipo:

- En el árbol de grupos
- En la pantalla de definición de la configuración
- En la pestaña **Configuración** del equipo
- En el listado de equipos exportado

Árbol de grupos

Selecciona el menú de contexto de la rama apropiada y haz clic en el menú emergente **Configuraciones** para mostrar una ventana con las configuraciones asignadas a la carpeta.

A continuación, se indica la información mostrada por cada entrada:

- **Tipo de configuración**:
  - Configuración de proxy e idioma
  - Configuración de ajustes por equipo
  - Configuración de seguridad para estaciones y servidores
  - Configuración de seguridad para dispositivos Android
  - Configuración para seguimiento de información personal

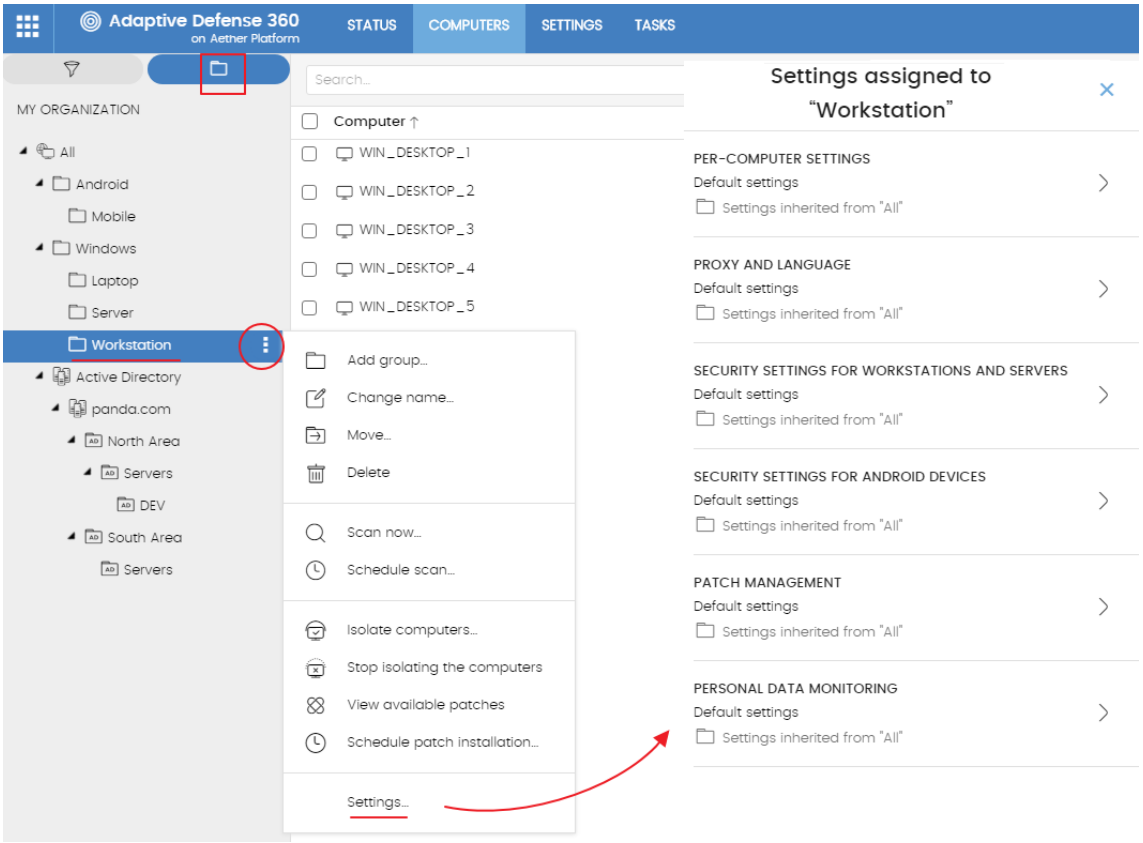


Figura 58: configuraciones asignadas desde el árbol de grupos

- **Nombre de la configuración**: nombre asignado por el administrador en la creación de la configuración.
- **Tipo de herencia aplicada**
  - **Configuración heredada de...:** la configuración fue asignada a la carpeta padre indicada, y los equipos que pertenecen a la rama actual la heredan.
  - **Asignada directamente a este grupo**: la configuración de los equipos es la que el administrador asigno de forma manual a la carpeta.

Pantalla de definición de la configuración

Para ver los equipos y grupos asignados a la configuración sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Configuraciones** y selecciona el tipo de configuración en el menú lateral.

- Selecciona una configuración en el listado de configuraciones.
- Si la configuración esta asignada a uno o más equipos o grupos, se mostrará el botón **Ver equipos**.

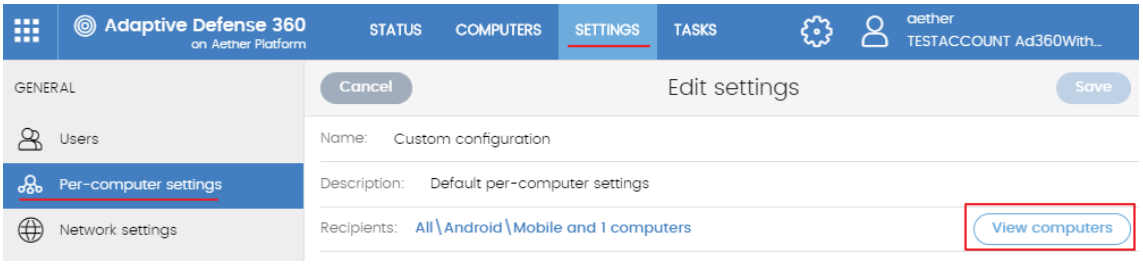


Figura 59: acceso al listado de equipos asignados a una configuración

- Haz clic en el botón **Ver equipos**. Se mostrará la zona **Equipos** con un único listado formado por todos los equipos que tienen la configuración asignada, tanto si se asignó de forma individual o mediante grupos de equipos. En la parte superior de la ventana se mostrará el criterio de filtrado establecido.

Pestaña configuración del equipo

En el menú superior **Equipos**, seleccionando un equipo del panel de la derecha se mostrará la ventana de detalle. En la pestaña **Configuración** se listan los perfiles asignados al equipo.

Exportar listado de equipos

Desde el árbol de equipos (árbol de grupos o árbol de filtros) haz clic en el menú contextual y elige la opción **Exportar**.

Consulta el capítulo 7 para obtener una descripción completa de todos los campos del fichero csv exportado.

9. Configuración del agente y de la protección local

Roles del agente
Acceso vía proxy
Comunicación en tiempo real
Idiomas
Contraseña y anti-tampering

9.1. Introducción

El administrador puede cambiar el funcionamiento de varios aspectos del agente Panda instalado en los equipos de la red:

- El papel o rol que el equipo representa para el resto de puestos y servidores protegidos.
- Las protecciones frente al *tampering* o manipulación indebida del software **Panda Adaptive Defense 360** por parte de amenazas avanzadas y APTs.
- Configuración del tipo de comunicación de los equipos con la nube de **Panda Security.**

9.2. Configuración de los roles del agente Panda

El agente Panda instalado en los equipos de la red puede tener tres roles diferentes:

- Proxy
- Descubridor
- Cache

Para asignar un rol a un equipo con el agente Panda ya instalado haz clic en el menú superior **Configuración** y en el panel lateral **Configuración de red**. Se mostrarán tres pestañas: **Proxy e idioma**, **Cache** y **Descubrimiento.**

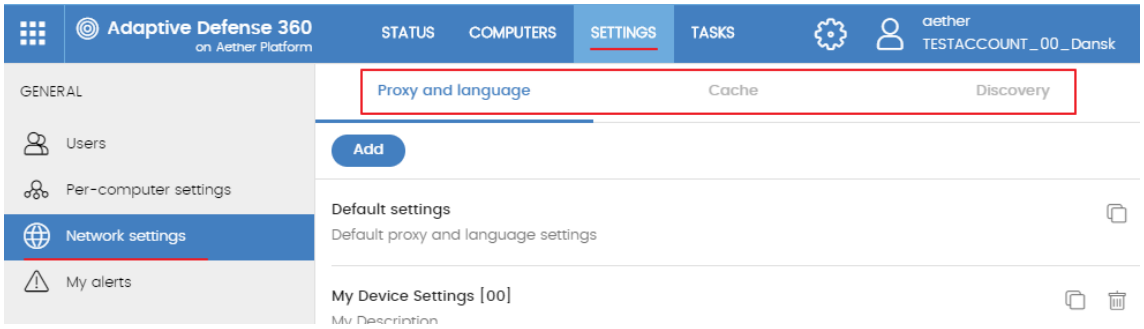


Figura 60: pantalla de selección de configuración de rol

9.2.1 Rol de Proxy

Para los equipos que no tienen acceso directo a internet, **Panda Adaptive Defense 360** permite la utilización del proxy instalado en la red. En el caso de no existir ningún proxy accesible, es posible asignar el rol de proxy a un equipo con **Panda Adaptive Defense 360** instalado.

> ***No se permite la descarga de parches y actualizaciones del módulo Panda Patch Management a través de un equipo con el rol de proxy asignado. Los equipos que descarguen parches deberán de tener acceso a la nube de Panda Security directamente o a través de un proxy corporativo.***

Asignar el rol de proxy a un equipo

- Haz clic en la pestaña **Proxy e idioma** y selecciona una configuración de tipo **Proxy e idioma** ya generada o crea una nueva.
- Despliega la sección **Proxy** y selecciona **Panda Adaptive Defense 360 proxy**
- Haz clic en **Seleccionar equipo**.
- En la ventana de selección de equipo haz clic en **Añadir proxy.** Se mostrará un listado de todos los equipos administrados que no tengan el rol de proxy previamente asignado.
- Selecciona los equipos que servirán de proxy para el resto de puestos y servidores protegidos con **Panda Adaptive Defense 360**.

Retirar el rol de cache a un equipo

- Haz clic en la pestaña **Proxy e idioma** y selecciona una configuración de tipo **Proxy e idioma** ya generada o crea una nueva.
- Despliega la sección **Proxy** y selecciona **Panda Adaptive Defense 360 proxy.**
- Haz clic en **Seleccionar equipo**.
- Haz clic en el icono  del equipo que quieres retirar el rol de proxy.

9.2.2 Rol de cache / repositorio

Panda Adaptive Defense 360 permite asignar el rol de caché a uno o más puestos de la red. Estos equipos descargan y almacenan de forma automática todos los ficheros necesarios para que otros puestos con **Panda Adaptive Defense 360** instalado puedan actualizar el archivo de identificadores, el agente y el motor de protección, sin necesidad de acceder a Internet. De esta manera se produce un ahorro de ancho de banda, ya que cada equipo no descargará de forma independiente las actualizaciones, sino que se hará una única vez de forma centralizada.

Asignar el rol de cache a un equipo

- Haz clic en la pestaña superior **Cache** dentro de **Configuración**, **Configuración de red.**
- Haz clic en el botón **Añadir equipo caché**.
- Utiliza la herramienta de búsqueda situada en la parte superior de la ventana para localizar rápidamente equipos candidatos a tener el rol de cache.
- Selecciona uno o varios equipos de la lista y pulsa **Aceptar**.

A partir de ese momento el equipo seleccionado adoptará el rol de caché y comenzará la descarga de todos los archivos necesarios, manteniendo sincronizado su repositorio de forma automática. El resto de los puestos de la subred contactarán con el cache para la descarga de actualizaciones.

Retirar el rol de cache a un equipo

- Haz clic en el menú superior **Configuración**, panel lateral **Configuración de red,** pestaña **Caché**

- Haz clic en el icono  del equipo que quieres retirar el rol caché.

Requisitos y limitaciones de un equipo con rol cache

- El ámbito de un equipo con rol de cache está limitado al segmento de red al que esté conectada su interface. Si un equipo cache tiene varias tarjetas de red podrá servir de repositorio en cada uno de los segmentos a los que esté conectado.

Se recomienda asignar un equipo como rol cache en cada segmento de la red de la compañía

- El resto de equipos descubrirán de forma automática la presencia de un nodo cache y redirigirán hacia él sus peticiones de actualización.
- Se requiere la asignación de una licencia de protección al nodo cache para su funcionamiento.
- La configuración del cortafuegos debe de permitir el tráfico SSDP (uPnP) entrante y saliente en el puerto UDP 21226 y 18226 TCP.

Descubrir nodos cache

En el momento de la asignación del rol al equipo, éste lanzará un broadcast hacia los segmentos de red a los que pertenecen sus interfaces. Los puestos recibirán la publicación del servicio y, en el caso de que en un mismo segmento haya más de un nodo cache designado, los equipos se conectarán al más adecuado en función de los recursos libres que posea.

Adicionalmente, cada cierto tiempo los equipos de la red preguntarán si existe algún nodo con el rol de cache instalado.

Dimensionamiento de un nodo cache

El dimensionamiento de un equipo con el rol de cache asignado depende completamente del número de conexiones simultáneas en los picos de carga y del tipo de tráfico que gestione (descargas de ficheros de firmas, instaladores etc). Como aproximación un equipo con el rol de cache asignado puede servir en torno a 1000 equipos de forma simultánea.

9.2.3 Rol de descubridor

La pestaña **Descubrimiento** está directamente relacionada con el procedimiento de instalación y despliegue de **Panda Adaptive Defense 360** en la red del cliente. Consulta el capítulo 6 para obtener más información acerca del proceso de descubrimiento e instalación de **Panda Adaptive Defense 360.**

9.3. Configuración del acceso a través de proxy

Configurar el uso de proxy

Para configurar la salida de uno o varios equipos a través de un proxy es necesario crear una configuración de tipo **Proxy e idioma**. Sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red**, pestaña **Proxy e idioma.**
- Haz clic en el botón **Editar** o selecciona una configuración ya creada para modificarla.
- En la sección **Proxy** elige el tipo de proxy a asignar a los equipos.
  - **No usar proxy**: acceso directo a Internet.
  - **Proxy corporativo**: acceso a Internet vía proxy instalado en la red de la organización.
  - **Proxy Panda Adaptive Defense 360:** acceso a través del agente **Panda Adaptive Defense 360** instalado en un equipo de la red.

- **No usar proxy**

Los equipos sin una configuración de proxy acceden de forma directa a la nube de Panda Security para descargar las actualizaciones y enviar los reportes de estado del equipo. El software **Panda Adaptive Defense 360** utilizará la configuración del equipo para comunicarse con Internet.

- **Proxy corporativo**

- **Dirección**: dirección IP del servidor de proxy.
- **Puerto**: puerto del servidor de proxy.
- **El proxy requiere autenticación**: habilitar si el proxy requiere información de usuario y contraseña.
- **Usuario**
- **Contraseña**

- **Proxy de Panda Adaptive Defense 360**

Permite centralizar todas las comunicaciones de la red a través de un equipo con un agente Panda instalado.

Para configurar el envío de las comunicaciones del equipo a un proxy **Panda Adaptive Defense 360** haz clic en el link **Seleccionar equipo** para desplegar una ventana con el listado de equipos disponibles que tienen el rol de proxy en la red.

En las máquinas designadas como Proxy Panda Adaptive Defense 360, los puertos UDP 21226 y TCP 3128 no podrán ser utilizados por otras aplicaciones. Adicionalmente la configuración del cortafuegos del equipo deberá de permitir el tráfico entrante y saliente por ambos puertos.

Mecanismo de fallback

Cuando un agente Panda no puede conectar con la plataforma **Aether** se ejecuta la siguiente lógica de fallback para restaurar la conexión mediante otro camino disponible:

- Si la salida a internet estaba configurada a través de proxy corporativo o proxy Panda Adaptive Defense 360 y no responde, se intenta el acceso directo.
- Internet Explorer: el agente Panda intenta recuperar la configuración de proxy de Internet Explorer impersonado como el usuario logeado en el equipo.
  - Si la configuración de las credenciales para el uso del proxy está definida de forma explícita este método de acceso no se podrá utilizar.
  - Si la configuración de proxy de Internet Explorer utiliza PAC (Proxy Auto-Config) se recupera la URL del archivo de configuración, siempre que el protocolo de acceso al recurso sea HTTP o HTTPs.
- WinHTTP / WinInet: se lee la configuración del proxy por defecto.
- WPAD (Web Proxy Autodiscovery Protocol): se pregunta a la red mediante DNS o DHCP para recuperar la url de descubrimiento que apunta al archivo PAC de configuración.

9.4. Configuración de la comunicación en tiempo real

Las comunicaciones en tiempo real entre los equipos protegidos y el servidor **Panda Adaptive Defense 360** requieren el mantenimiento de una conexión abierta por cada puesto de forma permanente. En aquellos casos donde el número de conexiones abiertas afecte al rendimiento del proxy instalado en la red, o el impacto en el consumo de ancho de banda sea elevado al cambiar simultáneamente las configuraciones de un gran número de equipos, puedes desactivar las comunicaciones en tiempo real.

Para los puestos de usuario y servidores aislados de la red, las comunicaciones en tiempo real con la nube de Panda Security a través de un equipo con el rol de proxy Panda Adaptive Defense 360 asignado están deshabilitadas y se realizan por el método ordinario. Esta limitación no afecta a los equipos que utilizan un proxy corporativo para acceder a Internet.

Deshabilitar las comunicaciones en tiempo real

- Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red**, pestaña **Proxy e idioma.**
- Haz clic en el botón **Editar** o selecciona una configuración ya creada para modificarla.
- En la sección **Proxy** despliega la sección **Opciones avanzadas.**

- Desactiva la casilla **Activar la comunicación en tiempo real.**

Al deshabilitar las comunicaciones en tiempo real, los equipos se comunicarán con el servidor **Panda Adaptive Defense 360** cada 15 minutos.

9.5. Configuración del idioma del agente

Para asignar el idioma del agente Panda a uno o varios equipos es necesario crear una configuración de tipo **Proxy e idioma**. Sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red**, pestaña **Proxy e idioma.**
- Haz clic en el botón editar o selecciona una configuración ya creada para modificarla.
- En la sección idioma elige el idioma de entre los disponibles:
  - Español
  - Inglés
  - Sueco
  - Francés
  - Italiano
  - Alemán
  - Portugués
  - Húngaro
  - Ruso
  - Japonés
  - Finlandés

Si se produce un cambio de idioma y la consola local de Panda Adaptive Defense 360 estaba abierta se pedirá un reinicio de la consola local. Este procedimiento no afecta a la seguridad del equipo.

9.6. Configuración de contraseña y anti-tampering

9.6.1 Anti-tamper

Muchas amenazas avanzadas incorporan técnicas para desactivar el software de seguridad instalado en los equipos y así sortear todas sus funcionalidades de protección. Este comportamiento también es práctica habitual de los hackers y **Panda Adaptive Defense 360** incorpora tecnología *anti-tamper* que impide la modificación no autorizada del funcionamiento de la solución.

Habilitar anti-tamper

- Haz clic en el menú superior **Configuración**, panel lateral **Ajustes de equipo.**
- Haz clic en una configuración existen o selecciona **Añadir** para crear una nueva.
- Despliega la sección **Seguridad frente a manipulaciones no deseadas de las protecciones:**
  - **Activar anti-tamper:** impide que los usuarios o ciertos tipos de malware puedan detener las protecciones. Requiere el establecimiento de una contraseña ya que es posible que el administrador o el equipo de soporte necesiten detener temporalmente desde la consola local las protecciones para diagnosticar problemas.

9.6.2 Protección del agente mediante contraseña

Para evitar que el usuario modifique las características de protección o desinstale completamente el software **Panda Adaptive Defense 360**, el administrador puede establecer una contraseña local que cubra ambos casos.

Asignar una contraseña local

- Haz clic en el menú superior **Configuración**, panel lateral **Ajustes de equipo.**
- Haz clic en una configuración existente o selecciona **Añadir** para crear una nueva.
- Despliega la sección **Seguridad frente a manipulaciones no deseadas de las protecciones:**
  - **Solicitar contraseña para desinstalar Aether desde los equipos**: evita que el usuario desinstale el software Panda Adaptive Defense 360 protegiéndolo con una contraseña.
  - **Permitir activar/desactivar temporalmente las protecciones desde la consola de los equipos**: permite administrar las capacidades de seguridad del equipo desde la consola local. Requiere el establecimiento de una contraseña.

10. Configuración de seguridad para estaciones y servidores

10.1. Introducción

Panda Adaptive Defense 360 centraliza en el menú superior **Configurar** toda la configuración de seguridad para estaciones de trabajo y servidores. Haciendo clic en el panel de la izquierda **Estaciones y servidores** se mostrará un listado con todas las configuraciones de seguridad ya creadas.

En este capítulo explican todos los parámetros incluidos en la configuración de seguridad para estaciones y servidores. También se indicarán algunas recomendaciones prácticas para asegurar los puestos de trabajo de la red, minimizando los inconvenientes en su manejo al usuario.

10.2. Introducción a la configuración de estaciones y servidores

La configuración para estaciones y servidores se divide en 9 apartados. Al hacer clic en cada uno de ellos se mostrará un desplegable con su configuración asociada. A continuación, se muestran los 9 apartados con una breve explicación.

- **General**: establece el comportamiento de las actualizaciones, desinstalaciones de la competencia y exclusiones de ficheros que no se analizarán.
- **Protección avanzada (Dispositivos Windows)**: establece el comportamiento de la protección avanzada y de la protección anti exploit frente a APTs, amenazas dirigidas y malware avanzado o que utiliza exploits conocidos y de tipo zero-day.
- **Antivirus**: establece el comportamiento de la protección antimalware tradicional frente a virus y amenazas.
- **Firewall (Dispositivos Windows):** establece el comportamiento del cortafuegos y del IDS que protege al equipo de los ataques de red.
- **Control de dispositivos (Dispositivos Windows):** determina el acceso del usuario a los periféricos conectados al equipo.
- **Control de acceso a páginas web**: regula las visitas del usuario a categorías de páginas web.
- **Antivirus para servidores Exchange**: analiza los mensajes entrantes y salientes de los servidores de correo Exchange en busca de amenazas.
- **Anti spam para servidores Exchange**: analiza los mensajes entrantes y salientes de los servidores de correo Exchange en busca de correo no deseado.
- **Filtrado de contenidos para servidores Exchange**: regula el tipo de contenidos que puede recibir el servidor Exchange.

Funcionalidad	Windows	macOS	Linux	Windows Exchange
Protección avanzada	X			
Protección antiexploit	X			
Antivirus	X	X	X	X
Firewall & IDS	X			
Protección de correo	X			
Protección web	X	X	X	
Control de dispositivos	X			
Control de acceso a páginas web	X	X	X	
Anti-Spam				X
Filtrado de contenidos				X

Tabla 12: funcionalidades de seguridad por plataforma de usuario

10.3. Configuración General

La configuración general permite establecer el comportamiento de **Panda Adaptive Defense 360** en lo relativo a las actualizaciones, desinstalación de programas de la competencia y exclusiones de ficheros y carpetas que no se analizarán por el antivirus tradicional.

10.3.1 Actualizaciones

Consulta el capítulo 14 Actualización del Software para obtener información acerca de los procedimientos necesarios para actualizar el agente, la protección y el fichero de firmas de software instalado en el equipo del usuario.

10.3.2 Desinstalar otros productos de seguridad

Consulta el capítulo 6 Instalación del software Panda Adaptive Defense 360 para establecer el comportamiento de la instalación de la protección en el caso de que otro producto de seguridad este instalado previamente en el equipo del usuario.

Consulta el Apéndice III: Listado de des instaladores para obtener un listado de todos los productos de la competencia que Panda Adaptive Defense 360 es capaz de desinstalar automáticamente del equipo del usuario.

10.3.3 Exclusiones

Esta configuración afecta tanto a la protección antivirus como a la protección avanzada.

Exclusiones configura los elementos del equipo que no serán analizados en busca de malware. Al añadir una exclusión de un elemento ejecutable con extensión .exe o .com, **Panda Adaptive Defense 360** permitirá la ejecución de todas las librerías y binarios utilizados en el programa excluido, excepto aquellos ya conocidas y clasificadas como amenazas. En cualquier caso, los elementos excluidos se siguen monitorizando y acabarán siendo clasificados como goodware o malware.

Ficheros en disco

Se indican los ficheros en el disco de los equipos protegidos que no serán analizados por **Panda Adaptive Defense 360.**

- **Extensiones**: permite especificar extensiones de ficheros que no serán analizadas.
- **Carpetas**: permite especificar carpetas cuyo contenido no será analizado.
- **Ficheros**: permite especificar ficheros específicos que no serán analizados.
- **Exclusiones recomendadas para Exchange**: al hacer clic en el botón **Añadir**, se cargan de forma automática las exclusiones recomendadas por Microsoft para optimizar el rendimiento del producto en servidores Exchange.

Excluir archivos adjuntos de correo:

Permite especificar una lista de extensiones de ficheros que no serán analizados en el caso de encontrarse como adjuntos en mensajes de correo.

10.4. Protección avanzada (Equipos Windows)

10.4.1 Comportamiento de la protección avanzada

La protección avanzada establece los diferentes modos de bloqueo frente al malware desconocido, protegiendo al equipo de APTs y amenazas avanzadas.

- **Protección avanzada**: permite activar o desactivar el motor de protección contra amenazas avanzadas, especifico de **Panda Adaptive Defense 360.**
- **Modo de funcionamiento**:
  - **Auditoria**: En el modo auditoria solo se informa de las amenazas detectadas, pero no se bloquea ni se desinfecta el malware encontrado.
  - **Hardening**: permite la ejecución de los programas desconocidos ya instalados en el equipo del usuario. Los programas desconocidos que vienen de Internet o de unidades de almacenamiento externas serán bloqueados hasta su clasificación. Los programas clasificados como malware serán desinfectados o eliminados.

- **Lock**: Bloquea la ejecución de todos los programas desconocidos hasta que estén clasificados, y los ya clasificados como malware.

10.4.2 Anti exploit

La protección anti exploit bloquea de forma automática y sin intervención del usuario en la mayor parte de los casos los intentos de explotación de vulnerabilidades de procesos instalados en el equipo del usuario.

Funcionamiento de la protección anti-exploits

Los equipos de la red pueden contener procesos con fallos de programación. Estos procesos son conocidos como "procesos vulnerables" y, aunque sean programas legítimos, no interpretan correctamente ciertas secuencias de datos que recogen del exterior.

Cuando un proceso vulnerable recibe información con determinados patrones conocidos por los hackers, se produce un mal funcionamiento interno, que deriva en una inyección en las regiones de memoria gestionadas por el proceso vulnerable de fragmentos de código específicamente preparados por el hacker. Estos procesos así afectados reciben el nombre de "procesos comprometidos".

Esta inyección de código provoca que el proceso comprometido ejecute acciones para las que no fue programado, generalmente peligrosas y que comprometen la seguridad del equipo. La protección anti-exploit de **Panda Adaptive Defense 360** detecta esta inyección de código malicioso en los procesos vulnerables ejecutados por el usuario.

Panda Adaptive Defense 360 bloquea los ataques de tipo exploit mediante dos cursos de acción diferentes, dependiendo del exploit encontrado:

- **Bloqueo del exploit**

Se detecta la inyección de código en el proceso vulnerable cuando todavía no se ha completado. El proceso no llega a comprometerse y el riesgo del equipo es nulo, con lo que no se requiere detener el proceso afectado ni reiniciar el equipo de usuario. Por lo tanto, no implica pérdida de información por parte del proceso afectado.

El usuario puede recibir una notificación del bloqueo dependiendo de la configuración establecida por el administrador.

- **Detección del exploit**

Panda Adaptive Defense 360 detecta la inyección de código en el proceso vulnerable cuando ya se ha producido. Debido a que el proceso vulnerable ya contiene el código malicioso es imperativo cerrarlo antes de que ejecute acciones que puedan poner en peligro la seguridad del equipo.

Independientemente del tiempo transcurrido desde la detección hasta el cierre del proceso **Panda Adaptive Defense 360** considera en riesgo el equipo, aunque es evidente que es un factor dependiente del tiempo que se tarde en cerrar el proceso afectado y del propio malware. **Panda Adaptive Defense 360** puede cerrar el proceso de forma automática para minimizar los efectos adversos, o delegar en el usuario la decisión, pidiéndole permiso de forma explícita para limpiarlo de la memoria.

En el caso de que el administrador haya configurado un cierre automático para minimizar la posibilidad de efectos adversos, el usuario puede sufrir la perdida de información gestionada por el proceso afectado. Si, por el contrario, el administrador ha delegado en el usuario la decisión, el usuario podrá salvar la información, minimizando la posibilidad de pérdida de información.

En los casos en que no sea posible cerrar el proceso afectado se pedirá permiso al usuario para reiniciar el equipo completo.

Configuración de la detección anti - exploits

- **Anti-exploit**: habilita la protección contra exploits
  - **Auditar**: se notificará en la consola Web la detección del exploit, pero no se tomarán acciones contra él ni se informará al usuario del equipo. La notificación también puede producirse vía correo electrónico según la configuración de las alertas por correo electrónico a través de la opción **Preferencias** del botón de configuración general.
  - **Bloquear**: bloquea los ataques de tipo exploit. Puede requerir el cierre del proceso afectado por el exploit.
    - **Informar del bloqueo al usuario del equipo**: el usuario recibe una notificación, pero el proceso comprometido se cierra de forma automática si es necesario.
    - **Pedir permiso al usuario**: el usuario recibe una petición de autorización para el cierre del proceso comprometido por el exploit en caso de ser necesario. Esta opción resulta útil para que el usuario pueda salvar la información crítica antes producirse el cierre del proceso. Si se requiere el reinicio del equipo se pedirá confirmación al usuario, independientemente de la configuración **Pedir permiso al usuario**.

Dado que muchos exploits continúan ejecutando código malicioso, hasta que no se produzca el cierre del proceso la incidencia no se marcará como resuelta en el panel de elementos maliciosos y exploit de la consola Web.

10.4.3 Privacidad

Panda Adaptive Defense 360 puede incluir el nombre y la ruta completa de los ficheros enviados para su posterior visualización en los informes y en las herramientas de análisis forense. Si no deseas que esta información sea enviada a la nube de Panda Security desactiva la casilla apropiada en la pestaña **Privacidad**.

Adicionalmente **Panda Adaptive Defense 360** puede mostrar la información de la cuenta de usuario que estaba logeada en el equipo donde se detectó malware. Si no deseas que esta

información sea enviada a la nube de Panda Security desactiva la casilla apropiada en la pestaña **Privacidad**.

10.4.4 Uso de la red

Los ficheros ejecutables encontrados en el equipo del usuario y que sean desconocidos para la plataforma **Panda Adaptive Defense 360** serán enviados a la nube de Panda Security para su análisis. El impacto en el rendimiento de la red del cliente debido al envío de los ejecutables desconocidos está configurado de forma predeterminada (máximo de 50 Mbytes por hora y agente) para pasar desapercibido. Un fichero desconocido se envía una sola vez para todos los clientes que usan **Panda Adaptive Defense 360**. Además, se han implementado mecanismos de gestión del ancho de banda con el objetivo de minimizar el impacto en la red del cliente.

Para configurar el número máximo de megas que un agente podrá enviar en una hora introducir el valor y hacer clic en **Ok**. Para establecer transferencias ilimitadas dejar el valor a 0.

10.5. Antivirus

En esta sección podrás configurar el comportamiento general del motor de antivirus basado en ficheros de firmas.

- **Protección de archivos**: activa o desactiva la protección antivirus relativa al sistema de ficheros.
- **Protección de correo:** activa o desactiva la protección antivirus relativa al cliente de correo instalado en el equipo del usuario.
- **Protección web:** activa o desactiva la protección antivirus relativa al cliente web instalado en el equipo del usuario.

La acción a ejecutar por **Panda Adaptive Defense 360** ante un fichero de tipo malware o sospechoso queda definida en los laboratorios de Panda Security y sigue las siguientes reglas:

- **Ficheros conocidos como malware desinfectable**: se desinfectan y se elimina el fichero original quedando sustituido por una copia desinfectada y sin peligro para el usuario.
- **Ficheros conocidos como malware no desinfectable**: Para los casos en los que no sea posible una desinfección se guarda una copia de seguridad y el fichero original se elimina.

10.5.1 Amenazas a detectar

Permite configurar el tipo de amenazas que **Panda Adaptive Defense 360** buscará y eliminará en el sistema de archivos, cliente de correo y web instalados en el equipo del usuario.

- **Detectar virus**
- **Detectar herramientas de hacking y PUPs**

- **Bloquear acciones maliciosas**: activa tecnologías anti exploit y heurísticas que analizan localmente el comportamiento de los procesos, buscando actividades sospechosas.
- **Detectar Phishing**

10.5.2 Tipos de archivos

En esta sección se establecen los tipos de archivos que **Panda Adaptive Defense 360** analizará:

- **Analizar comprimidos en disco**
- **Analizar comprimidos en mensajes de correo**
- **Analizar todos los archivos independientemente de su extensión cuando son creados o modificados (No recomendado):** por cuestiones de rendimiento no se recomienda analizar todos los ficheros ya que muchos tipos de ficheros de datos no pueden presentar amenazas a la seguridad del equipo.

10.6. Firewall (Equipos Windows)

Panda Adaptive Defense 360 ofrece tres herramientas básicas para filtrar el tráfico de red que recibe o envía los equipos protegidos:

- **Protección mediante reglas de sistema**: son las reglas que describen características de las comunicaciones establecidas por el equipo (puertos, IPs, protocolos etc), con el objetivo de permitir o denegar los flujos de datos que coincidan con las reglas configuradas.
- **Protección de programas**: establece un conjunto de reglas que permitan o denieguen la comunicación a determinados programas instalados en el equipo de usuario.
- **Sistema de detección de intrusos**: permite detectar y rechazar patrones de tráfico malformado que afecten a la seguridad o al rendimiento del equipo protegido.

10.6.1 Modo de funcionamiento

Se distinguen dos modos de funcionamiento, accesibles mediante el control **La configuración firewall la establece el usuario de cada equipo**:

- **Activado** (firewall en modo usuario o auto administrado): el propio usuario podrá configurar desde la consola local el firewall de su equipo.
- **Desactivado** (firewall en modo administrador): el administrador configura el cortafuegos de los equipos a través de perfiles de configuración.

10.6.2 Tipo de red

Los equipos de usuario portátiles pueden conectarse a redes con un grado de seguridad muy diverso, según se trate de accesos públicos como la red wifi de un cibercafé, o redes gestionadas o de acceso limitado como la red de la empresa. Para ajustar el comportamiento por defecto del cortafuegos, el administrador de la red deberá de seleccionar el tipo de red al que se conectan usualmente los equipos del perfil configurado.

- **Red pública**: son las redes que se encuentran en cibercafés, aeropuertos, etc. Implica establecer limitaciones en el nivel de visibilidad de los equipos protegidos y en su utilización, sobre todo a la hora de compartir archivos, recursos y directorios.
- **Red de confianza**: son las redes que se encuentran en oficinas y domicilios. El equipo es perfectamente visible para el resto de usuarios de la red, y viceversa. No hay limitaciones al compartir archivos, recursos y directorios.

La variación del comportamiento del software **Panda Adaptive Defense 360** según la red seleccionada se refleja en la consola en el número de reglas añadidas de forma automática. Estas reglas se pueden ver en **Reglas de programa** y **Reglas de conexión** como **reglas de Panda**.

10.6.3 Reglas de programa

En esta sección se establecen los programas del usuario que se podrán comunicar con la red y los que tendrán bloqueado el envío y recepción de datos.

Para desarrollar una correcta estrategia de protección es necesario seguir los pasos mostrados a continuación, en el orden indicado:

1 Establecer la acción por defecto.

- **Permitir:** establece una estrategia permisiva basada en aceptar por defecto las conexiones de todos los programas cuyo comportamiento no haya sido definido explícitamente mediante una regla en el paso 3. Este es el modo configurado por defecto y considerado el más básico.
- **Denegar**: establece una estrategia restrictiva basada en denegar por defecto las conexiones de los programas cuyo comportamiento no haya sido definido explícitamente mediante una regla en el paso 3. Este es el modo avanzado de funcionamiento ya que requiere añadir reglas con todos los programas que los usuarios utilizan de forma habitual; de otro modo las comunicaciones de esos programas serán denegadas, afectando probablemente a su buen funcionamiento.

2 Activar reglas de Panda

Activa las reglas generadas automáticamente por Panda Security para el tipo de red definido anteriormente.

Figura 61: controles de edición de reglas de programa

3 Añade reglas para definir el comportamiento específico de una aplicación

Los controles situados a la derecha permiten subir **(1)**, bajar **(2)**, añadir **(3)**, editar **(4)** y borrar **(5)** reglas de programas. Las casillas de selección **(6)** permiten determinar sobre qué reglas se realizarán las acciones.

Al crear una regla es necesario indicar los siguientes campos:

- **Descripción**
- **Programa**: permite seleccionar el programa cuyo comportamiento en red se va a controlar.
- **Conexiones permitidas para este programa:**
  - **Permitir conexiones entrantes y salientes**: El programa se podrá conectar a la red (Internet y redes locales) y también permitirá que otros programas o usuarios se conecten con él. Existen ciertos tipos de programas que requieren este tipo de permisos para funcionar correctamente: programas de intercambio de archivos, aplicaciones de chat, navegadores de Internet, etc.
  - **Permitir conexiones salientes**: El programa se podrá conectar a la red, pero no aceptará conexiones externas por parte de otros usuarios o aplicaciones.
  - **Permitir conexiones entrantes**: El programa aceptará conexiones externas de programas o usuarios procedentes de Internet, pero no tendrá permisos de salida.
  - **Denegar todas las conexiones**: El programa no podrá acceder a la red.
  - **Permisos avanzados**:
    - **Acción**: Establece la acción que ejecutará **Panda Adaptive Defense 360** si la regla coincide con el tráfico examinado.
      - **Permitir**: permite el tráfico.
      - **Denegar**: bloquea el tráfico. Se hace un Drop de la conexión.
    - **Sentido**: establece la dirección del tráfico para protocolos orientados a conexión como TCP.
      - **Salientes**: tráfico con origen el equipo de usuario y destino otro equipo de la red.
      - **Entrantes**: tráfico con destino el equipo de usuario y origen otro equipo de la red.
    - **Zona**
    - **Protocolo**: permite especificar el protocolo de nivel 3 del tráfico generado por el programa a controlar.
      - **Todos**
      - **TCP**
      - **UDP**
    - **IPs**:
      - **Todos**: la regla no tiene en cuenta los campos IP de origen y destino de la conexión.
      - **Personalizado**: permite definir la IP de origen o destino del tráfico a controlar. Especifica más de una IP separadas por ‘,’ o utiliza el carácter ‘-‘ para

establecer rangos de IPs.

- **Puertos**: permite seleccionar el puerto de la comunicación. Selecciona **Personalizado** para añadir varios puertos separados por comas y rangos de puertos utilizando guiones.

10.6.4 Regla de conexión

Las reglas de conexiones son reglas tradicionales de filtrado de tráfico TCP/IP. **Panda Adaptive Defense 360** extrae el valor de ciertos campos de las cabeceras de cada paquete que reciben o envían los equipos protegidos, y explora el listado de reglas introducido por el administrador. Si alguna regla coincide con el tráfico examinado se ejecuta la acción asociada.

Las reglas de conexiones afectan a todo el sistema, independientemente del proceso que las gestione, y son prioritarias con respecto a las reglas configuradas anteriormente para la conexión de los programas a la red.

Para desarrollar una correcta estrategia de protección frente a tráfico no deseado o peligroso es necesario seguir los pasos mostrados a continuación, en el orden que se indica:

1 Establecer la acción por defecto del cortafuegos, situada en Reglas para programas.

- **Permitir:** establece una estrategia permisiva basada en aceptar por defecto las conexiones cuyo comportamiento no haya sido definido mediante reglas en el paso 3. Este es el modo básico de configuración: todas las conexiones no descritas mediante reglas serán automáticamente aceptadas.
- **Denegar:** establece una estrategia restrictiva basada en denegar por defecto las conexiones cuyo comportamiento no haya sido definido mediante reglas en el paso 3. Este es el modo avanzado de funcionamiento: todas las conexiones no descritas mediante reglas serán automáticamente denegadas.

2 Activar reglas de Panda

Activa las reglas generadas automáticamente por Panda Security para el tipo de red definido anteriormente.

3 Añade reglas que describan conexiones de forma específica junto a una acción asociada.

Los controles situados a la derecha permiten subir **(1)**, bajar **(2)**, añadir **(3)**, editar **(4)** y borrar **(5)** reglas de conexión. Las casillas de selección **(6)** permiten determinar sobre que reglas se realizarán las acciones.

Figura 62: controles de edición de reglas de red

El orden de las reglas en la lista es un elemento a tener en cuenta: su aplicación se evalúa en orden descendente y, por lo tanto, al desplazar una regla hacia arriba o abajo en la lista, se modificará la prioridad en su aplicación.

A continuación, se describen los campos que forman una regla de sistema:

- **Nombre de regla**
- **Descripción**
- **Acción**: Establece la acción que ejecutará **Panda Adaptive Defense 360** si la regla coincide con el tráfico examinado.
  - **Permitir**: permite el tráfico
  - **Denegar**: bloquea el tráfico. Se hace un Drop de la conexión
- **Sentido**: establece la dirección del tráfico para protocolo orientados a conexión como TCP.
  - **Salientes**: tráfico saliente
  - **Entrantes**: tráfico entrante
- **Zona**
- **Protocolo**: permite especificar el protocolo de la regla. Según la elección se mostrarán unos controles u otros para identificar de forma precisa el protocolo en cuestión:
  - **TCP, UPD, TCP/UDP:** permite describir reglas TCP y / o UDP incluyendo puertos locales y remotos.
    - **Puertos locales:** permite especificar el puerto de la conexión utilizado en el equipo del usuario. Selecciona **Personalizado** para añadir varios puertos separados por comas y rangos de puertos utilizando guiones.
    - **Puertos remotos:** permite especificar el puerto de la conexión utilizado en el equipo remoto. Selecciona **Personalizado** para añadir varios puertos separados por comas y rangos de puertos utilizando guiones.
  - **ICMP:** permite crear reglas que describen mensajes ICMP, indicando su tipo y subtipo.
  - **IP Types:** permite crear reglas para el protocolo IP y otros protocolos se orden superior.
- **Direcciones IP:** especifica las direcciones IP de origen o destino del tráfico.
- **Direcciones MAC**: especifica las direcciones MAC de origen o destino del tráfico.

Las direcciones MAC de origen y destino se reescriben cada vez que el tráfico atraviesa un proxy, enrutador etc. Los paquetes llegarán al destino con la MAC del último dispositivo que manipuló el tráfico.

10.6.5 Bloquear intrusiones

El módulo IDS permite detectar y rechazar tráfico mal formado y especialmente preparado para impactar en el rendimiento o la seguridad del equipo a proteger. Este tipo de tráfico puede provocar un mal funcionamiento de los programas del usuario que lo reciben, resultando en problemas de seguridad y permitiendo la ejecución de aplicaciones de forma remota por parte del hacker, extracción y robo de información etc.

Panda Adaptive Defense 360 identifica 15 tipos de patrones genéricos que pueden ser activados o desactivados haciendo clic en la casilla apropiada. A continuación, se detallan los tipos de tráfico mal formado soportados y una explicación de cada uno de ellos:

- **IP explicit path**: Se rechazan los paquetes IP que tengan la opción de "explicit route". Son paquetes IP que no se encaminan en función de su dirección IP de destino, en su lugar la información de encaminamiento es fijada de ante mano.
- **Land Attack**: Comprueba intentos de denegación de servicios mediante bucles infinitos de pila TCP/IP al detectar paquetes con direcciones origen y destino iguales.
- **SYN flood:** lanza inicios de conexión TCP de forma masiva para obligar al equipo a comprometer recursos para cada una de esas conexiones. Se establece un límite máximo de conexiones TCP abiertas para evitar una sobrecarga del equipo atacado.
- **TCP Port Scan**: detecta si un equipo intenta conectarse a varios puertos del equipo protegido en un tiempo determinado. Se filtran tanto las peticiones de apertura de puerto como las respuestas al equipo sospechoso, para que el origen del tráfico de escaneo no obtenga información del estado de los puertos
- **TCP Flags Check**: Detecta paquetes TCP con combinaciones de flags inválidas. Actúa como complemento a las defensas de "Port Scanning" al detener ataques de este tipo como "SYN & FIN" y "NULL FLAGS" y los de "OS identification" ya que muchas de estas pruebas se basan en respuestas a paquetes TCP inválidos.
- **Header lengths**
  - **IP**: Se rechazan los paquetes entrantes con un tamaño de cabecera IP que se salga de los límites establecidos.
  - **TCP**: Se rechazan los paquetes entrantes con un tamaño de cabecera TCP que se salga de los límites establecidos.
  - **Fragmentation control**: Realiza comprobaciones sobre el estado de los fragmentos de un paquete a reensamblar, protegiendo al equipo de ataques por consumo excesivo de memoria en ausencia de fragmentos, redireccionado de ICMP disfrazado de UDP y scanning de máquina disponible.
- **UDP Flood**: Se rechazan los paquetes UDP que llegan a un determinado puerto si exceden en cantidad a un número determinado en un periodo determinado.
- **UDP Port Scan**: Protección contra escaneo de puertos UDP.
- **Smart WINS**: Se rechazan las respuestas WINS que no se corresponden con peticiones que el equipo haya solicitado.
- **Smart DNS**: Se rechazan las respuestas DNS que no se corresponden con peticiones que el equipo haya solicitado.
- **Smart DHCP**: Se rechazan las respuestas DHCP que no se corresponden con peticiones que el equipo haya solicitado.
- **ICMP Attack**: Este filtro implementa varias comprobaciones:
  - **SmallPMTU**: Mediante la inspección de los paquetes ICMP se detectan valores inválidos en el tamaño del paquete utilizados para generar una denegación de servicio o ralentizar el tráfico saliente.
  - **SMURF**: Envío de grandes cantidades de tráfico ICMP (echo request) a la dirección de broadcast de la red con la dirección de origen cambiada (spoofing) a la dirección de la víctima. La mayoría de los equipos de la red responderán a la víctima, multiplicando

el tráfico por cada equipo de la subred. Se rechazan las respuestas ICMP no solicitadas si estás superan una determinada cantidad en un segundo.

- **Drop unsolicited ICMP replies**: Se rechazan todas las respuestas ICMP no solicitadas o que hayan expirado por el timeout establecido.

- **ICMP Filter echo request**: se rechazan las peticiones de Echo request.
- **Smart ARP**: Se rechazan las respuestas ARP que no se corresponden con peticiones que el equipo protegido haya solicitado para evitar escenarios de tipo ARP cache poison.
- **OS Detection**: Falsea datos en respuestas al remitente para engañar a los detectores de sistemas operativos y así evitar posteriores ataques dirigidos a aprovechar las vulnerabilidades asociadas al sistema operativo detectado. Esta defensa se complementa con la de "TCP Flags Check".

10.7. Control de dispositivos (Equipos Windows)

Dispositivos de uso común como llaves USB, unidades de CD/DVD, dispositivos de imágenes, bluetooth, módems o teléfonos móviles pueden constituir también una vía de infección para los equipos de la red.

Control de dispositivos permite definir el comportamiento del equipo protegido al conectar u operar con un dispositivo extraíble o de almacenamiento masivo. Para ello, hay que seleccionar el dispositivo o dispositivos que se desea autorizar y asignar un nivel de utilización.

Figura 63: configuración del control de dispositivos

Para activar el control de dispositivos sigue los pasos mostrados a continuación:

- Marca la casilla **Activar control de dispositivos** (1)
- Elige en el desplegable correspondiente el nivel de autorización a aplicar para el tipo de dispositivo a limitar su uso **(2).**
  - En el caso de las llaves USB y las unidades CD/DVD se puede elegir entre **Bloquear**, **Permitir lectura** o **Permitir lectura y escritura**.
  - Para Bluetooth, dispositivos de imágenes, modems USB y teléfono móviles las opciones son **Permitir** y **Bloquear**.

10.7.1 Equipos permitidos

Se puede dar el caso de no permitirse el uso de una familia dispositivos y que, sin embargo, sea necesario autorizar el uso de un dispositivo concreto perteneciente a esa familia.

Esta situación se puede solucionar elaborando una "lista blanca": una lista de dispositivos cuyo uso se permitirá, aunque pertenezcan a grupos de dispositivos que se hayan marcado como no autorizados.

Para ello **Panda Adaptive Defense 360** crea un listado de dispositivos conectados por cada equipo. Haz clic en icono  de **Equipos permitidos** para mostrar un listado con todos los dispositivos conectados a los equipos del parque informático. Elige aquellos que quieras excluir del bloqueo general previamente configurado. Con el botón  podrás borrar exclusiones ya creadas.

10.7.2 Exportar e importar listas de dispositivos permitidos

Una vez la lista de dispositivos permitidos esté finalizada podrás exportarla a un archivo de texto. Esta operación también puede realizarse a la inversa: es decir, configurar en un archivo de texto la lista con los datos de los dispositivos que se desean permitir y a continuación importar esa lista desde la consola Web de **Panda Adaptive Defense 360**.

Para exportar e importar listados de exclusiones ya configurados despliega las opciones de **Exportar** e **Importar** del menú de contexto  .

10.7.3 Obtención del identificador único del dispositivo

En el caso de querer utilizar dispositivos sin restricciones, pero sin esperar a que el usuario conecte los dispositivos en su equipo para poder excluirlos de forma manual, es posible obtener el identificador de estos dispositivos. Para ello sigue los pasos mostrados a continuación:

- En el Administrador de dispositivos de Windows, accede a las propiedades del dispositivo USB que quieres identificar de forma única para excluirlo.
- Accede a la pestaña Detalles y seleccionamos la propiedad Recursos en el desplegable Propiedad. A continuación, debería mostrarse un valor llamado CM_DEVCAP_UNIQUEID
- De nuevo en el desplegable Propiedad, selecciona Ruta de acceso a instancia del dispositivo y obtendrás el identificador único de dispositivo.

En el supuesto de que no se muestre ningún valor denominado CM_DEVCAP_UNIQUEID no será posible realizar la identificación del dispositivo de forma única. Lo que sí podremos hacer es utilizar como identificador el correspondiente al hardware del dispositivo.

En el desplegable Propiedad selecciona Identificador de hardware y se mostrará el identificador correspondiente, que será el que podrás utilizar. En este caso, al usar este identificador se excluirá

del control de dispositivos a todos los productos USB de la gama que posean ese identificador, ya que no habrá manera de diferenciar a unos de otros.

Una vez tengas los identificadores únicos podrás elaborar una lista blanca e importarla tal y como se ha mostrado en el punto anterior.

10.8. Control de acceso a páginas web

Con esta protección el administrador de la red podrá restringir el acceso a determinadas categorías Web y configurar URLs individuales a las que autorizará o restringirá el acceso. Esto contribuirá a la optimización del ancho de banda de la red y a la productividad de la empresa.

Para activar o desactivar el control de acceso páginas web haz clic en el botón **Activar el control de acceso a páginas web**.

10.8.1 Configurar horarios del control de accesos a páginas Web

Con la configuración de horarios podrás restringir el acceso a determinadas categorías de páginas Web y listas negras durante las horas de trabajo, y autorizarlo en el horario no laborable o en el fin de semana.

Para activar el control horario de accesos a páginas Web elija la opción **Activar solo durante las siguientes horas.**

A continuación, selecciona las horas en las que se quiera que el control horario esté activado. Para activarlo sólo en un horario determinado, marca la casilla correspondiente y utiliza la cuadrícula para señalar las horas en las que se activará.

- Para seleccionar días completos haz clic en el día de la semana.
- Para seleccionar una misma hora en todos los días de la semana haz clic en la hora.
- Para seleccionar todos los días del mes haz clic en el botón **Seleccionar todo.**
- Para limpiar toda la selección y comenzar de cero, haz clic en el botón **Vaciar.**

10.8.2 Denegar el acceso a páginas Web

Panda Adaptive Defense 360 agrupa las páginas web en 64 categorías. Tan solo es necesario seleccionar aquellas categorías a las que se desea denegar el acceso.

Para ello selecciona las categorías a denegar el acceso. Cuando el usuario visite una página Web que pertenezca a una categoría denegada, se le mostrará en el navegador un aviso indicando el motivo.

Denegar el acceso a páginas de categoría desconocida

Es posible denegar el acceso a páginas no categorizadas, Para ello haz clic en el botón de activación **Denegar acceso a las páginas cuya categoría sea desconocida.**

Las webs internas o alojadas en intranets y accesibles a través de los puertos 80 u 8080 pueden ser clasificadas como pertenecientes a una categoría desconocida, y por tanto ser denegado su acceso. Para mitigar esta situación el administrador podrá añadir las páginas Web desconocidas que sean necesarias a la lista blanca de exclusiones.

10.8.3 Lista de direcciones y dominios permitidos o denegados

Es posible especificar listas de páginas Web a las que siempre se permitirá (lista blanca) o denegará (lista negra) el acceso, independientemente de la categoría a la que pertenezcan.

Podrás modificar ambas listas en cualquier momento.

- Introduce en la caja de texto la URL del dominio o dirección.
- Haz clic en **Añadir.**
- Utiliza los botones **Eliminar** y **Vaciar** para modificar la lista.
- Finalmente, haz clic en **Aceptar** para guardar la configuración.

La coincidencia de las URLs indicadas en lista blanca y lista negra puede ser completa o parcial. En caso de URLs largas es suficiente con indicar el comienzo de la URL para conseguir una coincidencia.

10.8.4 Base de datos de URLs accedidas desde los equipos

Cada equipo de la red recopila información sobre las URLs visitadas. Esta información solo se puede consultar desde el propio equipo durante un plazo de 30 días.

Los datos almacenados son:

- Identificador del usuario.
- Protocolo (http o https).
- Dominio
- URL
- Categorías devueltas
- Acción (Permitir/denegar).
- Fecha de acceso
- Contador acumulado de accesos por categoría y dominio.

10.9. Antivirus para servidores Exchange

Para activar la protección de servidores Exchange es necesario disponer de un número de licencias igual a la cantidad de buzones en la compañía que requieren protección.

La protección para servidores Exchange es aplicable a las versiones 2003, 2007, 2010, 2013 y 2016 y está formada por tres módulos:

- Antivirus
- Anti-spam
- Filtrado de contenidos

Además, según el momento en el que **Panda Adaptive Defense 360** efectúa el análisis dentro del flujo de correo, se distinguen dos formas de protección: protección de buzones y protección de transporte.

La Tabla 13 muestra las combinaciones de módulo de protección, modo de análisis y versiones de Exchange soportados.

Módulo de protección / modo de análisis	Antivirus	AntiSpam	Filtrado de contenidos
Buzón	2003, 2007, 2010		
Transporte	2003, 2007, 2010, 2013, 2016	2003, 2007, 2010, 2013, 2016	2003, 2007, 2010, 2013, 2016

Tabla 13: módulos de protección, modos de análisis y versiones Microsoft Exchange soportadas

10.9.1 Configuración de la protección Antivirus según el modo de análisis

La protección antivirus para Exchange permite elegir entre dos tipos de análisis:

- Protección de buzones
- Protección de transporte

Protección de buzones

Se utiliza en los servidores Exchange con el rol de Mailbox y permite analizar las carpetas / buzones en segundo plano o cuando el mensaje es recibido y almacenado en la carpeta del usuario.

La protección de buzones solo se ofrece para el módulo Antivirus en los servidores Microsoft Exchange 2003, 2007 y 2010.

El comportamiento de la protección de los buzones es ligeramente diferente según se trate de Exchange 2013 – 2016 y el resto de versiones.

En Exchange 2013 y 2016 no se permite manipular el mensaje analizado; si el correo contiene un elemento peligroso se introduce íntegro en cuarentena. El usuario protegido con **Panda Adaptive Defense 360** recibirá un mensaje con el asunto original, pero con el cuerpo sustituido por un mensaje de advertencia indicando que, en caso de querer recuperar el mensaje original, contacte con el administrador de la red.

Para el resto de versiones de Exchange se ejecuta la acción programada por Panda Security ante la detección de un elemento clasificado como malware: desinfectar el adjunto si es posible o introducirlo en cuarentena si no es posible. El usuario protegido con **Panda Adaptive Defense 360** recibirá el mensaje con los adjuntos desinfectados o, en caso de que no fuera posible su desinfección, un fichero "security_alert.txt" de sustitución, describiendo el motivo de la detección.

Protección de transporte

Se utiliza en servidores Exchange con el rol de Acceso de clientes, Edge Transport y Hub, y permite analizar el tráfico que es atravesado por el servidor Microsoft Exchange.

Analiza en busca de virus, herramientas de hacking y programas potencialmente no deseados sospechosos, con destino a buzones situados en el servidor Exchange.

El administrador tiene la posibilidad de activar o desactivar la protección de buzones y/o de transporte haciendo clic en la casilla apropiada.

10.9.2 Software a detectar

Haz clic en los botones de activación para detectar diferentes tipos de amenazas:

- Detectar virus
- Detectar herramientas de hacking y PUPs

10.9.3 Escaneo inteligente de buzones

El escaneo inteligente de buzones aprovecha los momentos de baja actividad del servidor Exchange para examinar los correos almacenados en sus buzones. Además, sólo comprueba los archivos que no han sido previamente analizados con el fichero de firmas descargado. Cuando el fichero de firmas se actualiza, **Panda Adaptive Defense 360** lanzará otro escaneo inteligente de buzones de forma automática.

10.9.4 Restauración de mensajes con virus y otras amenazas

Configura el servidor SMTP que reenviará los mensajes restaurados desde la consola de administración. Para ello escribe la configuración siguiente:

- **Servidor SMTP**: dirección IP o dominio del servidor de correo
- **El servidor requiere autenticación**: haz clic en el botón de activación si el servidor SMTP no es open relay.

- **Usuario**
- **Contraseña**

Si no se configura ningún servidor SMTP, los mensajes se restaurarán en una carpeta del disco duro del servidor Exchange.

10.10. Anti spam para servidores Exchange

Para activar o desactivar esta protección, utiliza el botón de activación **Detectar Spam.**

Al activar la protección Anti Spam **Panda Adaptive Defense 360** muestra una ventana emergente sugiriendo añadir varias reglas de exclusión para mejorar el rendimiento del servidor de correo.

10.10.1 Acción para mensajes de spam

Selecciona la acción a realizar con los mensajes de spam:

- **Dejar pasar el mensaje**: Se añadirá la etiqueta Spam al asunto de los mensajes. Esta será la opción configurada por defecto.
- **Mover el mensaje a**... Será necesario especificar la dirección de correo electrónico a la que se moverá el mensaje, con la etiqueta Spam añadida en el asunto.
- **Borrar el mensaje**
- **Marcar con SCL** (Spam Confidence Level).

SCL

SCL -Spam Confidence Level- es una escala de valores comprendidos entre el 0 y el 9 que se aplican a los mensajes de correo electrónico susceptibles de ser spam. El valor 9 se asigna a los mensajes que con total probabilidad son spam. El 0 es el valor que se aplica a los mensajes que no son spam. Este valor SCL se puede utilizar para marcar los mensajes que posteriormente serán tratados en función de un umbral configurable en el Directorio Activo. De esta forma la protección adjudica al mensaje el valor SCL correspondiente y posteriormente se procede a su entrega.

A continuación, será el administrador, en función del umbral determinado en el Directorio Activo, quien seleccione la acción que finalmente se realizará con el mensaje.

10.10.2 Direcciones y dominios permitidos

Son listas de direcciones y dominios cuyos mensajes no serán analizados por la protección anti-spam (lista blanca).

Añade varias direcciones y dominios separados por el carácter “,”

10.10.3 Direcciones y dominios de spam

Son listas de dominios y direcciones cuyos mensajes serán interceptados por la protección y eliminados (lista negra).

Al configurar las listas es importante tener en cuenta:

- Si un dominio se encuentra en lista negra y una dirección perteneciente a dicho dominio se encuentra en lista blanca, se permitirá dicha dirección, pero no el resto de direcciones del dominio.
- Si un dominio se encuentra en lista blanca y una dirección perteneciente a dicho dominio se encuentra en lista negra, dicha dirección no será aceptada, pero sí el resto de direcciones de dicho dominio.
- Si un dominio (por ejemplo: domain.com) se encuentra en lista negra y un subdominio de este (ej: mail1.domain.com) se encuentra en lista blanca, se permitirán direcciones de dicho subdominio, pero no el resto de direcciones del dominio o de otros subdominios diferentes.
- Si un dominio se encuentra en lista blanca también se considerarán incluidos en lista blanca todos sus subdominios.

10.11. Filtrado de contenidos para servidores Exchange

El filtrado de contenidos permite filtrar los mensajes de correo electrónico en función de cuál sea la extensión de los archivos adjuntos incluidos en ellos.

Una vez establecida la lista de mensajes susceptibles de albergar adjuntos sospechosos, podrás indicar qué acción deseas que la protección realice con dichos mensajes.

También se puede aplicar el filtrado de contenidos a mensajes que incluyan adjuntos con dobles extensiones.

- **Acción a realizar**: selecciona si deseas borrar los mensajes o desviarlos a otra dirección de correo electrónico. Esto puede resultar útil para analizar a posteriori los adjuntos recibidos.
- **Considerar archivos adjuntos peligrosos los que tienen las siguientes extensiones**: considera como peligrosos los archivos adjuntos con alguna extensión concreta. Una vez marcada la casilla, utiliza los botones **Añadir**, **Eliminar**, **Vaciar** o **Restaurar** para configurar la lista de extensiones que deseas bloquear.
- **Considerar archivos adjuntos peligrosos todos los que tienen doble extensión, excepto en los siguientes casos**: el filtrado de contenidos impedirá la entrada de todos los mensajes de correo electrónico con adjuntos de doble extensión, excepto aquellos cuyos adjuntos tengan las extensiones seleccionadas. Utiliza los botones **Añadir**, **Eliminar**, **Vaciar** o **Restaurar** para configurar la lista de dobles extensiones permitidas.

Registro de detecciones

Todas las detecciones producidas en un servidor Exchange son almacenadas localmente en un archivo CSV. De esta forma se ofrece al administrador la posibilidad de obtener información adicional acerca de la imposibilidad de entrega de los mensajes a sus destinatarios.

El fichero recibe el nombre ExchangeLogDetections.csv y se almacena en la carpeta

%AllUsersProfile%\Panda Security\Panda Cloud Office Protection\Exchange

El contenido del fichero se dispone en formato tabular con la siguiente distribución de campos:

- **Date**: fecha de la llegada del correo al servidor Exchange.
- **From**
- **To**
- **Subjet**
- **Attachments**: listado con los ficheros adjuntos al correo.
- **Protection**
- **Action**

11. Configuración de seguridad Android

Configuración de dispositivos Android
Actualizaciones
Antivirus

11.1. Introducción

Panda Adaptive Defense 360 centraliza en el menú superior **Configuración** toda la configuración de los parámetros de seguridad para smartphones y tablets. Haciendo clic en el panel de la izquierda **Dispositivos Android** se mostrará un listado con todas las configuraciones de seguridad ya creadas.

En este capítulo se repasarán todos los parámetros incluidos en la configuración de seguridad para dispositivos Android, al tiempo que se mostrarán algunas recomendaciones prácticas para asegurar móviles y tablets, minimizando los inconvenientes en su manejo al usuario.

11.2. Introducción a la configuración de dispositivos Android

La configuración para dispositivos Android se divide en 3 apartados. Al hacer clic en cada uno de ellos se mostrará un desplegable con su configuración asociada. A continuación, se muestran los apartados con una breve explicación:

- **Actualizaciones**: permite establecer el tipo de conexión que utilizara el dispositivo para descargar as actualizaciones de la nube de Panda Security.
- **Antivirus**: permite establecer la configuración del antivirus.

11.3. Actualizaciones

La configuración de las actualizaciones se describe en el capítulo 14 Actualización del Software.

11.4. Antivirus

La protección antivirus para smartphones Android protege a móviles y tablets frente a la instalación de aplicaciones con malware y PUPs analizando bajo demanda o de forma permanente tanto el dispositivo móvil como las tarjetas de memoria SD conectadas.

Haz clic en el botón de activación **Activar protección permanente antivirus** para activar la detección de malware.

Exclusiones

La protección para Android permite realizar exclusiones de cualquiera de las aplicaciones instaladas. Introduce los nombres de los paquetes a excluir separados por el carácter “,”

Para localizar el nombre del paquete correspondiente a una aplicación instalada búscala en la Google Play. En la URL de su ficha se mostrará el parámetro id, que contiene la cadena que identifica de forma única a la aplicación.

12. Panda Data Control (supervisión de información sensible)

12.1. Introducción

Panda Data Control es el módulo de seguridad de **Panda Adaptive Defense 360** que ayuda a cumplir con las regulaciones sobre protección de datos como la GDPR, y a dar visibilidad y supervisar la información personal (*PII*) almacenada en la infraestructura IT de las empresas.

Panda Data Control descubre, audita y monitoriza en tiempo real el ciclo de vida completo de los ficheros PII: desde los datos en reposo, las operaciones efectuadas sobre ellos y su comunicación al exterior.

Consulta la Guía de administración de Panda Data Control para obtener más información sobre la consola de gestión específica para este servicio.

12.2. Requisitos de Panda Data Control

12.2.1 Plataformas soportadas

Panda Data Control es compatible con la plataforma Microsoft Windows desde la versión XP SP3 en adelante y Windows 2003 SP1 y superiores. Otros sistemas operativos como Linux o macOS no están soportados.

12.2.2 Entidades soportadas

Panda Adaptive Defense 360 aplica algoritmos de Machine Learning y expresiones regulares en cada fichero compatible encontrado para buscar información personal. Los datos reconocidos como PII son los siguientes:

- Cuentas bancarias.
- Tarjetas de crédito.
- Número de identidad personal y fiscal.
- Direcciones IP.
- Direcciones de correo electrónico.
- Números de teléfono.
- Números de carnet de conducir.
- Números de pasaporte.
- Números de la seguridad social.
- Nombres y apellidos.
- Localidades y países.
- Direcciones y códigos postales.

12.2.3 Países soportados

El formato de las distintas entidades reconocidas varía dependiendo del país. **Panda Data Control** soporta la detección de entidades de los países mostrados a continuación:

- Alemania
- España
- Francia
- Suecia
- UK
- Italia
- Portugal
- Países Bajos
- Suiza
- Finlandia
- Dinamarca

12.2.4 Componentes IFilter

Panda Data Control requiere ciertos componentes de terceros instalados en el equipo del usuario para poder interpretar correctamente el contenido de los archivos del usuario. Estos componentes reciben el nombre de "IFilters" y no forman parte del paquete de instalación **de Panda Adaptive Defense 360**. Microsoft Search, Microsoft Exchange Server y Microsoft Sharepoint Server entre otros servicios del sistema operativo y productos independientes utilizan los componentes IFilter para indexar los ficheros del usuario y habilitar la búsqueda por contenido.

Cada formato de fichero compatible tiene su propio componente IFilter asociado, y muchos de ellos vienen ya preinstalados en la instalación básica de Windows, aunque otros tienen que ser instalados o actualizados de forma manual.

Microsoft Filter Pack es un paquete de distribución gratuito que contiene todos los componentes IFilter asociados a la suite de ofimática Microsoft Office. Una vez instalado, **Panda Data Control** será capaz de analizar el contenido de todos los formatos de fichero soportados por la suite.

12.2.5 Instalación del componente Microsoft Filter Pack

Microsoft Filter Pack y Microsoft Office

El componente Microsoft Filter Pack viene incluido en la suite de ofimática Office, aunque solo se instalarán de forma automática los componentes IFilter que se corresponden con los productos de la suite instalados en el equipo del usuario. Para tener la seguridad de que todos los componentes estén disponibles en el equipo en su versión 2010, consulta el punto **Instalación independiente del Microsoft Filter Pack**.

Instalación independiente del Microsoft Filter Pack

Para instalar el Microsoft Filter Pack haz clic en la siguiente URL:

https://www.microsoft.com/en-us/download/details.aspx?id=17062

El paquete es compatible con Windows XP SP3, Windows 2013 SP1 y superiores, aunque en algunos casos se requerirá la instalación de la librería Microsoft Core XML Services 6.0.

12.3. Configuración de Panda Data Control

Para acceder a la configuración de **Panda Data Control:**

- Haz clic en el menú superior **Configuración**, menú lateral **Información sensible.**
- Haz clic en el botón **Añadir**, se abrirá la ventana de configuración de **Panda Data Control.**

12.3.1 Búsqueda de los equipos que no cumplen con los requisitos de Panda Data Control

Para poder analizar el contenido de los ficheros, **Panda Data Control** requiere tener instalados en el equipo del usuario todos los componentes iFilters asociados a los formatos de fichero compatibles.

Para localizar los equipos que no tienen instalado alguno o ninguno de los componentes iFilter haz clic en el enlace **Comprobar ahora** de la pantalla de configuración. Se abrirá la zona **Equipos** con un listado filtrado por el criterio **Equipos sin Microsoft Filter Pack**.

12.3.2 Seguimiento de información personal

Panda Data Control busca y monitoriza ficheros PII de una forma equivalente a como **Panda Adaptive Defense 360** busca y monitoriza los ficheros del usuario en busca de virus y amenazas.

Monitorización de ficheros PII

Panda Data Control monitoriza las acciones de los procesos ejecutadas sobre ficheros identificados como PII. Estos ficheros contienen información personal (DNIs, nombre y apellidos, direcciones y otros) de clientes, proveedores, trabajadores de la empresa etc.

Para que **Panda Data Control** comience a monitorizar las acciones de los procesos ejecutadas sobre ficheros PII almacenados en el puesto de usuario o servidor, haz clic en el botón de activación **Activar seguimiento de información personal**.

Buscar información personal en todo el equipo (recomendado)

Panda Data Control ejecuta un barrido completo del sistema de ficheros para buscar los ficheros PII y crear una base de datos con la información personal encontrada. Cada vez que la tecnología

de identificación de información personal se actualice, el software **Panda Adaptive Defense 360** volverá a recorrer el sistema de ficheros de forma automática para actualizar la base de datos.

No es posible ni necesario ejecutar un análisis bajo demanda. El sistema lanzará automáticamente un análisis del sistema de ficheros cada vez que se actualice la inteligencia de Data Control, y la primera vez que se active esta funcionalidad.

Para que el software **Panda Adaptive Defense 360** recorra todo el sistema de ficheros en busca de archivos con información personal:

- Haz clic en el botón de activación **Buscar información personal en todo el equipo (recomendado).**

12.3.3 Búsquedas de información en los equipos

Panda Data Control permite localizar ficheros por su nombre o contenido, siempre que hayan sido previamente indexados. Para activar las búsquedas de ficheros haz clic en el botón **Permitir realizar búsquedas de información en los equipos** y **Panda Data Control** comenzará el proceso de indexación de los ficheros almacenados en los equipos de los usuarios**.**

Para ver el estado de la indexación haz clic en el link **Ver estado de indexación de los equipos**. Se abrirá el listado **Estado de Data Control**, explicado más adelante en este capítulo. El listado muestra el estado de **Panda Data Control** en cada equipo de la red que tenga una licencia de este módulo asignada.

12.4. Paneles / Widgets disponibles

A continuación, se detallan los distintos widgets implementados en el dashboard de **Panda Data Control,** las distintas áreas y zonas activas incorporadas y los tooltips y su significado. Para acceder haz clic en el menú superior **Estado**, panel lateral **Data Control**.

12.4.1 Estado de Data control

Muestra los equipos donde **Panda Data Control** está funcionando correctamente y aquellos que presentan algún tipo de error. El estado de los equipos se representa mediante un círculo con distintos colores y contadores asociados. El panel representa en porcentaje y de forma gráfica los equipos que comparten un mismo estado.

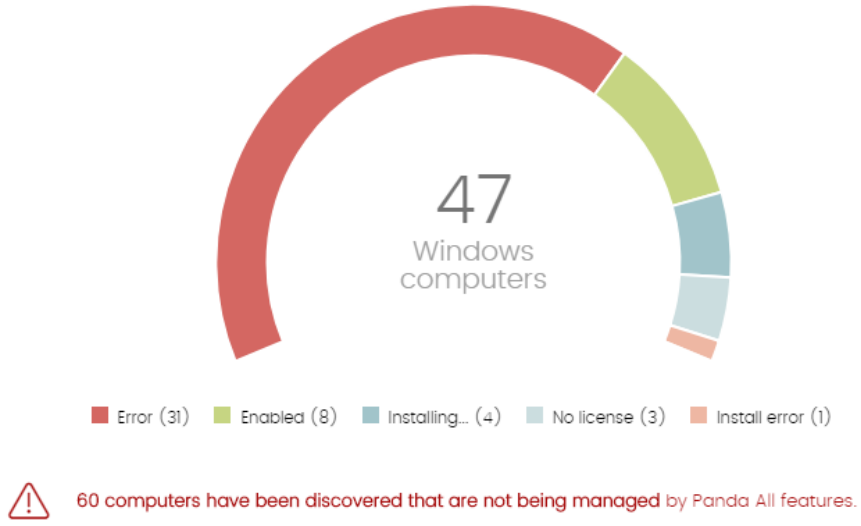


Figura 64: panel Estado de Data Control

- **Significado de las series**

- **Error**: equipos con **Panda Data Control** instalado pero que, por alguna razón, el módulo no responde a las peticiones desde los servidores de Panda Security.
- **Sin licencia**: equipos no gestionados por **Panda Data Control** debido a la falta de licencias suficientes, o a la no asignación de licencias disponibles.
- **Instalando**: equipos en los que **Panda Data Control** se encuentra en proceso de instalación.
- **Error instalando**: equipos cuya instalación no se pudo completar.
- **Desactivada**: equipos que no tienen activada la opción **Activar seguimiento de información personal** o la opción **Búsquedas de información en los equipos**, en la configuración de información sensible.
- **Activada**: equipos que tienen activada la opción **Activar seguimiento de información personal** y la opción **Búsquedas de información en los equipos**, en la configuración de información sensible.
- **Parte central**: suma de los equipos que no tienen **Panda Data Control** en funcionamiento pero que son compatibles con el servicio.

- **Filtros pre establecidos desde el panel**

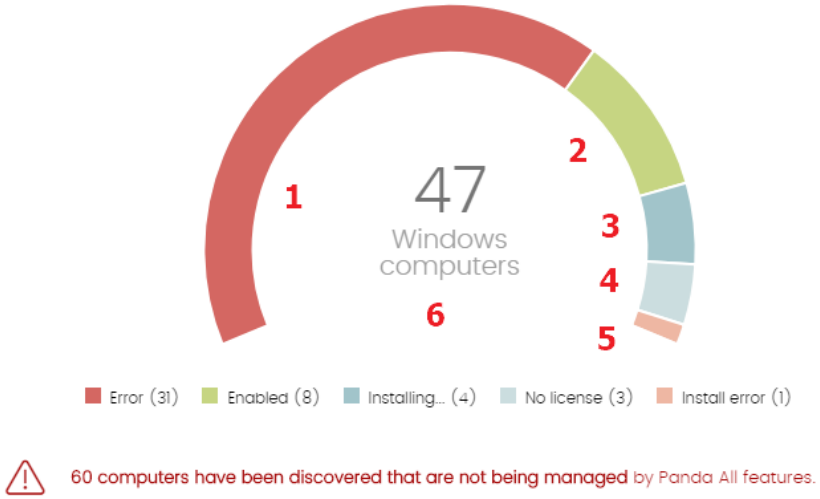


Figura 65: zonas activas del panel Estado de Data Control

El listado se muestra con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

- **(1)** Listado **Estado de Data Control** filtrado por **Estado de Data Control** = Error
- **(2)** Listado **Estado de Data Control** filtrado por **Estado de protección** = Seguimiento de información personal activado
- **(3)** Listado **Estado de Data Control** filtrado por **Estado de protección** = Instalando...
- **(4)** Listado **Estado de Data Control** filtrado por **Estado de protección** = Sin licencia
- **(5)** Listado **Estado de Data Control** filtrado por **Estado de protección** = Error instalando
- **(6)** Listado **Estado de Data Control** filtrado por **Estado de protección** = Sin filtros

12.4.2 Equipos sin conexión

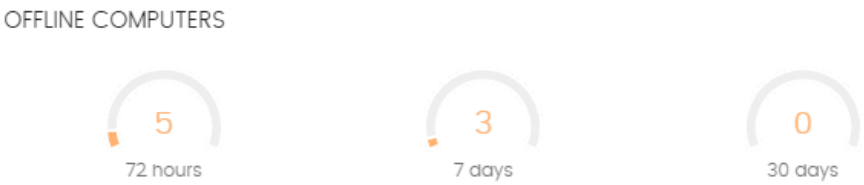


Figura 66: panel Equipos sin conexión

Equipos sin conexión muestra los equipos de la red que no han conectado con la nube de Panda Security en un determinado periodo de tiempo. Estos equipos son susceptibles de tener algún tipo de problema y requerirán una atención especial por parte del administrador.

- **Significado de las series**

- **72 horas**: número de equipos que no enviaron su estado en las últimas 72 horas.

- **7 días**: número de equipos que no enviaron su estado en las últimas 7 días.
- **30 días**: número de equipos que no enviaron su estado en las últimas 30 días.

- **Filtros pre establecidos desde el panel**

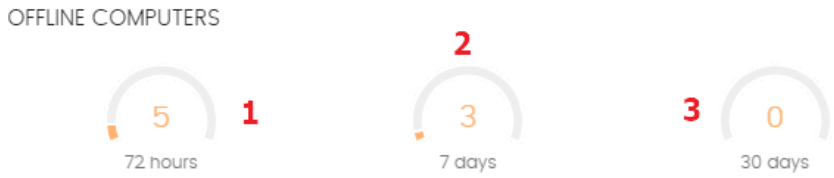


Figura 67: zonas activas del panel Equipos sin conexión

El listado se muestra con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

- **(1)** Listado **Estado de Data Control** filtrado por **Última conexión** = Hace más de 72 horas
- **(2)** Listado **Estado de Data Control** filtrado por **Última conexión** = Hace más de 7 días
- **(3)** Listado **Estado de Data Control** filtrado por **Última conexión** = Hace más de 30 días

12.4.3 Estado de la actualización

Muestra el estado de los equipos con respecto a la actualización del motor de **Panda Data Control**.

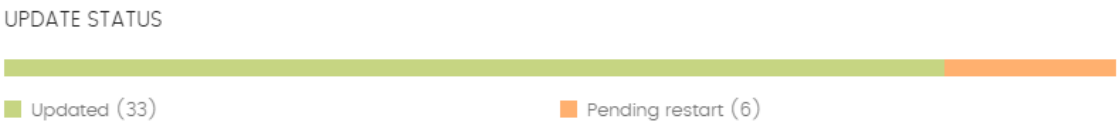


Figura 68: panel Estado de la actualización

- **Significado de las series**

- **Actualizados**: número de equipos con el motor **Panda Data Control** actualizado.
- **Desactualizados**: número de equipos con el motor **Panda Data Control** desactualizado.
- **Pendientes de reinicio**: número de equipos que han descargado el motor **Panda Data Control** pero todavía no se han reiniciado, con lo que todavía no se ha actualizado.

- **Filtros pre establecidos desde el panel**

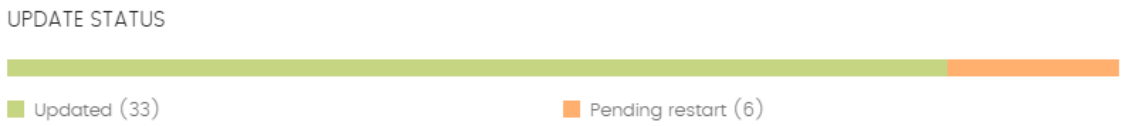


Figura 69: zonas activas del panel Estado de la actualización

El listado se muestra con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

- **(1)** Listado **Estado de Data Control** filtrado por **Protección actualizada** = Si
- **(2)** Listado **Estado de Data Control** filtrado por **Protección actualizada** = Pendiente de reinicio
- **(3)** Listado **Estado de Data Control** filtrado por **Protección actualizada** = No

12.4.4 Estado de la indexación

Muestra el estado de los equipos con respecto al estado de indexación de las unidades de almacenamiento conectadas.

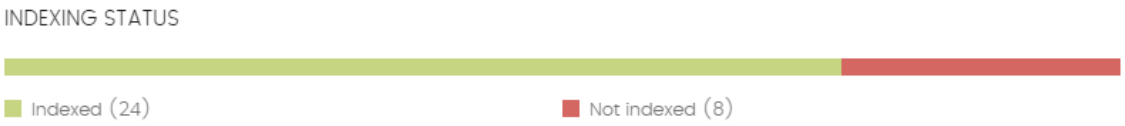


Figura 70: panel Estado de la indexación

- **Significado de las series**

- **Indexado**: número de equipos con los contenidos de las unidades de almacenamiento completamente indexados.
- **No indexado**: número de equipos con los contenidos de las unidades de almacenamiento sin indexar.
- **Indexando**: número de equipos con contenidos en proceso de indexación.

- **Filtros pre establecidos desde el panel**

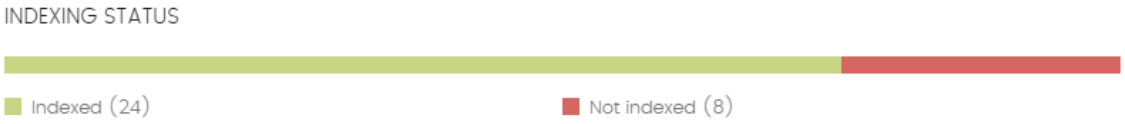


Figura 71: zonas activas del panel Estado de la indexación

El listado se muestra con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

- **(1)** Listado **Estado de Data Control** filtrado por **Estado de indexación** = Indexando
- **(2)** Listado **Estado de Data Control** filtrado por **Estado de indexación** = No indexado
- **(3)** Listado **Estado de Data Control** filtrado por **Estado de indexación** = Indexando

12.5. Listados disponibles

12.5.1 Listado Estado de Data Control

Este listado muestra todos los equipos de la red e incorpora filtros relativos al estado del módulo **Panda Data Control** para localizar aquellos puestos de trabajo o dispositivos móviles que cumplen los criterios establecidos en el panel.

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Seguimiento de información personal	Estado del módulo Panda Data Control.	Error instalando y Error Desactivado Instalando Activado Sin licencia
Búsquedas	Indica si Panda Data Control puede buscar ficheros en los dispositivos de almacenamiento del equipo, y si no es posible, indica la causa.	Error instalando y Error Desactivado Instalando Activado Sin licencia

Campo	Comentario	Valores
Actualizado	Indica si el módulo de Panda Data Control instalado en el equipo coincide con la última versión publicada o no. Al pasar el puntero del ratón por encima del campo se indica la versión de la protección instalada	Actualizado Pendiente de reinicio No
Microsoft Filter Pack	Indica si todos los componentes necesarios del paquete Microsoft Filter Pack están instalados o no en el equipo.	Instalado No instalado Información no disponible
Estado de indexación	Indica el estado del proceso de indexación de ficheros.	Indexando Indexado No indexado No disponible
Ultima conexión	Fecha del ultimo envío del estado de Panda Adaptive Defense 360 a la nube de Panda Security.	Fecha

Tabla 14: campos del listado Estado de Data Control

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	Estación Portátil Dispositivo móvil Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Versión del agente		Cadena de caracteres
Fecha instalación	Fecha en la que el Software Panda Adaptive Defense 360 se instaló con éxito en el equipo.	Fecha

Campo	Comentario	Valores
Fecha de la última conexión	Fecha del ultimo envío del estado del equipo a la nube de Panda Security.	Fecha
Fecha de la última actualización	Fecha de la última actualización del agente.	Fecha
Plataforma	Sistema operativo instalado en el equipo.	Windows Linux macOS Android
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Protección actualizada	Indica si el módulo de la protección instalado en el equipo es la última versión publicada.	Binario
Versión de la protección	Versión interna del módulo de protección.	Cadena de caracteres
Conocimiento actualizado	Indica si el fichero de firmas descargado en el equipo es la última versión publicada.	Binario
Fecha de última actualización	Fecha de la descarga del fichero de firmas.	Fecha
Seguimiento de información personal	Estado del módulo Panda Data Control.	Error instalando Error Desactivado Instalando Activado Sin licencia
Búsquedas	Indica si Panda Data Control puede buscar ficheros en los dispositivos de almacenamiento del equipo, y si no es posible, indica la causa.	Error instalando Error Desactivado Instalando Activado Sin licencia
Microsoft Filter Pack	Indica si todos los componentes necesarios del paquete Microsoft Filter Pack están instalados o no en el equipo.	Instalado No instalado No disponible
Estado de indexación	Indica el estado del proceso de indexación de ficheros.	Indexando Indexado No indexado No disponible
Estado de aislamiento	Indica si el equipo ha sido aislado de la red o se comunica con sus equipos vecinos de forma normal.	Aislado No aislado
Fecha error instalación	Fecha en la que se intentó la instalación del módulo Panda Data Control y se produjo el error.	Fecha

Campo	Comentario	Valores
Error instalación	Motivo del error de instalación	Cadena de caracteres

Tabla 15: campos del fichero exportado Estado de protección de los equipos

Herramienta de filtrado

Campo	Comentario	Valores
Tipo de equipo	Filtra los equipos según su clase	Estación Portátil Dispositivo móvil Servidor
Buscar equipo	Filtra los equipos según su nombre	Cadena de caracteres
Ultima conexión	Filtra los equipos según la fecha del último envío del estado de Panda Data Control a la nube de Panda Security	Todos Más de 72 horas Más de 7 días Más de 30 días
Protección actualizada	Filtra los equipos según la versión de la protección instalada.	Todos Si No Pendiente de reinicio
Estado de indexación	Filtra los equipos según el estado del proceso de indexación de ficheros.	Indexando Indexado No indexado No disponible
Microsoft Filter Pack	Filtra los equipos si tienen o no instalados todos los componentes necesarios del paquete Microsoft Filter Pack.	Todos Falso Verdadero
Estado de Data Control	Filtra los equipos según el estado del módulo Panda Data Control.	Instalando... Activado Seguimiento de información personal desactivado Búsqueda de información en el equipo desactivado Error Error Instalando Sin licencia

Tabla 16: campos de filtrado para el listado Estado de Data Control

12.6. Búsqueda de ficheros

Panda Data Control localiza ficheros por su nombre, extensión o contenido en las unidades de almacenamiento indexadas de los equipos de la red mediante el widget **Búsquedas** del panel de control.

Las búsquedas se ejecutan en tiempo real: tan pronto como el administrador lanza una búsqueda, ésta se despliega en los equipos de la red y comienza a reportar resultados conforme se van produciendo, sin esperar a completar la ejecución por completo.

Para acceder al widget **Búsquedas** haz clic en el menú superior **Estado**, panel lateral **Data Control**.

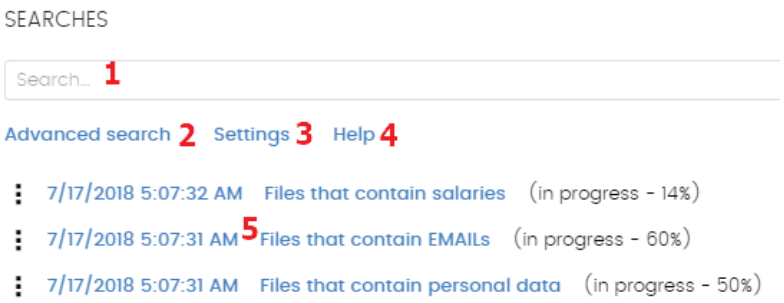


Figura 72: panel Búsquedas

El widget contiene los controles mostrados a continuación:

- **(1)** Caja de texto para introducir los términos a buscar. Consulta en el punto 12.6.5 Sintaxis de las búsquedas para una descripción de los comandos aceptados por **Panda Data Control**.
- **(2) Búsqueda avanzada**: limita el ámbito de búsqueda.
- **(3) Configuración:** acceso al listado de perfiles de configuración de **Panda Data Control**. Para más información consulta el punto 12.3 Configuración de Panda Data Control.
- **(4) Ayuda:** enlace a la página web de soporte de Panda Security donde se muestra la sintaxis de las búsquedas de **Panda Data Control** actualizada con los últimos cambios introducidos.
- **(5) Búsquedas almacenadas:** búsquedas definidas anteriormente y que pueden ser relanzadas en el parque informático.

12.6.1 Propiedades y requisitos de las búsquedas

Para completar con éxito una búsqueda es necesario cumplir con los siguientes requisitos:

- La cuenta de usuario que lanza la búsqueda desde la consola web tiene que tener asignado un rol con el permiso **Buscar información en los equipos**. Consulta el capítulo 22 Control y supervisión de la consola de administración para obtener más información sobre los roles.
- Los equipos sobre los que se efectúan las búsquedas deben de contar con una licencia de **Panda Data Control** asignada.
- Los equipos sobre los que se efectúan las búsquedas deben de tener asignada una configuración de **Información sensible** con las opciones **Buscar información personal en todo el equipo (recomendado) y Permitir realizar búsquedas de información en los equipos** habilitadas.

Propiedades de las búsquedas

- El número de búsquedas simultáneas en la consola de administración por cuenta de usuario es 10. Pasado este número se mostrará un mensaje de error en pantalla.
- El número máximo de búsquedas guardadas por cuenta de usuario es 30. Pasado este número se mostrará un mensaje de error en pantalla.
- El número máximo de resultados en total por cada búsqueda es 10.000 registros. Pasado este número los resultados no se mostrarán en la consola.
- El número máximo de resultados por cada máquina es 10.000 / número de máquinas sobre las que se ejecuta la búsqueda. De esta forma, si se busca sobre un parque de 100 máquinas, el número máximo de resultados mostrados será 10.000 / 100 = 100 resultados por máquina.
- El número mínimo de resultados mostrados por equipo independientemente del número de equipos de la red es 10.
- El número máximo de equipos sobre los que se ejecutan búsquedas de forma simultánea es 50. Si el número total de equipos que participaran en la búsqueda es mayor, las búsquedas más allá del límite de 50 se mantendrán en espera hasta que las primeras se vayan completando.
- se encolarán hasta que los equipos con búsquedas en curso se vayan completando.

12.6.2 Crear una búsqueda

Crear una búsqueda libre

- Haz clic en el menú superior **Estado**, panel lateral **Data Control.**
- Introduce en la caja de texto del widget **Búsquedas** los términos de búsqueda según la sintaxis mostrada en el punto 12.6.5 Sintaxis de las búsquedas.
- Haz clic en el icono  o pulsa la tecla Enter.

Una vez introducida la búsqueda se abrirá la ventana **Resultados de la búsqueda**. Consulta el punto 12.6.3 Búsquedas almacenadas para editar la búsqueda introducida.

Crear una búsqueda guiada

- Haz clic en el menú superior **Estado**, panel lateral **Data Control**.
- Haz clic en el enlace **Búsqueda avanzada**.
- Elige en el selector **Búsqueda guiada**
- Configura los parámetros de la búsqueda.

Parámetros de búsqueda avanzada

- **Nombre de la búsqueda**: establece un nombre para la búsqueda almacenada.
- **Buscar archivos con**: introduce el contenido a buscar. Se incluyen tres cajas de texto:
  - **Alguna de estas palabras o frases exactas**: busca los ficheros que contienen alguna o todas las palabras o entidades indicadas.
  - **Todas estas palabras o frases exactas**: busca los ficheros que contienen todas las palabras o entidades indicadas.

- **Ninguna de estas palabras o frases exactas**: busca los ficheros que no contienen ninguna de las palabras o entidades indicadas.
- **Filtrar por tipo de archivo**: selecciona el tipo de archivo donde se buscará el contenido introducido. Consulta el apartado 12.7 Extensiones de programas soportados por Panda Data Control.

- **Limitar la búsqueda a**:
  - **Equipos**:
    - **Todos:** busca el contenido introducido en todos los equipos que tengan una licencia de **Panda Data Control** asignada y esté habilitada la opción de búsqueda en su configuración.
    - **Los siguientes equipos**: muestra un listado de los equipos que tengan una licencia de **Panda Data Control** asignada. Indica con las casillas de selección los equipos en los que se buscará el contenido introducido.
    - **Los siguientes grupos de equipos**: muestra el árbol de carpetas con la jerarquía de equipos configurada en **Panda Adaptive Defense 360**. Indica con la casilla de selección los grupos donde se buscará el contenido introducido.
- Cancelar automáticamente la búsqueda: indica el tiempo de espera para los equipos apagados o sin conexión antes de cancelar la búsqueda.

12.6.3 Búsquedas almacenadas

Tanto las búsquedas libres como las guiadas se almacenan para poder ser lanzadas posteriormente de forma rápida.

Una vez creada una nueva búsqueda, ésta aparecerá en el widget **Búsquedas** con la fecha y hora de su creación, junto al nombre y una leyenda indicando su estado (**En cuso**, **Cancelada**) o sin estado (Finalizada).

Editar una búsqueda almacenada

Para cambiar el nombre de una búsqueda almacenada haz clic en el menú de contexto de la búsqueda y elige **Cambiar nombre**.

Volver a lanzar una búsqueda almacenada

Haz clic en el menú de contexto de la búsqueda y elige **Relanzar búsqueda**. El estado de la búsqueda cambiará e indicará el porcentaje de la tarea realizada.

Cancelar y eliminar búsquedas almacenadas

Haz clic en el menú de contexto de la búsqueda y elige **Cancelar** para interrumpir la búsqueda o en **Borrar** para cancelarla y borrarla del widget **Búsquedas**.

12.6.4 Visualizar los resultados de una búsqueda

Para visualizar el resultado de una búsqueda accede al listado **Buscar en los equipos** de dos formas:

- Haciendo clic en una búsqueda almacenada.
- Creando una nueva búsqueda.

Este listado muestra los equipos que contienen la cadena de búsqueda introducida, junto al nombre del fichero encontrado y otra información útil.

Cabecera de listado

Configura los parámetros de la búsqueda rápida:

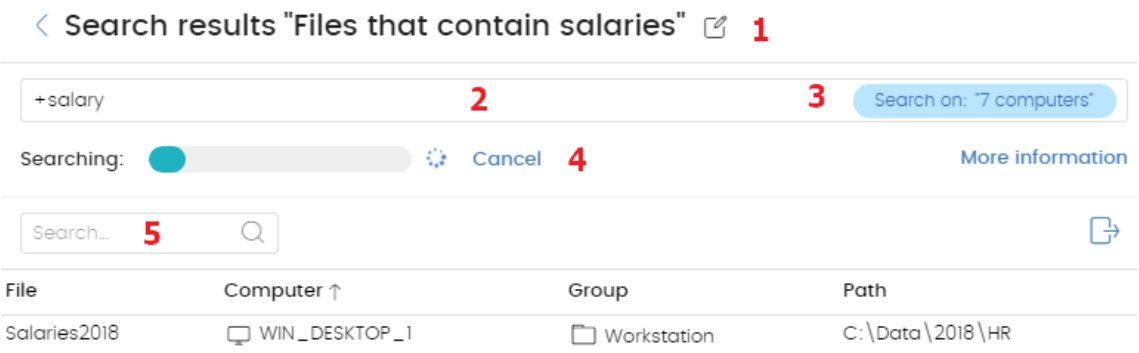


Figura 73: ventana Resultados de una búsqueda

- **(1) Icono** : cambia el nombre de la búsqueda.
- **(2) Caja de texto**: contenido de la búsqueda.
- **(3) Buscar en: "x equipos"**: abre la ventana de búsqueda avanzada para refinarla.
- **(4) Buscando**: estado de la búsqueda (**En curso**, **Cancelada).** Si la búsqueda no se ha iniciado o ha terminado no se indica el estado.
- **(5) Caja de texto Buscar**: filtra los resultados mostrados en la tabla de resultados por el nombre de equipo.

Campos del listado

Campo	Comentario	Valores
Archivo	Nombre del fichero encontrado.	Cadena de caracteres
Equipo	Nombre del equipo donde se encontró el fichero.	Cadena de caracteres
Grupo	Grupo de Panda Adaptive Defense 360 al que pertenece el equipo.	Cadena de caracteres
Ruta	Ruta dentro del dispositivo de almacenamiento donde se encuentra el fichero.	Cadena de caracteres

Tabla 17: campos del listado Búsqueda de información personal en los equipos

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Archivo	Nombre del fichero encontrado.	Cadena de caracteres

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se encontró el fichero.	Cadena de caracteres
Grupo	Grupo de Panda Adaptive Defense 360 al que pertenece el equipo.	Cadena de caracteres
Ruta	Ruta dentro del dispositivo de almacenamiento donde se encuentra el fichero.	Cadena de caracteres
DNIs	Indica si se detectó una o más entidades del tipo Documento Nacional de Identidad o equivalentes (Documento de identidad, Cédula de identidad / ciudadanía, Registro civil etc) en el fichero.	Booleano
Pasaportes	Indica si se detectó una o más entidades del tipo Pasaporte en el fichero.	Booleano
Tarjeta de crédito	Indica si se detectó una o más entidades del tipo Número de tarjeta de crédito en el fichero.	Booleano
Cuentas bancarias	Indica si se detectó una o más entidades del tipo Número de cuenta bancaria en el fichero.	Booleano
Permisos de conducir	Indica si se detectó una o más entidades del tipo Permiso de conducir en el fichero.	Booleano
Números de la Seguridad Social	Indica si se detectó una o más entidades del tipo Número de la seguridad social en el fichero.	Booleano
Direcciones de correo electrónico	Indica si se detectó una o más entidades del tipo Dirección de correo electrónico en el fichero.	Booleano
NIFs	Indica si se detectó una o más entidades del tipo Número de Identificación Fiscal en el fichero.	Booleano
IPs	Indica si se detectó una o más entidades del tipo Dirección IP en el fichero.	Booleano
Nombres y apellidos	Indica si se detectó una o más entidades del tipo Nombre y apellidos en el fichero.	Booleano
Direcciones	Indica si se detectó una o más entidades del tipo Dirección en el fichero.	Booleano
Códigos postales	Indica si se detectó una o más entidades del tipo Código postal en el fichero.	Booleano
Números de teléfono	Indica si se detectó una o más entidades de tipo Número de teléfono en el fichero.	Booleano

Tabla 18: campos del fichero exportado Búsqueda de información personal en los equipos

12.6.5 Sintaxis de las búsquedas

Panda Data Control permite búsquedas flexibles de ficheros por contenido utilizando texto plano y modificadores para acotar el ámbito de los resultados. El resultado del proceso de indexación almacena el contenido textual del fichero en un formato normalizado que debe ser tenido en cuenta a la hora de generar búsquedas por contenido.

Sintaxis admitida en búsquedas rápidas

- **Palabra**: busca "palabra" en el contenido del documento y en los metadatos.
- **PalabraA PalabraB**: busca "palabraa" o "palabrab" (operador OR) en el contenido del documento.
- **"PalabraA PalabraB"**: busca "palabraa" y "palabrab" seguidas en el contenido del documento.
- **+PalabraA +PalabraB**: busca "palabraa" y "palabrab" en el contenido del documento.
- **+Palabraa -Palabrab**: busca "palabraa" y no "palabrab" en el contenido del documento.
- **Palabra***: busca todas las palabras que empiezan por "palabra". El carácter "*" solo se permite al final de la cadena de caracteres a buscar.
- **Pa?abra**: busca todas las palabras que empiezan por "pa", terminan por "abra" y tienen entre los dos grupos un único carácter alfabético. El carácter "?" puede ir colocando en cualquier punto de la cadena de caracteres a buscar.
- **Palabra~**: busca todas las palabras que contienen la cadena de caracteres "palabra".

Sintaxis admitida en búsquedas guiadas

En las búsquedas guiadas no se utilizan los caracteres "+" y "-". En su lugar las palabras a buscar se distribuyen en las diferentes cajas de texto presentadas en la pantalla. Si utilizas los caracteres "+" y "-" éstos formarán parte de la búsqueda.

Entidades disponibles

Para acotar el ámbito de los resultados **Panda Data Control** admite el uso de calificadores para indicar entidades o características del fichero en las búsquedas rápidas y avanzadas. Los calificadores disponibles son:

- **PiiType**: especifica si un tipo de entidad fue detectada en el fichero.
- **HasPii**: indica que el fichero contiene entidades detectadas.
- **Filename**: indica el nombre del fichero.
- **FileExtension**: indica la extensión del fichero.

Los valores admitidos para los calificadores son:

- **PiiType:BANKACCOUNT**: ficheros que contienen una o más entidades de tipo Cuenta bancaria.
- **PiiType:CREDITCARD**: ficheros que contienen una o más entidades de tipo Tarjeta de crédito.
- **PiiType:IDCARD**: ficheros que contienen una o más entidades de tipo Documento de

identidad (documento nacional de identidad, Cédula de identidad / ciudadanía, Registro civil etc.).

- **PiiType:SSN**: ficheros que contienen una o más entidades de tipo Número de la seguridad social.
- **PiiType:IP**: ficheros que contienen una o más entidades de tipo Dirección IP.
- **PiiType:EMAIL**: ficheros que contienen una o más entidades de tipo Dirección de correo electrónico.
- **PiiType:PHONE**: ficheros que contienen una o más entidades de tipo Teléfono
- **PiiType:ADDRESS**: ficheros que contienen una o más entidades de tipo Dirección.
- **PiiType:FULLNAME**: ficheros que contienen una o más entidades de tipo Nombre y apellidos
- **PiiType:PASSPORT**: ficheros que contienen una o más entidades de tipo Número de pasaporte
- **PiiType:DRIVERLIC**: ficheros que contienen una o más entidades de tipo Numero de licencia / permiso de conducción.
- **HasPii:True**: ficheros que contienen alguna entidad detectada.
- **Filename**:"nombre del fichero": ficheros que tienen como nombre la cadena indicada.
- **Fileextension**: "extensión del fichero": ficheros que tienen como extensión la cadena indicada.

Sintaxis de las búsquedas con entidades

Las entidades se pueden utilizar en todos los tipos de búsqueda (rápida o guiada) de forma individual o combinadas con otras cadenas de caracteres.

- **PiiType:IDCARD**: busca todos los ficheros con alguna entidad detectada de tipo Documento de identidad.
- **+PiiType:IDCARD +"Panda Security"**: busca el fichero que contiene el listado de documentos de identidad (con alguna detección de entidad IDCARD) de la empresa (que contenta la cadena de caracteres "Panda Security").
- **+Filename:analisis* +fileextension:docx -PiiType:fullname**: busca todos los ficheros de análisis (su nombre empieza por la palabra "análisis") en formato Word (extensión docx) y no están firmados (no se detectó ninguna entidad de tipo Fullname – Nombre y apellidos.)

12.6.6 Proceso de normalización y búsqueda de cadenas

Los datos extraídos de los ficheros encontrados en el equipo del usuario se almacenan en una base de datos en el propio equipo tras aplicar un proceso de normalización. Este proceso varía si **Panda Data Control** considera el dato como una entidad PII o un texto sin identificar.

El proceso de normalización afecta de forma directa a las búsquedas, ya que se compara ésta con los datos almacenados después de sufrir el proceso de normalización. Es decir, la búsqueda se ejecuta sobre los datos normalizados y no sobre los datos originales contenidos en los ficheros del usuario.

Caracteres de separación

Panda Data Control emplea un grupo de caracteres especiales que considera como separadores entre palabras y que puede retirar completamente o sustituir por un único espacio. El grupo de caracteres es el siguiente:

- Retorno de carro: \r
- Salto de línea: \n
- Tabulador: \t
- Caracteres: " : ; ! ? - + _ * = ( ) [ ] { } , . | % \ / ’

Transformación de las cadenas indexadas a minúsculas

Independientemente de que la cadena de caracteres sea reconocida como una entidad o no, antes de almacenarla en la base de datos se transforma a minúsculas. Las búsquedas del administrador también son transformadas a minúsculas, con lo que escribir en mayúsculas o minúsculas no afecta al resultado de la búsqueda.

Reglas generales para normalizar los datos reconocidos como una entidad

- En las entidades formadas por caracteres numéricos (teléfonos, números de cuentas bancarias etc.) se elimina el conjunto de caracteres separadores y se almacena la cadena resultante como una única entidad. Por ejemplo “1.42.67.116-C” se almacena como la entidad de tipo IDCARD “14267116C”.
- Las entidades de tipo Dirección IP y Correo electrónico se almacenan tal cual.
- En las entidades Nombre y Apellidos y Dirección cada palabra se almacena de forma independiente y se eliminan las que contengan números. Por ejemplo “Calle Santiago de Compostela 5 1º Izquierda” se almacenará como “calle”, “santiago”, “de”, “compostela”, “izquierda”.

Reglas generales para normalizar los datos no reconocidos como una entidad

- Los datos numéricos y alfanuméricos (palabras formadas por letras y números) que no sean detectadas como una entidad son eliminados en el proceso de normalización, y por lo tanto su búsqueda no devuelve ningún resultado.
- Cada carácter de separación encontrado divide la cadena de caracteres en dos palabras independientes e impide el almacenamiento del carácter separador. Por ejemplo la cadena “casa.bosque” se almacena como “casa” y “bosque” y el carácter separador “.” se descarta.

Consejos para construir búsquedas compatibles con el proceso de normalización

- Utiliza preferiblemente letras en minúsculas.
- Los caracteres numéricos que forman parte de cadenas que no son identificados como una entidad compatible con **Panda Data Control** se eliminan en el proceso de normalización, y por tanto no deben ser incluidos en las búsquedas.
- Para buscar **números de cuentas bancarias, números de tarjetas de crédito, números de identidad, números de la seguridad social, números de pasaporte, números de permiso** elimina los caracteres de separación.
- Para buscar **direcciones IP** y **direcciones de correo electrónico** introdúcelas tal cual.

- Para buscar **números de teléfono** elimina los caracteres de separación, introduciendo el código del país si es necesario sin el signo "+".
- Para buscar **direcciones físicas, nombres y apellidos** elimina los caracteres numéricos.

12.7. Extensiones de programas soportados por Panda Data Control

Nombre de la suite	Producto	Extensiones
Office	Word	• DOC • DOT • DOCX • DOCM • RTF
	Excel	• XLS • XLSM • XLSX • XLSB
	PowerPoint	• PPT • PPS • PPSX • PPSM • SLDX • SLDM • POTX • PPTM • PPTX • POTM
OpenOffice	Writer	• ODM • ODT • OTT • OXT • STW • SXG • SXW
	Draw	• ODG • OTG • STD
	Math	• ODF • SXM
	Base	• ODB

Nombre de la suite	Producto	Extensiones
	Impress	• OTP • ODP • STI • SXI
	Calc	• OTS • ODS • SXC
Texto plano		TXT
Navegadores web	• Internet Explorer • Chrome • Opera • Otros	• HTM • HTML • MHT • OTH
Cliente de correo	• Outlook • Outlook Express	EML
Otros	Adobe Acrobat Reader	PDF
	Extensible Markup Language	XML
	Contribute	STC
	ArcGIS Desktop	SXD

Tabla 19: listado de extensiones de programas soportadas

12.8. Empaquetadores y algoritmos de compresión soportados

Nombre del compresor / empaquetador / algoritmo	Extensiones
7-ZIP	.7z
bzip2	.bz2
gzip	.gz
Binhex	.hqx
LHARC	.lha .lzh

Nombre del compresor / empaquetador / algoritmo	Extensiones
Lempel-Ziv & Haruyasu	.lzh
Lempel–Ziv–Oberhumer / lzop	.lzo
Multi-Purpose Internet Mail	.mme
Lotus Notes Traveler	.nts
Winrar	.rar
Tar	.tar
Tar & Gzip	.tgz
Uuencode	.uu .uue
XXEncoding	.xx .xxe
PkZip / PKWare	.zip

Tabla 20: listado de extensiones de empaquetadores / compresores soportados

13. Panda Patch Management (Actualización de programas vulnerables)

13.1. Introducción

Panda Patch Management es un módulo integrado en la plataforma Aether que localiza los equipos de la red que contienen software con vulnerabilidades conocidas, y los actualiza de forma automática y centralizada. De esta forma minimiza la superficie de ataque, evitando que el malware aproveche fallos del software instalado en los equipos de los usuarios y servidores para infectarlos.

Panda Patch Management es compatible con sistemas operativos Windows y detecta aplicaciones de terceros pendientes de actualizar o en EoL (End of Life), así como los parches y actualizaciones publicados por Microsoft para todos sus productos (sistemas operativos, bases de datos, suites ofimáticas etc).

Los equipos Windows XP SP3 y Windows server 2003 SP2 requieren un equipo con el rol de caché / repositorio instalado en el mismo segmento de red para poder reportar y e instalar los parches pendientes. Un equipo Windows XP SP3 o Windows server 2003 SP2 con el rol de cache / repositorio asignado tampoco podrá descargar parches.

Toda la funcionalidad de **Panda Patch Management** se concentra en los puntos de la consola de administración mostrados a continuación:

- **Configuración del descubrimiento de parches a aplicar**: a través del perfil de configuración **Gestión de parches**, accesible desde el panel lateral en el menú superior **Configuración**.
- **Visibilidad del estado de actualización del parque IT**: mediante widgets en un panel de control independiente, accesible desde el menú superior **Estado**, panel lateral **Gestión de parches**.
- **Listados de parches pendientes de aplicar**: desde los listados **Estado de gestión de parches**, **Parches disponibles** y **Programas "End of Life"** accesibles desde el menú superior **Estado**, panel lateral **Mis listados, Añadir**.
- **Histórico de parches instalados**: desde el listado **Historial de instalaciones**, accesible desde el menú superior **Estado**, panel lateral **Mis listados, Añadir.**
- **Parcheo de equipos**: desde el menú superior **Tareas** y creando una tarea programada de tipo **Instalar parches**. También se pueden parchear los equipos desde los menús de contexto del árbol de grupos en el menú superior **Equipos,** de los listados y desde **Detalle de equipo**.

13.2. Flujo general de trabajo

Panda Patch Management es una herramienta integral que gestiona el parcheo y actualización de los sistemas operativos y programas instalados en los equipos de la red. Para conseguir reducir de forma eficiente la superficie de ataque de los equipos, es necesario seguir los pasos mostrados a continuación:

- Comprobar que **Panda Patch Management** funciona correctamente en los equipos instalados.
- Comprobar que los parches publicados están instalados.
- Instalar los parches seleccionados.
- Comprobar que los programas instalados en los equipos no han entrado en EoL.
- Comprobar puntualmente el histórico de instalaciones de parches y actualizaciones.
- Comprobar puntualmente el estado del parcheo de equipos con incidencias.

13.2.1 Comprueba que Panda Patch Management funciona correctamente

Sigue los pasos mostrados a continuación:

- Comprueba que los equipos de la red tienen una licencia asignada de **Panda Patch Management** y que el módulo está instalado y en funcionamiento. Utiliza el widget **Estado de gestión de parches**.
- Comprueba que los equipos con una licencia de **Panda Patch Management** asignada se comunican con la nube de Panda Security. Utiliza el widget **Tiempo desde la última comprobación.**
- Comprueba que los equipos donde se instalarán los parches tienen el servicio Windows Update en ejecución con las actualizaciones automáticas desactivadas.

Se recomienda desactivar las actualizaciones automáticas de la configuración del servicio Windows Update para que Panda Patch Management pueda decidir cuándo se producirán, de lo contrario, el servicio de actualizaciones de Windows se solapará con el ofrecido por Panda Patch Management. Independientemente de la configuración del servicio, para ciertos parches de Microsoft se requiere que Windows Update esté en funcionamiento.

13.2.2 Comprueba que los parches publicados están instalados

Los parches y actualizaciones se publican de forma constante según los proveedores del software instalado en la red detectan vulnerabilidades y las corrigen. Estos parches tienen asociada una criticidad y un tipo.

- Para obtener una visión general de los parches pendientes de instalar según su tipo y criticidad utiliza el widget **Criticidad de los parches**.
- Para ver los parches pendientes de instalación en un equipo o grupo de equipos:
  - En el árbol de equipos (menú superior **Equipos**, pestaña **Carpeta** en el panel lateral) haz clic en el menú de contexto de un grupo que contenga equipos Windows y selecciona **Visualizar parches disponibles**. Se mostrará el listado **Parches disponibles** filtrado por el grupo

    ó

  - en el panel de equipos (menú superior **Equipos**, panel derecho) haz clic en el menú de contexto de un equipo y selecciona **Visualizar parches disponibles**. Se mostrará el listado **Parches disponibles** filtrado por el equipo.

- Para obtener una visión global detallada de los parches pendientes de instalar:
  - En el menú superior **Estado** haz clic en el panel lateral **Mis listados, Añadir** y selecciona el listado **Parches disponibles**.
  - Utiliza la herramienta de filtrado para acotar la búsqueda.
- Para buscar los equipos que no tienen instalado un parche concreto:
  - En el menú superior **Estado** haz clic en el panel lateral **Mis listados, Añadir** y selecciona el listado **Parches disponibles**.
  - Utiliza la herramienta de filtrado para acotar la búsqueda.
  - Haz clic en el menú de contexto del equipo – parche a buscar y selecciona el menú **Visualizar equipos** con el parche disponible para su instalación.

13.2.3 Instala los parches

Los parches y actualizaciones se instalan mediante tareas rápidas o programadas. Las tareas rápidas instalan el parche en tiempo real pero no reinician el equipo del usuario, aunque sea requisito para completar la instalación. Las tareas programadas permiten configurar los parámetros de la actualización de parches. Consulta el capítulo 15 Tareas para obtener información general sobre las Tareas en **Panda Adaptive Defense 360**.

Aunque la consola de administración es una herramienta muy flexible que permite instalar los parches de múltiples maneras, de una forma general se siguen las siguientes estrategias:

- Para instalar uno o varios parches concretos utiliza el listado **Parches disponibles** y configura la herramienta de filtrado.
- Para instalar todos los parches de un tipo o criticidad, utiliza las tareas inmediatas o programadas.
- Para instalar parches en equipos concretos o en un grupo utiliza el Árbol de grupos.

A continuación, se indican las combinaciones posibles de parches y destinos, y se describen los pasos a ejecutar en cada una de ellas.

Destino / parche	Uno o varios parches específicos	Uno, varios o todos los tipos de parches
Uno o varios equipos	Listado Parches disponibles (1)	Tareas (1)
Un grupo	Listado Parches disponibles (2)	Tareas (2)
Varios o todos los grupos	Listado Parches disponibles (3)	Tareas (3)

Tabla 21: instalación de parches según el destino y el conjunto de parches instalado

Listado Parches disponibles (1)

Para instalar uno o más parches concretos en uno o varios equipos:

- En el menú superior **Estado** haz clic en el panel lateral **Mis listados Añadir** y selecciona el listado **Parches disponibles**.
- Utiliza la herramienta de filtrado para acotar la búsqueda.
- Haz clic en las casillas de selección de los equipos – parches a instalar y selecciona **Instalar** en la barra de acciones para crear una tarea rápida o **Programar instalación** para crear una tarea programada.

Tareas (1)

Para instalar uno varios o todos los tipos de parches en uno o varios equipos:

- En el menú superior **Equipos**, pestaña **Carpetas** del árbol de equipos (panel izquierdo) haz clic en el grupo al que pertenecen los equipos. Si los equipos pertenecen a varios grupos haz clic en el grupo raíz Todos.
- Haz clic en las casillas de selección de los equipos que recibirán el grupo de parches
- En la barra de acciones haz clic en **Programar la instalación de parches**
- Configura la tarea, haz clic en el botón **Guardar** y publícala.

Listado Parches disponibles (2)

Para instalar un parche concreto en un grupo de equipos:

- En el menú superior **Equipos**, pestaña **Carpetas** del árbol de equipos (panel izquierdo) haz clic en el menú de contexto del grupo.
- Haz clic en el menú **Visualizar parches disponibles**. Se mostrará el listado **Parches disponibles** filtrado por el grupo.
- Utiliza el campo **Parche** de la herramienta de filtrado para listar únicamente el parche a instalar.
- Selecciona todos los equipos del listado con las casillas de selección.
- Haz clic en **Instalar** en la barra de acciones para crear una tarea rápida o **Programar instalación** para crear una tarea programada.

Para instalar varios parches concretos en un grupo de equipos repite el punto anterior tantas veces como parches se quieran instalar.

Tareas (2)

Para instalar uno, varios o todos los tipos de parches en un grupo de equipos:

- En el menú superior **Equipos**, pestaña **Carpetas** del árbol de equipos (panel izquierdo) haz clic en el menú de contexto del grupo.
- Haz clic en el menú **Programar instalación de parches**. Se mostrará la ventana de la tarea.
- Configura la tarea con el tipo o tipos de parches que se instalarán en el grupo, haz clic en el botón **Guardar** y publícala.

Listado Parches disponibles (3)

Para instalar un parche concreto en varios grupos de equipos:

- En el menú superior **Estado** haz clic en el panel lateral **Mis listados Añadir** y selecciona el listado **Parches disponibles**.
- Utiliza la herramienta de filtrado para acotar la búsqueda del parche.

- Haz clic en una casilla del parche a instalar y selecciona **Programar instalación** para crear una tarea.
- Haz clic en el menú superior **Tareas** y edita la tarea creada en el punto anterior.
- En el campo **Destinatarios** añade los grupos que recibirán el parche en **Grupos de equipos** y elimina los **Equipos Adicionales**.
- Haz clic en **Atrás**, configura la tarea y haz clic en **Guardar**.
- Publica la tarea.

Para instalar varios parches concretos en varios grupos de equipos repite el apartado anterior tantas veces como parches tengas que instalar.

Tareas (3)

Para instalar uno, varios o todos los tipos de parches en varios o todos los grupos de equipos:

- En el menú superior haz clic en **Tareas**, haz clic en **Añadir tarea** y selecciona **Instalar parches**.
- Establece el campo **Destinatarios** para determinar los equipos y grupos que recibirán la tarea de instalación
- Establece los parches a instalar para determinar el tipo de parche que se instalará.
- Haz clic en **Guardar** y publica la tarea.

13.2.4 Comprueba que los programas no han entrado en EoL.

Los programas que han entrado en EoL no reciben ningún tipo de actualización por parte de los proveedores de software, de forma que se recomienda sustituirlos por alternativas equivalentes o por versiones más avanzadas.

Para localizar los programas en EOL:

- Haz clic en el menú superior **Estado**, panel lateral **Mis listados, Añadir.**
- Selecciona el listado **Programas "End of Life".**

El listado contiene una entrada por cada par equipo – programa en EoL.

13.2.5 Comprueba el histórico de instalaciones de parches y actualizaciones

Para determinar si un parche concreto está instalado en los equipos de la red:

- Haz clic en el menú superior **Estado**, panel lateral **Mis listados, Añadir.**
- Selecciona el listado **Historial de instalaciones.**

El listado contiene una entrada por cada par equipo – parche instalado, junto con información sobre su nombre, versión, programa o sistema operativo al que afecta y criticidad / tipo del parche.

13.2.6 Comprueba el nivel de parcheo de los equipos con incidencias

Consulta el capítulo 16 Visibilidad del malware y del parque informático para más información sobre las herramientas de visibilidad de la seguridad del parque administrado.

Panda Adaptive Defense 360 relaciona los equipos que tienen incidencias detectadas con su nivel de parcheo, de forma que es posible determinar si un equipo infectado o con amenazas detectadas tiene o no aplicados todos los parches que se han publicado.

Para ver si un equipo con una incidencia detectada tiene parches pendientes de instalación

- En el menú superior **Estado**, widgets **Actividad del malware, Actividad de PUPs, Actividad de Exploits, Programas actualmente bloqueados en clasificación y Amenazas detectadas por el antivirus** haz clic en una amenaza - equipo. Se mostrará la información de la amenaza detectada en el equipo.
- En la sección **Equipo afectado** haz clic en el botón **Visualizar parches disponibles**. Se mostrará el listado **Parches disponibles** filtrado por el equipo.
- Selecciona todos los parches disponibles para este equipo y haz clic en la barra de acciones **Instalar** para crear una tarea inmediata que parcheará el equipo.

Debido a que el proceso de parcheo puede implicar la descarga de parches desde la nube de Panda Security y por lo tanto retrasar su aplicación en el tiempo, se recomienda aislar el equipo de la red si el equipo ha sido infectado y muestra tráfico de red en su ciclo de vida. De esta forma se minimiza el riesgo de propagación de la infección en la red del cliente mientras el proceso de parcheo se completa. Consulta el capitulo 18 Análisis forense para obtener información sobre el ciclo de vida del malware. Consulta el capítulo 19 Herramientas de resolución para aislar un equipo de la red.

13.3. Configuración del descubrimiento de parches sin aplicar

Panda Patch Management mantiene un inventario de los parches y actualizaciones pendientes de instalación de todos los equipos de la red que tienen una licencia del módulo asignada y en funcionamiento.

Para configurar el descubrimiento de parches y actualizaciones:

- Haz clic en el menú superior **Configuración**, panel lateral **Gestión de parches.**
- Haz clic en el botón **Añadir** y completa la configuración con la información mostrada a continuación.
- Asigna la nueva configuración a los equipos de la red con una licencia **Panda Patch Management** activada.

13.3.1 Configuración general

Haz clic en el selector **Buscar parches automáticamente** para activar la búsqueda de parches. Si el selector no está activado los parches pendientes de instalación no se mostrarán en los listados, aunque las tareas de instalación de parches podrán aplicarlos de forma independiente.

13.3.2 Frecuencia de la búsqueda

Buscar parches con la siguiente frecuencia establece cada cuanto tiempo **Panda Patch Management** consulta los parches instalados en los equipos y los compara con las bases de datos de parches disponibles en la nube.

13.3.3 Criticidad de los parches

Establece la criticidad de los parches que **Panda Patch Management** busca en las bases de datos de parches disponibles en la nube.

La criticidad de cada parche está establecida por cada proveedor del software afectado por la vulnerabilidad. Este criterio de clasificación no es uniforme y se recomienda comprobar previamente la descripción del parche para aquellos que no estén clasificados como "criticos", con el objetivo de evitar su instalación si no se padecen los síntomas descritos.

13.4. Widget / paneles disponibles

A continuación, se detallan los distintos widgets implementados en el panel de control **Gestión de parches,** sus distintas áreas y zonas activas incorporadas y los tooltips y su significado.

13.4.1 Estado de gestión de parches

Muestra tanto los equipos donde **Panda Patch Management** está funcionando correctamente como aquellos con errores y problemas en la instalación o en la ejecución del módulo. El estado del módulo se representa mediante un círculo con distintos colores y contadores asociados. El panel representa en porcentaje y de forma gráfica los equipos que comparten un mismo estado.

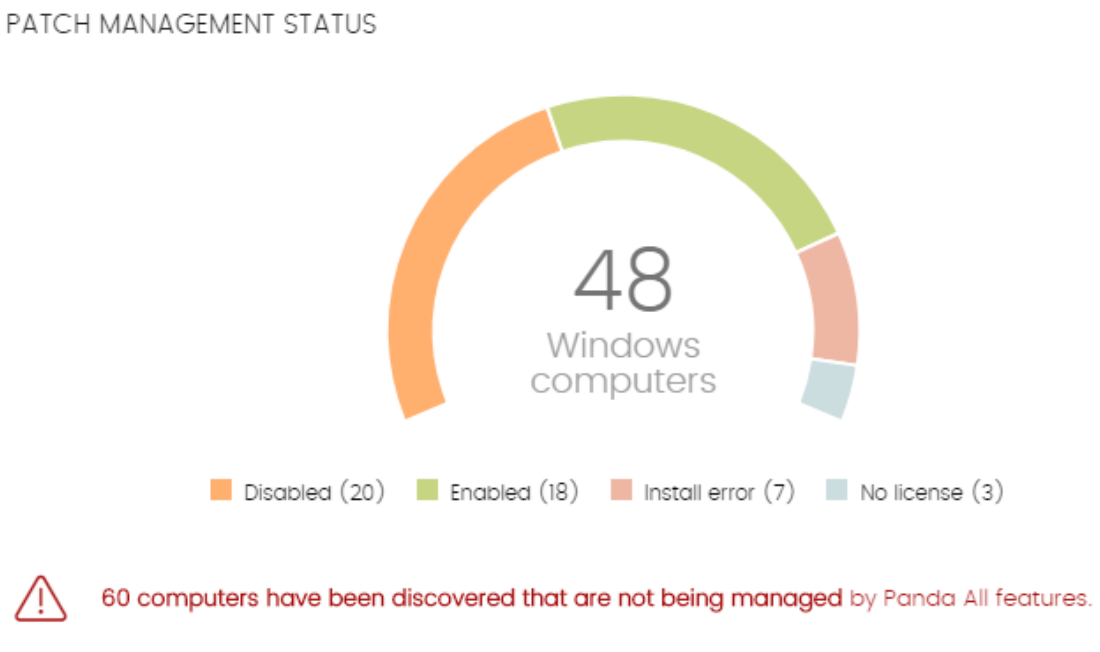


Figura 74: panel de Estado de gestión de parches

- **Significado de las series**

- **Activado**: indica el porcentaje de equipos en los que **Panda Patch Management** se instaló sin errores, su ejecución no presenta problemas y la configuración asignada permite buscar parches automáticamente.
- **Desactivado**: indica el porcentaje de equipos en los que **Panda Patch Management** se instaló sin errores, su ejecución no presenta problemas y la configuración asignada no permite buscar parches automáticamente.
- **Sin licencia**: equipos sin servicio de gestión de parches debido a que no se dispone de licencias suficientes, o no se les ha asignado una licencia disponible.
- **Error instalando**: indica los equipos donde el módulo no se pudo instalar.
- **Parte central**: refleja el número de total de equipos compatibles con el módulo **Panda Patch Management**.

- **Filtros pre establecidos desde el panel**

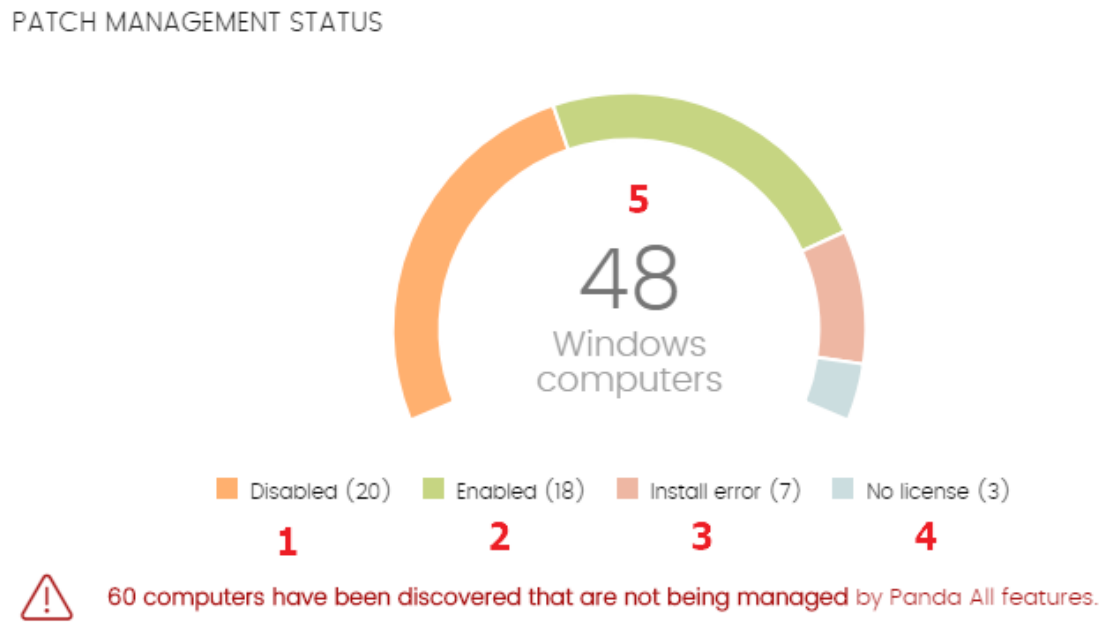


Figura 75: zonas activas del panel Estado de gestión de parches

El listado se muestra con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

- **(1)** Listado **Estado de gestión de parches** filtrado por **Estado de gestión de parches** = Desactivado
- **(2)** Listado **Estado de gestión de parches** filtrado por **Estado de gestión de parches** = Activado
- **(4)** Listado **Estado de gestión de parches** filtrado por **Estado de gestión de parches** = Sin licencia
- **(3)** Listado **Estado de gestión de parches** filtrado por **Estado de gestión de parches** = Error instalando
- **(5)** Listado **Estado de gestión de parches** sin filtrado

13.4.2 Tiempo desde la última comprobación

Figura 76: panel Tiempo desde la última comprobación

Muestra los equipos de la red que no han conectado con la nube de Panda Security en un determinado periodo de tiempo para comprobar su estado de parcheo. Estos equipos son

susceptibles de tener algún tipo de problema y requerirán una atención especial por parte del administrador.

- **Significado de las series**

- **72 horas**: número de equipos que no comprobaron su estado de parcheo en las últimas 72 horas.
- **7 días**: número de equipos que no comprobaron su estado de parcheo en las últimas 7 días.
- **30 días**: número de equipos que no comprobaron su estado de parcheo en los últimas 30 días.

- **Filtros pre establecidos desde el panel**

Figura 77: zonas activas del panel Tiempo desde la ultima comprobación

El listado se muestra con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

- **(1)** Listado **Estado de gestión de parches** filtrado por **Última comprobación** = Hace más de 3 días y **Estado de gestión de parches** = Activado y Desactivado.
- **(2)** Listado **Estado de gestión de parches** filtrado por **Última conexión** = Hace más de 7 días y **Estado de gestión de parches** = Activado y Desactivado.
- **(3)** Listado **Estado de gestión de parches** filtrado por **Última conexión** = Hace más de 30 días y **Estado de gestión de parches** = Activado y Desactivado.

13.4.3 Últimas tareas de instalación de parches

Muestra un listado de las últimas tareas de instalación de parches y actualizaciones creadas. Este widget está formado por varios enlaces que permiten gestionar las tareas de instalación de parches:

- Haz clic en una tarea para editar su configuración.
- Haz clic en el link **Ver todas** para acceder directamente al menú superior **Tareas** donde se muestran todas las tareas creadas.
- Haz clic en el link **Ver historial de instalaciones** para acceder al listado **Historial de instalaciones** con todas las tareas de instalación de parches terminadas con éxito o con error.

Figura 78: panel de Últimas tareas de instalación de parches

13.4.4 Criticidad de los parches

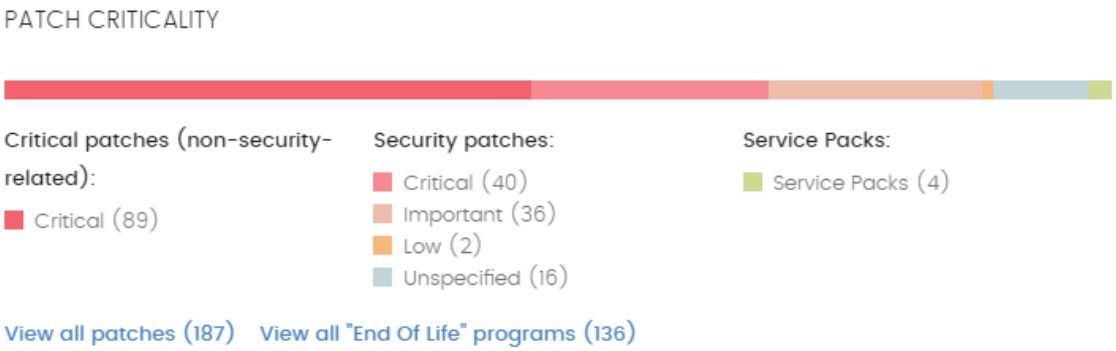


Figura 79: panel Criticidad de los parches

Muestra un recuento de parejas parche - equipo sin aplicar, distribuido por la categoría del parche. Cada parche no aplicado se contabiliza tantas veces como equipos no lo tengan instalado.

- **Significado de las series**

- **Parches críticos (no de seguridad) - Críticos**: número de parches clasificados como de importancia crítica, no relativos a la seguridad del sistema y que no han sido aplicados todavía.
- **Parches de seguridad - Críticos**: número de parches clasificados como de importancia crítica relativos a la seguridad del sistema y que no han sido aplicados todavía.
- **Parches críticos seguridad - Importantes**: número de parches clasificados de importancia relativos a la seguridad del sistema y que no han sido aplicados todavía.
- **Parches críticos de seguridad - Baja**: número de parches clasificados como de importancia baja relativos a la seguridad del sistema y que no han sido aplicados todavía.
- **Parches críticos de seguridad – No clasificados**: número de parches sin determinar su importancia relativos a la seguridad del sistema y que no han sido aplicados todavía.
- **Service Packs – Service Packs**: número de paquetes de parches y actualizaciones que no han sido aplicados todavía.
- **Ver todos los parches**: número de parches de cualquier importancia relativos o no a la seguridad del sistema y que no han sido aplicados todavía.

- **Ver todos los programas "End of Life"**: número de programas encontrados en los equipos que han dejado de mantenerse por sus respectivos proveedores.

- **Filtros pre establecidos desde el panel**

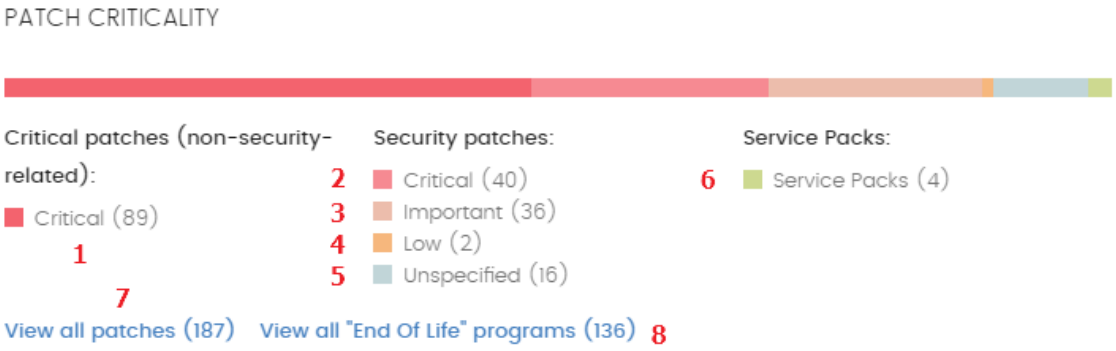


Figura 80: zonas activas del panel Criticidad de los parches

El listado se muestra con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

- **(1)** Listado **Parches disponibles** filtrado por **Criticidad** = Critica (no de seguridad).
- **(2)** Listado **Parches disponibles** filtrado por **Criticidad** = Critica (de seguridad).
- **(3)** Listado **Parches disponibles** filtrado por **Criticidad** = Importante (de seguridad).
- **(4)** Listado **Parches disponibles** filtrado por **Criticidad** = Baja (de seguridad).
- **(5)** Listado **Parches disponibles** filtrado por **Criticidad** = No clasificado (de seguridad).
- **(6)** Listado **Parches disponibles** filtrado por **Criticidad** = Service Pack.
- **(7)** Listado **Parches disponibles** sin filtros.
- **(8)** Listado **Programas "End of Life"** sin filtros.

13.5. Listados disponibles

13.5.1 Listado de Estado de gestión de parches

Este listado muestra en detalle todos los equipos de la red compatibles con **Panda Patch Management**, incorporando filtros que permiten localizar aquellos puestos de trabajo y servidores que no estén recibiendo el servicio por alguno de los conceptos mostrados en el panel asociado.

Campo	Comentario	Valores
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres

Campo	Comentario	Valores
Gestión de parches	Estado del módulo.	Activado Desactivado Error instalando (motivo del error) Sin licencia
Ultima comprobación	Fecha en la que Panda Patch Management consultó a la nube para comprobar si se han publicado nuevos parches.	Fecha
Ultima conexión	Fecha del ultimo envío del estado de Panda Adaptive Defense 360 a la nube de Panda Security.	Fecha

Tabla 22: campos del listado Estado de gestión de parches

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	Estación Portátil Dispositivo móvil Servidor
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Versión del agente		Cadena de caracteres
Fecha instalación	Fecha en la que el módulo Panda Patch Management se instaló con éxito en el equipo.	Fecha
Fecha de la última conexión	Fecha de la última vez que el agente se conectó con la nube de Panda Security	Fecha
Plataforma	Sistema operativo instalado en el equipo	Windows Linux macOS Android

Campo	Comentario	Valores
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado	Cadena de caracteres
Servidor Exchange	Versión del servidor de correo instalada en el servidor	Cadena de caracteres
Protección actualizada	Indica si el módulo de la protección instalado en el equipo es la última versión publicada	Booleano
Versión de la protección	Versión interna del módulo de protección	Cadena de caracteres
Fecha de última actualización	Fecha de la descarga del fichero de firmas	Fecha
Estado de gestión de parches	Estado del módulo.	Activado Desactivado Error instalando Sin licencia
Pendiente de reinicio	El equipo no se ha reiniciado para completar la instalación de uno o más parches descargados.	Binario
Fecha de la última comprobación	Fecha en la que Panda Patch Management consultó a la nube para comprobar si se han publicado nuevos parches.	Fecha
Estado de aislamiento	Indica si el equipo ha sido aislado de la red o se comunica con sus equipos vecinos de forma normal.	Aislado No aislado
Fecha error instalación	Fecha en la que se intentó la instalación del módulo Panda Patch Management y se produjo el error.	Fecha
Error instalación	Motivo del error de instalación-	Error en la descarga Error en la ejecución

Tabla 23: campos del fichero exportado Estado de gestión de parches

Herramienta de filtrado

Campo	Comentario	Valores
Tipo de equipo	Clase del dispositivo	Estación Portátil Servidor
Ultima comprobación	Fecha en la que Panda Patch Management consultó a la nube para comprobar si se han publicado nuevos parches.	Todos Hace más de 3 días Hace más de 7 días Hace más de 30 días
Ultima conexión	Fecha de la última vez que el agente se conectó con la nube de Panda Security	Fecha
Parches pendientes de reinicio	El equipo no se ha reiniciado para completar la instalación de uno o más descargados.	Booleano

Campo	Comentario	Valores
Estado de gestión de parches	Estado del módulo.	Activado Desactivado Error instalando Sin licencia

Tabla 24: campos de filtrado para el listado Estado de gestión de parches

13.5.2 Listado de Parches disponibles

Muestra el detalle de todos los parches sin instalar en los equipos de la red y publicados por Panda Security. Cada línea del listado refleja un par parche – equipo de la red.

Campo	Comentario	Valores
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo Windows con parches pendientes de aplicar.	Cadena de caracteres
Versión	Numero de versión del programa desactualizado.	Numérico
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc).	Cadena de caracteres
Criticidad	Importancia de la actualización y tipo.	Crítica (no de seguridad) Crítica (de seguridad) Importante (de seguridad) Moderada (de seguridad) Baja (de seguridad) No clasificado (de seguridad) Service Pack

Tabla 25: campos del listado Parches disponibles

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	Estación Portátil Dispositivo móvil Servidor
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres

Campo	Comentario	Valores
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo Windows con parches pendientes de aplicar.	Cadena de caracteres
Versión	Numero de versión del programa desactualizado.	Numérico
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc).	Cadena de caracteres
Criticidad	Importancia de la actualización y tipo.	Crítica (no de seguridad) Crítica (de seguridad) Importante (de seguridad) Moderada (de seguridad) Baja (de seguridad) No clasificado (de seguridad) Service Pack
CVEs	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Identificador KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y sus requisitos si los hubiera.	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación	Fecha
Ultima vez visto	Fecha en la que el equipo fue descubierto por última vez.	Fecha
Es descargable	Indica si el parche está disponible para su descarga o requiere un contrato adicional con el proveedor del software para acceder a aquel.	Booleano
Tamaño de la descarga (KB)	Tamaño del parche en formato comprimido. La aplicación de parches y actualizaciones puede requerir más espacio en el dispositivo de almacenamiento del equipo que el indicado en este campo.	Numérico

Tabla 26: campos del fichero exportado Parches disponibles

Herramienta de filtrado

Campo	Comentario	Valores
Tipo de equipo	Clase del dispositivo.	Estación Portátil Servidor
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo Windows con parches pendientes de aplicar.	Cadena de caracteres
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc)	Cadena de caracteres
CVE	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Criticidad	Indica la importancia de la actualización y tipo	Crítica (no de seguridad) Crítica (de seguridad) Importante (de seguridad) Moderada (de seguridad) Baja (de seguridad) No clasificado (de seguridad) Service Pack
Mostrar parches no descargables	Indica los parches disponibles para su descarga o los que requieren un contrato adicional con el proveedor del software para acceder a aquel.	Booleano

Tabla 27: campos de filtrado para el listado Parches disponibles

13.5.3 Listado de Programas End of Life

Muestra los programas que ya no tienen soporte por parte de sus proveedores y que por tanto son un objetivo especialmente vulnerable para el malware y las amenazas.

Campo	Comentario	Valores
Equipo	Nombre del equipo con software en EoL.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa en EoL.	Cadena de caracteres
Versión	Versión del programa en EoL	Cadena de caracteres

Campo	Comentario	Valores
EOL	Fecha en la que el programa entró en EoL	Fecha

Tabla 28: campos del listado Programas EoL

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	Estación Portátil Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa en EoL.	Cadena de caracteres
Versión	Versión del programa en EoL	Cadena de caracteres
EoL	Fecha en la que el programa entró en EoL	Fecha
Ultima vez visto	Fecha en la que el equipo fue descubierto por última vez.	Fecha

Tabla 29: campos del fichero exportado Programas EoL

Herramienta de filtrado

Campo	Comentario	Valores
Buscar equipo	Nombre del equipo	Cadena de caracteres

Tabla 30: campos de filtrado para el listado Programas EoL

13.5.4 Listado de Historial de instalaciones

Muestra los parches que **Panda Adaptive Defense 360** intentó instalar y los equipos que los recibieron en un intervalo determinado.

Campo	Comentario	Valores
Fecha	Fecha en la que se instaló el parche o actualización.	Fecha
Equipo	Nombre del equipo que recibió el parche o actualización.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa o versión del sistema operativo Windows que recibió el parche.	Cadena de caracteres
Versión	Versión del programa o sistema operativo que recibió el parche.	Cadena de caracteres
Parche	Nombre del parche instalado.	
Criticidad	Importancia del parche instalado.	Crítica (no de seguridad) Crítica (de seguridad) Importante (de seguridad) Moderada (de seguridad) Baja (de seguridad) No clasificado (de seguridad) Service Pack
Instalación	Estado de la instalación del parche o actualización.	Instalado Pendiente de reinicio Error

Tabla 31: campos del listado Historial de instalaciones

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	Estación Portátil Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Fecha	Ultima fecha de intento de instalación.	Fecha

Campo	Comentario	Valores
Programa	Nombre del programa o versión del sistema operativo Windows que recibió el parche.	Cadena de caracteres
Versión	Versión del programa o sistema operativo que recibió el parche.	Cadena de caracteres
Parche	Nombre del parche instalado.	Cadena de caracteres
Criticidad	Importancia del parche instalado.	Crítica (no de seguridad) Crítica (de seguridad) Importante (de seguridad) Moderada (de seguridad) Baja (de seguridad) No clasificado (de seguridad) Service Pack
CVEs (Common Vulnerabilities and Exposures)	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Identificador de KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y sus requisitos si los hubiera.	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación	Fecha
Instalación	Estado de la instalación del parche o actualización	Instalado Pendiente de reinicio Error
Error de instalación	El módulo de Panda Patch Management no se instaló correctamente	Imposible realizar la descarga: Instalador no disponible Imposible realizar la descarga: Fichero corrupto Espacio insuficiente en disco
URL de descarga	URL para descargar el parche de forma individual	Cadena de caracteres

Tabla 32: campos del fichero exportado Historial de instalaciones

Herramienta de filtrado

Campo	Comentario	Valores
Tipo de equipo	Clase del dispositivo	Estación Portátil Servidor
Buscar equipo	Nombre del equipo	Cadena de caracteres

Campo	Comentario	Valores
Desde	Fecha de inicio para el intervalo de búsqueda.	Fecha
Hasta	Fecha de finalización para el intervalo de búsqueda.	Fecha
Criticidad	Importancia del parche instalado.	Crítica (no de seguridad) Crítica (de seguridad) Importante (de seguridad) Moderada (de seguridad) Baja (de seguridad) No clasificado (de seguridad) Service Pack
Instalación	Estado de la instalación del parche o actualización.	Instalado Pendiente de reinicio Error
CVE	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres

Tabla 33: campos de filtrado para el listado Historial de instalaciones

13.6. Descarga e instalación de parches

Para instalar los parches y actualizaciones **Panda Patch Management** utiliza la infraestructura de tareas implementada en **Panda Adaptive Defense 360**.

La instalación de parches publicados por Microsoft no se completará con éxito si el servicio Windows Update esta deshabilitado en el equipo del usuario o servidor.

13.6.1 Instalación de parches

Para favorecer la velocidad de configuración a la hora de parchear equipos, las tareas de parcheo se pueden generan con algunos, todos o ningún parámetro preconfigurado, dependiendo del lugar en la consola de administración desde donde se creen:

- Desde el menú superior **Tareas**.
- Desde el listado **Parches disponibles**.
- Desde el Árbol de carpetas.
- Desde el Panel de equipos.

Los parámetros de configuración que se pueden preconfigurar son:

- **Destinos**: equipos que recibirán el parche o grupo de parches. Grupos y puestos de usuario o servidores.

- **Parches**: actualizaciones específicas a instalar.
- **Tipo de tarea**: inmediata o programada.

Menú superior Tareas

Permite crear tareas desde cero, sin especificar de antemano los parches a instalar o los equipos que recibirán las tareas de instalación.

Para crear una tarea de instalación de parches:

- En el menú superior **Tareas** haz clic en el botón **Añadir tarea** y elige **Instalar parche.**
- En el campo **Destinatarios** selecciona los grupos y equipos que recibirán la tarea.
- Establece la programación de la tarea. Consulta el capítulo 15 Tareas para más información.
- Determina los parches a instalar según su tipo. Al crear una tarea desde cero no se permiten especificar parches individuales.
- Establece las opciones de reinicio en el caso de que sea un requisito reiniciar el puesto de trabajo o servidor para completar la instalación del parche:
  - **No reiniciar automáticamente**: al terminar la tarea de instalación de parches se le muestra al usuario del equipo una ventana con las opciones **Reiniciar ahora** y **Recordar más tarde**. En caso de elegir ésta última, se volverá a mostrar a las 24 horas siguientes.
  - **Reiniciar automáticamente solo las estaciones de trabajo**: al terminar la tarea de instalación de parches se muestra al usuario del equipo una ventana con las opciones **Reiniciar ahora**, **Botón de minimizar** y **Cuenta atrás de 4 horas**. Cada 30 minutos se maximizará la pantalla como recordatorio de la proximidad del reinicio. Cuando falte menos de una hora para el reinicio el botón de minimizar se deshabilitará. Cuando la cuenta atrás se haya completado el equipo se reiniciará automáticamente.
  - **Reiniciar automáticamente solo los servidores**: el comportamiento es idéntico a la opción **Reiniciar automáticamente solo las estaciones de trabajo**.
  - **Reiniciar automáticamente tanto las estaciones de trabajo como los servidores**: el comportamiento es idéntico a la opción **Reiniciar automáticamente solo las estaciones de trabajo.**
- Haz clic en el botón **Guardar** y publica la tarea.

Listado Parches disponibles

Permite crear tareas con parches concretos a instalar y equipos preconfigurados.

Para crear una tarea de instalación de parches desde el listado de parches disponibles:

- En el menú superior **Estado** haz clic en el panel lateral mis listados, añadir y selecciona Parches disponibles
- Selecciona los pares parche – equipo que recibirán la actualización.
- Si has seleccionado varios parches, en la barra de acciones elige **Instalar** (tarea inmediata) o **Programar instalación** (tarea programable) para instalar los parches.
  - Las tareas inmediatas se publican de forma automática

- Las tareas programas programadas no se publican de forma inmediata y pueden requerir algún cambio en su configuración. Haz clic en el menú superior Tareas para editarlas y publicarlas.

- Si has seleccionado un único par parche – equipo puedes utilizar el menú de contexto del equipo para **Instalar** o **Programar instalación**.

Árbol de carpetas

Permite crear tareas con un grupo de equipos preconfigurados. Las tareas creadas serán siempre de tipo programado.

Para crear una tarea programada de instalación de parches desde el Árbol de carpetas:

- En el menú superior **Equipos** haz clic en el menú de contexto del grupo de equipos que recibirá la tarea programada de instalación de parches.
- Selecciona **Programar instalación de parches**.
- Haz clic en el menú superior **Tareas** y edita la tarea para configurar el tipo de parches que se van a instalar.
- Haz clic en el botón **Guardar** y publica la tarea.

Panel de equipos

Permite crear tareas con equipos específicos. Las tareas creadas serán siempre de tipo programado.

Para crear una tarea programada de instalación de parches desde el panel de equipos:

- En el menú superior **Equipos** haz clic en el grupo al que pertenecen los equipos que recibirán la tarea programada de instalación de parches.
- En el panel de la derecha establece con las casillas de selección los equipos que recibirán la tarea de instalación de parches.
- Selecciona **Programar instalación de parches** en la barra de acciones. Si los parches solo serán recibidos por un único puesto de usuario o servidor puedes utilizar el menú contextual del equipo.
- Haz clic en el menú superior **Tareas** y edita la tarea para configurar el tipo de parches que se van a instalar.
- Haz clic en el botón **Guardar** y publica la tarea.

13.6.2 Descarga de parches y ahorro de ancho de banda

Antes de la instalación de un parche es necesaria su descarga desde la nube de Panda Security. Esta descarga se produce de forma transparente e independiente en cada equipo cuando la tarea de instalación se lanza. Para minimizar el ancho de banda consumido se puede aprovechar la infraestructura de nodos cache / repositorios instalada en la red del cliente.

No es posible la descarga de parches ni actualizaciones a través de un nodo con el rol proxy asignado. Si el equipo o nodo con el rol de cache / repositorio no tiene acceso directo a la nube de Panda o

indirecto a través de un proxy corporativo, no se descargará ningún parche ni actualización. Consulta el capítulo 22 Control y supervisión de la consola de administración para más información sobre los roles de Panda Adaptive Defense 360.

Los nodos cache / repositorio almacenan los parches durante periodo de máximo de 30 días; transcurrido el cual los parches se eliminarán. Si un equipo solicita a un nodo caché la descarga de un parche y éste no lo tiene en su repositorio el equipo dará un tiempo al nodo caché para que descargue el parche. Este tiempo depende del tamaño del parche a descargar. Si no es posible la descarga, el equipo la iniciará de forma directa.

Una vez aplicados los parches en los equipos, éstos se borrarán del medio de almacenamiento del equipo.

13.6.3 Secuenciación de tareas de instalación

Las tareas de instalación de parches pueden requerir la descarga de parches desde la nube de Panda Security si los nodos con el rol de cache / repositorio no tienen almacenados los parches. En este escenario, las tareas inmediatas inician la descarga de los parches necesarios en el momento en que se crean, de forma que puede darse un alto consumo de ancho de banda si estas tareas afectan a muchos equipos o el volumen de la descarga es alto.

Las tareas programadas de instalación de parches comienzan la descarga de parches en el momento en que así está marcado en su configuración, pero si varias tareas coinciden en el punto de inicio se introduce un retardo aleatorio de hasta un máximo de 2 minutos para evitar el solapamiento de descargas y minimizar hasta cierto punto el consumo de ancho de banda.

14. Actualización del Software

Actualización del motor de protección
Actualización del agente de comunicaciones
Actualización del conocimiento

14.1. Introducción

Panda Adaptive Defense 360 es un servicio cloud gestionado y por lo tanto el cliente no necesita ejecutar tareas de actualización de la infraestructura de back-end encargada de soportar el servicio de protección; sin embargo, sí es necesaria la actualización del software instalado en los equipos de la red del cliente.

Los elementos instalados en el equipo del usuario son tres:

- Agente de comunicaciones **Aether Platform**
- Motor de la protección **Panda Adaptive Defense 360**
- Archivo de identificadores / fichero de firmas para la protección antivirus tradicional

Dependiendo de la plataforma a actualizar, el procedimiento y las posibilidades de configuración varían tal y como se indica en la Tabla 34:

Módulo	Plataforma			
	Windows	macOS	Linux	Android
Agente Panda	Bajo demanda			
Protección Panda Adaptive Defense 360	Configurable	Configurable	Configurable	No
Archivo de identificadores	Habilitar / Deshabilitar	Habilitar / Deshabilitar	Habilitar / Deshabilitar	No

Tabla 34: tipos de actualización por plataforma y módulo

- **Bajo demanda:** el administrador puede iniciar la actualización una vez que esté disponible, pudiendo de esta forma retrasarla hasta el momento que considere oportuno.
- **Configurable**: el administrador podrá definir ventanas de actualización recurrentes y en el futuro mediante la consola, siendo posible además desactivar la actualización.
- **Habilitar / Deshabilitar**: El administrador puede desactivar la actualización. Si la actualización está activada ésta se producirá automáticamente cuando esté disponible.
- **No**: El administrador no puede influir en el proceso de actualización. Las actualizaciones se efectuarán cuando estén disponibles y no es posible deshabilitarlas.

14.2. Configuración de la actualización del motor de protección

La configuración de la actualización del motor de protección **Panda Adaptive Defense 360** se realiza creando y asignando un perfil de configuración de tipo ajustes por equipo, accesible desde el menú superior **Configuración**, en el panel de la izquierda de la consola de administración.

14.2.1 Actualizaciones

Para habilitar la actualización automática del módulo de protección **Panda Adaptive Defense 360** haz clic en el botón de activación **Actualizar automáticamente Aether en los dispositivos.** Esta acción habilitará el resto de configuraciones de la página. Si esta opción esta deshabilitada, el módulo de protección no se actualizará nunca.

Se desaconseja totalmente deshabilitar la actualización del motor de protección. Los equipos con la protección sin actualizar serán más vulnerables en el medio plazo frente a las amenazas avanzadas y el malware.

Aplicar actualizaciones en rangos de horas

Indica los siguientes parámetros para que los equipos apliquen las actualizaciones disponibles dentro de un rango de horas concreto:

- Hora de inicio
- Hora de fin

Para aplicar las actualizaciones en cualquier momento haz clic en la casilla de selección **A cualquier hora.**

Aplicar actualizaciones en fechas determinadas

Utiliza el desplegable para indicar las fechas en las que la actualización se aplicará:

- **En cualquier fecha**: las actualizaciones se aplicarán el día que estén disponibles. Esta opción no limita la actualización de **Panda Adaptive Defense 360** a fechas concretas.
- **Los siguientes días de la semana**: utiliza las casillas de selección para establecer los días de la semana en los que **Panda Adaptive Defense 360** se actualizará. La actualización se producirá el primer día de la semana que coincida con la selección del administrador en caso de haber una actualización disponible.
- **Los siguientes días del mes**: utiliza los desplegables para establecer un rango de días hábiles dentro del mes en los que **Panda Adaptive Defense 360** se actualizará. La actualización se producirá el primer día del mes que coincida con los seleccionados por el administrador en caso de haber una actualización disponible.
- **Los siguientes días**: utiliza los desplegables para establecer un rango de días hábiles dentro del calendario en los que **Panda Adaptive Defense 360** se actualizará. Los rangos definidos en esta opción se establecen de forma absoluta para casos en que el administrador quiera establecer rangos que no se repiten en el tiempo. De esta forma, se permite definir rangos de fechas concretas de actualización, pasadas las cuales dejan de tener efecto. Este método requiere redefinir los rangos de actualización de forma constante una vez hayan vencido.

Reinicio de equipos

Panda Adaptive Defense 360 permite definir la lógica de reinicios en caso de que sea necesario, mediante el desplegable situado al final de la pantalla de configuración:

- **No reiniciar automáticamente**: se mostrará al usuario una ventana en intervalos de tiempo cada vez más cortos, aconsejando el reinicio de la máquina para aplicar la actualización.
- **Reiniciar automáticamente sólo las estaciones de trabajo**
- **Reiniciar automáticamente sólo los servidores**
- **Reiniciar automáticamente tanto estaciones de trabajo como servidores**

14.3. Configuración de la actualización del agente de comunicaciones

La actualización del agente Panda se realiza bajo demanda. **Panda Adaptive Defense 360** incluirá una notificación en la consola de administración indicando la disponibilidad de una nueva versión disponible del agente, y el administrador podrá lanzar la actualización cuando lo desee.

La actualización del agente Panda no requiere reinicio del equipo del usuario y suele implicar cambios y mejoras en la consola de administración que facilitan la gestión de la seguridad.

14.4. Configuración de la actualización del conocimiento

La configuración de la actualización del fichero de firmas en **Panda Adaptive Defense 360** se realiza en el perfil de configuración de seguridad asignado al equipo, según sea su tipo.

14.4.1 Dispositivos Windows, Linux y Mac

La configuración se realiza en los perfiles de tipo **Estaciones y Servidores**, accesibles desde el panel de la izquierda en el menú superior **Configuración**.

En la pestaña **General** las opciones disponibles son:

- **Actualizaciones automáticas de conocimiento**: Permite habilitar o deshabilitar la descarga del fichero de firmas. Si se deshabilita el fichero de firmas nunca será actualizado.

Se desaconseja totalmente deshabilitar la actualización del conocimiento. Los equipos con la protección sin actualizar serán más vulnerables en el corto plazo frente a las amenazas avanzadas y el malware.

- **Realizar un análisis en segundo plano cada vez que se actualice el conocimiento**: permite lanzar de forma automática un análisis cada vez que un fichero de firmas se descargue en el equipo. El análisis tendrá prioridad mínima para no interferir en el trabajo del usuario.

14.4.2 Dispositivos Android

La configuración se realiza en los perfiles **Dispositivos Android**, accesibles desde el panel de la izquierda en el menú superior **Configuración**.

Panda Adaptive Defense 360 permite limitar las actualizaciones del Software de forma que no consuman datos de conexiones móviles sujetas a tarificación.

Haz clic en el botón de activación para restringir las actualizaciones a aquellos momentos en que el smartphone o tablet tenga conexión wifi disponible.

15. Tareas

15.1. Introducción

Una tarea es un recurso implementado en **Panda Adaptive Defense 360** que permite enlazar un proceso a dos variables adicionales: repetición y aplazamiento de la acción.

- **Repetición**: una tarea se puede configurar para su ejecución de forma puntual, o repetida a lo largo del tiempo.
- **Aplazamiento**: una tarea se puede configurar para ser ejecutada en el momento en que se crea (tarea inmediata), o aplazada en el tiempo (tarea programada).

15.1.1 Proceso general de lanzamiento de una tarea

El proceso de lanzamiento de una tarea se divide en tres pasos, mostrados a continuación.

- **Creación y configuración de la tarea:** se determinan los equipos afectados, las características de la tarea, el momento en que será lanzada, el número de veces que se ejecutará y el comportamiento en caso de error.
- **Publicación de la tarea una vez creada:** las tareas creadas se introducen en el programador de tareas de **Panda Adaptive Defense 360** para ser lanzadas en el momento marcado por su configuración.
- **Ejecución de la tarea** cuando se alcancen las condiciones especificadas en su definición.

15.2. Creación de tareas

Dependiendo de la necesidad de configurar todos los parámetros de una tarea, ésta se puede establecer desde varios puntos dentro de la consola:

- Zona de Tareas
- Árbol de equipos
- Zona Equipos
- Listados

El recurso principal para crear una tarea es la zona **Tareas** del menú superior de la consola. En esta ventana se definen las tareas desde cero, controlando todos los aspectos del proceso (destinatarios, aplazamiento, repetición, publicación etc.)

La zona **Equipos,** el Árbol de equipos y los listados permiten programar y lanzar tareas de forma ágil, sin necesidad de pasar por todo el proceso de configuración y publicación de la tarea, si bien se pierde algo de flexibilidad en su definición.

15.3. Creación de tareas desde la zona Tareas

Para crear una nueva tarea, desde el menú superior haz clic en **Tareas**. Accederás a una ventana donde están listadas todas las tareas creadas, indicando su estado. Para crear una tarea nueva haz clic en el botón **Añadir** y elige el tipo de tarea en el desplegable; se mostrará una ventana con los datos de la tarea, distribuidos en tres zonas:

- **Información general**: nombre de la tarea y descripción.
- **Destinatarios**: equipos que recibirán la tarea.
- **Programación**: configuración del momento en que se lanzará la tarea.

15.3.1 Destinatarios de la tarea

- Haz clic en el link **Destinatarios de la tarea** para abrir una nueva ventana donde seleccionar los equipos que recibirán la tarea configurada.
- Haz clic en el botón  para agregar un nuevo equipo y en el botón  para eliminar los equipos seleccionados.

Para acceder a la ventana de selección de equipos es necesario salvar previamente la tarea.

15.3.2 Programación horaria y repetición de la tarea

La programación horaria se especifica mediante tres parámetros:

- **Empieza**: marca el comienzo de la tarea.
- **Tiempo máximo de ejecución**: indica el tiempo máximo que la tarea puede tardar en completarse, vencido el cual se cancelará con error si no ha terminado.
- **Repetir**: establece cada cuanto tiempo la tarea se vuelve a activar, tomando como referencia la fecha marcad en **Empieza.**

Empieza

- **Lo antes posible (activado)**: la tarea se lanza en el momento si el equipo está disponible (encendido y accesible desde la nube), o en el momento en que se encuentre disponible dentro del margen definido en el desplegable **Equipo apagado**.
- **Lo antes posible (desactivado)**: la tarea se lanza en la fecha seleccionada en el calendario, indicando si se tiene en cuenta la hora del equipo o la hora del servidor **Panda Adaptive Defense 360.**
- **Equipo apagado**: si el equipo está apagado o inaccesible, la tarea no se podrá lanzar. El sistema de programación de tareas permite establecer la caducidad de la tarea, retrasar el lanzamiento un intervalo de tiempo definido por el usuario, desde 0 (la tarea caduca de forma inmediata si el equipo no está disponible) a infinitivo (la tarea siempre está activa y se espera a que el equipo esté disponible de forma indefinida).
  - **No ejecutar**: la tarea se cancela si en el momento del lanzamiento el equipo no está encendido.
  - **Dar un margen de**: permite definir un intervalo de tiempo dentro del cual, si el equipo

inicialmente no estaba disponible y vuelve a estarlo, la tarea será lanzada.

- **Ejecutar cuando encienda:** no establece ningún intervalo de tiempo, se espera de forma indefinida a que el equipo esté accesible para lanzar la tarea.

Tiempo máximo de ejecución

- **Sin límite**: la duración de la ejecución de la tarea no está definida, pudiéndose extenderse hasta el infinito.
- **1,2, 8 o 24 horas**: la duración de la ejecución de la tarea está acotada. Transcurrido el tiempo indicado, la tarea se cancela con error si no ha terminado previamente.
- **Repetir**: establece un intervalo de repetición cada día, semana mes o año tomando como referencia la fecha indicada en **Empieza.**

15.3.3 Publicación de tareas

Una vez creada y configurada, la tarea aparecerá en el listado de tareas configuradas, pero no quedará activada hasta su publicación.

Haz clic en el botón **Publicar ahora** para publicar una tarea e introducirla en el programador de tareas de **Panda Adaptive Defense 360**, el cual marcará el momento en que se lanzará la tarea según su configuración.

15.4. Gestión de tareas

Haz clic en el menú superior **Tareas** para listar, borrar, copiar, cancelar o visualizar los resultados de las tareas creadas.

15.4.1 Listado de tareas creadas

Este listado muestra en detalle todas las tareas creadas, su tipo, estado y otra información relevante.

Campo	Comentario	Valores
Icono	Tipo de la tarea	 Tarea de tiempo instalación de paches  Tarea de tipo análisis bajo demanda
Nombre	Nombre de la tarea creada	Cadena de caracteres
Fecha	Fecha de creación de la tarea	Fecha

Tabla 35: campos del listado Estado de protección de los equipos

Herramienta de filtrado

Campo	Comentario	Valores
Tipo de tarea	Clase de la tarea	Análisis Desinfección Programación de parches
Buscar tarea	Nombre de la tarea	Cadena de caracteres
Programación	Frecuencia de la repetición de la tarea	Todos Inmediata Una vez Programada
Ordenar listado	Criterio de ordenación de las tareas creadas.	Ordenar por fecha de creación Ordenar por nombre Ascendente Descendente

Tabla 36: campos de filtrado para el listado Estado de protección de los equipos

15.4.2 Modificación de tareas publicadas

Haciendo clic en el nombre de la tarea creada se mostrará la ventana de configuración de la tarea, donde es posible modificar cualquier parámetro de la misma.

Las tareas publicadas solo admiten cambio de nombre y de descripción. Para modificar una tarea publicada es necesario copiarla.

Cancelación de las tareas publicadas

Para cancelar una tarea ya publicada haz clic en el link **Cancelar**. La tarea se cancelará, aunque no se borrará de la ventana de tareas para poder acceder a sus resultados.

Borrado de tareas

Las tareas ejecutadas no se eliminan automáticamente, para ello es necesario hacer clic en el icono  .

Al borrar una tarea se borrarán también sus resultados.

Copia de tareas

Haciendo clic en el icono  de una tarea se creará una nueva con su misma configuración.

Ver los resultados de una tarea

Una tarea publicada permite mostrar los resultados obtenidos hasta el momento haciendo clic en el link **Ver resultados**. Se abrirá una ventana con los resultados y una serie de filtros que permiten localizar los datos importantes de forma fácil.

Los campos de la tabla de tareas se muestran en la Tabla 37:

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se registró la tarea.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo	Cadena de caracteres
Estado	**Pendiente**: la tarea se intentó iniciar, pero la máquina no estaba disponible en ese momento. Se establece un periodo de espera según su configuración **En progreso**: la tarea se está realizando en este momento **Con éxito**: la tarea terminó con éxito **Fallida**: la tarea terminó con error **Expirada**: la tarea no llegó a comenzar por haber expirado el plazo configurado **Cancelada**: La tarea fue cancelada de forma manual	Cadena de caracteres
Fecha de comienzo	Fecha de inicio de la tarea.	Fecha
Fecha fin	Fecha de finalización de la tarea.	Fecha
Detecciones	Número de detecciones realizadas en el equipo	Numérico

Tabla 37: parámetros de filtrado sobre el resultado de tareas

Los filtros de búsqueda se muestran en la Tabla 38:

Campo	Comentario	Valores
Fecha	Desplegable con las fechas en las que la tarea pasó a estado activo según su programación configurada. Una tarea activa se puede lanzar en el momento o esperar a que la máquina esté disponible. Esta fecha se indica en la columna fecha	Fecha
Detecciones	Especifica si se muestran los equipos con alguna detección o los equipos limpios en la lista de tareas.	Binario
Estado	**Pendiente**: la tarea todavía no se ha iniciado por no haber alcanzado la ventana de ejecución configurada **En progreso**: la tarea se está ejecutando en este momento. **Con éxito**: la tarea terminó con éxito. **Con error**: la tarea terminó con error. Cancelada (no se puedo iniciar a la hora programada) **Cancelada:** la tarea fue cancelada de forma manual.	Enumeración

Tabla 38: filtros de búsqueda de tareas

Edición de tareas

Para editar una tarea creada o publicada haz clic en su nombre. Se mostrará la ventana de edición con los mismos campos que los incluidos en la ventana de creación de tareas.

Para visualizar un listado de todos los equipos que recibirán la tarea, haz clic en el botón **Ver equipos**. Se mostrará el listado de equipos de la zona **Equipos** con la acción y el tipo de tarea creada como filtro.

15.5. Actualización de los destinatarios en las tareas programadas

El conjunto de equipos sobre los que aplica una tarea puede ser difícil de determinar debido a dos factores:

- Los grupos son entidades de agrupación dinámicas, que pueden variar a lo largo del tiempo.
- Las tareas son acciones ejecutadas sobre grupos y definidas en un momento concreto, aunque su ejecución (repetida o no) se puede aplazar en el tiempo.

De esta manera una tarea sobre uno o varios grupos, definida en el momento T1, tiene como destinatarios los equipos que forman los grupos seleccionados, pero en el momento de ejecución T2, los miembros de esos grupos pueden haber cambiado.

A la hora de resolver los equipos que pertenecen a un grupo, se distinguen tres casos según el tipo de tarea:

- Tareas inmediatas
- Tareas programadas de ejecución única
- Tareas programadas de ejecución repetida

15.5.1 Tareas inmediatas

Estas tareas se crean, se publican y se lanzan de forma atómica una única vez. El grupo destinatario se evalúa en el momento en que el administrador crea la tarea. Los equipos afectados parecerán en estado **Pendiente** en la tarea.

Añadir equipos a la tarea

No se admite añadir nuevos equipos a la tarea. Aunque se asignen nuevos equipos al grupo destinatario, estos no recibirán la tarea.

Quitar equipos de la tarea

Sí se pueden retirar equipos de la tarea. Moviendo equipos del grupo destinatario de la tarea a otro grupo, éstos cancelarán la tarea.

15.5.2 Tareas programadas de ejecución única

Estas tareas admiten dos estados con respecto a la posibilidad de cambiar los integrantes del grupo de equipos destinatario:

Tareas cuya ejecución comenzó hace menos de 24 horas

En las primeras 24 horas de la ejecución de estas tareas, el administrador puede añadir o retirar equipos a la tarea o a los grupos destinatarios.

Se marca un plazo de 24 horas para abarcar todos los usos horarios en aquellas multinacionales con presencia en varios países.

Tareas cuya ejecución comenzó hace más de 24 horas.

Una vez cumplido el plazo de 24 horas, no es posible añadir nuevos equipos y, aunque se asignen nuevos equipos al grupo destinatario, éstos no recibirán la tarea. Sin embargo, es posible retirar equipos de la tarea, y mover equipos fuera del grupo destinatario cancelará las tareas en curso sobre estos equipos.

15.5.3 Tareas programadas de ejecución repetida

Estas tareas admiten agregar o eliminar equipos destinatarios en cualquier momento hasta su cancelación o finalización.

Las tareas programadas de ejecución repetida no muestran los equipos destinatarios en estado **Pendiente** de forma automática, sino que éstos se irán mostrando de forma progresiva a medida que la plataforma Aether reciba información del estado de la tarea de cada equipo.

16. Visibilidad del malware y del parque informático

Esquema general del menú Estado
Paneles y Widgets
Introducción a los listados
Listados disponibles
Listados incluidos por defecto

16.1. Introducción

Panda Adaptive Defense 360 le ofrece al administrador tres grandes grupos de herramientas para visualizar el estado de la seguridad y del parque informático que gestiona:

- El panel de control, con información actualizada en tiempo real.
- Listados personalizables de incidencias, malware detectado y dispositivos gestionados junto a su estado.
- Informes con información del estado del parque informático, recogida y consolidada a lo largo del tiempo.

> *Los informes consolidados se tratarán en el capítulo 21 Informes.*

Las herramientas de visualización y monitorización determinan en tiempo real el estado de la seguridad de la red y el impacto de las brechas de seguridad que se puedan producir para facilitar la adopción de las medidas de seguridad apropiadas.

16.2. Esquema general del menú Estado

El menú **Estado** reúne las principales herramientas de visibilidad y está formado por varias secciones, mostradas a continuación.

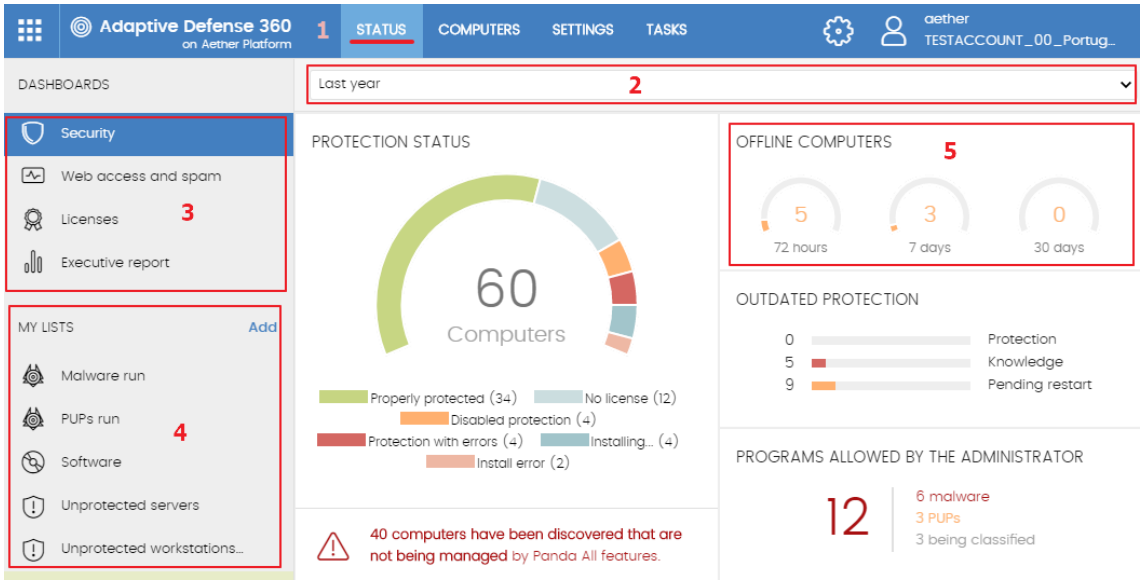


Figura 81: ventana de Estado con el panel de control y acceso a los listados

Acceso al panel de control (1)

El acceso al panel de control se realiza mediante el menú superior **Estado**. Desde el panel de control se acceden a los diferentes widgets, así como a los listados.

Los widgets o paneles gráficos representan aspectos concretos del parque de equipos gestionado, dejando a los listados la entrega de datos más detallados.

Selector del intervalo de tiempo (2)

El panel de control muestra la información relevante en el intervalo de tiempo fijado por el administrador mediante la herramienta situada en la parte superior de la ventana **Estado**. Los intervalos disponibles son:

- Últimas 24 h
- Últimos 7 días
- Último mes
- Último año

No todos los paneles soportan el filtrado de datos por el último año. Los paneles que no soporten este intervalo de tiempo mostrarán una leyenda en la parte superior indicándolo.

Selector de panel (3)

- **Seguridad**: estado de la seguridad del parque informático.
- **Accesos web y spam**: filtrado de la navegación y del correo no solicitado en servidores Microsoft Exchange.
- **Licencias:** consulta el capítulo 5 para obtener más información acerca de la gestión de licencias.
- **Informe ejecutivo:** consulta el capítulo 21 para obtener más información acerca de la configuración y generación de informes.

Este capítulo trata de los recursos contenidos en las secciones **Seguridad** y **Accesos web y spam**.

Mis listados (4)

Los listados son tablas de datos con la información presentada en los paneles. Esta información se presenta con gran nivel de detalle e implementa herramientas de búsqueda y distribución que ayudan a localizar los datos requeridos.

Paneles informativos / Widgets (5)

El panel de control está formado por widgets o paneles informativos centrados en un único aspecto de la seguridad de la red.

Los paneles se generan en tiempo real y son interactivos: pasando el ratón por encima de los elementos se muestran tooltips con información extendida.

Todas las gráficas incluyen una leyenda que permite determinar el significado de cada serie representada, e incorporan zonas activas que al ser seleccionadas abren distintos listados asociados al widget con filtros predefinidos.

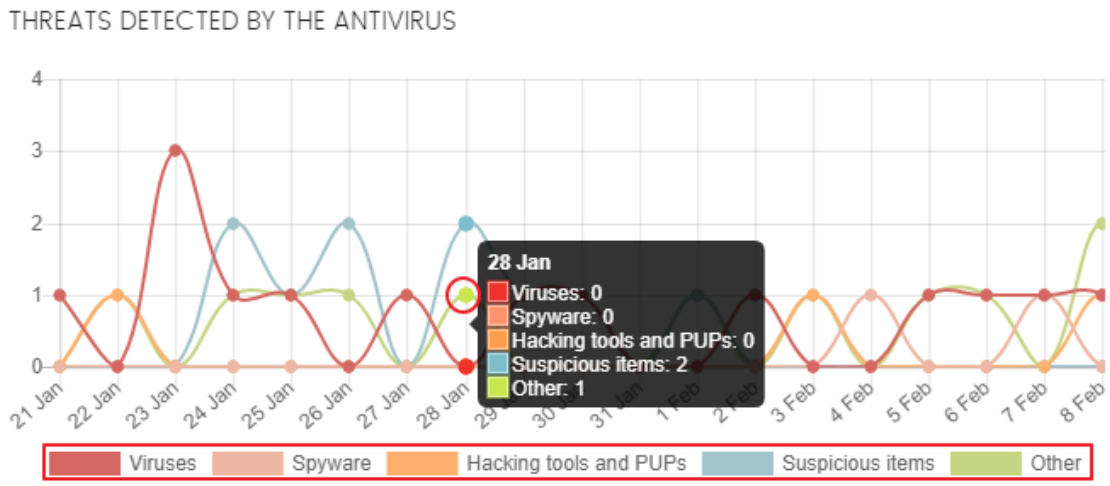


Figura 82: tooltips con información extendida y leyendas de las series representadas

Panda Adaptive Defense 360 utiliza varios tipos de gráficas para mostrar la información de la forma más conveniente según el tipo de dato representado:

- Gráficos de tarta
- Histogramas
- Gráficas de líneas

Haz clic en los elementos para mostrar listados con información detallada.

16.3. Paneles / Widgets disponibles

A continuación, se detallan los distintos widgets implementados en el dashboard de **Panda Adaptive Defense 360,** las distintas áreas y zonas activas incorporadas y los tooltips y su significado.

16.3.1 Estado de protección

Estado de protección muestra tanto los equipos donde **Panda Adaptive Defense 360** está funcionando correctamente como aquellos con errores y problemas en la instalación o en la ejecución del módulo de protección. El estado de los equipos es representado mediante un círculo con distintos colores y contadores asociados.

El panel representa en porcentaje y de forma gráfica los equipos que comparten un mismo estado.

La suma de los porcentajes de las diferentes series puede resultar más de un 100% debido a que los estados no son mutuamente excluyentes y un mismo equipo puede encontrarse en varias series a la vez.

Figura 83: panel de Estado de protección

- **Significado de las series**

- **Correctamente protegido**: indica el porcentaje de equipos en los que **Panda Adaptive Defense 360** se instaló sin errores y su ejecución no presenta problemas.
- **Instalando**: indica el porcentaje de equipos en los que **Panda Adaptive Defense 360** se encuentra en proceso de instalación.
- **Sin licencia**: los equipos sin licencia son aquellos a los que no se les está aplicando la protección debido a que no se dispone de licencias suficientes, o no se les ha asignado una licencia disponible.
- **Protección desactivada**: son equipos que no tienen activada la protección antivirus ni la protección avanzada, si ésta última se encuentra disponible para el sistema operativo del equipo en particular.
- **Protección con error**: incluye a todos los equipos con **Panda Adaptive Defense 360** instalado pero que, por alguna razón, el módulo de la protección no responde a las peticiones desde los servidores de Panda Security.
- **Error instalando**: indica los equipos cuya instalación no se pudo completar.
- **Parte central**: en la parte central del gráfico de tarta se indican los equipos desprotegidos del total de equipos vistos por **Panda Adaptive Defense 360**. Para que un equipo sea visible tiene que tener el agente Panda instalado.

- **Filtros pre establecidos desde el panel**

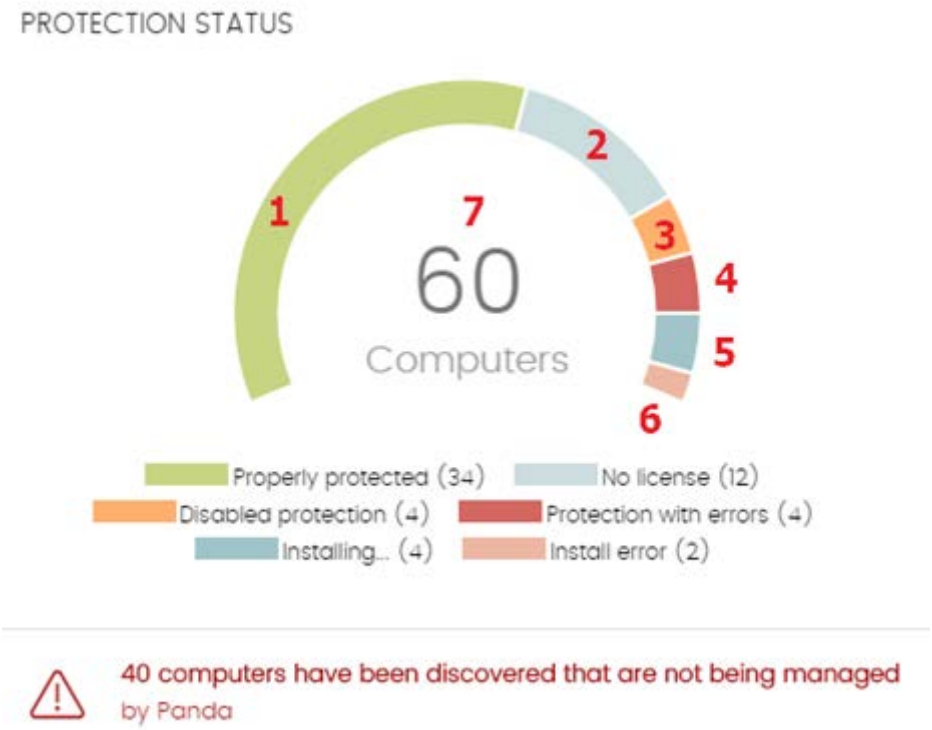


Figura 84: zonas activas del panel Equipos desprotegidos

El listado se muestra con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

- **(1)** Listado **Estado de protección de los equipos** filtrado por **Estado de protección** = Correctamente protegido
- **(2)** Listado **Estado de protección de los equipos** filtrado por **Estado de protección** = Instalando...
- **(3)** Listado **Estado de protección de los equipos** filtrado por **Estado de protección** = Protección desactivada
- **(4)** Listado **Estado de protección de los equipos** filtrado por **Estado de protección** = Protección con error
- **(5)** Listado **Estado de protección de los equipos** filtrado por **Estado de protección** = Sin licencia
- **(6)** Listado **Estado de protección de los equipos** filtrado por **Estado de protección** = Error instalando
- **(7)** Listado **Estado de protección de los equipos** sin filtros Equipos sin conexión

16.3.2 Equipos sin conexión

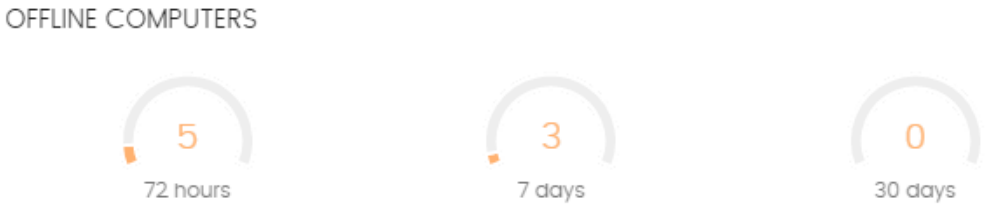


Figura 85: panel Equipos sin conexión

Equipos sin conexión muestra los equipos de la red que no han conectado con la nube de Panda Security en un determinado periodo de tiempo. Estos equipos son susceptibles de tener algún tipo de problema y requerirán una atención especial por parte del administrador.

- **Significado de las series**

- **72 horas**: número de equipos que no enviaron su estado en las últimas 72 horas.
- **7 días**: número de equipos que no enviaron su estado en las últimas 7 días.
- **30 días**: número de equipos que no enviaron su estado en las últimas 30 días.

- **Filtros pre establecidos desde el panel**

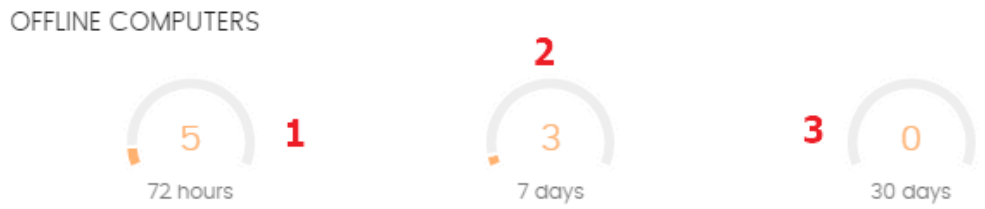


Figura 86: zonas activas del panel Equipos sin conexión

El listado se muestra con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

- **(1)** Listado **Equipos sin conexión** filtrado por **Última conexión** = Hace más de 72 horas
- **(2)** Listado **Equipos sin conexión** filtrado por **Última conexión** = Hace más de 7 días
- **(3)** Listado **Equipos sin conexión** filtrado por **Última conexión** = Hace más de 30 días

16.3.3 Protección desactualizada

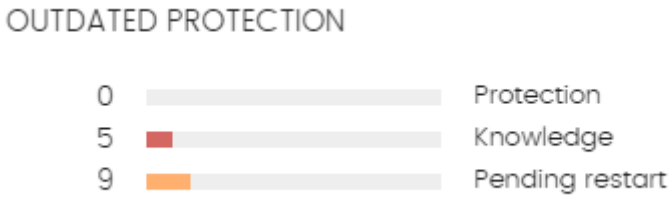


Figura 87: panel de Protección desactualizada

Protección desactualizada muestra los equipos cuya última versión del fichero de firmas instalada difiere en más de 3 días del fichero publicado por Panda Security. También muestra los equipos cuya versión del motor de protección difiere en más de 7 días del publicado por Panda Security. Por lo tanto, estos equipos pueden ser vulnerables frente a los ataques de amenazas.

- **Significado de las series**

El panel muestra el porcentaje y el número de equipos vulnerables por estar desactualizados, divididos en tres conceptos:

- **Protección**: desde hace 7 días el equipo tiene un motor de protección instalado anterior a la última versión publicada por Panda Security.
- **Conocimiento**: desde hace 3 días el equipo no se actualiza con el fichero de firmas publicado.
- **Pendiente de reinicio**: el equipo requiere un reinicio para completar la actualización.

- **Filtros pre establecidos desde el panel**

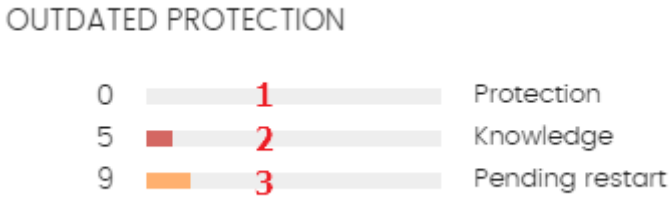


Figura 88: zonas activas de Protección desactualizada

El listado se muestra con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

- **(1)** Listado **Estado de protección de los equipos** filtrado por **Protección actualizada** = No
- **(2)** Listado **Estado de protección de los equipos** filtrado por **Conocimiento** = No
- **(3)** Listado **Estado de protección de los equipos** filtrado por **Protección actualizada** = Pendiente de reinicio

16.3.4 Programas actualmente bloqueados en clasificación

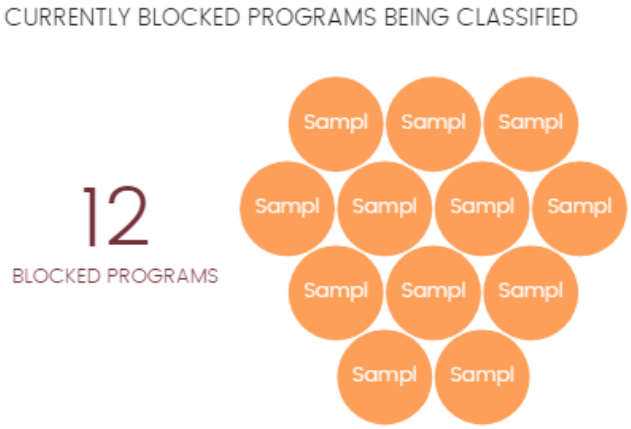


Figura 89: panel de Progamas actualmente bloqueados en clasificación

La información mostrada en **Programas Actualmente bloqueados en clasificación** es un histórico de los elementos bloqueados que aún no han sido clasificados. De esta forma, abarca desde la puesta en marcha del servicio en el cliente hasta el momento actual, y no se verá afectada por la selección del intervalo de tiempo establecida por el administrador.

En el panel de ejemplo se muestran un total de 12 elementos bloqueados en clasificación. Se trata de 12 aplicaciones que han sido bloqueadas y se están investigando. Cada una de ellas se representa con un círculo.

El número total de elementos bloqueados en clasificación representa las aplicaciones diferentes (distinto MD5) que están siendo bloqueadas. Este número es independiente de la cantidad de intentos de ejecución que cada aplicación bloqueada ha llevado a cabo en cada equipo de la red.

Cada versión encontrada del programa (distinto MD5) será mostrada de forma independiente.

El tamaño de las burbujas es una función del número de equipos donde se encontró el programa desconocido que fue bloqueado. De esta forma, un proceso que se ejecuta en muchos equipos tendrá asignada una única burbuja de gran tamaño, frente a un proceso que solo se ha ejecutado en un único equipo, que quedará representado con una burbuja más pequeña.

- **Significado de las series**

En el panel de control, las aplicaciones bloqueadas se muestran con el código de colores indicado a continuación:

- **Naranja**: para las aplicaciones con probabilidad media de ser malware.
- **Naranja oscuro**: para las aplicaciones con probabilidad alta de ser malware.
- **Rojo**: para las aplicaciones con probabilidad muy alta de ser malware.

Al pasar el ratón por encima, cada círculo se amplía, mostrando su nombre completo y una serie de iconos que representan acciones clave:

Figura 90: repreresentación gráfica de un programa en clasificación

- **Carpeta**: el programa ha leído datos del disco duro del usuario.
- **Bola del mundo**: el programa estableció una conexión con otro equipo.

- **Filtros pre establecidos desde el panel**

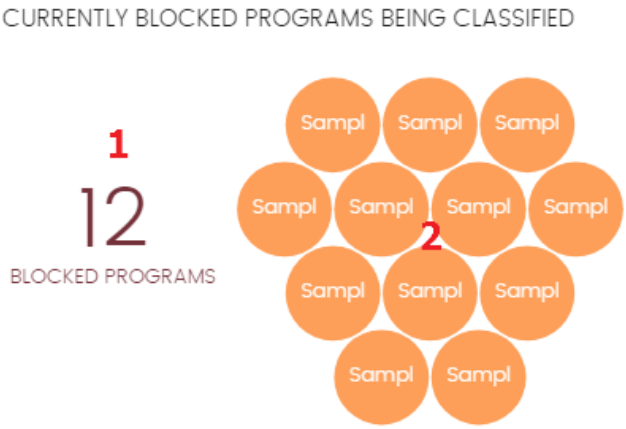


Figura 91: zonas activas del panel Programas actualmente bloqueados en clasificación

El listado se muestra con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

- **(1)** Listado **Programas actualmente bloqueados en clasificación** sin filtros
- **(2)** Listado **Programas actualmente bloqueados en clasificación** filtrado por **Buscar** = Hash

16.3.5 Programas permitidos por el administrador

Figura 92: panel Programas permitidos por el administrador

Panda Adaptive Defense 360 bloquea todos los programas clasificados como malware y, adicionalmente, dependiendo de la configuración de la protección avanzada, también bloqueará los programas no vistos anteriormente hasta que sean analizados y emitida una clasificación sobre su seguridad.

En el caso de que un usuario no pueda esperar a que se emita esta clasificación, o el administrador quiera permitir la ejecución de un elemento ya clasificado como amenaza, **Panda Adaptive Defense 360** implementa recursos para evitar estos bloqueos de ejecución.

Panda Adaptive Defense 360 permite la ejecución de todas las librerías y binarios utilizados en el programa permitido por el administrador, excepto aquellos ya conocidas y clasificadas como amenazas.

- **Significado de las series**

El panel representa el número total de elementos que el administrador excluyó del bloqueo, desagregados en tres conceptos:

- Malware
- PUP
- En clasificación

- **Filtros pre establecidos desde el panel**

Figura 93: zonas activas del panel Programas permitidos por el adminitrador

- **(1)** Listado **Programas permitidos por el administrador** sin filtros

- **(2)** Listado **Programas permitidos por el administrador** filtrado por **Clasificación actual** = malware
- **(3)** Listado **Programas permitidos por el administrador** filtrado por **Clasificación actual** = PUP
- **(4)** Listado **Programas permitidos por el administrador** filtrado por **Clasificación actual** = En clasificación (bloqueados y sospechosos)

16.3.6 Actividad del malware / PUP

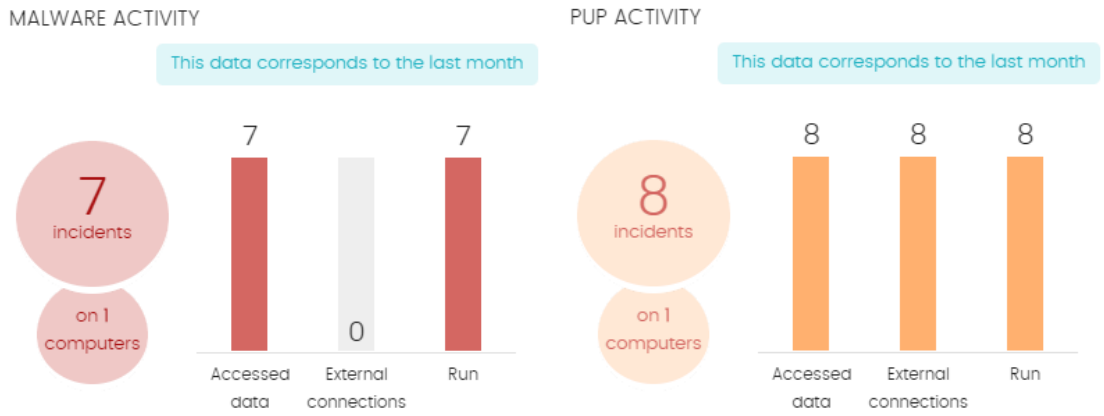


Figura 94: panel de Actividad del malware / PUP

Muestra las incidencias detectadas en los procesos ejecutados por los equipos de usuario y servidores Windows, así como en sus sistemas de ficheros. Estas incidencias son reportadas tanto por el análisis en tiempo real como por las tareas de análisis bajo demanda.

Panda Adaptive Defense 360 genera una incidencia en el panel Actividad de malware / PUP por cada pareja equipo – amenaza – tipo de amenaza distinta encontrada en la red. Si la causa original del aviso no es resuelta, se generarán un máximo de 2 incidencias cada 24 horas por cada equipo – amenaza encontrada que requiera la atención del administrador.

- **Significado de las series**

- **Número de incidencias / avisos en Número de equipos detectadas.**
- **Acceso a datos**: Número de avisos que incluyen uno o varios accesos a información del usuario contenida en el disco duro de su equipo.
- **Conexiones exteriores**: número de avisos que establecieron conexiones con otros equipos.
- **Ejecutado**: Número de muestras malware que se llegaron a ejecutar.

Actividad del malware, Actividad de PUPs y Actividad de exploits muestran datos con un intervalo máximo de 1 mes. En el caso de que el administrador establezca un periodo de tiempo mayor se mostrará un texto explicativo en la parte superior del panel.

- **Filtros pre establecidos desde el panel**

El listado se muestra con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

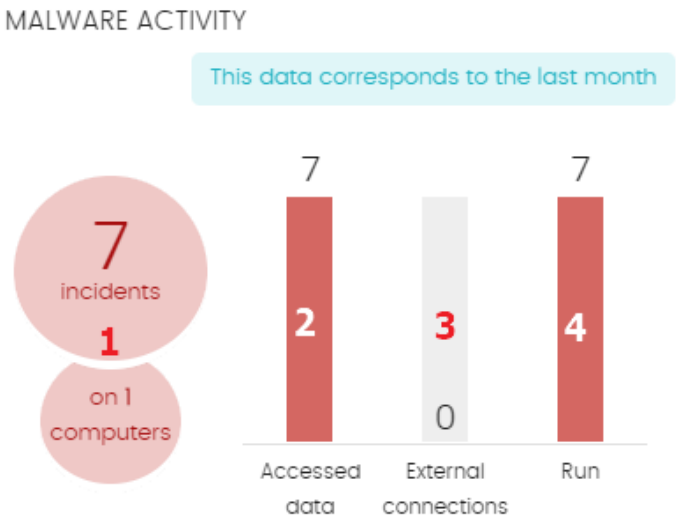


Figura 95: zonas activas del panel Actividad del malware / PUP

- **(1)** Listado **Actividad del malware** filtrado por **Tipo de amenaza** = (Malware O PUP)
- **(2)** Listado **Actividad del malware** filtrado por **Acceso a datos** = Verdadero
- **(3)** Listado **Actividad del malware** filtrado por **Conexiones externas** = Verdadero
- **(4)** Listado **Actividad del malware** filtrado por **Ejecutado** = Verdadero

16.3.7 Actividad de exploits

Figura 96: panel de Actividad de exploits

Actividad de exploits muestra el número de ataques por explotación de vulnerabilidades recibidos en los equipos Windows de la red. **Panda Adaptive Defense 360** genera una incidencia en el panel Actividad de exploits por cada pareja equipo –exploit distinto encontrada en la red. Si el ataque

se repite, se generarán un máximo de 10 incidencias cada 24 horas por cada equipo – exploit encontrado.

- **Significado de las series**

- **Número de incidencias / ataques en Número de equipos detectadas.**

- **Filtros pre establecidos desde el panel**

El listado **Actividad de exploits** se muestra sin filtros pre configurados al hacer clic en cualquier zona del widget.

16.3.8 Clasificación de todos los programas ejecutados y analizados

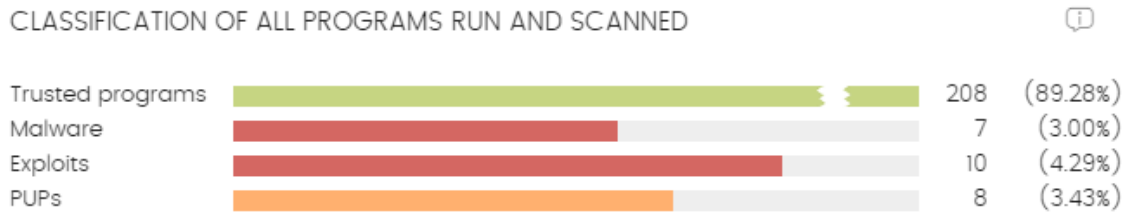


Figura 97: panel de Clasificación de todos los programas ejecutados y analizados

El objetivo de este panel es determinar de forma rápida el porcentaje de aplicaciones goodware y malware vistas y clasificadas en la red del cliente, para el intervalo de tiempo establecido por el administrador.

- **Significado de las series**

El panel consta de cuatro barras horizontales junto al número de eventos asociado y el porcentaje sobre el total.

> *Este panel muestra datos de elementos clasificados para todo el parque informático, y no solo de aquellos equipos sobre los cuales el administrador tenga permisos según sus credenciales de acceso a la consola. Los elementos no clasificados no se muestran en este panel.*

- **Aplicaciones confiables**: aplicaciones vistas en el parque del cliente que han sido analizadas y su clasificación ha sido goodware.
- **Aplicaciones maliciosas:** programas que han intentado ejecutarse o han sido analizados en el parque del cliente, y han sido clasificadas como malware o ataques dirigidos.

- **Exploits**: número de intentos de explotación de aplicaciones detectados en la red.
- **Aplicaciones potencialmente no deseadas** programas que han intentado ejecutarse o han sido analizados en el parque del cliente, y han sido clasificadas como malware de tipo PUP.

- **Filtros pre establecidos desde el panel**

El listado se muestra con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

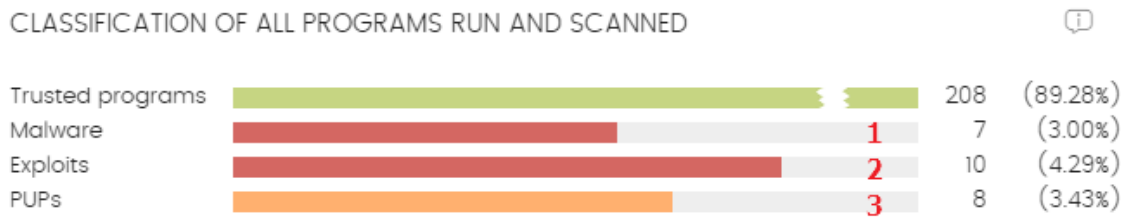


Figura 98: zonas activas del panel Clasificación de todos los programas ejecutados y analizados

Haz clic en las barras de **Maliciosos**, **Exploit** y **PUPs** para mostrar un listado asociado al tipo de información:

- **(1)** Listado **Actividad del malware** sin filtros preconfigurados
- **(2)** Listado **Actividad de exploit** sin filtros preconfigurados
- **(3)** Listado **Actividad de PUPs** sin filtros preconfigurados

16.3.9 Amenazas detectadas por el antivirus

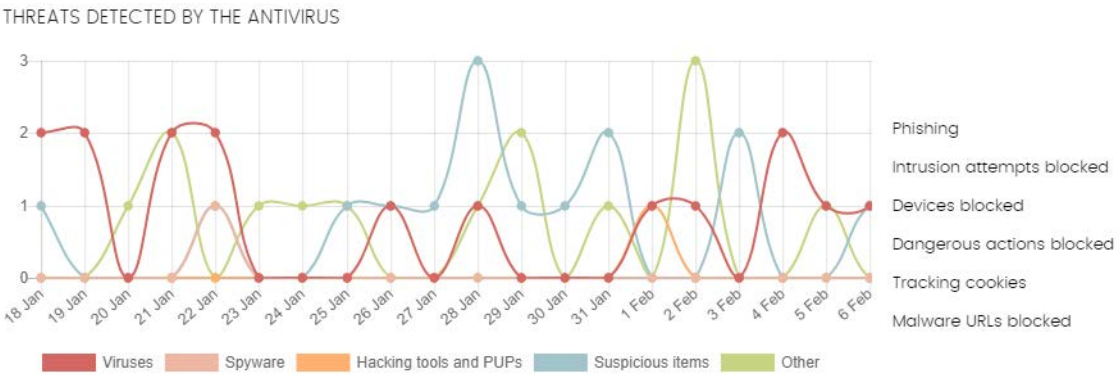


Figura 99: panel Amenazas detectadas por el antivirus

Amenazas detectadas por el antivirus consolida todos los intentos de intrusión que **Panda Adaptive Defense 360** gestionó en el periodo de tiempo establecido.

Los datos reflejados abarcan todos los vectores de infección y todas las plataformas soportadas, de manera que el administrador pueda disponer de datos concretos (volumen, tipo, forma de ataque) relativos a la llegada de malware a la red, durante un intervalo de tiempo determinado.

- **Significado de las series**

Este panel está formado por dos secciones: un gráfico de líneas y un listado resumen.

El diagrama de líneas representa las detecciones encontradas en el parque informático a lo largo del tiempo separadas por tipo de malware:

- Virus y spyware
- Herramientas de hacking y PUPs
- Sospechosos
- Phising
- Otros

En el eje de las Ys se muestran las ocurrencias y en el de las Xs las fechas.

El listado de la derecha muestra eventos relevantes que el administrador puede querer revisar en busca de síntomas o situaciones potenciales de peligro.

- **Intentos de intrusión bloqueados**: son ataques detenidos por el Cortafuegos y el Sistema de prevención de intrusos.
- **Dispositivos bloqueados**: periféricos bloqueados por el módulo de Control de dispositivos.
- **Operaciones peligrosas bloqueadas**: detecciones realizadas por análisis del comportamiento local.
- **Tracking cookies**: cookies detectadas para registrar la navegación de los usuarios.
- **URL con malware bloqueadas**: direcciones Web que apuntaban a páginas con malware.

- **Filtros pre establecidos desde el panel**

El listado se muestra con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel.

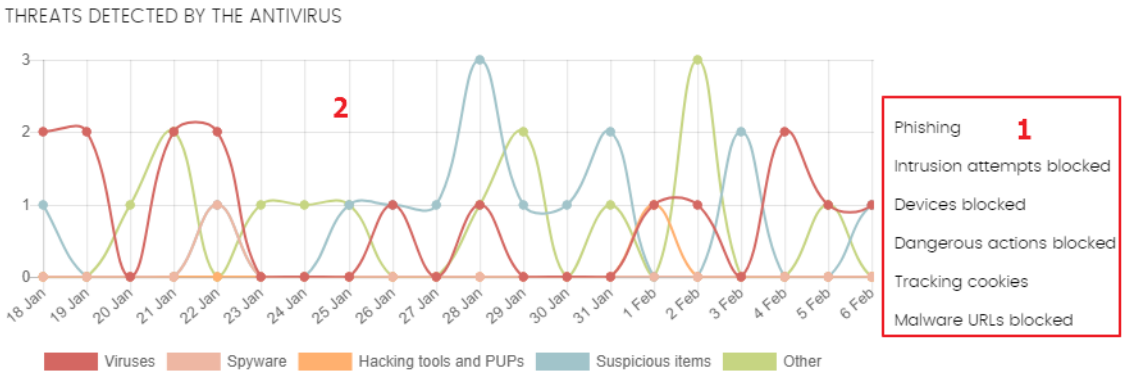


Figura 100: zonas activas del panel Amenazas detectadas por el antivirus

- **(1)** Listado **Amenazas detectadas por el antivirus** filtrado por **Tipo de amenaza** = (Phishing O Intentos de intrusión bloqueados O dispositivos bloqueados O Acciones peligrosas bloqueadas O Tracking cookies O URLs con malware)
- **(2)** Listado **Amenazas detectadas por el antivirus** sin filtro

16.3.10 Filtrado de contenidos en servidores Exchange

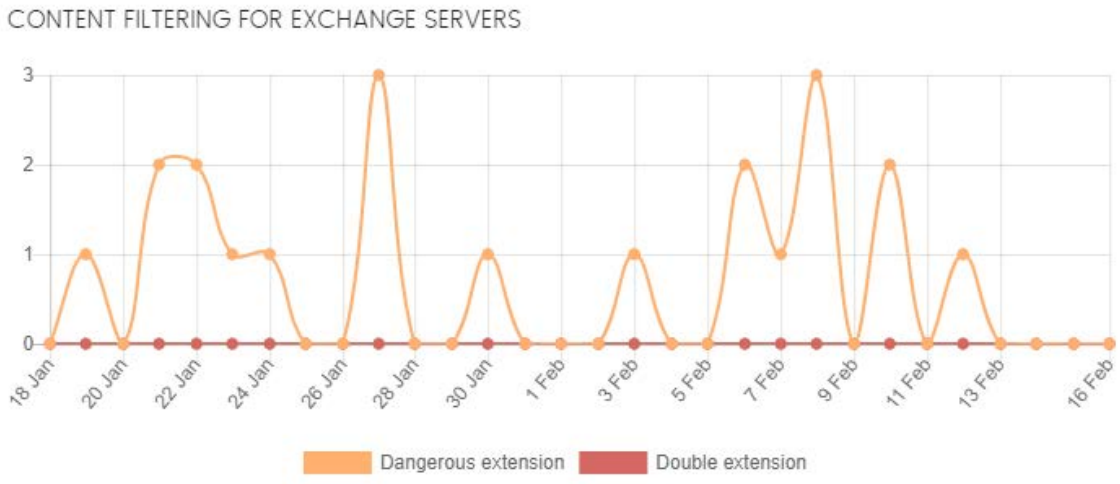


Figura 101: panel Filtrado de contenidos en servidores Exchange

Este panel muestra la cantidad de mensajes que fueron bloqueados por el filtro de contenidos del servidor Exchange.

- **Significado de las series**

Este panel presenta dos series de datos de tipo histórico: el número de mensajes filtrados por contener adjuntos con extensión peligrosa, y por doble extensión.

Al pasar el ratón por las series se muestra un tooltip con la siguiente información:

- **Extensión peligrosa**: número de mensajes filtrados por contener adjuntos con extensión peligrosa.
- **Doble extensión**: número de mensajes filtrados por contener adjuntos con doble extensión.

16.3.11 Accesos a páginas web

Este panel muestra mediante un gráfico de tarta la distribución de categorías Web solicitadas por los usuarios de la red.

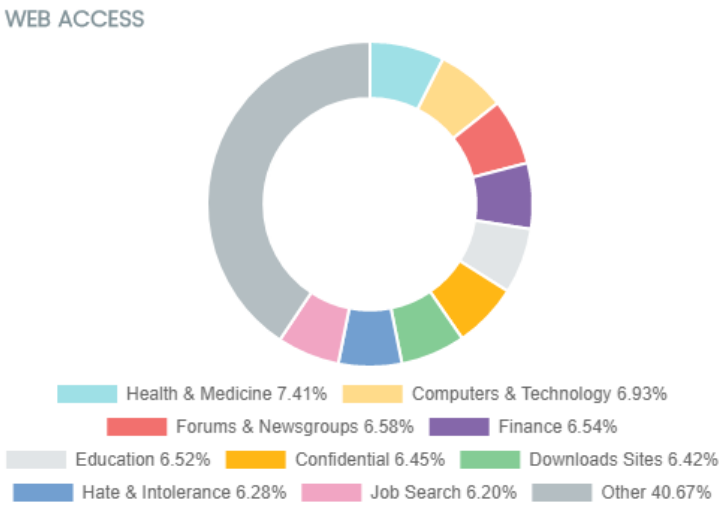


Figura 102: panel Accesos a páginas web

- **Significado de las series**

El panel de tipo tarta muestra los 10 grupos de páginas web más importantes que **Panda Adaptive Defense 360** soporta a la hora de categorizar las páginas web navegadas por los usuarios de la red:

- Odio e intolerancia
- Actividades criminales
- Búsqueda de empleo
- Contactos y anuncios personales
- Finanzas
- Confidencial
- Ocio y espectáculos
- Gobierno
- Drogas ilegales
- Otros

En la zona de la leyenda del panel se muestran los porcentajes de peticiones que encajan con cada categoría.

- **Filtros pre establecidos desde el panel**

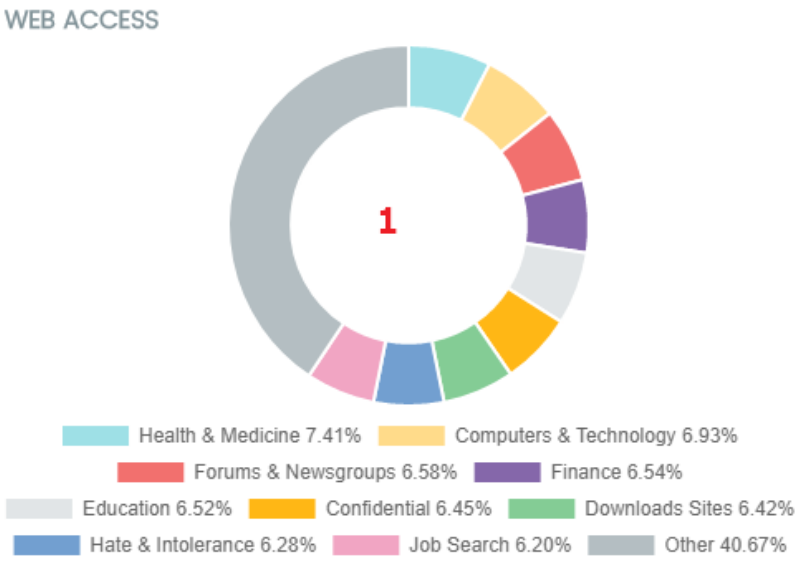


Figura 103: zonas activas del panel Accesos a páginas web

- **(1)** Listado **Accesos a páginas web por equipo** filtrado por **Categoría** = Categoría seleccionada

16.3.12 Categorías más accedidas (top 10)

Top 10 most accessed categories

Category	Access attempts	Computers
Job Search	4848	60
Computers & Technology	4800	62
Illegal Drugs	4759	60
Entertainment	4647	61
Health & Medicine	4578	60
Criminal Activity	4566	60
Forums & Newsgroups	4512	60
Downloads Sites	4495	60
Games	4471	60
Dating & Personals	4424	60

See full report

Figura 104: panel Categorías más accedidas

En este panel se destalla en número de accesos y el número de equipos que han accedido a las 10 categorías de páginas más visitadas.

Cada categoría indica el número de accesos totales en el rango de fechas seleccionado, y el número de equipos que han accedido una o más veces a esa categoría.

- **Filtros pre establecidos desde el panel**

Figura 105: zonas activas del panel Categorías mas accedidas (Top 10)

Al hacer clic en cada una de las categorías del panel se establece un filtro.

- **(1)** Listado **Accesos a páginas web por equipo** filtrado por **Categoría** = Categoría seleccionada
- **(2)** Listado **Accesos a páginas web por equipo** sin filtrar

16.3.13 Categorías más accedidas por equipo (top 10)

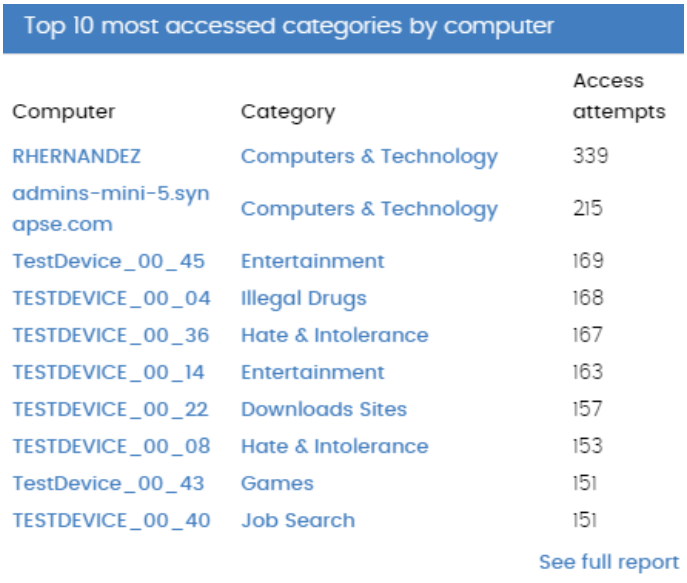
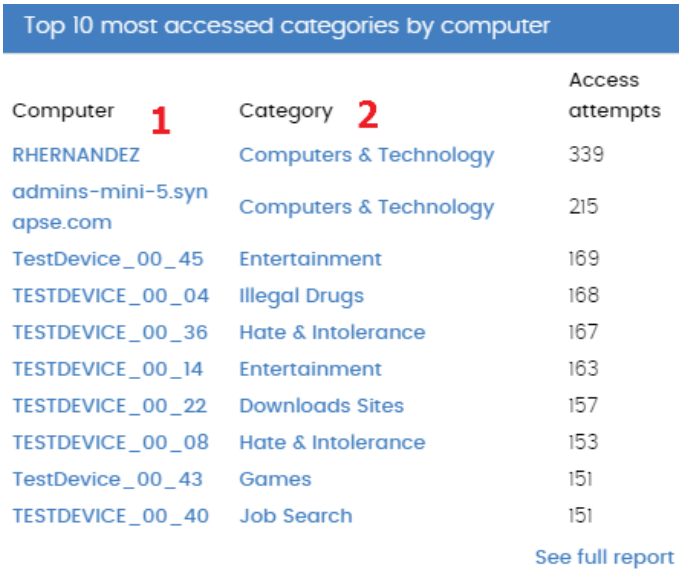


Figura 106: panel Categorías más accedidas por equipo (Top 10)

En este panel se detallan en número de accesos ordenados por categorías de los 10 equipos que más han visitado a la web.

- **Filtros pre establecidos desde el panel**



Top 10 most accessed categories by computer

Computer 1	Category 2	Access attempts
RHERNANDEZ	Computers & Technology	339
admins-mini-5.synapse.com	Computers & Technology	215
TestDevice_00_45	Entertainment	169
TESTDEVICE_00_04	Illegal Drugs	168
TESTDEVICE_00_36	Hate & Intolerance	167
TESTDEVICE_00_14	Entertainment	163
TESTDEVICE_00_22	Downloads Sites	157
TESTDEVICE_00_08	Hate & Intolerance	153
TestDevice_00_43	Games	151
TESTDEVICE_00_40	Job Search	151

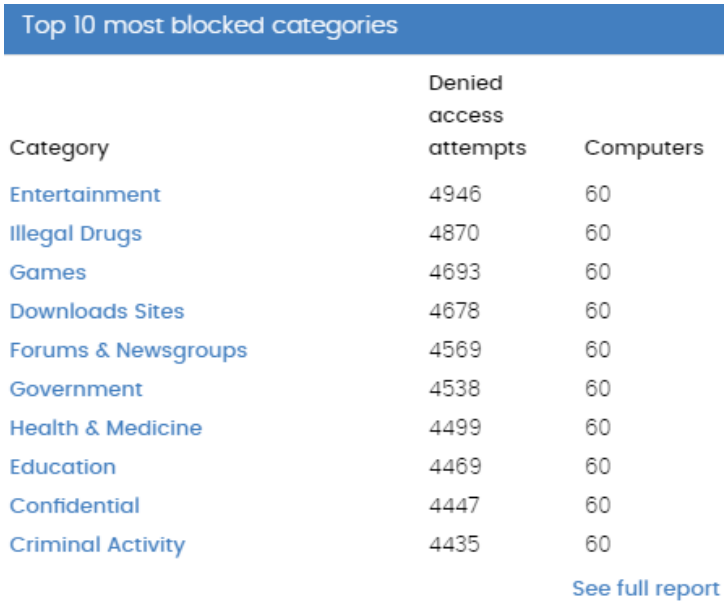
See full report

Figura 107: zonas activas del panel Categoías más acedidas por equipo (Top 10)

Al hacer clic en los elementos mostrados se establece un tipo de filtro diferente.

- **(1)** Listado **Accesos a páginas web por equipo** filtrado por **Equipo** = Equipo seleccionado
- **(2)** Listado **Accesos a páginas web por equipo** filtrado por **Categoría** = Categoría seleccionada

16.3.14 Categorías más bloqueadas (top 10)



Top 10 most blocked categories

Category	Denied access attempts	Computers
Entertainment	4946	60
Illegal Drugs	4870	60
Games	4693	60
Downloads Sites	4678	60
Forums & Newsgroups	4569	60
Government	4538	60
Health & Medicine	4499	60
Education	4469	60
Confidential	4447	60
Criminal Activity	4435	60

See full report

Figura 108: panel Categorias más bloqueadas (Top 10)

En este panel se indican las 10 categorías de páginas más bloqueadas de la red, junto al número de accesos bloqueados y el número de equipos que realizaron la visita y fueron bloqueados.

- **Filtros pre establecidos desde el panel**

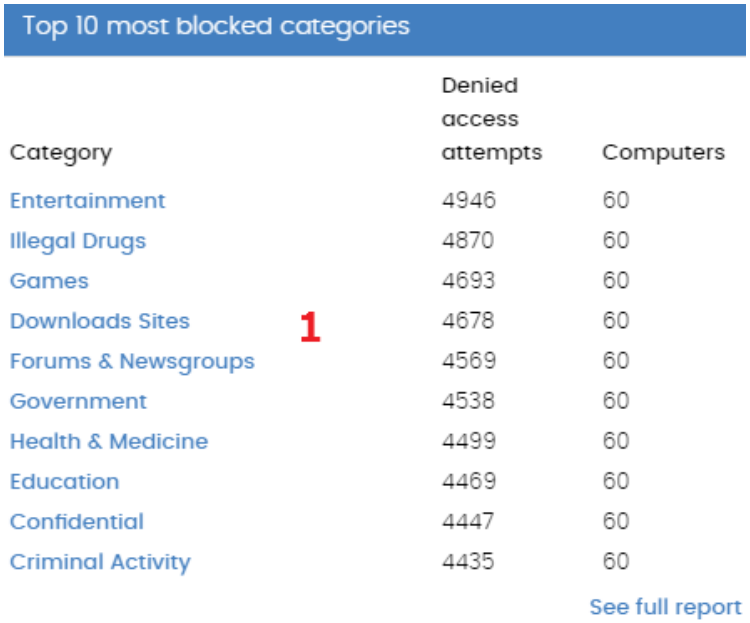


Figura 109: zonas activas del panel Categorias más bloqueadas (Top 10)

- **(1)** Listado **Accesos a páginas web por equipo** filtrado **por Categoría** = Categoría seleccionada

16.3.15 Categorías más bloqueadas por equipo (Top 10)

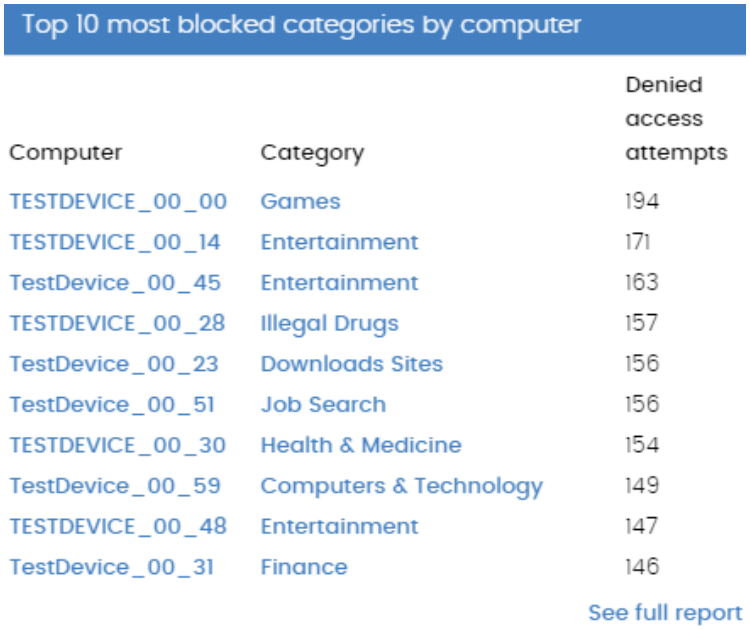


Figura 110: panel categorías más bloqueadas por equipo (Top 10)

El panel muestra los 10 pares equipo – categoría con mayor número de accesos bloqueados de la red, indicando el nombre del equipo, la categoría y el número de accesos denegados por cada par equipo – categoría.

- **Filtros pre establecidos desde el panel**

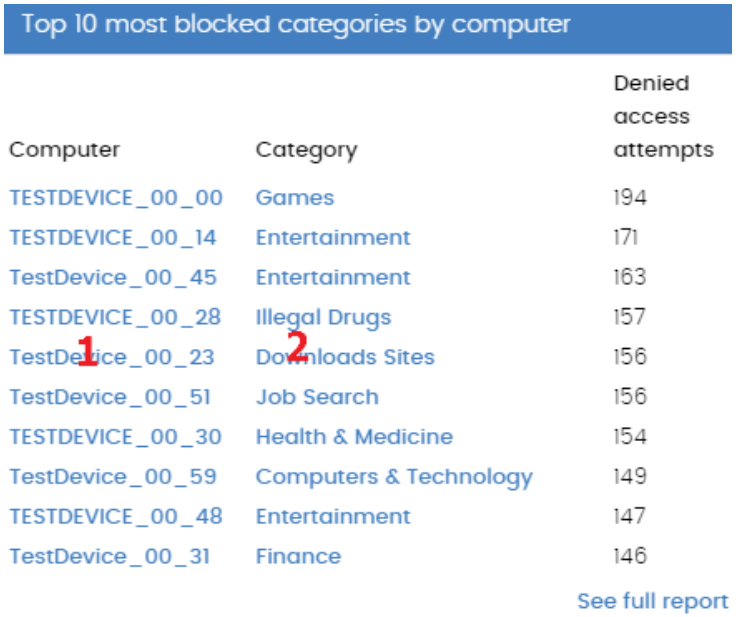


Figura 111: zonas activas del panel Categorías más bloqueadas por equipo (Top 10)

- **(1)** Listado **Accesos a páginas web por equipo** filtrado por **Nombre de equipo** = Equipo seleccionado
- **(2)** Listado **Accesos a páginas web por equipo** filtrado por **Categoría** = Categoría seleccionada

16.4. Introducción a los listados

Panda Adaptive Defense 360 estructura la información recogida en dos niveles: un primer nivel que representa de forma gráfica los datos mediante paneles o widgets y un segundo nivel más detallado, donde la información se representa mediante listados compuestos por tablas. La mayor parte de los paneles tienen un listado asociado de manera que el administrador puede acceder de forma rápida a un resumen gráfico de la información para después profundizar mediante los listados en caso de requerir más información.

16.4.1 Plantillas, configuraciones y vistas

Los listados son, en realidad, *Plantillas*, que admiten una o más *Configuraciones*. Una plantilla puede entenderse como una fuente de datos sobre un apartado específico tratado por **Panda Adaptive Defense 360**.

Una *Configuración* es una asignación específica de valores a las herramientas de búsqueda y filtrado asociada a cada plantilla.

La *Configuración* de una *Plantilla* da como resultado una *Vista de listado* o simplemente, *"Listado"*, que el administrador puede modificar y copiar para poder consultar posteriormente. De esta forma

el administrador puede ahorrar tiempo definiendo búsquedas y filtros sobre *Listados* que más tarde volverá a utilizar.

Figura 112:generación de tres listados a partir de una misma plantilla / fuente de datos

Plantillas de listado

Existen 11 plantillas correspondientes a otros tantos tipos de información, resumidos a continuación:

- Amenazas detectadas por el antivirus
- Intentos de intrusión bloqueados
- Dispositivos bloqueados
- Actividad de Malware y PUP
- Actividad de exploits
- Programas actualmente bloqueados en clasificación
- Accesos a páginas web por categoría
- Accesos a páginas web por equipo
- Estado de protección de los equipos
- Licencias
- Equipos no administrados descubiertos

Adicionalmente, existen otras plantillas accesibles directamente desde el menú de contexto de ciertos listados o desde algunos widgets del panel de control. El acceso a estos listados se indica en su descripción.

Configuraciones

En el actual contexto de listados, una configuración especifica un filtro de información definido por el administrador asociado a una plantilla. Cada plantilla tiene diferentes filtros de información según el tipo de datos que muestra.

El administrador puede establecer tantas configuraciones de filtros sobre una misma plantilla como quiera, con el objetivo de facilitar las diferentes lecturas de una misma fuente de datos.

Vistas de listado / listados

La unión de una *Plantilla* y una *Configuración* da como resultado una vista particular del listado. Una plantilla puede tener varias vistas asociadas, si el administrador ha creado otras tantas configuraciones tomando como base una misma plantilla.

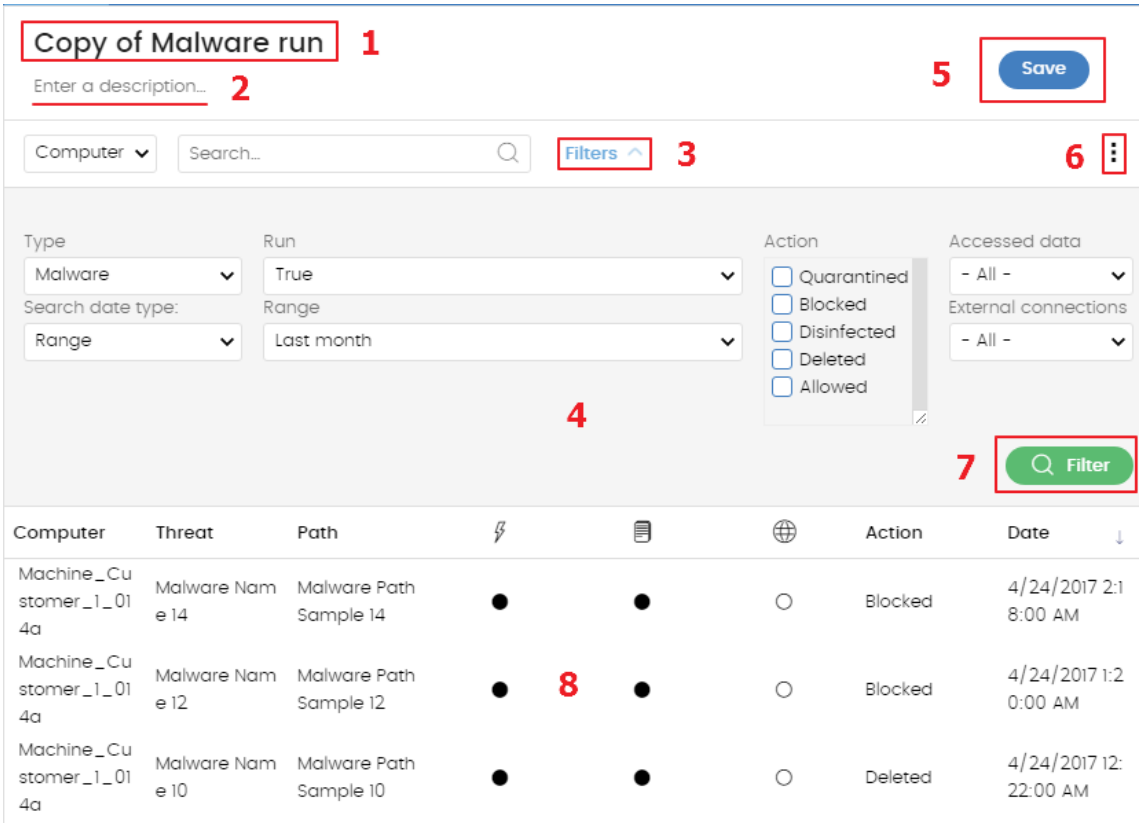


Figura 113: vista general de un listado

16.4.2 Panel Mis listados

Todos los listados creados se muestran en el panel izquierdo bajo la rama **Mis listados**, en el menú superior **Estado**.

16.4.3 Crear un listado personalizado

Hay cuatro formas de añadir un nuevo listado personalizado / vista:

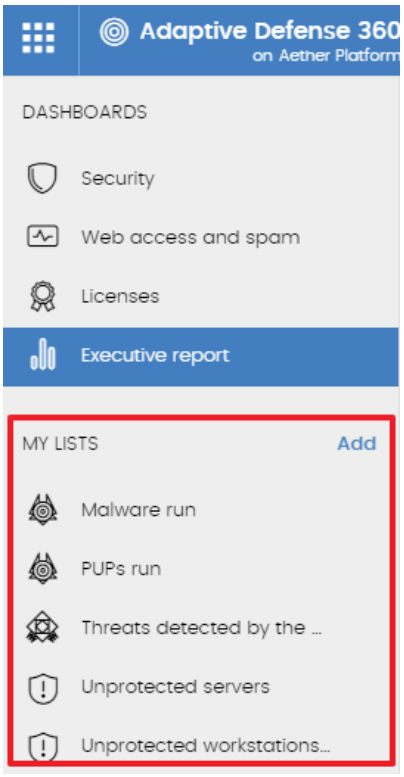


Figura 114: panel lateral Mis listados

- **Desde el panel lateral Mis listados**

Al hacer clic sobre el link **Añadir** del panel **Mis listados** se muestra una ventana con un desplegable que contiene las 11 plantillas disponibles.

- **Desde un panel del dashboard**

- Haz clic en un widget en el panel de control para abrir su plantilla asociada.
- Haz clic en el menú de contexto **(6)** y selecciona **Copiar**. Se creará un nuevo listado.
- Modifica los filtros, el nombre y la descripción del listado y haz clic en el botón **Guardar (5).**

- **Desde un listado ya creado**

- Haz una copia de un listado ya generado mediante el menú contextual **(6)** y haz clic en **Copiar**.

- **Desde el menú de contexto del panel Mis listados**

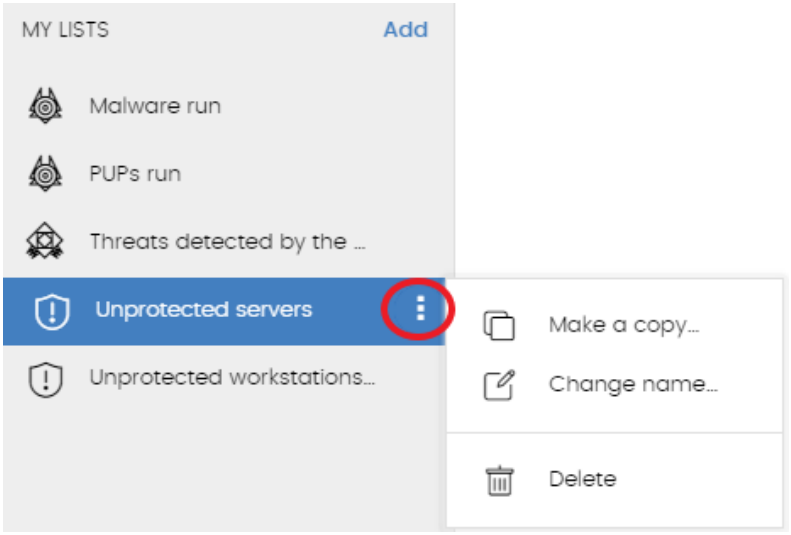


Figura 115: menú de contexto de los listados accesibles desde el Panel de listados

- Haz clic en el menú de contexto asociado al listado a copiar.
- Haz clic en **Hacer una copia.**
- Se creará una nueva vista de la plantilla que podrás modificar a tu gusto.

16.4.4 Borrar un listado

Puedes borrar un listado de dos maneras posibles:

- **Desde el panel mis listados**

- Haz clic el menú de contexto asociado al nombre del listado en el panel **Mis Listados.**
- Haz clic en el icono .

- **Desde el propio listado**

- Haz clic en el menú de contexto **(6).**
- Haz clic en el icono del menú desplegado.

16.4.5 Configurar un listado personalizado

- Asigna un nuevo nombre al listado **(1).** Por defecto la consola forma un nuevo nombre para el listado añadiendo la cadena "Nuevo" al tipo de listado o "Copia" si el listado es la copia de uno anterior.
- Asigna una descripción **(2)**: este paso es opcional.
- Haz clic en el link **Filtros (3)** para desplegar el bloque de búsqueda y configuración.

- Ajusta el filtro de información **(4)** para mostrar los datos relevantes.
- Haz clic en **Filtrar (7)** para aplicar el filtro configurado con el objetivo de comprobar si el filtrado configurado se ajusta a las necesidades. En el cuerpo del listado **(8)** se mostrará la búsqueda resultado.
- Haz clic en el botón **Guardar (5)**. El listado se añadirá en el panel de la izquierda bajo **Mis listados**, y será accesible a partir de ese momento haciendo clic en su nombre.

Además, en el botón de menú **(6)** se incluye la opción de exportar el listado en formato csv y la opción de hacer una copia del listado.

La exportación de listados en formato csv amplía la información mostrada en los listados de la consola Web. Estos campos están documentados más adelante en cada listado.

16.4.6 Acciones sobre equipos en los listados

En los listados **Licencias** y **Estado de protección de los equipos** se incorporan casillas de selección por cada equipo. Al marcar uno o más equipos, se muestra la barra de acciones en la parte superior de la ventana, para facilitar la administración de los puestos de usuario y servidores seleccionados.

16.5. Listados disponibles

16.5.1 Listado de Estado de protección de los equipos

Este listado muestra en detalle todos los equipos de la red, incorporando filtros que permiten localizar aquellos puestos de trabajo o dispositivos móviles que no estén protegidos por alguno de los conceptos mostrados en el panel asociado.

Campo	Comentario	Valores
Equipo	Nombre del equipo desprotegido	Cadena de caracteres
Protección avanzada **Antivirus**	Estado de la protección avanzada Estado de la protección antivirus	No instalado Error Activado Desactivado Sin licencia

Campo	Comentario	Valores
Protección actualizada	Indica si el módulo de la protección instalado en el equipo coincide con la última versión publicada o no. Al pasar el puntero del ratón por encima del campo se indica la versión de la protección instalada	Actualizado No actualizado (7 días sin actualizar desde la publicación) Pendiente de reinicio
Conocimiento	Indica si el fichero de firmas descargado en el equipo coincide con la última versión publicada o no. Al pasar el puntero del ratón por encima del campo se indica la fecha de actualización de la versión descargada	Actualizado No actualizado (3 días sin actualizar desde la publicación)
Ultima conexión	Fecha del ultimo envío del estado de Panda Adaptive Defense 360 a la nube de Panda Security	Fecha

Tabla 39: campos del listado Estado de protección de los equipos

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio	Cadena de caracteres
Tipo de equipo	Clase del dispositivo	Estación Portátil Dispositivo móvil Servidor
Equipo	Nombre del equipo	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo	Cadena de caracteres
Descripción		Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo	Cadena de caracteres
Versión del agente		Cadena de caracteres
Fecha instalación	Fecha en la que el Software Panda Adaptive Defense 360 se instaló con éxito en el equipo	Fecha
Fecha de la última actualización	Fecha de la última actualización del agente	Fecha

Campo	Comentario	Valores
Plataforma	Sistema operativo instalado en el equipo	Windows Linux macOS Android
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado	Cadena de caracteres
Servidor Exchange	Versión del servidor de correo instalada en el servidor	Cadena de caracteres
Protección actualizada	Indica si el módulo de la protección instalado en el equipo es la última versión publicada	Binario
Versión de la protección	Versión interna del módulo de protección	Cadena de caracteres
Conocimiento actualizado	Indica si el fichero de firmas descargado en el equipo es la última versión publicada	Binario
Fecha de última actualización	Fecha de la descarga del fichero de firmas	Fecha
Protección avanzada **Antivirus de archivo** **Antivirus de correo** **Antivirus de navegación web** **Protección firewall** **Control de dispositivos** **Antivirus para Exchange server** **Antispam para Exchange server** **Control de acceso a páginas web**	Estado de la protección asociada	No instalado Error Activado Desactivado Sin licencia

Tabla 40: campos del fichero exportado Estado de protección de los equipos

Herramienta de filtrado

Campo	Comentario	Valores
Tipo de equipo	Clase del dispositivo	Estación Portátil Dispositivo móvil Servidor
Buscar equipo	Nombre del equipo	Cadena de caracteres
Ultima conexión	Fecha del último envío del estado de Panda Adaptive Defense 360 a la nube de Panda Security	Todos Más de 72 horas Más de 7 días Más de 30 días

Campo	Comentario	Valores
Protección actualizada	Indica si la protección tiene la última versión publicada o no	Todos Si No Pendiente de reinicio
Plataforma	Sistema operativo instalado en el equipo	Todos Windows Linux Mac Android
Conocimiento	Estado de la actualización del fichero de firmas para la protección antivirus	Binario
Motivo de desprotección		No instalado Protección con error Activado Protección Desactivada Sin licencia Sin protección

Tabla 41: campos de filtrado para el listado Estado de protección de los equipos

16.5.2 Listado de Programas actualmente bloqueados en clasificación

En este listado se muestra una tabla con aquellos ficheros que, sin haber sido completada su clasificación, **Panda Adaptive Defense 360** ha detectado de forma preliminar algún riesgo en su ejecución. Estos ficheros son bloqueados durante el tiempo empleado en su clasificación.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se encontró el fichero desconocido	Cadena de caracteres
Ruta	Nombre del fichero desconocido y ruta en el equipo del usuario	Cadena de caracteres
Ha accedido a datos	El fichero desconocido ha accedido a datos que residen en el equipo del usuario	Binario
Se ha comunicado con equipos externos	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos	Binario
Modo de protección	Indica el modo en el que se encontraba la protección avanzada en el momento del descubrimiento del fichero desconocido	Audit Hardening Lock
Probabilidad de que sea malicioso	Posibilidad de que finalmente el fichero desconocido sea una amenaza	Media, Alta, Muy Alta

Campo	Comentario	Valores
Fecha	Fecha en la que se detectó por primera vez el fichero desconocido	Fecha

Tabla 42: campos del listado Programas actualmente bloqueados

Campos mostrados en fichero exportado

Consulta el capítulo 18 Análisis forense para obtener información sobre el listado detallado.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se encontró el fichero desconocido	Cadena de caracteres
Amenaza	Nombre del fichero desconocido	Cadena de caracteres
Ruta	Nombre del fichero desconocido y ruta en el equipo del usuario	Cadena de caracteres
Modo de protección	Especifica el modo en el que se encontraba la protección en el momento del descubrimiento del fichero desconocido	Monitor Hardening Lock
Acceso a datos	El fichero desconocido ha accedido a ficheros que residen en el equipo del usuario	Binario
Conexiones externas	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos	Binario
Probabilidad de que sea malicioso	Posibilidad de que finalmente el fichero desconocido sea una amenaza	Media, Alta, Muy Alta
Fecha	Fecha en la que se detectó por primera vez el fichero desconocido	Fecha
Tiempo de exposición	Tiempo que la amenaza ha permanecido en el parque del cliente sin clasificar	Fecha
Usuario	Cuenta de usuario bajo la cual el programa se ha ejecutado	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo	Cadena de caracteres

Campo	Comentario	Valores
Equipo origen de la amenaza	En el caso de que el programa bloqueado venga de un equipo de la red del cliente, indica el nombre del equipo	Cadena de caracteres
IP origen de la amenaza	En el caso de que el programa bloqueado venga de un equipo de la red del cliente, indica la dirección IP del equipo	Cadena de caracteres
Usuario origen de la amenaza	Usuario logeado en la máquina origen del programa bloqueado	Cadena de caracteres

Tabla 43: campos del fichero exportado Programas actualmente bloqueados

Herramienta de filtrado

Campo	Comentario	Valores
Tipo de fecha de búsqueda	**Rango**: permite establecer un intervalo de fechas desde el momento actual hacia atrás	Últimas 24 horas Últimos 7 días Último mes
Buscar	**Equipo**: dispositivo donde reside el elemento desconocido **Amenaza:** nombre del archivo **Hash**: Cadena resumen de identificación del archivo **Origen de la amenaza**: permite buscar por el usuario, la IP o el nombre del equipo origen del elemento bloqueado	Cadena de caracteres
Modos de protección	Indica el modo en el que se encontraba la protección avanzada en el momento de la detección del fichero desconocido	Hardering Lock
Acceso a datos	El fichero desconocido ha accedido a datos que residen en el equipo del usuario	Binario
Conexiones externas	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos	Binario

Tabla 44: campos de filtrado para el listado Programas actualmente bloqueados

16.5.3 Listado Historial de programas bloqueados

Muestra un histórico de todos eventos que se han producido a lo largo del tiempo relativos a las amenazas y ficheros desconocidos en clasificación que el administrador permitió su ejecución.

Este listado no tiene su panel correspondiente y es accesible únicamente mediante el botón **Historial** del listado **Programas actualmente bloqueados en clasificación**, situado en la esquina superior derecha.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se encontró el fichero desconocido	Cadena de caracteres
Ruta	Nombre del fichero desconocido y ruta en el equipo del usuario	Cadena de caracteres
Acción	Acción ejecutada por Panda Adaptive Defense 360	Bloqueado Reclasificado a GW Reclasificado a MW Reclasificado a PUP
Ha accedido a datos	El fichero desconocido ha accedido a datos que residen en el equipo del usuario	Binario
Se ha comunicado con equipos externos	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos	Binario
Modo de protección	Indica el modo en el que se encontraba la protección avanzada en el momento de la detección del fichero desconocido	Audit Hardening Lock
Excluido	El fichero desconocido ha sido desbloqueado / excluido por el administrador para permitir su ejecución	Binario
Probabilidad de que sea malicioso	Posibilidad de que finalmente el fichero desconocido sea malware	Media, Alta, Muy Alta
Fecha	Fecha en la que se detectó por primera vez el fichero desconocido	Fecha

Tabla 45: campos del listado Historial de programas bloqueados

Campos mostrados en fichero exportado

Consulta el capítulo 18 Análisis forense para obtener información sobre el listado detallado

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se encontró el fichero desconocido	Cadena de caracteres
Amenaza	Nombre del fichero desconocido	Cadena de caracteres
Ruta	Ruta en el equipo del usuario del fichero desconocido	Cadena de caracteres

Campo	Comentario	Valores
Modo de protección	Indica el modo en el que se encontraba la protección avanzada en el momento de la detección del fichero desconocido	Audit Hardening Lock
Acción	Acción ejecutada por Panda Adaptive Defense 360	Bloqueado Reclasificado a GW Reclasificado a MW Reclasificado a PUP
Acceso a datos	El fichero desconocido ha accedido a datos que residen en el equipo del usuario	Binario
Conexiones exteriores	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos	Binario
Excluido	El fichero desconocido ha sido desbloqueado / excluido por el administrador para permitir su ejecución	Binario
Probabilidad de que sea malicioso	Posibilidad de que finalmente el fichero desconocido sea malware	Media, Alta, Muy Alta
Fecha	Fecha en la que se detectó por primera vez el fichero desconocido	Fecha
Tiempo de exposición	Tiempo que el fichero desconocido ha permanecido en el parque del cliente sin clasificar	Fecha
Usuario	Cuenta de usuario bajo la cual el programa se ha ejecutado	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo	Cadena de caracteres
Equipo origen de la amenaza	Equipo origen del programa bloqueado	Equipo origen del programa bloqueado
IP origen de la amenaza	IP origen del programa bloqueado	IP origen del programa bloqueado
Usuario origen de la amenaza	Usuario origen del programa bloqueado	Usuario origen del programa bloqueado

Tabla 46: campos del fichero exportado Historial de programas bloqueados

Herramienta de filtrado

Campo	Comentario	Valores
Buscar	**Equipo**: dispositivo donde reside el fichero desconocido **Amenaza**: nombre de la amenaza **Hash**: Cadena resumen de identificación del archivo **Amenaza**	Cadena de caracteres

Campo	Comentario	Valores
	Origen del programa bloqueado: permite buscar por el usuario, la IP o el nombre del equipo origen del elemento bloqueado	
Rango	Permite establecer un intervalo de fechas desde el momento actual hacia atrás	Últimas 24 horas Últimos 7 días Último mes
Acción	Acción desencadenada por Panda Adaptive Defense 360	Bloqueado Reclasificado a GW Reclasificado a MW Reclasificado a PUP
Excluido	El fichero desconocido ha sido desbloqueado / excluido por el administrador para permitir su ejecución	Binario
Modos de protección	Indica el modo en el que se encontraba la protección avanzada en el momento de la detección del fichero desconocido	Hardening Lock
Acceso a datos	El fichero desconocido ha accedido a datos que residen en el equipo del usuario	Binario
Conexiones externas	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos	Binario

Tabla 47: campos del fichero exportado Historial de programas bloqueados

16.5.4 Listado de Programas permitidos por el administrador

Este listado muestra en detalle todos los elementos en clasificación o clasificados como amenazas que el administrador actualmente está permitiendo su ejecución.

Este listado solo es accesible desde el widget Programas permitidos por el administrador

Campo	Comentario	Valores
Amenaza	Nombre del malware o PUP que se permite su ejecución. Si es un elemento desconocido se indica el nombre del fichero en su lugar	Cadena de caracteres
Tipo	Tipo del fichero	Malware PUP Bloqueado Bloqueado reclasificado a Malware / PUP Bloqueado reclasificado a Good-ware

Campo	Comentario	Valores
Archivo	Nombre del fichero desconocido o que contiene la amenaza	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo	Cadena de caracteres
Permitido por	Usuario de la consola que creó la exclusión	Cadena de caracteres
Permitido desde	Fecha en la que el administrador creó la exclusión del fichero	Fecha
Borrar	Permite retirar la exclusión del fichero	

Tabla 48: campos del listado Programas permitidos por el administrador

Campos incluidos en fichero exportado

Campo	Comentario	Valores
Amenaza	Nombre del malware o PUP que se permite su ejecución. Si es un elemento desconocido se indica el nombre del fichero en su lugar	Cadena de caracteres
Tipo actual	Tipo del fichero en el momento en el que se accede al listado	Malware PUP Bloqueado Bloqueado reclasificado a Malware / PUP Bloqueado reclasificado a Goodware
Tipo original	Tipo del fichero en el momento en el que se comenzó a permitir su bloqueo	Malware PUP Bloqueado Bloqueado reclasificado a Malware / PUP Bloqueado reclasificado a Goodware1
Archivo	Nombre del fichero desconocido o que contiene la amenaza	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo	Cadena de caracteres
Permitido por	Usuario de la consola que creó la exclusión	Cadena de caracteres
Permitido desde	Fecha en la que el administrador creó la exclusión del fichero	Fecha

Tabla 49: campos del fichero exportado Programas permitidos por el administrador

Herramienta de filtrado

Campo	Comentario	Valores
Buscar	**Amenaza**: nombre del malware o PUP **Permitido por**: usuario de la consola que	Cadena de caracteres

Campo	Comentario	Valores
	creó la exclusión **Archivo**: nombre del fichero que contiene la amenaza **Hash**: cadena resumen de identificación del archivo	
Clasificación actual	Tipo del fichero en el momento en el que se accede al listado	Malware PUP Goodware En clasificación (Bloqueados y sospechoso)
Clasificación original	Tipo del fichero en el momento en el que se comenzó a permitir su bloqueo	Malware PUP Bloqueado Sospechoso

Tabla 50: campos de filtrado para el listado Programas permitidos por el administrador

16.5.5 Listado Historial de Programas permitidos por el administrador

Muestra un histórico de todos eventos que se han producido a lo largo del tiempo relativos a las amenazas y ficheros desconocidos en clasificación que el administrador permitió su ejecución.

Este listado no tiene su panel correspondiente y es accesible únicamente mediante el botón **Historial** del listado **Programas permitidos por el administrador**, situado en la esquina superior derecha.

Campo	Comentario	Valores
Amenaza	Nombre del malware o PUP que se permite su ejecución. Si es un elemento desconocido se indica el nombre del fichero en su lugar	Cadena de caracteres
Tipo	Tipo de la amenaza que se permitió su ejecución	Malware PUP Bloqueado Sospechoso
Archivo	Nombre del fichero desconocido o que contiene la amenaza	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo	Cadena de caracteres
Acción	Acción aplicada sobre el elemento permitido	Exclusión eliminada por el usuario Exclusión eliminada por reclasificación Exclusión añadida por el usuario Exclusión mantenida por reclasificación
Usuario	Cuenta de usuario de la consola que inicio el cambio en el fichero	Cadena de caracteres

Campo	Comentario	Valores
	permitido	
Fecha	Fecha en la que se produjo el evento	Fecha

Tabla 51: campos del listado Historial de Programas permitidos por el administrador

Campos incluidos en fichero exportado

Campo	Comentario	Valores
Amenaza	Nombre del malware o PUP que se permite su ejecución. Si es un elemento desconocido se indica el nombre del fichero en su lugar	Cadena de caracteres
Tipo actual	Ultimo tipo de la amenaza que se permitió su ejecución	Malware PUP Bloqueado Sospechoso
Tipo original	Tipo del fichero cuando se produjo el evento	
Archivo	Nombre del fichero desconocido o que contiene la amenaza	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo	Cadena de caracteres
Acción	Acción aplicada sobre el elemento permitido	Exclusión eliminada por el usuario Exclusión eliminada por reclasificación Exclusión añadida por el usuario Exclusión mantenida por reclasificación
Usuario	Cuenta de usuario de la consola que inicio el cambio en el fichero permitido	Cadena de caracteres
Fecha	Fecha en la que se produjo el evento	Fecha

Tabla 52: campos del fichero exportado Historial de Programas permitidos por el administrador

Herramienta de filtrado

Campo	Comentario	Valores
Buscar	**Usuario:** Cuenta de usuario de la consola que inicio el cambio en el fichero permitido **Archivo**: Nombre del fichero que contiene la amenaza **Hash**: Cadena resumen de identificación del archivo	Cadena de caracteres
Clasificación actual	Tipo del fichero en el momento en el	Malware

Campo	Comentario	Valores
	que se accede al listado	PUP Goodware En clasificación (Bloqueados y sospechoso)
Clasificación original	Tipo del fichero en el momento en el que se comenzó a permitir su bloqueo	Malware PUP Bloqueado Sospechoso
Acción	Acción aplicada sobre el elemento permitido	Exclusión eliminada por el usuario Exclusión eliminada por reclasificación Exclusión añadida por el usuario Exclusión añadida por reclasificación

Tabla 53: campos de filtrado para el listado Historial de Programas permitidos por el administrador

16.5.6 Listado de Actividad del malware / PUP

Muestra al administrador el listado de las amenazas encontradas en los equipos protegidos con **Panda Adaptive Defense 360**. Este detalle es necesario para poder localizar el origen los problemas, determinar la gravedad de las incidencias y, si procede, tomar las medidas necesarias de resolución y de actualización de la política de seguridad de la compañía.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se ha detectado a la amenaza	Cadena de caracteres
Amenaza	Nombre de la amenaza detectada	Cadena de caracteres
Ruta	Ruta completa donde reside el fichero infectado	Cadena de caracteres
Ejecutado alguna vez	La amenaza se llegó a ejecutar y el equipo puede estar comprometido	Binario
Ha accedido a datos	La amenaza ha accedido a datos que residen en el equipo del usuario	Binario
Se ha comunicado con equipos externos	La amenaza se comunica con equipos remotos para enviar o recibir datos	Binario
Acción	Acción aplicada sobre el malware	Movido a cuarentena Bloqueado Desinfectado Eliminado Permitido
Fecha	Fecha de la detección de la amenaza en el equipo	Fecha

Tabla 54: campos del listado de Actividad del malware / PUP

Campos mostrados en fichero exportado

Consulta el capítulo 18 Análisis forense para obtener información sobre el listado detallado.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se ha detectado a la amenaza	Cadena de caracteres
Amenaza	Nombre de la amenaza detectada	Cadena de caracteres
Ruta	Ruta completa donde reside el fichero infectado	Cadena de caracteres
Acción	Acción aplicada sobre el malware	Movido a cuarentena Bloqueado Desinfectado Eliminado Permitido
Ejecutado	La amenaza se llegó a ejecutar y el equipo puede estar comprometido	Binario
Acceso a datos	La amenaza ha accedido a datos que residen en el equipo del usuario	Binario
Conexiones externas	La amenaza se comunica con equipos remotos para enviar o recibir datos	Binario
Excluido	La amenaza ha sido excluida por el administrador para permitir su ejecución	Binario
Fecha	Fecha de la detección de la amenaza en el equipo	Fecha
Tiempo de exposición	Tiempo que la amenaza ha permanecido en el parque del cliente sin clasificar	Cadena de caracteres
Usuario	Cuenta de usuario bajo la cual la amenaza se ha ejecutado	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo	Cadena de caracteres
Equipo origen de la infección	En el caso de que el intento de infección venga de un equipo de la red del cliente, indica el nombre del equipo	Cadena de caracteres
IP origen de la infección	En el caso de que el intento de infección venga de un equipo de la red del cliente, indica la dirección IP del equipo	Cadena de caracteres
Usuario origen de la infección	Usuario logeado en la máquina origen de la infección	Cadena de caracteres

Tabla 55: campos del fichero exportado Actividad del malware / PUP

Herramienta de filtrado

Campo	Comentario	Valores
Buscar	**Equipo**: dispositivo donde se realizó la detección **Amenaza**: nombre de la amenaza **Hash**: Cadena resumen de identificación del archivo **Origen de la infección**: permite buscar por el usuario, la IP o el nombre del equipo origen del fichero infectado.	Cadena de caracteres
Tipo	Tipo de amenaza a mostrar	Malware PUP
Rango	Permite establecer un intervalo de fechas desde el día presente hacia atrás	Últimas 24 horas Últimos 7 días Último mes Último año
Ejecutado	La amenaza se llegó a ejecutar y el equipo puede estar comprometido	Binario
Acción	Acción aplicada sobre la amenaza	Movido a cuarentena Bloqueado Desinfectado Eliminado Permitido
Acceso a datos	La amenaza ha accedido a datos que residen en el equipo del usuario	Binario
Conexiones externas	La amenaza se comunica con equipos remotos para enviar o recibir datos	Binario

Tabla 56: campos de filtrado para el listado Actividad del malware / PUP

16.5.7 Listado de Actividad de exploits

Muestra al administrador el listado de equipos con programas comprometidos por intentos de explotación de vulnerabilidades. Este detalle es necesario para poder localizar el origen los problemas, determinar la gravedad de las incidencias y, si procede, tomar las medidas necesarias de resolución y de actualización de la política de seguridad de la compañía.

Panda Adaptive Defense 360 ejecuta una acción por cada exploit detectado:

- **Permitido**: la protección anti-exploit está configurada en modo "Auditar". El exploit se ejecutó.
- **Bloqueado**: el exploit fue bloqueado antes de su ejecución.
- **Permitido por el usuario**: se preguntó al usuario del equipo si finalizar el proceso comprometido y el usuario decidió permitir que el exploit continuara ejecutándose.
- **Proceso finalizado**: el exploit fue eliminado, pero se llegó a ejecutar parcialmente.
- **Pendiente de reinicio**: se informó al usuario de la necesidad de reiniciar el equipo para eliminar completamente el exploit. Mientras tanto éste se seguirá ejecutando.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se ha detectado a la amenaza	Cadena de caracteres
Programa comprometido	Programa que recibió el ataque de tipo exploit	Cadena de caracteres
Acción	Acción aplicada sobre el exploit	Permitido por el usuario Permitido Bloqueado Proceso finalizado Pendiente de reinicio
Exploit ejecutado	Determina si el exploit se llegó a ejecutar o fue bloqueado antes de afectar al programa vulnerable	Binario
Fecha	Fecha de la detección del intento de exploit en el equipo	Fecha

Tabla 57: campos del listado de Actividad de exploits

Campos mostrados en fichero exportado

Consulta el capítulo 18 Análisis forense para obtener información sobre el listado detallado

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se ha detectado a la amenaza	Cadena de caracteres
Programa comprometido	Programa que recibió el ataque de tipo exploit	Cadena de caracteres
Usuario	Cuenta de usuario bajo la cual se ejecutaba el programa que recibió el exploit	Cadena de caracteres
Hash	Cadena resumen de identificación del programa comprometido	Cadena de caracteres
Last action	Acción aplicada sobre el exploit	Permitido por el usuario Permitido por el administrador Bloqueo inmediato Bloqueo tras finalizar proceso
Riesgo	Determina si el equipo está o ha estado en situación riesgo o el exploit se pudo bloquear antes de afectar al programa vulnerable	Binario
Fecha	Fecha de la detección del intento de exploit en el equipo	Fecha

Tabla 58: campos del fichero exportado Actividad del malware / PUP

Herramienta de búsqueda

Campo	Comentario	Valores
Buscar	**Equipo**: dispositivo donde se realizó la detección **Hash**: Cadena resumen de identificación del programa comprometido.	Cadena de caracteres
Rango	Permite establecer un intervalo de fechas desde el día presente hacia atrás	Últimas 24 horas Últimos 7 días Último mes
Exploit ejecutado	Determina si el exploit se llegó a ejecutar o fue bloqueado antes de afectar al programa vulnerable	Binario
Acción	Acción aplicada sobre el exploit	Permitido por el usuario Permitido Bloqueado Proceso finalizado Pendiente de reinicio

Tabla 59: campos de filtrado para el listado Actividad de exploits

16.5.8 Listado de Amenazas detectadas por el antivirus

El listado de detecciones ofrece información consolidada y completa de todas las detecciones hechas en todas las plataformas soportadas y desde todos los vectores de infección analizados, utilizados por los hackers para intentar infectar equipos en la red.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se realizó la detección	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo	Cadena de caracteres
Grupo	Grupo dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo	Cadena de caracteres  Grupo Todos  Grupo nativo  Grupo Directorio activo
Tipo de amenaza	Clase de la amenaza detectada	Virus Spyware Herramientas de hacking y PUPs Phising Sospechosos Acciones peligrosas bloqueadas Tracking cookies URLs con malware Otros
Ruta	Ruta del sistema de ficheros donde reside la amenaza	Cadena de caracteres

Campo	Comentario	Valores
Acción	Acción desencadenada por Panda Adaptive Defense 360	Borrado Desinfectado En cuarentena Bloqueado Proceso terminado
Fecha	Fecha de la detección	Fecha

Tabla 60: campos del listado Amenazas detectadas por el antivirus

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio	Cadena de caracteres
Tipo de equipo	Clase del dispositivo	Estación Portátil Dispositivo móvil Servidor
Equipo	Nombre del equipo donde se realizó la detección	Cadena de caracteres
Nombre malware	Nombre de la amenaza detectada	Cadena de caracteres
Tipo de amenaza	Clase de la amenaza detectada	Virus Spyware Herramientas de hacking y PUPs Phising Sospechosos Acciones peligrosas bloqueadas Tracking cookies URLs con malware Otros
Tipo de malware	Subclase de la amenaza detectada	Cadena de caracteres
Número de detecciones	Número de veces que Panda Adaptive Defense 360 detectó la amenaza en el equipo y en la fecha indicada.	Numérico
Acción	Acción desencadenada por Panda Adaptive Defense 360	Movido a cuarentena Borrado Bloqueado Proceso terminado
Detectado por	Determina el motor que detectó la amenaza	Control de dispositivos Protección de Antispam para Exchange Protección de Contenido para Exchange Protección de Buzones para Exchange Protección de Transporte para Exchange Protección de ficheros Firewall Protección de correo Panda Adaptive Defense

Campo	Comentario	Valores
		Análisis bajo demanda Control de acceso Web Protección Web
Ruta de detección	Ruta del sistema de ficheros donde reside la amenaza	Cadena de caracteres
Excluido	La amenaza ha sido excluida del análisis por el administrador para permitir su ejecución	Binario
Fecha	Fecha de la detección	Fecha
Grupo	Grupo dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo donde se realizó la detección	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo	Cadena de caracteres
Descripción		Cadena de caracteres

Tabla 61: campos del fichero exportado Amenazas detectadas por el antivirus

Herramienta de filtrado

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se realizó la detección	Cadena de caracteres
Tipo de fecha de búsqueda	**Rango**: permite establecer un intervalo de fechas desde el día1 presenta hacia atrás **Rango personalizado**: permite establecer una fecha concreta del calendario	Últimas 24 horas Últimos 7 días Último mes Último año
Tipo de equipo	Clase del dispositivo	Estación Portátil Dispositivo móvil Servidor
Tipo de Amenazas	Clase de amenaza	Virus Spyware Herramientas de hacking y PUPs Phising Sospechosos Acciones peligrosas bloqueadas Tracking cookies URLs con malware Otros

Tabla 62: campos de filtrado para el listado Amenazas detectadas por el antivirus

16.5.9 Listado de Dispositivos bloqueados

Este listado muestra en detalle todos los equipos de la red que tienen limitado el acceso a alguno de los periféricos conectados.

Campo	Comentario	Valores
Equipo	Nombre del equipo desprotegido	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo	Cadena de caracteres  Grupo Todos  Grupo nativo  Grupo Directorio activo
Tipo	Familia del dispositivo afectado por la configuración de seguridad	Unidades de almacenamiento extraíbles Dispositivos de captura de imágenes Unidades de CD/DVD Dispositivos Bluetooth Módems Dispositivos móviles
Acción	Tipo de acción efectuada sobre el dispositivo	Bloquear Permitir Lectura Permitir Lectura y escritura
Fecha	Fecha en la se aplicó la acción	Fecha

Tabla 63: campos del listado Dispositivos bloqueados

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio	Cadena de caracteres
Tipo de equipo	Clase del dispositivo	Estación Portátil Dispositivo móvil Servidor
Equipo	Nombre del equipo	Cadena de caracteres
Nombre	Nombre del periférico conectado al equipo y afectado por la configuración de seguridad	Cadena de caracteres
Id. de instancia	Identificador del dispositivo afectado	Cadena de caracteres
Número de detecciones	Número de veces que se detectó una operación no permitida sobre el dispositivo	Numérico

Campo	Comentario	Valores
Acción	Tipo de acción efectuada sobre el dispositivo	Bloquear Permitir Lectura Permitir Lectura y escritura
Detectado por	Módulo que detecto la operación no permitida	Control de dispositivos
Fecha	Fecha en la se detectó la operación no permitida	Fecha
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo	Cadena de caracteres
Descripción		Cadena de caracteres

Tabla 64: campos del fichero exportado Dispositivos bloqueados

Herramienta de filtrado

Campo	Comentario	Valores
Tipo de equipo	Clase del dispositivo	Estación Portátil Dispositivo móvil Servidor
Buscar equipo	Nombre del equipo	Cadena de caracteres
Tipo de fecha de búsqueda	**Rango**: permite establecer un intervalo de fechas desde el día1 presenta hacia atrás **Rango personalizado**: permite establecer una fecha concreta del calendario	Últimas 24 horas Últimos 7 días Último mes
Tipo de dispositivo	Familia del dispositivo afectado por la configuración de seguridad	Unidades de almacenamiento extraíbles Dispositivos de captura de imágenes Unidades de CD/DVD Dispositivos Bluetooth Módems Dispositivos móviles

Tabla 65: campos de filtrado para el listado Dispositivos bloqueados

16.5.10 Listado de Accesos a páginas web por categoría

Campo	Comentario	Valores
Categoría	Categoría a la que pertenece la página accedida	Enumeración de las categorías soportadas
Accesos permitidos	Número de accesos que se han permitido a la categoría de página indicada en el campo Categoría.	Numérico
Dispositivos permitidos	Número de equipos que han podido acceder a páginas pertenecientes a la categoría de página indicada en el campo Categoría.	Numérico
Accesos denegados	Número de accesos que se han denegado a la categoría de página indicada en el campo Categoría.	Numérico
Equipos denegados	Número de equipos que no han podido acceder a páginas pertenecientes a la categoría de página indicada en el campo Categoría.	Numérico

Tabla 66: Campos del listado Accesos a páginas web por categoría

Campos mostrados en el fichero exportado

Campo	Comentario	Valores
Categoría	Categoría a la que pertenece la página accedida	Enumeración de las categorías soportadas
Accesos permitidos	Número de accesos que se han permitido a la categoría de página indicada en el campo Categoría.	Numérico
Dispositivos permitidos	Número de equipos que han podido acceder a páginas pertenecientes a la categoría de página indicada en el campo Categoría.	Numérico
Accesos denegados	Número de accesos que se han denegado a la categoría de página indicada en el campo Categoría.	Numérico
Equipos denegados	Número de equipos que no han podido acceder a páginas pertenecientes a la categoría de página indicada en el campo Categoría.	Numérico

Tabla 67: Campos del fichero exportado Accesos a páginas web por equipo

Herramienta de filtrado

Campo	Comentario	Valores
Tipo de fecha de búsqueda	**Rango**: permite establecer un intervalo de fechas desde el día presente hacia atrás **Fecha personalizada**: permite establecer una fecha concreta del calendario	Últimas 24 horas Últimos 7 días Último mes Último año

Campo	Comentario	Valores
Categoría	Categoría a la que pertenece la página accedida	Enumeración de las categorías soportadas

Tabla 68: Campos de filtrado para el listado Accesos a páginas web por equipo

16.5.11 Listado de Accesos a páginas web por equipo

El acceso a páginas web por equipo lista todos los equipos encontrados en la red indicando el número de accesos permitidos y denegados por cada categoría accedida.

Campo	Comentario	Valores
Equipo	Nombre del equipo	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo	Cadena de caracteres
Grupo	Grupo dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo	Cadena de caracteres  Grupo Todos  Grupo nativo  Grupo Directorio activo
Categoría	Categoría a la que pertenece la página accedida	Enumeración de las categorías soportadas
Accesos permitidos	Número de accesos que se han permitido a la categoría de página indicada en el campo Categoría,	Numérico
Accesos denegados	Numero de accesos que se han denegado a la categoría de página indicada en el campo Categoría.	Numérico

Tabla 69: campos del listado Accesos a páginas web por equipo

Campos mostrados en el fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio	Cadena de caracteres
Tipo de equipo	Clase del dispositivo	Estación Portátil Dispositivo móvil Servidor
Equipo	Nombre del equipo	Cadena de caracteres
Categoría	Categoría a la que pertenece la página accedida	Enumeración de las categorías soportadas
Accesos permitidos	Número de accesos que se han permitido a la categoría de página indicada en el campo Categoría	Numérico

Campo	Comentario	Valores
Accesos denegados	Numero de accesos que se han denegado a la categoría de página indicada en el campo Categoría	Numérico
Grupo	Grupo dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo	Cadena de caracteres
Descripción		Cadena de caracteres

Tabla 70: campos del fichero exportado Accesos a páginas web por equipo

Herramienta de búsqueda

Campo	Comentario	Valores
Tipo de fecha de búsqueda	**Rango**: permite establecer un intervalo de fechas desde el día presente hacia atrás **Rango personalizado**: permite establecer una fecha concreta del calendario	Últimas 24 horas Últimos 7 días Último mes
Categoría	Categoría a la que pertenece la página accedida	Enumeración de las categorías soportadas
Tipo de equipo	Clase del dispositivo	Estación Portátil Dispositivo móvil Servidor
Equipo	Nombre del equipo	Cadena de caracteres

Tabla 71: campos de filtrado para el listado Accesos a páginas web por equipo

16.5.12 Listado de Licencias

El listado de Licencias se trata en el capítulo 5 Licencias.

16.5.13 Listado de Equipos no administrados descubiertos

El listado de **Equipos no administrados descubiertos** se trata en el capítulo 6.

16.6. Listados incluidos por defecto

La consola de administración incluye cuatro listados pre generados:

- Estaciones y portátiles desprotegidos
- Malware ejecutado

- PUPs ejecutados
- Servidores desprotegidos

Estaciones y portátiles desprotegidos

Este listado permite localizar a todos los equipos de escritorio y portátiles, sin importar el sistema operativo instalado, considerados vulnerables a las amenazas debido a un problema en el funcionamiento de la protección:

- Equipos en proceso de instalación del software **Panda Adaptive Defense 360** o con error en la instalación.
- Equipos con la protección desactivada o en estado de error.
- Equipos sin licencia asignada o con licencia caducada.

Malware ejecutado

Localiza los equipos de la red que han ejecutado una amenaza en este último mes. Estos equipos son susceptibles de estar infectados por una de estas razones:

- El administrador desbloqueó un elemento desconocido antes de su clasificación y resulto ser malware.
- El administrador excluyó del análisis una amenaza conocida para habilitar su ejecución.
- El equipo se encuentra en modo Audit o en modo Hardening y la amenaza ya existían previamente a la instalación de **Panda Adaptive Defense 360.**

PUPs ejecutados

Localiza los equipos de la red que han ejecutado un programa no deseado en este último mes. Estos equipos son susceptibles de estar infectados por una de estas razones:

- El administrador desbloqueó un elemento desconocido antes de su clasificación y resulto ser un programa no deseado.
- El administrador excluyó del análisis un programa no deseado para habilitar su ejecución.
- El equipo se encuentra en modo **Audit** o en modo Hardening y el programa no deseado ya existían previamente a la instalación de **Panda Adaptive Defense 360.**

Servidores desprotegidos

Este listado permite localizar a todos los equipos de tipo servidor, sin importar el sistema operativo instalado, considerados vulnerables a las amenazas debido a un problema en el funcionamiento de la protección:

- Servidores en proceso de instalación del software **Panda Adaptive Defense 360** o con error en la instalación.
- Servidores con la protección desactivada o en estado de error.
- Servidores sin licencia asignada o con licencia caducada.

17. Gestión de amenazas, elementos en clasificación y cuarentena

17.1. Introducción

Panda Adaptive Defense 360 es capaz de equilibrar la eficacia del servicio de seguridad ofrecido, con el impacto sobre la actividad diaria que percibirán los usuarios protegidos. Este equilibro se consigue a través de varias herramientas configurables por el administrador:

- Gestión del bloqueo de los procesos en clasificación
- Gestión de la ejecución de los procesos clasificados como amenazas
- Gestión de la zona de backup / cuarentena

Gestión del bloqueo de los procesos desconocidos

Para reforzar la protección de la red, **Panda Adaptive Defense 360** incorpora el modo **Hardening** y **Lock** en su perfil de configuración avanzada de Windows, impidiendo la ejecución procesos desconocidos en los equipos de los usuarios.

Para obtener más información sobre los modos de protección avanzados consulta el capítulo 10 Configuración de seguridad para estaciones y servidores.

Las tecnologías Machine Learning ejecutadas en las plataformas Big Data de Panda Security analizan los procesos desconocidos, clasificándolos de forma automática dentro del intervalo de tiempo de 24 horas desde que fueron vistos por primera vez. La clasificación de un proceso desconocido produce una categoría no ambigua (goodware o malware) compartida para todos los clientes de Panda Security, de forma que puedan beneficiarse del conocimiento acumulado hasta la fecha.

Durante el tiempo de clasificación, **Panda Adaptive Defense 360** bloqueará la ejecución de los procesos en estudio, evitando así potenciales situaciones de peligro; sin embargo, en una minoría de casos el análisis automatizado no es capaz de clasificar el proceso desconocido con el 99'999% de certeza que se exige, y es necesaria la intervención de un experto en análisis de malware, que estudie de forma manual la muestra.

En estos casos, y si la ejecución inmediata del proceso fuera necesaria para el funcionamiento de la empresa, el administrador puede considerar necesario asumir ciertos riesgos permitir su ejecución sin esperas.

Gestión de la ejecución de los procesos clasificados como malware

En otras situaciones el administrador puede querer permitir la ejecución de ciertos tipos de malware que, a pesar de estar considerados como amenazas, implementan algunas funcionalidades valoradas por los usuarios. Este es el caso por ejemplo de PUPs, programas generalmente en forma de barras de navegador, que ofrecen capacidades de búsquedas al tiempo que recolectan información privada del usuario o confidencial de la empresa con objetivos publicitarios.

Gestión de la cuarentena

Finalmente, el administrador puede querer tener acceso a los elementos considerados como amenazas y, por lo tanto, eliminados de los equipos de los usuarios.

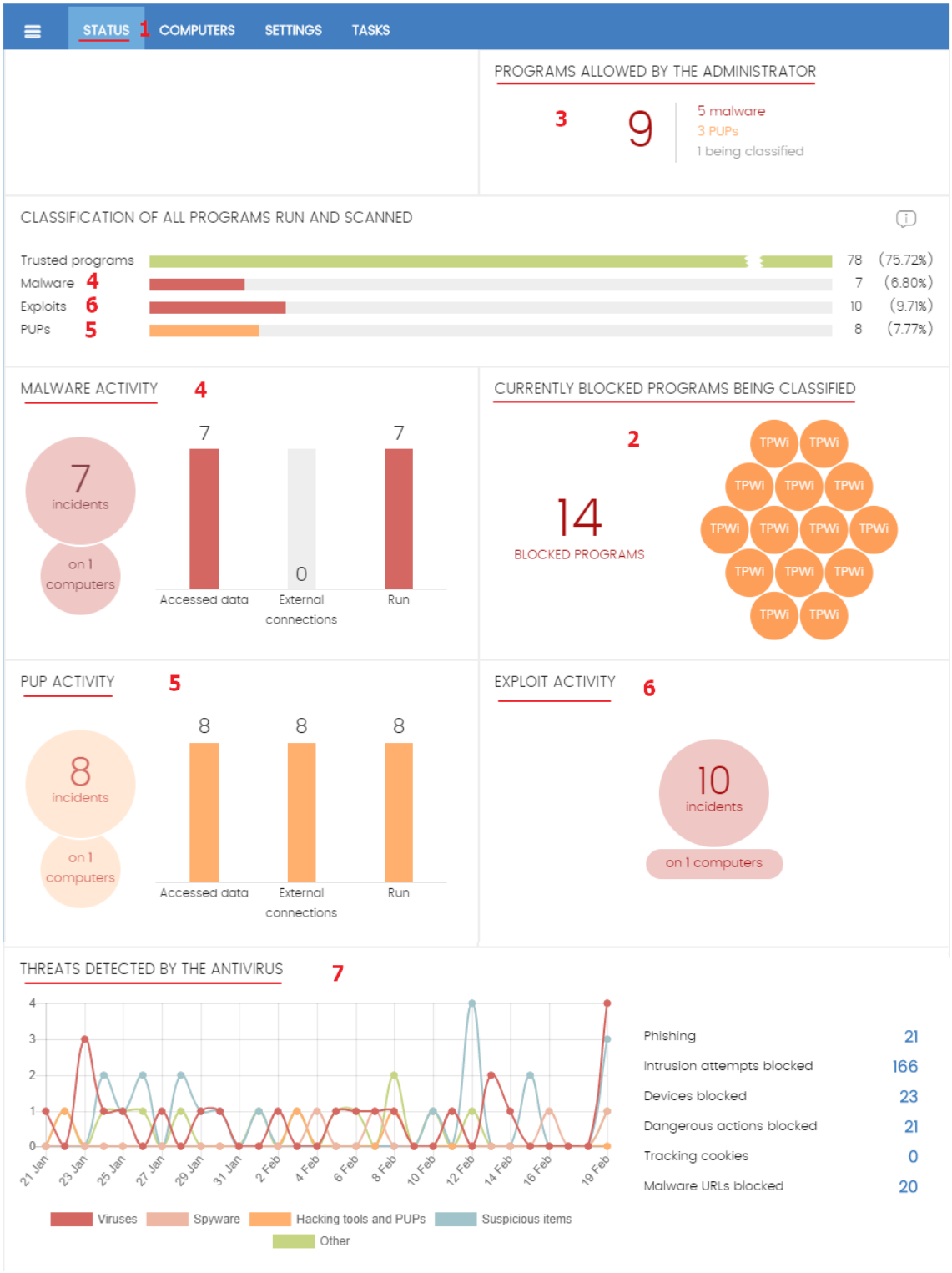


Figura 116: acceso a las herramientas de gestión de bloqueados y exclusiones desde el panel de control

17.2. Acceso a los recursos para la gestión de bloqueados y exclusiones

Los elementos bloqueados y excluidos se gestionan desde la zona Estado de la consola de administración. A continuación, se muestra una guía de referencia rápida que permite localizar cada uno de los recursos de forma rápida.

Todos los recursos mostrados son accesibles desde el Menú superior **Estado (1).** Haz clic en los widgets apropiados del panel de control mostrados en la Figura 116.

Listados de elementos bloqueados por Panda Adaptive Defense 360

- **Para listar los elementos actualmente bloqueados por estar clasificados como malware:** Panel Actividad de malware y Panel Clasificación de todos los programas ejecutados y analizados **(4).**
- **Para listar los elementos actualmente bloqueados por estar clasificados como PUP:** Panel Actividad de PUP y Panel Clasificación de todos los programas ejecutados y analizados **(5).**
- **Para listar los elementos actualmente bloqueados por estar clasificados como Exploit:** Panel Actividad de Exploit y Panel Clasificación de todos los programas ejecutados y analizados **(6)**
- **Para listar los elementos actualmente bloqueados por estar clasificados como virus:** Panel Amenazas detectadas por el antivirus **(7).**
- **Para listar los elementos actualmente bloqueados por estar en proceso de clasificación:** Panel Programas actualmente bloqueados en clasificación **(2).**

Listados de elementos excluidos del bloqueo por el administrador

- **Para listar los programas clasificados como amenaza, PUP o desconocidos actualmente excluidos de bloqueos:** Panel Programas permitidas por el administrador **(3).**
- **Para listar un histórico de los programas actualmente excluidos:** Panel Programas permitidos por el administrador **(3)**, menú contextual Histórico.
- **Para listar los cambios de estado de un programa excluido:** Panel Programas permitidos por el administrador **(3)**, menú contextual Histórico.
- **Para listar los programas clasificados como afectados por un Exploit y permitidos por el sistema:** Panel Actividad de Exploit y Panel Clasificación de todos los programas ejecutados y analizados **(6)**

Añadir y eliminar exclusiones

- **Para añadir una exclusión sobre un malware**: Panel Actividad de malware **(4)**, selección de una amenaza, **No volver a detectar.**
- **Para añadir una exclusión sobre un PUP**: Panel Actividad del PUP **(5)**, selección de una amenaza, **No volver a detectar.**
- **Para añadir una exclusión sobre un virus**: Panel Amenazas detectadas por el antivirus **(6)**, selección de una amenaza, **Restaurar y no volver a detectar.**
- **Para eliminar una exclusión:** Panel Programas permitidos por el administrador **(3)**, selección de una amenaza con el icono  .

Cambio de comportamiento de los bloqueos

- **Para cambiar el comportamiento de las reclasificaciones**: Panel Programas permitidos por el administrador **(3)**, link Cambiar comportamiento**.**

17.3. Diagrama de estados de los procesos conocidos vs desconocidos

Panda Adaptive Defense 360 bloquea por defecto todos los programas clasificados como malware y, adicionalmente, dependiendo de la configuración de la protección avanzada, también bloqueará los programas no vistos anteriormente hasta que sean analizados y emitida una clasificación sobre su seguridad.

En el caso de que un usuario no pueda esperar a que se emita una clasificación, o el administrador quiera permitir la ejecución de un elemento clasificado como malware, **Panda Adaptive Defense 360** permite la creación de exclusiones, mediante las cuales un programa en clasificación o clasificado como malware podrá ejecutarse.

IMPORTANTE: De forma general se desaconseja el desbloqueo de elementos. Los elementos bloqueados por estar clasificados como peligrosos representan un riesgo cierto para la integridad de los sistemas de IT de la empresa y sus datos. Para los elementos bloqueados por ser desconocidos existe una probabilidad alta de que terminen siendo clasificados como peligrosos. Por estas razones se recomienda evitar a toda costa el desbloqueo de elementos desconocidos o clasificados como malware / PUP.

17.3.1 Diagrama de estados para ficheros conocidos

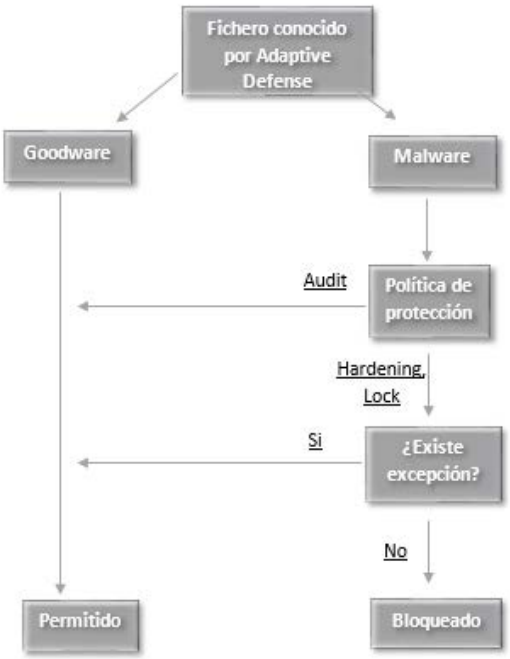


Figura 117: diagrama de acciones para procesos conocidos y ya clasificados

En el caso de un fichero clasificado por **Panda Adaptive Defense 360** como malware y una política de protección avanzada distinta de **Audit**, los ficheros serán bloqueados a no ser que el administrador genere una excepción que permita su ejecución.

17.3.2 Ficheros desconocidos

En el caso de los ficheros desconocidos (sin clasificar) y una política de protección avanzada distinta de **Audit**, los ficheros se bloquearán a no ser que el administrador de la red genere una excepción. Independientemente de la excepción, **Panda Adaptive Defense 360** clasificará el fichero y, dependiendo del resultado y de la política de reclasificación elegida, el fichero se bloqueará o se seguirá ejecutando.

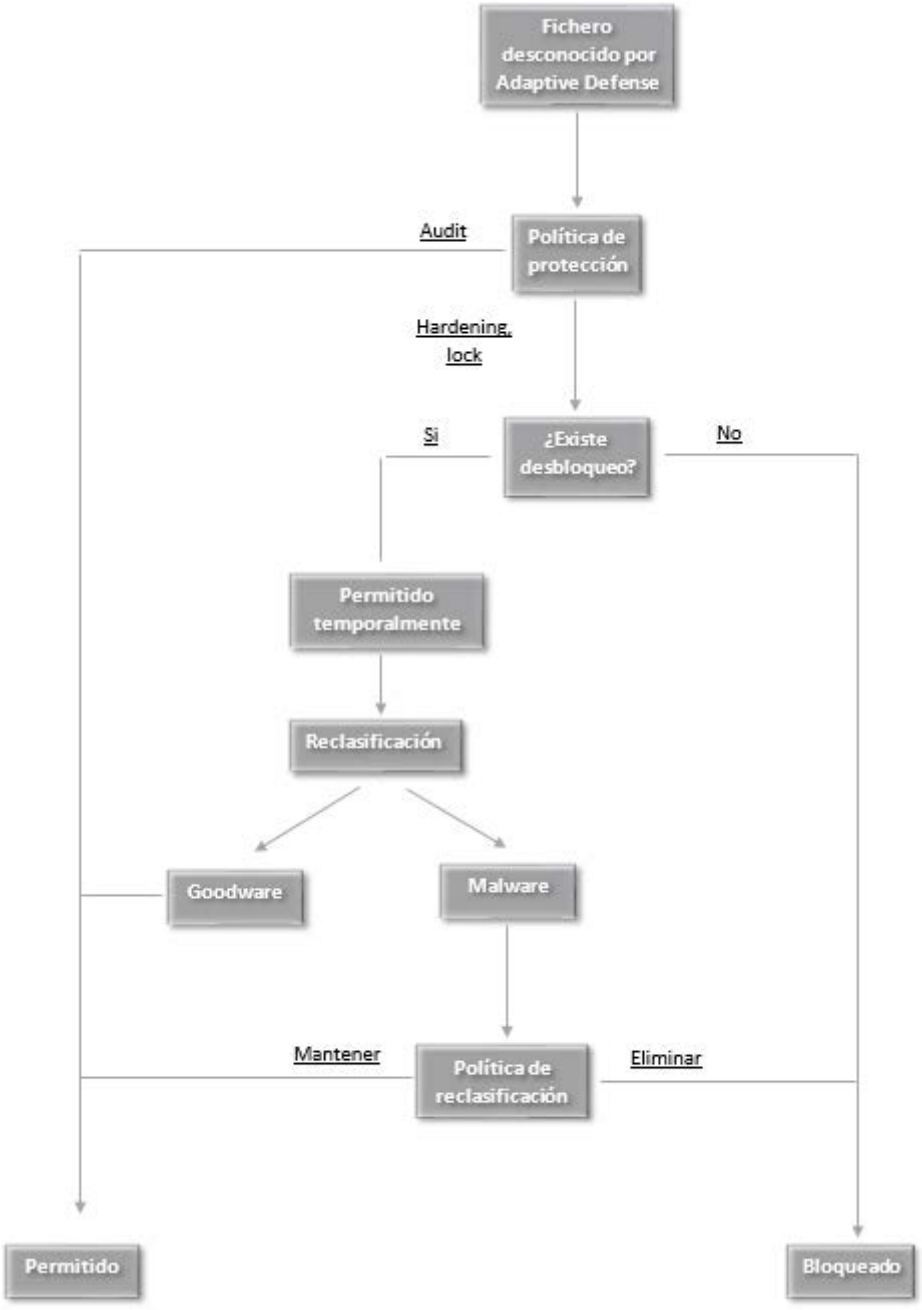


Figura 118: diagrama de acciones para procesos desconocidos

17.4. Política de reclasificación

La política de reclasificación permite determinar el comportamiento automático de **Panda Adaptive Defense 360** cuando un elemento desbloqueado por el administrador cambia su estado interno y es necesario tomar una nueva decisión.

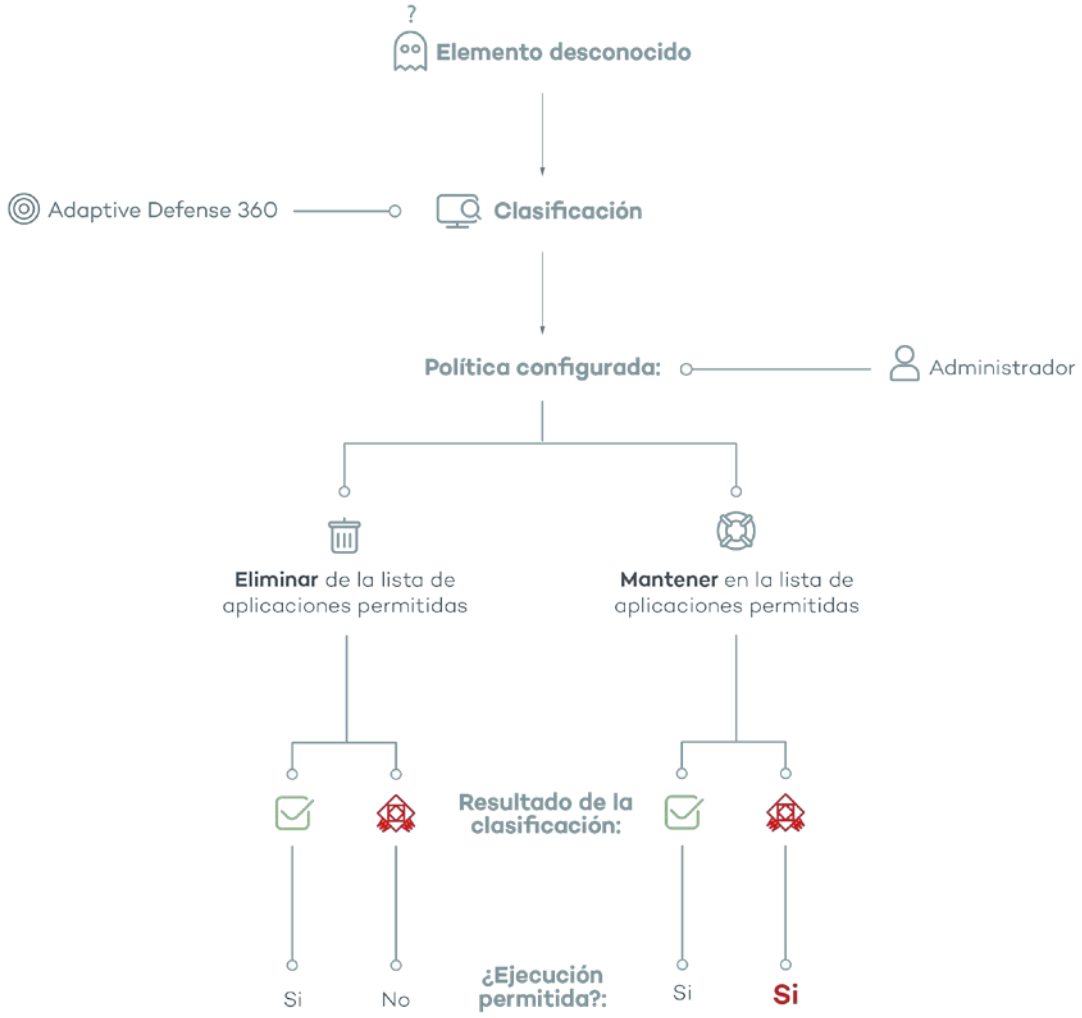


*Figura 119: comportamiento de **Panda Adaptive Defense 360** ante la política de reclasificación elegida y el resultado de la clasificación*

En los casos en los que el administrador desbloquea un elemento desconocido previamente bloqueado por **Panda Adaptive Defense 360**, lo normal es que con el tiempo el elemento pase a ser conocido y clasificado como malware o goodware. Si el elemento es clasificado como goodware no requiere ningún tipo de consideración adicional ya que el sistema continuará permitiendo su ejecución. Por el contrario, si el elemento es clasificado como malware, la política de reclasificación entra en juego, permitiendo al administrador definir el comportamiento de **Panda Adaptive Defense 360**:

- **Eliminar de la lista de Programas permitidos por el administrador**: si el fichero desconocido se ha clasificado como goodware se seguirá ejecutando de forma normal, si es clasificado como malware la exclusión se eliminará de forma automática y el fichero quedará nuevamente bloqueado, a no ser que el administrador genere una nueva exclusión manual para ese fichero.
- **Mantener en la lista de Programas permitidos por el administrador**: tanto si el fichero desconocido se ha clasificado como goodware o malware la exclusión se mantiene y el fichero seguirá ejecutándose.

17.4.1 Cambio de la política de reclasificación

Desde el menú superior **Estado**, en el panel **Programas permitidos por el administrador**, el link **Cambiar comportamiento** muestra una ventana emergente donde se puede seleccionar la política de reclasificación a aplicar.

La política de reclasificación es general para todos los equipos de la red e independiente de la configuración asignada

En caso de seleccionar **Mantener en la lista de Programas permitidos por el administrador**, se mostrará en el listado **Programas permitidos por el administrador** una franja de color rojo indicando que esta elección puede dar lugar a situaciones potencialmente peligrosas. Un escenario típico es el de un elemento desconocido originalmente, desbloqueado por el administrador para poder ser ejecutado mientras se clasifica y que, una vez terminado su análisis, resulta ser peligroso. En este caso se continuaría su ejecución por no eliminarse la exclusión de forma automática debido a la política de reclasificación **Mantener en la lista de Programas permitidos por el administrador** elegida.

17.4.2 Trazabilidad de las reclasificaciones

Es importante conocer en todo momento si **Panda Adaptive Defense 360** ha reclasificado un elemento desconocido, sobre todo si el administrador ha elegido la política de **Mantener en la lista de Programas permitidos por el administrador**.

Trazabilidad mediante el Histórico de Programas permitidos

Para visualizar el histórico de reclasificaciones y eventos de un fichero excluido, desde **Programas permitidos por el administrador** haz clic en el menú contextual para mostrar el histórico de Programas permitidos. En este listado podrás buscar por el nombre de la amenaza y en el campo **acción** se detallará el tipo de evento que se ha sucedido.

Trazabilidad mediante alertas

Las alertas le dan al administrador la posibilidad de recibir notificaciones por correo en el momento en que se producen los bloqueos por ficheros desconocidos. También puede recibir información de las reclasificaciones de los ficheros que previamente a desbloqueado.

Para habilitar las notificaciones por correo en bloqueos de ficheros desconocidos:

- En la zona **Configuración**, haz clic en la entrada **Mis alertas** del panel lateral y habilita los siguientes tipos de alertas:
  - Programas bloqueados en proceso de clasificación
  - Clasificaciones de archivos que han sido permitidos por el administrador

17.5. Añadir un desbloqueo / exclusión de elementos

Al añadir una exclusión o desbloqueo de un elemento, Panda Adaptive Defense 360 permite la ejecución de todas las librerías y binarios utilizados en el programa excluido o desbloqueado, excepto aquellos ya conocidas y clasificadas como amenazas.

Dependiendo de si el administrador quiere permitir la ejecución de un fichero en clasificación o de un fichero ya clasificado como amenaza, el control de exclusiones se realizará desde el panel **Programas actualmente bloqueados en clasificación** o desde **Actividad del Malware / PUP.**

17.5.1 Exclusión de elementos desconocidos pendientes de clasificación

Si los usuarios no pueden esperar a que el sistema haya completado la clasificación para liberar el bloqueo de forma automática, el administrador puede utilizar el botón **Desbloquear** al abrir un elemento bloqueado en el panel **Programas actualmente bloqueados en clasificación**.

Una vez desbloqueado el elemento desaparecerá del panel **Programas actualmente bloqueados en clasificación** ya que el administrador asume el riesgo de su ejecución. No obstante, **Panda Adaptive Defense 360** continuará analizando el proceso hasta completar su clasificación. El elemento desbloqueado aparecerá en el listado de **Amenazas permitidos por el administrador**, mostrado más adelante.

17.5.2 Exclusiones de elementos clasificados como malware o PUP

Excluir un elemento clasificado como malware es la operación equivalente a desbloquear un elemento bloqueado sin clasificar, si bien en este caso se está permitiendo la ejecución de un programa que **Panda Adaptive Defense 360** ya ha clasificado de forma efectiva como dañino o peligroso para el sistema.

Desde el panel **Actividad de malware / PUP** el administrador puede utilizar el botón **No volver a detectar** seleccionando previamente la amenaza que quiere permitir su ejecución.

Una vez excluido el elemento dejará de generar incidentes en los paneles de **Actividad de malware / PUP** y se añadirá al listado de **Amenazas y otros elementos excluidos,** tal y como se indica en el siguiente punto.

17.6. Gestión de los elementos excluidos

La gestión de los todos los elementos excluidos y el comportamiento del sistema ante reclasificaciones, tanto de procesos conocidos y clasificados como una amenaza como de desconocidos, se realiza desde el panel **Programas permitidos por el administrador**.

Este panel permite visualizar y gestionar los ficheros actualmente permitidos, así como acceder a un histórico de los elementos excluidos.

Listado de exclusiones en curso

Programas permitidos por el administrador muestra los elementos que tienen una exclusión activa. Todos los elementos que aparecen listados tienen permitida su ejecución.

Historial

Haciendo clic en el menú de contexto, **Historial** podrás visualizar el histórico de cambios realizado sobre los ficheros excluidos en **Panda Adaptive Defense 360**. El listado permite ver el ciclo de estados completo de un fichero, desde que entra en el listado de **Programas permitidos por el administrador** hasta que sale del mismo, pasando por los cambios de estado intermedios que el sistema o el administrador pueda haber aplicado.

17.7. Estrategias para la supervisión del proceso de clasificación en ficheros desconocidos

En el funcionamiento diario de un equipo protegido con **Panda Adaptive Defense 360** es posible que aparezca un pequeño porcentaje de programas desconocidos que tengan que ser clasificados. Dependiendo de la configuración avanzada, estos programas serán bloqueados hasta que los procesos de clasificación emitan un resultado (goodware o malware), con lo que los usuarios no podrán utilizar estos programas de forma temporal.

Si el departamento de IT controla la instalación de programas en los equipos de la red y quiere minimizar el impacto del software desconocido en el trabajo de los usuarios, pero a su vez no se quieren realizar concesiones a la seguridad (es decir, permitir temporalmente la ejecución de programas sin clasificar), es recomendable preparar de antemano la ejecución del software nuevo antes de su instalación y uso masivo.

El procedimiento de preparación se puede dividir en tres pasos, mostrados a continuación.

Configuración de un PC de pruebas

El objetivo es determinar si el software a utilizar posteriormente en la red es ya conocido como malware, o desconocido para Panda Security. Para ello se puede utilizar el PC de un usuario de la red, o utilizar un equipo dedicado a este objetivo. Este equipo deberá de tener asignada inicialmente una configuración de seguridad avanzada **Hardening**.

Instalación del software

En este paso se instala el software y se ejecuta de forma normal. Si **Panda Adaptive Defense 360** encuentra algún módulo o programa desconocido lo bloqueará mostrando una ventana emergente en el equipo. Además, se añadirá un nuevo elemento en el panel **Programas actualmente bloqueados en clasificación**. Internamente, **Panda Adaptive Defense 360** registrará los eventos generados por el uso del programa y enviará los binarios a la nube para poder estudiarlos.

Si no se han presentado bloqueos en el modo Hardening, el administrador deberá de cambiar la configuración a modo Lock y volver a ejecutar el programa recién instalado. En el caso de que aparezcan nuevos bloqueos el panel **Programas actualmente bloqueados en clasificación** los reflejará.

Reclasificación de programas bloqueados

En el momento en que **Panda Adaptive Defense 360** emita una clasificación de los programas bloqueados se enviará una notificación por correo al administrador avisando del desbloqueo si la clasificación es goodware, o su bloqueo por considerarse una amenaza. Cuando todos los procesos hayan sido reclasificados como goodware, el software instalado será apto para su ejecución en el parque informático.

Envío del programa directamente a la nube de Panda Security

Debido a que **Panda Adaptive Defense 360** está preparado para no impactar en el rendimiento de la red en el caso de tener que enviar ficheros a la nube de Panda Security, el envío de tales ficheros puede demorarse en el tiempo. Si quieres acelerar el envío ponte el contacto con el departamento de soporte de Panda Security.

17.8. Gestión de la zona de backup / cuarentena

La cuarentena en **Panda Adaptive Defense 360** es el área de backup donde se copian los elementos eliminados por haber sido clasificados como amenaza.

El almacenamiento de los elementos eliminados se realiza en el propio equipo del usuario, en el directorio `Quarantine` de la carpeta donde se instaló el software. Se trata de una carpeta inaccesible al resto de procesos del equipo y cifrada, de manera que no es posible el acceso ni la ejecución de los programas allí contenidos de forma directa, si no es a través de la consola Web.

La cuarentena es compatible con las plataformas Windows, macOS y Linux. No se soporta en dispositivos Android.

El envío de elementos al área de backup es automático y establecido por el departamento de Panda Labs en Panda Security, según sea su clasificación después de haber efectuado su análisis.

Una vez que los elementos sospechosos han sido enviados a Panda Security para su análisis, se pueden producir cuatro situaciones:

- Si se comprueba que los elementos son maliciosos, son desinfectados y posteriormente restaurados a su ubicación original, siempre y cuando exista desinfección para ello.
- Si se comprueba que los elementos son maliciosos y no existe manera de desinfectarlos, permanecerán en la cuarentena durante 7 días.
- Si se comprueba que no se trata de elementos perjudiciales, son restaurados directamente a su ubicación.
- Si se comprueba que son elementos sospechosos se almacenan durante 30 días como máximo. Si finalmente resultan ser goodware se restauran automáticamente.

Panda Adaptive Defense 360 no borra ningún fichero del equipo del usuario. Todos los elementos eliminados son en realidad enviados al área de backup

17.8.1 Visualización de los elementos en cuarentena

El administrador puede visualizar los elementos introducidos en la cuarentena mediante los listados y los widgets del Panel de control, indicados a continuación:

- Actividad de malware
- Actividad de PUP
- Amenazas detectadas por el antivirus

Con ayuda de las herramientas de filtrado se puede obtener el listado de elementos introducidos en cuarentena, reflejados en el campo **Acción** como “Movido a cuarentena” o “Eliminado”.

17.8.2 Restaurar elementos de cuarentena

Para restaurar un elemento en cuarentena haz clic en el botón **Restaurar y no volver a detectar**. Esta acción no solo copiará el fichero a su ubicación original, sino que restaurará los permisos, propietario, entradas del registro referidas al fichero y otra información referida al fichero.

18. Análisis forense

Detalle de amenazas y programas bloqueados
Tablas de acciones
Grafos de ejecución
Tablas Excel
Interpretación de las tablas y grafos

18.1. Introducción

El malware de nueva generación se caracteriza por pasar inadvertido durante largos periodos de tiempo, tiempo que es aprovechado para acceder a datos sensibles o a propiedad intelectual de la empresa. Su objetivo es obtener una contrapartida económica, cifrando documentos clave y realizando un chantaje o vendiendo la información obtenida a la competencia, entre otras estrategias comunes a este tipo de ataques informáticos.

Cuando el panel de control de **Panda Adaptive Defense 360** muestra un riesgo de infección, es necesario determinar hasta qué punto ha sido comprometida la red y cuál fue el origen de la infección. Para ello, hay que determinar las acciones que llevó a cabo el malware, y así poder tomar las medidas apropiadas. **Panda Adaptive Defense 360** es capaz de monitorizar de forma continuada todas las acciones ejecutadas por las amenazas, y almacenarlas para mostrar el curso de las mismas, desde su primera aparición en la red hasta su neutralización.

Panda Adaptive Defense 360 presenta este tipo de información de varias formas según el grado de detalle y tipo de información que se necesite:

- Páginas de detalle
- Tablas de acciones
- Diagramas de grafos
- Ficheros Excel

18.2. Detalle de las amenazas y de los programas actualmente bloqueados en clasificación

Desde el menú superior **Estado** accede a los listados de amenazas y programas bloqueados a través de los paneles:

- **Actividad de malware**
- **Actividad de PUPs**
- **Actividad de Exploits**
- **Programas actualmente bloqueados en clasificación**

Haz clic sobre una amenaza concreta para abrir la ventana **Detección del malware, Detección de PUP, Detección de Exploit o Detalles del programa bloqueado** para mostrar toda su información en la pestaña **Detalles.**

18.2.1 Detección de malware, PUP y programas bloqueados en clasificación

La ventana se divide en 5 secciones:

- **Información general**
- **Equipo afectado**

- **Impacto de la amenaza en el equipo**
- **Origen de la infección**
- **Apariciones en otros equipos**

Información general

- **Amenaza**: nombre de la amenaza y hash que la identifica.
- **Acción**: muestra el tipo de acción que **Panda Adaptive Defense 360** a ejecutado sobre el elemento.
  - Movido a Cuarentena
  - Bloqueado
  - Desinfectado
  - Eliminado

Consulta el capítulo 17 para obtener información sobre las acciones que el administrador puede ejecutar sobre los elementos encontrados.

Equipo afectado 

- **Equipo**: nombre del equipo donde se detectó la amenaza, dirección IP y carpeta a la que pertenece en el árbol de grupos.
- **Visualizar parches disponibles**: si el módulo Panda Patch Management está activado muestra los parches y actualizaciones pendientes de instalar en el equipo.
- **Usuario logeado**: usuario del sistema operativo bajo el cual se cargó y ejecutó o la amenaza.
- **Modo de protección**: configuración de la protección avanzada en el momento de producirse la detección (**Audit**, **Hardening**, **Lock**).
- **Ruta de detección**: ruta del sistema de ficheros donde reside la amenaza.

Impacto de la amenaza en el equipo 

- **Amenaza**: nombre de la amenaza detectada y cadena resumen de identificación del archivo (hash). Haz clic en los dos botones para ampliar información en Internet mediante el buscador Google y la web de Virustotal. Si la amenaza es de reciente aparición se mostrará la leyenda **Nueva amenaza**
- **Actividad**: resumen de las acciones más importantes ejecutadas por el malware:
  - **Se ha ejecutado** 
  - **Ha accedido a datos** 
  - **Ha intercambiado datos con otros equipos** 

- **Fecha de detección**
- **Tiempo de exposición**: tiempo que la amenaza ha permanecido en el sistema sin clasificar.

Origen de la infección

- **Equipo origen de la infección**: en el caso de que el intento de infección venga de un equipo de la red del cliente, indica el nombre del equipo.
- **IP origen de la infección**: en el caso de que el intento de infección venga de un equipo de la red del cliente, indica la dirección IP del equipo.
- **Usuario origen de la infección**: usuario logeado en la máquina origen de la infección

Apariciones en otros equipos

Muestra todos los equipos de la red donde fue visto el malware detectado.

- **Equipo**: nombre del equipo.
- **Ruta del archivo:** ruta y nombre del fichero que contiene el malware.
- **Fecha primera aparición**: fecha en la que la amenaza fue detectada por primera vez en ese equipo.

También se incluye un acceso a la gráfica de actividad del malware, tratada más adelante en este capítulo.

18.2.2 Detección exploit

La ventana se divide en 5 secciones:

- **Información general**
- **Equipo afectado**
- **Impacto de la amenaza en el equipo**
- **Origen de la infección**
- **Apariciones en otros equipos**

Información general

- **Programa comprometido**: nombre del programa que fue afectado por el exploit y hash que lo identifica.
- **Acción**: muestra el tipo de acción que **Panda Adaptive Defense 360** a ejecutado sobre el programa afectado por el exploit.
  - **Permitido**: la protección anti-exploit está configurada en modo **Audit**. El exploit se ejecutó.
  - **Bloqueado**: el exploit fue bloqueado antes de su ejecución.
  - **Permitido por el usuario**: se preguntó al usuario del equipo si finalizar el proceso comprometido y el usuario decidió permitir que el exploit continuara ejecutándose.
  - **Proceso finalizado**: el exploit fue eliminado, pero se llegó a ejecutar parcialmente.

- **Pendiente de reinicio**: se informó al usuario del equipo de la necesidad de reiniciar el equipo para eliminar completamente el exploit. Mientras tanto el exploit se seguirá ejecutando.

Equipo afectado

- **Equipo**: nombre del equipo donde se detectó la amenaza, dirección IP y carpeta a la que pertenece en el árbol de grupos.
- **Usuario logueado**: usuario del sistema operativo bajo el cual se cargó y ejecutó o la amenaza.
- **Modo de protección**: configuración de la protección avanzada en el momento de producirse la detección (**Audit**, **Hardening**, **Lock**).
- **Ruta de detección**: ruta del sistema de ficheros donde reside la amenaza.

Impacto del exploit en el equipo

- **Programa comprometido**: ruta y nombre del programa que recibió el intento de explotación. Si **Panda Adaptive Defense 360** detectó que el programa no está actualizado a la última versión publicada por el proveedor, mostrará el aviso **Programa vulnerable.**
- **Actividad** : indica si el exploit se llegó a ejecutar antes de ser detectado por **Panda Adaptive Defense 360**.
- **Fecha de detección**
- **Ultimas URLs accedidas:** listado con las URLs accedidas por el proceso vulnerable en el momento en que fue afectado por el exploit.

También se incluye un acceso a la gráfica de actividad del malware, tratada más adelante en este capítulo.

18.3. Tablas de acciones

Accede a los listados de amenazas y programas bloqueados desde el menú superior **Estado** a través de los paneles:

- **Actividad de malware**
- **Actividad de PUPs**
- **Actividad de Exploits**
- **Programas actualmente bloqueados en clasificación.**

Haz clic sobre una amenaza concreta para abrir la ventana **Detección del malware, Detección de PUP, Detección de Exploit** y **Detalles del programa bloqueado** para mostrar toda su información en la pestaña **Actividad.**

La información de la amenaza se muestra en una tabla de acciones, que incluye los eventos más relevantes producidos.

La cantidad de acciones ejecutadas por un proceso es muy alta, visualizarlas todas dificultaría la extracción de información útil para realizar un análisis forense.

El contenido de la tabla se presenta inicialmente ordenado por fecha, de esta forma es más fácil seguir el curso de la amenaza.

En la Tabla 72 se detallan los campos incluidos en la tabla de acciones:

Campo	Comentario	Valores
Fecha	Fecha de la acción registrada	Fecha
Nº veces	Número de veces que se ejecutó la acción. Una misma acción ejecutada varias veces de forma consecutiva solo aparece una vez en el listado de acciones con el campo Nº veces actualizado	Numérico
Acción	Tipo de acción registrada en el sistema y línea de comandos asociada a la ejecución de la acción	Descargado de Comunica con Accede a datos Es ejecutado por Ejecuta Es creado por Crea Es modificado por Modifica Es cargado por Carga Es borrado por Borra Es renombrado por Renombra Es matado por Mata proceso Crea hilo remoto Hilo inyectado por Es abierto por Abre Crea Es creado por Crea clave apuntando a Exe Modifica clave apuntando a Exe

Campo	Comentario	Valores
Path/URL/Clave de Registro /IP:Puerto	Entidad de la acción. Según sea el tipo de acción podrá contener diferentes valores	**Clave del registro**: acciones que impliquen modificación del registro de Windows **IP:Puerto**: acciones que implican una comunicación con un equipo local o remoto **Path**: acciones que implican acceso al disco duro del equipo **URL**: acciones que implican el acceso a una URL
Hash del Fichero/Valor del Registro /Protocolo-Dirección/Descripción	Campo que complementa a la entidad	**Hash del Fichero**: para todas las acciones que implican acceso a un fichero **Valor del Registro**: para todas las acciones que implican un acceso al registro **Protocolo-Dirección**: para todas las acciones que implican una comunicación con un equipo local o remoto. Los valores posibles son: • TCP • UDP • Bidirectional • UnKnown • Descripción
Confiable	El fichero está firmado digitalmente	Binario

Tabla 72: campos de la tabla de acciones de una amenaza

18.3.1 Sujeto y predicado en las acciones

El formato utilizado para presentar la información en el listado de acciones mantiene cierto paralelismo con el lenguaje natural:

- Todas las acciones tienen como sujeto el fichero clasificado como amenaza. Este sujeto no se indica en cada línea de la tabla de acciones porque es común para toda la tabla.
- Todas las acciones tienen un verbo que relaciona el sujeto (la amenaza clasificada) con un complemento, llamado entidad. La entidad se corresponde con el campo **Path/URL/Clave de Registro /IP:Puerto** de la tabla.
- La entidad se complementa con un segundo campo que añade información a la acción, indicado en el campo **Hash del Fichero/Valor del Registro /Protocolo-Dirección/Descripción**.

En la Tabla 73 se muestran dos acciones de ejemplo de un mismo malware hipotético:

Fecha	Nº veces	Accion	Path/URL/Registro/IP	Hash/Registro/Protocolo/Descripción	Confiable
3/30/2015 4:38:40 PM	1	Comunica con	54.69.32.99:80	TCP-Bidrectional	NO
3/30/2015 4:38:45 PM	1	Carga	PROGRAM_FILES|\MOVIES TOOLBAR\SAFETYN	9994BF035813FE8EB6BC98ECCBD5B0E1	NO

Tabla 73: listado de acciones de una amenaza de ejemplo

La primera acción indica que el malware (sujeto) se conecta (Acción **Connects with**) con la dirección IP `54.69.32.99:80` (entidad) mediante el protocolo TCP-Bidireccional.

La segunda acción indica que el malware (sujeto) carga (Acción **Loads**) la librería `PROGRAM_FILES|\MOVIES TOOLBAR\SAFETYNUT\SAFETYCRT.DLL` con hash `9994BF035813FE8EB6BC98ECCBD5B0E1.`

Al igual que en el lenguaje natural, en **Panda Adaptive Defense 360** se implementan dos tipos de oraciones:

- **Activa**: Son acciones predicativas (con un sujeto y un predicado) relacionados por un verbo en forma activa. En estas acciones, el verbo de la acción relaciona el sujeto, que siempre es el proceso clasificado como amenaza y un complemento directo, la entidad, que puede ser de múltiples tipos según la acción.
- **Pasiva**: Son acciones donde el sujeto (el proceso clasificado como amenaza) pasa a ser sujeto paciente (que recibe la acción, no la ejecuta) y el verbo viene en forma pasiva (ser + participio). En este caso el verbo pasivo relaciona el sujeto pasivo que recibe la acción con la entidad, que es la que realiza la acción.

Ejemplos de acciones activas son los siguientes:

- Comunica con
- Carga
- Crea

Ejemplos de acciones pasivas son los siguientes:

- Es creado por
- Descargado de

La Tabla 74 muestra una acción pasiva de ejemplo para un malware hipotético

Fecha	Nº veces	Accion	Path/URL/Registro/IP	Hash/Registro/Protocolo/Descripción	Confiable
3/30/2015 4:51:46 PM	1	Es ejecutado por	WINDOWS| \ explorer.exe	7522F548A84ABAD8FA516D E5AB3931EF	NO

Tabla 74: ejemplo de acción pasiva

En esta acción el malware (sujeto pasivo) es ejecutado (acción pasiva Es ejecutado por) por el programa `WINDOWS|\explorer.exe` (entidad) de hash `7522F548A84ABAD8FA516DE5AB3931EF`.

Las acciones de tipo Activo nos permiten inspeccionar en detalle los pasos que ha ejecutado la amenaza. Por el contrario, las acciones de tipo pasivo suelen reflejar el vector de infección utilizado por el malware (qué proceso lo ejecutó, qué proceso lo copió al equipo del usuario etc.).

18.4. Grafos de ejecución

Desde el menú superior **Estado** accede a los listados de amenazas y programas bloqueados a través de los paneles:

- **Actividad de malware**
- **Actividad de PUPs**
- **Actividad de Exploits**
- **Programas actualmente bloqueados en clasificación.**

Haz clic sobre una amenaza concreta para abrir la ventana Detección del malware, Detección de PUP, Detección de Exploit o Detalles del programa bloqueado, selecciona la pestaña Actividad y haz clic en el botón Ver gráfica de actividad.

Los grafos de ejecución representan de forma visual la información mostrada en las tablas de acciones, poniendo énfasis en el enfoque temporal. Los grafos se utilizan inicialmente para tener, de un solo vistazo, una idea general de las acciones desencadenadas por la amenaza.

18.4.1 Diagramas

La cadena de acciones en la vista de grafos de ejecución queda representada por dos elementos:

- **Nodos**: representan acciones en su mayoría, o elementos informativos
- **Líneas y flechas**: unen los nodos de acción e informativos para establecer un orden temporal y asignar a cada nodo el rol de “sujeto” o “predicado”.

Figura 120: ejemplo de amenaza representada mediante grafos

18.4.2 Nodos

Los nodos muestran la información mediante su icono asociado, color y un panel descriptivo que se muestra a la derecha de la pantalla cuando se seleccionan con el ratón.

El código de colores utilizado es el siguiente:

- **Rojo**: elemento no confiable, malware, amenaza.
- **Naranja**: elemento desconocido, no catalogado.
- **Verde**: elemento confiable, goodware.

La Tabla 75 lista los nodos de tipo acción junto con una breve descripción:

Símbolo	Descripción
	Fichero descargado Fichero comprimido creado
	Socket / comunicación usada
	Comenzada la monitorización
	Proceso creado

Símbolo	Descripción
	Fichero ejecutable creado Librería creada Clave en el registro creada
	Fichero ejecutable modificado Clave de registro modificada
	Fichero ejecutable mapeado para escritura
	Fichero ejecutable borrado
	Librería cargada
	Servicio instalado
	Fichero ejecutable renombrado
	Proceso detenido o cerrado
	Hilo creado remotamente
	Fichero comprimido abierto

Tabla 75: representación gráfica de acciones en el diagrama de grafos

La Tabla 76 lista los nodos de tipo descriptivo junto con una breve descripción

Símbolo	Descripción
	Nombre de fichero y extensión **Verde**: Goodware **Naranja**: No catalogado **Rojo**: Malware/PUP
	Equipo interno (está en la red corporativa) **Verde**: Confiable **Naranja**: desconocido **Rojo**: No confiable
	Equipos externos **Verde**: Confiable **Naranja**: desconocido **Rojo**: No confiable
	País asociado a la IP de un equipo externo
	Fichero y extensión
	Clave del registro

Tabla 76: tipos de nodo en el diagrama de grafos

18.4.3 Líneas y flechas

Las líneas del diagrama de grafos relacionan los diferentes nodos y ayudan a establecer visualmente el orden de ejecución de las acciones.

Los dos atributos de una línea son:

- **Grosor de la línea**: indica el número de veces que ha aparecido la relación en el diagrama. A mayor número de veces mayor tamaño de la línea
- **Flecha**: marca la dirección de la relación entre los dos nodos.

18.4.4 La línea temporal

La línea temporal o Timeline permite controlar la visualización de la cadena de acciones realizada por la amenaza a lo largo del tiempo. Mediante los botones situados en la parte inferior de la pantalla se puede visualizar el momento preciso donde la amenaza realizó cierta acción, y recuperar información extendida que puede ayudar en los procesos de análisis forense.

La línea temporal de los grafos de ejecución tiene este aspecto:

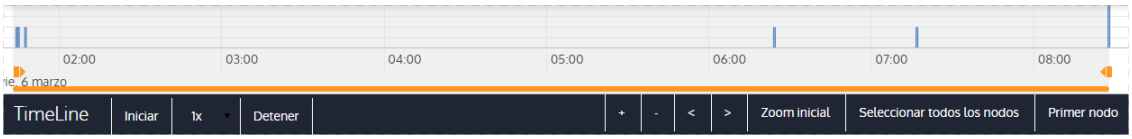


Figura 121: representación gráfica de la linea temporal de una amenaza

Inicialmente es posible seleccionar un intervalo concreto de la línea temporal arrastrando los selectores de intervalo hacia la izquierda o derecha para abarcar la franja temporal que más interese.

Figura 122: selectores del intervalo temporal a presentar

Una vez seleccionada la franja temporal, el grafo mostrará únicamente las acciones y nodos que caigan dentro de ese intervalo. El resto de acciones y nodos quedará difuminado en el diagrama.

Las acciones de la amenaza quedan representadas en la línea temporal como barras verticales acompañadas del time stamp, que marca la hora y minuto donde ocurrieron.

Figura 123: timestamp, fecha y acciones de la amenaza

18.4.5 Zoom in y Zoom out

Con los botones + y – de la barra temporal puedes hacer zoom in o zoom out para ganar mayor resolución en el caso de que haya muchas acciones en un intervalo de tiempo corto.

18.4.6 Timeline (línea temporal)

Para poder ver la ejecución completa de la amenaza y la cadena de acciones que ejecutó, se utilizan los siguientes controles:

- **Iniciar**: comienza la ejecución de la Timeline a velocidad 1x. Los grafos y las líneas de acciones irán apareciendo según se vaya recorriendo la línea temporal.
- **1x**: establece la velocidad de recorrido de la línea temporal.
- **Detener**: detiene la ejecución de la línea temporal.

- **+** y **-**: zoom in y zoom out de la línea temporal.
- : mueve la selección del nodo al inmediatamente anterior o posterior.
- **Zoom inicial**: recupera el nivel de zoom inicial si se modificó con los botones + y –.
- **Seleccionar todos los nodos**: mueve los selectores temporales para abarcar toda la línea temporal.
- **Primer nodo**: Establece el intervalo temporal en el inicio, paso necesario para iniciar la visualización de la TimeLine completa.

Para poder visualizar el recorrido completo de la Timeline primero selecciona "Primer nodo" y después "Iniciar". Para ajustar la velocidad de recorrido selecciona el botón 1x.

18.4.7 Filtros

En la parte superior del diagrama de grafos se encuentran los controles para filtrar la información que se mostrará.

Figura 124: filtros en el diagrama de grafos

Los criterios de filtrado disponibles son:

- **Acción**: desplegable que permite seleccionar un tipo de acción de entre todas las ejecutadas por la amenaza. De esta manera el diagrama solo mostrará los nodos que coincidan con el tipo de acción seleccionada y aquellos nodos adyacentes relacionados con esta acción.
- **Entidad**: desplegable que permite elegir una entidad (contenido del campo Path/URL/Entrada de registro /IP:Puerto).

18.4.8 Movimiento de los nodos y zoom general del grafo

Para mover el grafo en las cuatro direcciones y hacer zoom in o zoom out utiliza los controles situados en la parte superior derecha del grafo.

Para hacer zoom in y zoom out más fácilmente utiliza la rueda central del ratón.

El símbolo X permite salir de la vista de grafos. Si se prefiere ocultar la zona de botones Timeline para utilizar un mayor espacio de la pantalla haz clic en el icono  situado en la parte inferior derecha del grafo.

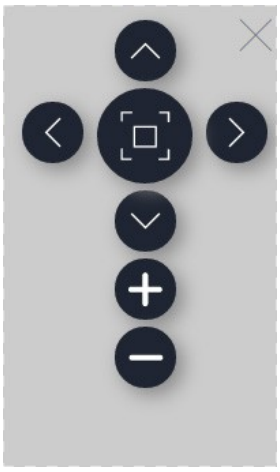


Figura 125: botonera para controlar el nivel de zoom del diagrama de grafos

Finalmente, el comportamiento del grafo representando en pantalla es configurable mediante el panel de la Figura 126, accesible al seleccionar el botón  situado en la zona superior izquierda del grafo.

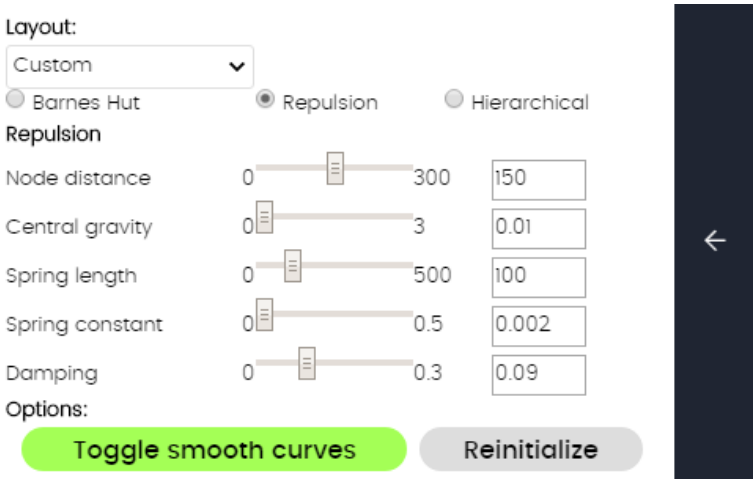


Figura 126: panel de configuración del diagrama de grafos

18.5. Tablas Excel

Desde el menú superior **Estado** accede a los listados de amenazas y programas bloqueados a través de los paneles:

- **Actividad de malware**
- **Actividad de PUPs**
- **Actividad de Exploits**
- **Programas actualmente bloqueados en clasificación.**

Haz clic sobre el menú de contexto y selecciona en el desplegable **Exportar listado y detalles**. Se descargará un fichero Excel con el ciclo de vida completo de todas las amenazas mostradas en el listado.

Campo	Comentario	Valores
Fecha	Fecha de la acción registrada	Fecha
Hash	Cadena resumen de identificación de la amenaza	Cadena de caracteres
Amenaza	Nombre de la amenaza	
Usuario	Cuenta de usuario bajo la cual se ejecutó la amenaza	Cadena de caracteres
Equipo	Nombre del equipo donde se encontró la amenaza	Cadena de caracteres
Ruta	Nombre de la amenaza y ruta en el equipo del usuario	Cadena de caracteres
Acceso a datos	La amenaza ha accedido a ficheros que residen en el equipo del usuario	Binario
Acción	Tipo de acción registrada en el sistema	Descargado de Comunica con Accede a datos Es ejecutado por Ejecuta Es creado por Crea Es modificado por Modifica Es cargado por Carga Es borrado por Borra Es renombrado por Renombra Es matado por Mata proceso Crea hilo remoto Hilo inyectado por Es abierto por Abre Crea Es creado por Crea clave apuntando a Exe Modifica clave apuntando a Exe
Línea de comandos	línea de comandos asociada a la ejecución de la acción	Cadena de caracteres
Fecha del evento		Cadena de caracteres

Campo	Comentario	Valores
Nº veces	Número de veces que se ejecutó la acción. Una misma acción ejecutada varias veces de forma consecutiva solo aparece una vez en el listado de acciones con el campo Nº veces actualizado	Numérico
Path/URL/Clave de Registro /IP:Puerto	Entidad de la acción. Según sea el tipo de acción podrá contener diferentes valores	**Clave del registro**: acciones que impliquen modificación del registro de Windows **IP:Puerto**: acciones que implican una comunicación con un equipo local o remoto **Path**: acciones que implican acceso al disco duro del equipo **URL**: acciones que implican el acceso a una URL
Hash del Fichero/Valor del Registro /Protocolo-Dirección/Descripción	Campo que complementa a la entidad	**Hash del Fichero**: para todas las acciones que implican acceso a un fichero **Valor del Registro**: para todas las acciones que implican un acceso al registro **Protocolo-Dirección**: para todas las acciones que implican una comunicación con un equipo local o remoto. Los valores posibles son: • TCP • UDP • Bidirectional • UnKnown • Descripción
Confiable	El fichero está firmado digitalmente	Binario

Tabla 77: campos del fichero exportado Listado y detalles

18.6. Interpretación de las tablas de acciones y grafos de actividad

Las tablas de acciones y grafos de actividad son representaciones de los volcados de evidencias recogidas en el equipo del cliente, que deberán ser interpretadas por el administrador de red de la empresa. Por esta razón se requieren ciertos conocimientos técnicos para poder extraer pautas e información clave en cada situación.

A continuación, se ofrecen unas directrices básicas a la hora de interpretar las tablas de acciones mediante varios ejemplos de amenazas reales.

El nombre de las amenazas aquí indicadas puede variar entre diferentes proveedores de seguridad. Para identificar un malware concreto se recomienda utilizar el hash de identificación.

18.6.1 Ejemplo 1: Visualización de las acciones ejecutadas por el malware Trj/OCJ.A

En la pestaña **Detalles** se muestra la información fundamental del malware encontrado. En este caso los datos relevantes son los siguientes:

- **Amenaza**: Trj/OCJ.A
- **Equipo**: XP-BARCELONA1
- **Ruta de detección**: `TEMP|\Rar$EXa0.946\appnee.com.patch.exe`

Actividad

La pestaña **Actividad** contiene acciones ya que el modo de **Panda Adaptive Defense 360** configurado era Hardening y el malware ya residía en el equipo en el momento en que **Panda Adaptive Defense 360** se instaló, siendo desconocido en el momento de su ejecución.

Hash

Con la cadena de hash se podrá obtener más información de recursos web como Virus total para tener una idea general de la amenaza y funcionamiento.

Ruta de detección

La ruta donde se detectó el malware por primera vez en el equipo pertenece a un directorio temporal y contiene la cadena RAR: la amenaza procede de un fichero empaquetado que el programa WinRar descomprimió temporalmente en el directorio, y dio como resultado el ejecutable appnee.com.patch.exe.

Pestaña Actividad

Paso	Fecha	Acción	Ruta
1	3:17:00	Es creado por	PROGRAM_FILES|\WinRAR\WinRAR.exe
2	3:17:01	Es ejecutado por	PROGRAM_FILES|\WinRAR\WinRAR.exe
3	3:17:13	Crea	TEMP|\bassmod.dll
4	3:17:34	Crea	PROGRAM_FILES|\Adobe\ACROBAT 11.0\Acrobat\AMTLIB.DLL.BAK
5	3:17:40	Modifica	PROGRAM_FILES|\Adobe\ACROBAT 11.0\Acrobat\amtlib.dll
6	3:17:40	Borra	PROGRAM_FILES|\ADOBE\ACROBAT 11.0\ACROBAT\AMTLIB.DLL.BAK

Paso	Fecha	Acción	Ruta
7	3:17:41	Crea	PROGRAM_FILES|\Adobe\ACROBAT 11.0\Acrobat\ACROBAT.DLL.BAK
8	3:17:42	Modifica	PROGRAM_FILES|\Adobe\ACROBAT 11.0\Acrobat\Acrobat.dll
9	3:17:59	Ejecuta	PROGRAM_FILES|\Google\ Chrome\Application\chrome.exe

Tabla 78: listado de acciones Trj/OCJ.A

Los pasos 1 y 2 indican que el malware fue descomprimido por el WinRar.Exe y ejecutado desde el mismo programa: el usuario abrió el fichero comprimido e hizo clic en el binario que contiene.

Una vez en ejecución en el paso 3 el malware crea una dll (bassmod.dll) en una carpeta temporal y otra (paso 4) en el directorio de instalación del programa Adobe Acrobat 11. En el paso 5 también modifica una dll de Adobe, quizá para aprovechar algún tipo de exploit del programa.

Después de modificar otras dlls lanza una instancia de Chrome y en ese momento termina la Timeline; **Panda Adaptive Defense 360** catalogó el programa como amenaza después de esa cadena de acciones sospechosas y ha detenido su ejecución.

En la Timeline no aparecen acciones sobre el registro, de modo que es muy probable que el malware no sea persistente o no haya podido ejecutarse hasta el punto de sobrevivir a un reinicio del equipo.

El programa Adobe Acrobat 11 ha resultado comprometido, de modo que se recomienda su reinstalación. Gracias a que **Panda Adaptive Defense 360** monitoriza ejecutables tanto si son goodware como malware, la ejecución de un programa comprometido será detectada en el momento en que desencadene acciones peligrosas, terminando en su bloqueo.

18.6.2 Ejemplo 2: Comunicación con equipos externos en BetterSurf

BetterSurf es un programa potencialmente no deseado que modifica el navegador instalado en el equipo del usuario e inyecta anuncios en las páginas Web que visite.

En la pestaña **Detalles** se muestra la información fundamental del malware encontrado. En este caso se cuenta con los siguientes datos:

- **Nombre**: PUP/BetterSurf
- **Equipo**: MARTA-CAL
- **Ruta de detección**: `PROGRAM_FILES|\VER0BLOCKANDSURF\N4CD190.EXE`
- **Tiempo de permanencia**: 11 días 22 horas 9 minutos 46 segundos

Tiempo de exposición

En este caso el tiempo de exposición ha sido muy largo: durante casi 12 días el malware ha estado latente en la red del cliente. Este comportamiento es cada vez más usual, y puede deberse a varios motivos: que el malware no haya realizado ninguna acción sospechosa hasta muy tarde, o que simplemente el usuario descargó el fichero, pero tardó en ejecutarlo. En ambos casos la amenaza no era conocida anteriormente, con lo cual no se disponía de una firma con la que el sistema antivirus pueda compararla.

Pestaña Actividad

Paso	Fecha	Acción	Ruta
1	08/03/2015 11:16	Es creado por	TEMP | \08c3b650-e9e14f.exe
2	18/03/2015 11:16	Es creado por	SYSTEM | \services.exe
3	18/03/2015 11:16	Carga	PROGRAM_FILES | \VER0BLOF\N4Cd190.dll
4	18/03/2015 11:16	Carga	SYSTEM | \BDL.dll
5	18/03/2015 11:16	Comunica con	127.0.0.1:13879
6	18/03/2015 11:16	Comunica con	37.58.101.205:80
7	18/03/2015 11:17	Comunica con	5.153.39.133:80
8	18/03/2015 11:17	Comunica con	50.97.62.154:80
9	18/03/2015 11:17	Comunica con	50.19.102.217:80

Tabla 79: listado de acciones PUP/BetterSurf

En este caso se puede apreciar como el malware establece comunicación con varias IPs. La primera de ellas (paso 5) es el propio equipo y el resto son IPs del exterior a las que se conecta por el puerto 80, de las cuales probablemente se descarguen los contenidos de publicidad.

La principal medida de prevención en este caso será bloquear las IPs en el cortafuegos corporativo.

Antes de añadir reglas para el bloqueo de IPs en el cortafuegos corporativo se recomienda consultar las IPs a bloquear en el RIR asociado (RIPE, ARIN, APNIC etc.) para comprobar la red del proveedor al que pertenecen. En muchos casos la infraestructura remota utilizada por el malware es compartida con servicios legítimos alojados en proveedores, tales como Amazon y otros, de modo que bloquear IPs equivaldría a bloquear también el acceso a páginas Web legítimas.

18.6.3 Ejemplo 3: acceso al registro con PasswordStealer.BT

PasswordStealer.BT es un troyano que registra la actividad del usuario en el equipo y envía la información obtenida al exterior. Entre otras cosas, es capaz de capturar la pantalla del usuario, registrar las teclas pulsadas y enviar ficheros a un servidor C&C (Command & Control).

En la pestaña **Detalles** se muestra la información fundamental de la amenaza encontrada. En este caso se cuenta con los siguientes datos relevantes:

- **Ruta de la detección**: APPDATA|`\microsoftupdates\micupdate.exe`

Por el nombre y la localización del ejecutable, el malware se hace pasar por una actualización de Microsoft. Este malware en concreto no tiene capacidad para contagiar equipos por sí mismo, requiere que el usuario ejecute de forma manual la amenaza.

Pestaña Actividad

El modo de **Panda Adaptive Defense 360** configurado era Hardening: el malware ya residía en el equipo en el momento en que **Panda Adaptive Defense 360** se instaló y era desconocido en el momento de su ejecución.

Tabla de acciones

Paso	Fecha	Acción	Ruta
1	31/03/2015 23:29	Es ejecutado por	PROGRAM_FILESX86 | \internet explorer\iexplore.exe
2	31/03/2015 23:29	Es creado por	INTERNET_CACHE | \Content.IE5\ QGV8PV80\ index[1].php
3	31/03/2015 23:30	Crea clave apuntando a Exe	\REGISTRY\USER\S-1-5[...]9-5659\Software\Microsoft\Wind ows\ CurrentVersion\Run?MicUpdate
4	31/03/2015 23:30	Ejecuta	SYSTEMX86 | \notepad.exe
5	31/03/2015 23:30	Hilo inyectado por	SYSTEMX86 | \notepad.exe

Tabla 80: listado de acciones PasswordStealer.BT

En este caso el malware es creado en el paso 2 por una página Web y ejecutado por el navegador Internet Explorer.

El orden de las acciones tiene una granularidad de 1 microsegundo. Por esta razón, las acciones ejecutadas dentro del mismo microsegundo pueden aparecer desordenadas en la Timeline, como sucede en el paso 1 y paso 2.

Una vez ejecutado, el malware se hace persistente en el equipo del usuario en el paso 3, añadiendo una rama en el registro que lanzará el programa en el inicio del sistema. Después comienza a ejecutar acciones propias del malware, tales como arrancar un notepad e inyectar código en uno de sus hilos.

Como acción de resolución en este caso, y en ausencia de un método de desinfección conocido, se puede minimizar el impacto de este malware borrando la entrada del registro. Es muy posible que en una maquina infectada el malware impida modificar dicha entrada; dependiendo del caso sería necesario arrancar el equipo en modo seguro o con un CD de arranque para borrar dicha entrada.

Ejemplo 4: Acceso a datos confidenciales en Trj/Chgt.F

Trj/Chgt.F fue publicado por wikileaks a finales de 2014 como herramienta utilizada por las agencias gubernamentales de algunos países para realizar espionaje selectivo.

En este ejemplo pasaremos directamente a la pestaña **Actividad** para observar el comportamiento de esta amenaza avanzada.

Tabla de acciones

Paso	Fecha	Acción	Ruta
1	4/21/2015 2:17:47 PM	Es ejecutado por	SYSTEMDRIVE | \Python27\pythonw.exe
2	4/21/2015 2:18:01 PM	Accede a datos	#.XLS
3	4/21/2015 2:18:01 PM	Accede a datos	#.DOC
4	4/21/2015 2:18:03 PM	Crea	TEMP | \doc.scr
5	4/21/2015 2:18:06 PM	Ejecuta	TEMP | \doc.scr
6	4/21/2015 2:18:37 PM	Ejecuta	PROGRAM_FILES | \Microsoft Office\Office12\WI NWORD.EXE
7	4/21/2015 8:58:02 PM	Comunica con	192.168.0.1:2042

Tabla 81: listado de acciones Trj/Chgt.F

Inicialmente el malware es ejecutado por el intérprete de Python (paso 1) para luego acceder a un documento de tipo Excel y otro de tipo Word (paso 2 y 3). En el paso 4 se ejecuta un fichero de

extensión scr, probablemente un salvapantallas con algún tipo de fallo o error que provoque una situación anómala en el equipo aprovechada por el malware.

En el paso 7 se produce una conexión de tipo TCP. La dirección IP es privada de modo que se estaría conectando a la red del propio cliente.

En este caso se deberá de comprobar el contenido de los ficheros accedidos para evaluar la pérdida de información, aunque viendo la Timeline la información accedida en principio no ha sido extraída de la red del cliente.

Panda Adaptive Defense 360 desinfectará por sí mismo la amenaza y bloqueará de forma automática posteriores ejecuciones del malware en este y en otros clientes.

19. Herramientas de resolución

Desinfección automática de equipos
Análisis / desinfección bajo demanda de equipos
Reiniciar equipos
Notificar un problema
Acceso externo a la consola

19.1. Introducción

Panda Adaptive Defense 360 cuenta con varias herramientas de resolución que permiten al administrador solucionar los problemas encontrados en las fases de Protección, Detección y Monitorización del ciclo de protección adaptativa.

Algunas de estas herramientas son automáticas y no necesitan que el administrador intervenga, otras sin embargo requieren la ejecución de acciones concretas a través de la consola Web.

La Tabla 82 muestra las herramientas disponibles por plataforma y su tipo (automático o manual).

Herramienta de resolución	Plataforma	Tipo	Objetivo
Desinfección automática de equipos	Windows, macOS, Linux, Android	Automático	Desinfectar o mover a cuarentena el malware encontrado en el momento de la infección de los equipos.
Análisis / Desinfección bajo demanda de equipos	Windows, macOS, Linux, Android	Automático (programado) / Manual	Analizar, desinfectar o mover a cuarentena el malware encontrado en los equipos protegidos en el momento que lo requiera el administrador o en franjas horarias concretas
Reinicio bajo demanda	Windows	Manual	Fuerza un reinicio del equipo para aplicar actualizaciones, completar desinfecciones manuales y corregir errores detectados en la protección
Aislamiento de equipos	Windows	Manual	Aísla el equipo de la red, impidiendo la extracción de información confidencial y la propagación de la amenaza a los equipos vecinos

Tabla 82: herramientas de resolución disponibles en Panda Adaptive Defense 360

19.2. Desinfección automática de equipos

La desinfección automática es realizada por la Protección avanzada en tiempo real y por la Protección antivirus.

Ante una detección de malware **Panda Adaptive Defense 360** desinfectará de forma automática los elementos afectados siempre y cuando exista un método de desinfección conocido. En su defecto, el elemento se moverá a cuarentena.

La desinfección automática no requiere de la intervención del administrador, si bien es necesario que esté seleccionada la casilla **Protección de archivos** en la configuración de seguridad asignada al equipo.

Consulta el capítulo 10 Configuración de seguridad para estaciones y servidores para más información sobre los modos de bloqueo en Panda Adaptive Defense 360 y configuraciones disponibles en el módulo antivirus.

Modo de protección avanzada	Protección antivirus	Comportamiento
Audit	Activado	Detección, Desinfección, Cuarentena
Hardening, Lock	Activado	Detección, Bloqueo de desconocidos, Desinfección, Cuarentena
Audit	Desactivado	Detección
Hardening, Lock	Desactivado	Detección, Bloqueo de desconocidos

Tabla 83: comportamiento del producto frente a las amenazas según la configuración del motor Panda Adaptive Defense y antivirus

19.3. Análisis / Desinfección bajo demanda de equipos

El análisis y desinfección bajo demanda de ficheros se realiza de dos maneras: mediante la creación de tareas de análisis programadas y mediante un análisis inmediato.

Consulta el capítulo 15 Tareas para obtener más información la gestión de las tareas programadas y su creación a través del menú superior Tareas.

19.3.1 Creación de tareas desde el Árbol de equipos

El árbol de equipos permite definir de forma rápida tareas de análisis para grupos completos de equipos.

- Haz clic en el menú superior **Equipos** y elige la vista carpetas del Árbol de equipos.
- Haz clic en el menú de contexto asociado al grupo de equipos destinatario de la tarea de análisis. Se mostrará el menú contextual de la rama del árbol elegida.
- En el menú contextual haz clic en una de las dos opciones:
  - **Analizar ahora**: crea una tarea con destinatario el grupo de equipos elegido, para su ejecución inmediata.
  - **Programar análisis**: muestra la zona **Tareas** para crear una nueva tarea repetida en el tiempo y / o aplazada. La plantilla de tarea estará parcialmente completada: el campo **Destinatarios** incluye el grupo elegido en el Árbol de Equipos. Completa el resto de la configuración tal y como se describe en el punto 15.3 Creación de tareas desde

la zona Tareas

Tareas inmediatas

Las tareas inmediatas (entrada **Analizar ahora** del menú de contexto) tienen las siguientes características:

- Permiten elegir el tipo de análisis (**Todo el ordenador** o **Áreas críticas).** Consulta el punto 15.3.2 Programación horaria y repetición de la tarea para obtener más información.
- No requieren especificar el momento de ejecución ni la repetición: son tareas puntuales que se ejecutan en el momento de su definición.
- No requieren la publicación de la tarea: **Panda Adaptive Defense 360** publica de forma automática estas tareas.
- Para informar del éxito o fracaso en la creación de la tarea inmediata se muestra un mensaje emergente en la consola de administración.

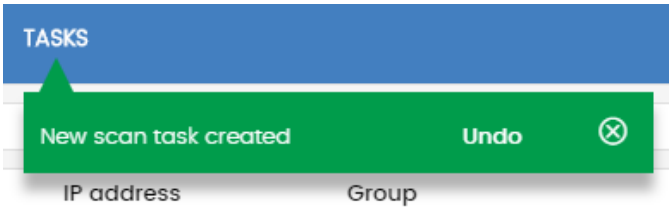


Figura 127: mensaje emergente de creación de una nueva tarea de análisis

- Para visualizar los resultados de las tareas inmediatas haz clic en el menú superior **Tareas**.

Tareas programadas

Las tareas programadas (entrada **Programar análisis** el menú de contexto) son idénticas a las tareas creadas desde la zona **Tareas** y mostradas en el punto 15.3 Creación de tareas desde la zona Tareas, si bien el campo destinatarios aparece completado con el grupo del Árbol de equipos seleccionado. Por lo tanto, es necesario indicar el momento de ejecución de la tarea, la repetición y publicar la tarea para su activación.

19.3.2 Creación de tareas desde el listado de equipos

La zona **Equipos** permite crear tareas inmediatas y programadas de forma similar al Árbol de equipos o la zona **Tareas**. En este caso, puedes elegir de forma independiente equipos que pertenecen a un mismo grupo o subgrupos.

Según sea del número de equipos destinatarios de la tarea, elige uno de los dos recursos mostrados a continuación:

- **Menú de contexto asociado al equipo**: un único equipo destinatario.
- **Casillas de selección y barra de acciones**: uno o varios equipos pertenecientes a un grupo o subgrupos.

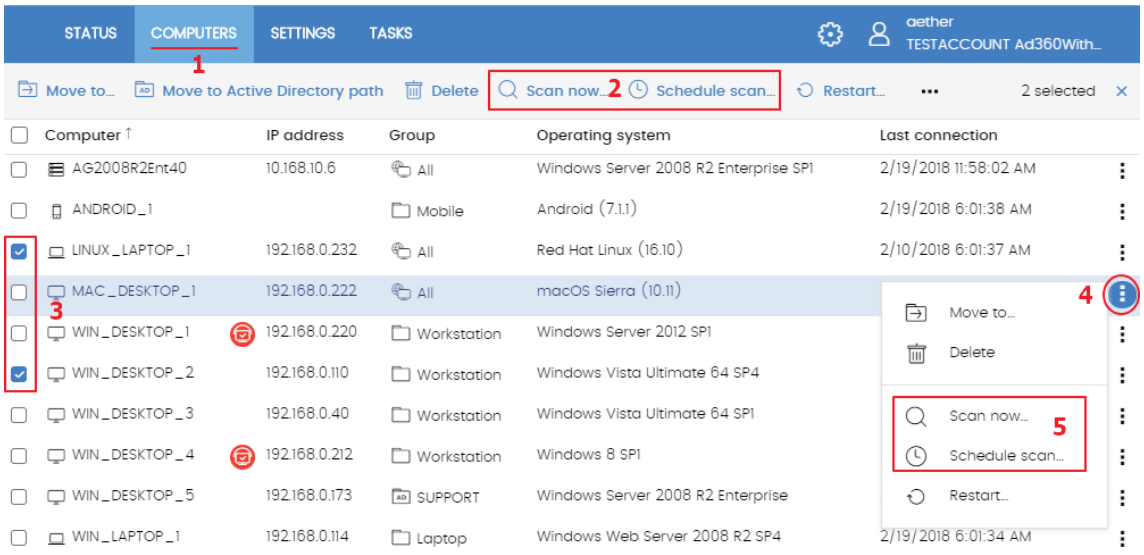


Figura 128: menús de contexto y barra de acciones disponibles para la creación rápida de tareas

Menú de contexto asociado al equipo

- Haz clic en el menú superior **Equipos (1)** y elige el grupo del Árbol de equipos al que pertenece el equipo a analizar.
- En el listado de equipos haz clic en el menú de contexto del equipo destinatario de la tarea de análisis. **(4)**
- En el menú de contexto **(5)**, haz clic en una de las dos ramas:
  - **Analizar ahora**: crea una tarea con destinatario el equipo elegido para ejecutarse inmediatamente.
  - **Programar análisis**: muestra la zona **Tareas** con una plantilla de tarea parcialmente completada. En el campo destinatarios se incluye el equipo elegido. Completa el resto de la configuración tal y como se describe en el punto 15.3 Creación de tareas desde la zona Tareas.

Casillas de selección y la barra de acciones

- Haz clic en el menú superior **Equipos (1)** y elige el grupo del Árbol de equipos al que pertenece el equipo o equipos a analizar.
- Selecciona los equipos destinatarios de la tarea con las casillas de verificación **(3)**. Se mostrará la barra de acciones **(2)** en la parte superior de la ventana.
- Haz clic en uno de los dos iconos:
  - **Analizar ahora**: crea una tarea con destinatario el grupo de equipos elegido para ejecutarse inmediatamente.
  - **Programar análisis**: muestra la zona Tareas con una plantilla de tarea parcialmente completada. En el campo destinatarios se incluye el grupo elegido en el **Árbol de Equipos**. Completa el resto de la configuración tal y como se describe en el punto 15.3 Creación de tareas desde la zona Tareas

19.3.3 Opciones de análisis

Las opciones de análisis permiten configurar los parámetros del motor de antivirus a la hora de realizar el escaneo del sistema de ficheros de los equipos. Se encuentran disponibles las opciones mostradas a continuación:

- **Tipo de análisis**
  - **Todo el ordenador**: Análisis profundo del equipo incluyendo a todos los dispositivos de almacenamiento conectados.
  - **Áreas críticas**: análisis rápido del equipo que incluye
    - %WinDir%\system32
    - %WinDir%\SysWow64
    - Memoria
    - Sistema de arranque
    - Cookies
  - **Elementos específicos**: permite introducir rutas de los dispositivos de almacenamiento masivo. Se admite el uso de variables de entorno. Se analizará la ruta indicada y todas las carpetas y ficheros que cuelguen de ella.
- **Detectar virus**: detección de programas que se pueden introducir en los ordenadores produciendo efectos nocivos. Esta opción está siempre activada.
- **Detectar herramientas de hacking y PUPs**: detección de programas que pueden ser utilizados por un hacker para causar perjuicios a los usuarios de un ordenador y detección de programas potencialmente no deseados.
- **Detectar archivos sospechosos**: en los análisis programados el software del equipo es analizado de forma estática, si ejecución. De este modo puede ser necesario activar los algoritmos de análisis heurístico para detectar todos los tipos de amenazas.
- **Analizar archivos comprimidos**
- **Excluir del análisis los siguientes archivos**
  - No analizar los archivos excluidos para las protecciones permanentes: los archivos marcados por el administrador como permitida su ejecución no serán analizados, junto a los archivos ya excluidos de forma global en la consola.
  - Extensiones
  - Archivos
  - Directorios

19.4. Reiniciar equipos

Para mantener los equipos actualizados a la última versión de la protección, o si se detecta algún error en la protección, el administrador podrá actuar remotamente desde la consola Web y reiniciar los equipos involucrados.

- Selecciona el menú superior **Equipos** y localiza el equipo desde el panel de equipos situado a la izquierda**.**

- Para reiniciar un único equipo: selecciona el menú de contexto del equipo en el listado de equipos.
- Para reiniciar varios equipos: mediante las casillas de selección, marca los equipos que quieres reiniciar y haz clic el menú de contexto global.
- Selecciona en el menú desplegable la opción **Reiniciar.**

19.5. Aislar un equipo

Aislar equipos funciona en puestos de trabajo y servidores Windows. Los equipos Linux, macOS y Android son incompatibles con esta tecnología.

Panda Adaptive Defense 360 aísla bajo demanda los equipos de la red para evitar la propagación de las amenazas y la comunicación y extracción de información confidencial.

Cuando un equipo está aislado, sus comunicaciones quedan restringidas a los servicios mostrados a continuación:

- El acceso al equipo desde la consola para que el administrador pueda analizar el problema y resolverlo mediante las herramientas suministradas por **Panda Adaptive Defense 360**.
- El acceso a los dispositivos y su control remoto mediante **Panda Systems Management,** para que el administrador pueda recoger información extendida y resolver los problemas mediante las herramientas de gestión remota (escritorio remoto, línea de comandos remota, visor de sucesos remoto etc.).

Para obtener un listado de las herramientas de gestión remota de Panda Systems Management consulta la Guía para administradores de red de Systems Management en https://www.pandasecurity.com/rfiles/enterprise/documentation/pcsm/01dwn_PCSM_Guide_ES.pdf

El resto de productos y servicios instalados en el equipo de usuario o servidor dejarán de poder comunicarse por red a no ser que el administrador establezca excepciones. Consulta el punto 19.5.4 Opciones avanzadas de aislamiento para más información.

19.5.1 Estados de los equipos aislados

Las operaciones **Aislar un equipo** y **Dejar de Aislar un equipo** se ejecutan en tiempo real, pero el proceso puede retrasarse si el equipo no está conectado a Internet. Para reflejar su situación exacta, **Panda Adaptive Defense 360** distingue los 4 estados a través de los iconos mostrados a continuación:

- **Intentando aislar**  : el administrador lanzó una petición para aislar uno o más equipos y se está procesando.

- **Aislado**  : el proceso de aislamiento se completó y el equipo tiene restringidas sus comunicaciones.
- **Intentando dejar de aislar**  : el administrador lanzó una petición para dejar de aislar uno o más equipos y se está procesando.
- **No aislado**: el proceso para retirar el aislamiento del equipo se completó. Las comunicaciones se permiten acorde la configuración definida en otros módulos (firewall, IDS), productos, o en el propio sistema operativo.

Estos iconos acompañan a la columna dirección IP en los listados de **Licencias**, **Estado de la protección** y en la zona **Equipos**.

19.5.2 Aislar uno o varios equipos de la red de la organización

Para aislar uno o varios equipos de la red:

- Haz clic en el menú superior **Equipos** o elige uno de los siguientes listados de equipos:
  - Listado **Estado de protección**
  - Listado **Licencias**
- Indica los equipos a aislar con las casillas de selección.
- En la barra de acciones selecciona **Aislar un equipo**. Se mostrará una ventana con un link a **Opciones avanzadas**.
- En **Opciones avanzadas** indica los programas que se seguirán comunicando con el resto de la red a pesar del aislamiento del equipo (exclusión de aislamiento).
- Haz clic en el botón **Aceptar**. El equipo cambiará de estado a **Intentando aislar el equipo.**

Para aislar un grupo de equipos:

- Haz clic en el menú superior **Equipos.**
- En el Árbol de equipos haz clic en la vista de carpetas y selecciona el grupo a aislar.
- En el menú de contexto selecciona la entrada **Aislar equipos** y haz clic en el botón **Aceptar**.
- Para aislar todos los equipos de la red despliega el menú de contexto del nodo **Todos**.

19.5.3 Quitar el aislamiento de un equipo

Para quitar el aislamiento de un equipo sigue los pasos mostrados a continuación:

- Sigue los pasos indicados en el punto 19.5.2
- En la barra de acciones selecciona **Dejar de aislar un equipo**.
- El equipo cambiará de estado a **Intentando dejar de aislar el equipo.**

19.5.4 Opciones avanzadas de aislamiento: exclusión de programas

Al aislar un equipo, solo se permite la comunicación de los procesos correspondientes a los productos de Panda Security. El resto de procesos, incluyendo a los programas de usuario, no podrán comunicarse con los equipos de la organización. Para excluir a ciertos programas de este comportamiento y permitir al usuario seguir utilizando el equipo en cierta medida o poder utilizar determinadas aplicaciones que ayuden al administrador a diagnosticar y resolver el problema, utiliza el link **Opciones avanzadas** de la ventana flotante mostrada al aislar un equipo.

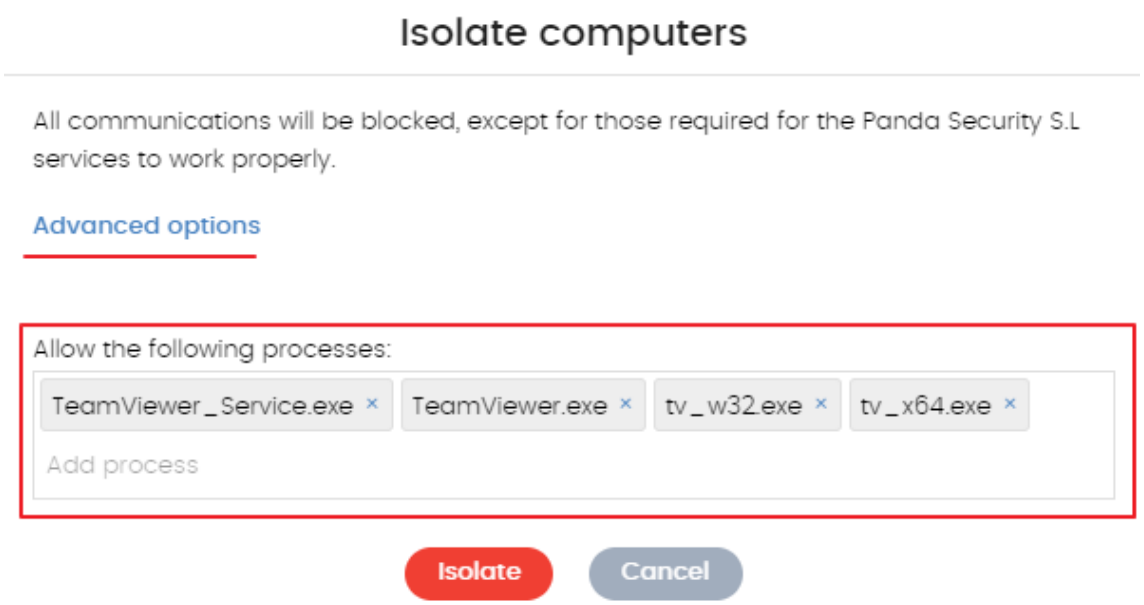


Figura 129: ventana de configuración del aislamiento

La caja de texto indica los programas a excluir del aislamiento. Estos programas podrán comunicarse con libertad con el resto de equipos de la organización o con el exterior, según indique la configuración del resto de módulos de **Panda Adaptive Defense 360**, de otros productos instalados en el equipo, o del cortafuegos del sistema operativo.

Para acelerar la configuración, la consola de administración retiene la última configuración de procesos excluidos del aislamiento introducida por el administrador. De esta manera, en la caja de texto de un equipo excluido no se mostrará su configuración especifica de procesos excluidos, sino la última configuración que utilizó el administrador en cualquier otro equipo.

19.5.5 Procesos permitidos y denegados de un equipo aislado

Panda Adaptive Defense 360 autoriza la comunicación de los procesos necesarios para poder funcionar correctamente y permitir al administrador realizar un análisis forense remoto y utilizar las herramientas de resolución implantadas en el producto y en Panda Systems Management. A continuación, se indican los procesos permitidos y denegados.

Procesos y servicios permitidos en un equipo aislado

- Los servicios necesarios para formar parte de la red corporativa: obtención de IP por DHCP, ARP, nombre de equipo por WINS, DNS etc.
- Comunicación con el Gateway por defecto.
- Comunicación del software Adaptive Defense 360 con la nube de Panda Security para el funcionamiento de los motores de protección, descarga de ficheros de firmas y administración remota mediante la consola web.
- Descubrimiento de equipos en máquinas aisladas con el rol de descubridor asignado.
- Servidor de ficheros en una máquina aislada con el rol de cache asignado.
- Proxy de conexiones en una máquina con el rol de proxy Panda asignado.
- Herramientas de acceso remoto de **Panda Systems Management** entre la máquina aislada y la máquina del administrador:
  - Línea de comandos remota
  - Escritorio remoto (VNC, RDP)
  - Transferencia de ficheros
  - Visor de sucesos remoto
  - Registro remoto
  - Administrador de tareas remoto
  - Información sobre las unidades
  - Editor del registro remoto
  - Tareas rápidas
- Monitorización por SNMP de dispositivos no compatibles con **Panda Systems Management** con el rol Nodo de conexión asignado.
- Ejecución de scripts, tareas etc.

Procesos y servicios bloqueados en un equipo aislado

- Conexión con el Windows Update del sistema operativo.
- Políticas de Windows Update y Patch Management.
- Comunicación con la red de scripts y módulos desarrollados por el administrador o integrados desde la ComStore de **Panda Systems Management**.
- Navegación web, ftp, correo y otros protocolos de Internet.
- Transferencia de ficheros por SMB entre los PCs de la red.

19.6. Notificar un problema

En algunas ocasiones es posible que el software **Panda Adaptive Defense 360** instalado en los equipos de la red presente un mal funcionamiento. Algunos de los síntomas pueden ser:

- Fallos en el reporte del estado del equipo.
- Fallos en la descarga de conocimiento o de las actualizaciones del motor.

- Motor en estado de error.

Si **Panda Adaptive Defense 360** presenta un mal funcionamiento en alguno de los equipos de la red, es posible contactar con el departamento de soporte de Panda Security a través de la consola y enviar de forma automatizada toda la información necesaria para efectuar un diagnóstico. Para ello haz clic en el menú superior **Equipos**, selecciona los equipos que presenten errores y haz clic en el menú de contexto. Se desplegará un menú con la opción **Indícanos el problema**.

19.7. Permitir el acceso externo a la consola Web

Para aquellos problemas que el administrador de la red no pueda resolver, existe la posibilidad de habilitar el acceso a la consola únicamente para equipo de soporte de Panda Security. Sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Configuración**, panel lateral **Usuarios.**
- En la pestaña usuarios haz clic en el control **Permitir al equipo de Panda Security S.L. acceder a mi consola.**

20. Alertas

Alertas por correo

20.1. Introducción

El sistema de alertas es un recurso utilizado por **Panda Adaptive Defense 360** para comunicar de forma rápida al administrador situaciones de importancia para el buen funcionamiento del servicio de seguridad.

En conjunto, las alertas informan al administrador de las situaciones mostradas a continuación:

- Detección de malware, PUP o exploits.
- Reclasificación de elementos desconocidos, malware o PUP.
- Bloqueo de procesos desconocidos para **Panda Adaptive Defense 360** y en proceso de clasificación.
- Cambios en el estado de las licencias.
- Errores de instalación y desprotegidos.

20.2. Alertas por correo

Las alertas por correo son mensajes enviados por **Panda Adaptive Defense 360** a las cuentas de correo de los administradores. El sistema genera mensajes cuando se producen determinados eventos, que se enviaron a las cuentas de correo configuradas como destinatarios.

20.2.1 Configuración de alertas por correo

Desde el menú superior **Configuración**, en el panel de la izquierda **Alertas** se muestra la ventana de configuración.

Desde esta ventana el administrador podrá indicar las direcciones de correo que recibirán los mensajes en **Enviar las alertas a la siguiente dirección**, así como habilitar o deshabilitar de forma global cada una de las alertas a enviar, y explicadas en el punto siguiente.

20.2.2 Visibilidad del administrador y envío de alertas

Las alertas se definen de forma independiente por cada usuario de la consola. El contenido de una alerta queda limitado por la visibilidad de los equipos administrados que tiene el rol del usuario.

20.2.3 Tipos de alertas

Detecciones de malware / PUP

Se generará un mensaje de este tipo en las condiciones mostradas a continuación:

- Por cada malware detectado en tiempo real en el equipo.
- Solo en máquinas Windows.
- Máximo de dos mensajes por cada equipo – malware – día.

El mensaje de correo mostrará la información indicada a continuación:

- Si es el primer o segundo mensaje generado para esa máquina – amenaza - día.
- Nombre del programa malicioso.
- Nombre del equipo donde fue detectado.
- Grupo al que pertenece el equipo.
- Fecha y hora de la detección en formato UTC.
- Ruta del programa malicioso.
- Hash.
- Tabla de acciones de programa (ciclo de vida) si consiguió ejecutarse antes del bloqueo.
- Apariciones de la amenaza en el parque: listado de equipos donde fue previamente visto el malware dentro de la red gestionada.

Detecciones de exploits

Se generará un mensaje de este tipo en las condiciones mostradas a continuación:

- Por cada detección de exploit que se produzca.
- Máximo de 10 alertas al día por equipo y exploit.
- Solo en máquinas Windows.

El mensaje de correo mostrará la información indicada a continuación:

- Nombre, ruta y hash del programa que recibió el intento de explotación.
- Nombre del equipo donde fue detectado.
- Grupo al que pertenece el equipo.
- Fecha y hora de la detección en formato UTC.
- Acción ejecutada por **Panda Adaptive Defense 360.**
- Nivel de riesgo del equipo.
- Valoración de la seguridad del programa atacado.
- Tabla de acciones de programa (ciclo de vida) si consiguió ejecutarse antes del bloqueo.
- Posible origen del exploit.

Programas bloqueados en proceso de clasificación

Se generará un mensaje de este tipo en las condiciones mostradas a continuación:

- Por cada programa desconocido detectado en el sistema de ficheros en tiempo real.
- Solo en máquinas Windows.

El mensaje de correo mostrará la información siguiente:

- Nombre del programa desconocido.
- Nombre del equipo donde fue detectado.
- Grupo al que pertenece el equipo.
- Fecha y hora de la detección en formato UTC.
- Ruta del programa desconocido.
- Hash.
- Tabla de acciones de programa (ciclo de vida) si consiguió ejecutarse antes del bloqueo.
- Apariciones del programa desconocido en el parque: listado de equipos donde fue previamente visto el programa desconocido dentro de la red gestionada.

Clasificaciones de archivos que han sido permitidos por el administrador

Los archivos permitidos por el administrador son aquellos archivos que, habiendo sido bloqueados por ser desconocidos para **Panda Adaptive Defense 360** o por haber sido clasificados como amenazas, el administrador ha permitido su ejecución. Por esta razón, el sistema generará correos de alerta cuando su clasificación se complete, ya que es posible que la acción emprendida por el sistema cambie después de la reclasificación, según se indique en la política de reclasificación configurada por el administrador.

Consulta el Capítulo 17 Gestión de amenazas, elementos en clasificación y cuarentena para obtener más información sobre las políticas de reclasificación.

- **Alerta de elemento reclasificado a goodware eliminando o manteniendo la exclusión**

El sistema emitirá un correo indicando los datos de un elemento que en su momento fue desconocido pero que el administrador permitió su ejecución. Ahora que ya está clasificado como goodware la exclusión se eliminará o se mantendrá según la política de reclasificación elegida. En ambos casos el resultado para el usuario es el mismo: el elemento se sigue pudiendo utilizar, pero se le avisa al administrador de la nueva situación, por si decide eliminar manualmente la exclusión sobre el elemento previamente configurada, o simplemente se le indica que la exclusión fue eliminada de forma automática.

- **Alerta de elemento reclasificado a Malware / PUP eliminando o manteniendo la exclusión**

El sistema emitirá un correo indicando los datos de un elemento que en su momento fue desconocido pero que el administrador permitió su ejecución. Ahora que ya está clasificado como amenaza la exclusión se elimina o se mantiene según la política de reclasificación elegida. Si la exclusión se mantiene se seguirá permitiendo la ejecución del elemento, poniendo en peligro la seguridad de la red. Si por el contrario la exclusión se elimina, el elemento dejará de estar disponible

para el usuario, anulando los efectos negativos futuros del elemento en el equipo del usuario y, por extensión, en la red de la empresa.

Detecciones de malware

Se generará un mensaje cada 15 minutos si se cumplen las condiciones mostradas a continuación:

- Cuando se produzcan detecciones de malware en tiempo real, con un análisis bajo demanda o análisis programado en el equipo.
- Compatible con máquinas Windows, Linux, macOS y Android.

El mensaje de correo mostrará la información indicada a continuación:

- Numero de amenazas de tipo malware detectadas en el intervalo de tiempo.
- Número de equipos afectados.

Detecciones de herramientas de hacking y PUPs

Se generará un mensaje cada 15 minutos si se cumplen las condiciones mostradas a continuación:

- Cuando se produzcan detecciones de malware de tipo hacking y PUPs en tiempo real, con un análisis bajo demanda o análisis programado en el equipo.
- Compatible con máquinas Windows, Linux, macOS y Android.

El mensaje de correo mostrará la información indicada a continuación:

- Numero de amenazas de tipo malware detectadas en el intervalo de tiempo.
- Número de equipos afectados

URLs con malware bloqueadas

Se generará un mensaje cada 15 minutos si se cumplen las condiciones mostradas a continuación:

- Cuando se produzcan detecciones de URL que apuntan a malware.
- Compatible con máquinas Windows, Linux, macOS y Android.

El mensaje de correo mostrará la información indicada a continuación:

- Numero de URL que apuntan a malware detectadas en el intervalo de tiempo.
- Número de equipos afectados.

Detecciones de phishing

Se generará un mensaje cada 15 minutos si se cumplen las condiciones mostradas a continuación:

- Cuando se produzcan detecciones de phishing.
- Compatible con máquinas Windows, Linux, macOS y Android.

El mensaje de correo mostrará la información indicada a continuación:

- Número de ataques de phishing detectadas en el intervalo de tiempo.
- Número de equipos afectados.

Intentos de intrusión bloqueados

Se generará un mensaje cada 15 minutos si se cumplen las condiciones mostradas a continuación:

- Cuando se produzcan intentos de intrusión bloqueados por el módulo IDS.
- Compatible con máquinas Windows.

El mensaje de correo mostrará la información indicada a continuación:

- Número de intentos de intrusión bloqueados en el intervalo de tiempo.
- Número de equipos afectados.

Dispositivos bloqueados

Se generará un mensaje cada 15 minutos si se cumplen las condiciones mostradas a continuación:

- Se ha producido accesos por parte del usuario a dispositivos y periféricos bloqueados por el administrador.
- Compatible con máquinas Windows, Linux, macOS y Android.

El mensaje de correo mostrará la información indicada a continuación:

- Número de accesos bloqueados a dispositivos.
- Número de equipos afectados.

Equipos con error en la protección y errores durante la instalación

Se generará un mensaje de este tipo en las condiciones mostradas a continuación:

- Por cada equipo desprotegido de la red.
- Equipos con la protección en estado de error o fallo en la instalación de la protección

El mensaje de correo mostrará la información siguiente:

- Nombre del equipo desprotegido.
- Grupo al que pertenece el equipo.
- Información relativa al equipo (Nombre, descripción, sistema operativo, dirección IP, Grupo, ruta del directorio activo, dominio).
- Fecha y hora en formato UTC.
- Motivo de la desprotección: **Protección con error** o **Error instalando.**

Equipos sin licencia

Se generará un mensaje de este tipo en las condiciones mostradas a continuación:

- Por cada equipo que intenta licenciarse, pero no lo consigue por falta de licencias libres.

El mensaje de correo mostrará la información siguiente:

- Nombre del equipo desprotegido.
- Grupo al que pertenece el equipo.
- Información relativa al equipo (Nombre, descripción, sistema operativo, dirección IP, Grupo, ruta del directorio activo, dominio).
- Fecha y hora en formato UTC.
- Motivo de la desprotección: **Equipo sin licencia.**

Adicionalmente, se generará un único mensaje en las condiciones mostradas a continuación:

- Por cada mantenimiento que caduque.

El mensaje de correo mostrará la información siguiente:

- Número de equipos que se han quedado sin licencia.
- Número de licencias que han caducado, asignadas al mantenimiento.
- Nombre del producto asignado al mantenimiento caducado.
- Fecha de caducidad del mantenimiento.

Errores durante la instalación

Se generará un mensaje de este tipo en las condiciones mostradas a continuación:

- Por cada uno de los equipos de la red, cada vez que se cree una nueva situación que derive en el cambio de estado de protegido a desprotegido.
- Si en un mismo momento se detectan varios motivos que derivan en el cambio de estado de protegido a desprotegido en un mismo equipo solo se genera una alerta con todos los motivos.
- Las razones de cambio de estado que generan una alerta son:
  - **Protección con error**: sólo se contempla el estado de las protecciones antivirus y protección avanzada, en aquellas plataformas que las soporten, y cuando las licencias del cliente las incluyan.
  - **Error instalando**: se enviará alerta cuando se haya producido un error en la instalación que requiera de la intervención del usuario (e.g., no hay espacio en disco), y no ante errores transitorios que podrían solucionarse autónomamente tras varios reintentos.
  - **Sin licencia**: cuando el equipo no haya recibido una licencia tras registrarse, porque no haber libres en ese momento.

- Las razones de cambio de estado que no generan una alerta son:
  - **Sin licencia**: cuando el administrador ha quitado la licencia al dispositivo o cuando Panda Adaptive Defense 360 haya retirado la licencia automáticamente al equipo por haberse reducido el número de licencias contratadas.
  - **Instalando**: por no resultar útil recibir una alerta cada vez que se instala un equipo.
  - **Protección desactivada**: este estado es consecuencia de un cambio de configuración voluntario.
  - **Desactualizada la protección**: no implica necesariamente que el equipo este desprotegido, pese a estar desactualizado.
  - **Pendiente de reinicio**: no implica necesariamente que el equipo este desprotegido.
  - **Desactualizado el conocimiento**: no implica necesariamente que el equipo este desprotegido

El mensaje de correo mostrará la información siguiente:

- Nombre del equipo
- Estado de la protección
- Razón del cambio del estado de la protección.

Equipos no administrados descubiertos

Se generará un mensaje de este tipo en las condiciones mostradas a continuación:

- Cada vez que un equipo descubridor termina un descubrimiento
- El descubrimiento ha encontrado equipos no vistos anteriormente en la red

El mensaje de correo mostrará la información siguiente:

- Nombre del equipo descubridor.
- Número de equipos descubiertos.
- Enlace al listado de los equipos descubiertos en la consola.

21. Informes

Generación bajo demanda de informes ejecutivos

Envío programado de informes ejecutivos

21.1. Introducción

Panda Adaptive Defense 360 permite generar y enviar de forma automática o manual informes ejecutivos que consolidan toda la información recogida en el periodo de tiempo establecido por el administrador.

21.2. Generación bajo demanda de informes ejecutivos

En el menú superior **Estado**, haz clic en el panel izquierdo **Informe ejecutivo** para mostrar la ventana de configuración de informes. La consola web muestra dos pestañas: **Visualizar** y **Programar**, haz clic en la pestaña **Visualizar** para configurar la generación de un informe ejecutivo bajo demanda.

21.2.1 Información requerida para la generación de informes bajo demanda

Será necesario suministrar la información mostrada a continuación:

- **Información de las siguientes fechas**: indica el intervalo de tiempo que abarcará el informe
  - **Último mes**
  - **Últimos 7 días**
  - **Últimas 24 horas**
- **Información de los siguientes equipos**: especifica de qué equipos se extraerán datos para generar el informe ejecutivo.
  - **Todos los equipos**
  - **Equipos seleccionados**: muestra el árbol de grupos, permitiendo seleccionar de forma individual los grupos mediante las casillas de selección.
- **Incluir el siguiente contenido**: permite seleccionar el tipo de información que será incluida en el informe.
  - **Estado de las licencias**: muestra la información de las licencias contratadas y consumidas. Consulta el capítulo 5 Licencias.
  - **Estado de la red**: muestra el funcionamiento de software **Panda Adaptive Defense 360** en los equipos de la red donde ha sido instalado. Incluye los widgets **Equipos desprotegidos** y **Protección desactualizada** del panel de control. Consulta el capítulo 16 Visibilidad del malware y del parque informático para obtener más información.
  - **Detecciones**: muestra las amenazas detectadas en la red. Incluye los widgets **Actividad del malware**, **Actividad de PUPs**, **Amenazas detectadas por el antivirus** y **Filtrado de contenidos en Exchange servers** del panel de control. Consulta el capítulo 16 Visibilidad del malware y del parque informático para obtener más información.
  - **Acceso web y Spam**: muestra la actividad web de los usuarios. Incluye los widgets **Accesos a páginas web**, **Categorías más accedidas (Top 10)**, **Categorías más accedidas por equipo (Top 10)**, **Categorías más bloqueadas (Top 10)**, **Categorías más bloqueadas por equipo (Top 10)** y **Spam detectado en Exchange Server**. Consulta el capítulo 16 Visibilidad del malware y del parque informático para obtener más información.

Una vez completada la información haz clic en el botón **Visualizar** para abrir una ventana independiente con el contenido del informe.

Comprueba que ni navegador ni ninguna extensión instalada impidan la visualización de pop ups.

21.3. Envío programado de informes ejecutivos

En el menú superior **Estado**, haz clic en el panel izquierdo **Informe ejecutivo** para mostrar la ventana de configuración de informes. La consola web muestra dos pestañas: **Visualizar** y **Programar**, haz clic en la pestaña **Programar** para configurar la generación periódica de un informe ejecutivo.

21.3.1 Información requerida para la generación de informes programados

La ventana de informes programados muestra una lista de todos los informes previamente configurados. Para agregar un nuevo informe programado haz clic en el botón **Añadir**. Para borrar un informe previamente generado haz clic en el icono  . Para editar un informe previamente creado haz clic en su nombre.

Para configurar un informe programado será necesario suministrar la información mostrada a continuación:

- **Nombre**: nombre del informe programado que se mostrará en la lista de informes configurados.
- **Enviar automáticamente**: permite programar el envío del informe o guardar la configuración sin enviarla, para poder generarlo de forma manual más adelante.
- **Fecha y ritmo de envío**: permite especificar la fecha del envío y cada cuanto tiempo se producirá. Selecciona **Todos los días**, **Todas las semanas** o **Todos los meses**. Dependiendo de la selección se ajustará el contenido de los desplegables mostrados para poder definir con precisión la fecha de envío.
- **La siguiente información**: al hacer clic en esta zona la ventana cambia y muestra los parámetros de configuración **Fechas**, **Equipos** y **Contenidos**:
  - **Información de las siguientes fechas**: indica el intervalo de tiempo que abarcara el informe.
    - **Último mes**
    - **Últimos 7 días**
    - **Últimas 24 horas**
  - **Información de los siguientes equipos**: especifica de qué equipos se extraerán datos para generar el informe ejecutivo.
    - **Todos los equipos**
    - **Equipos seleccionados**: muestra el árbol de grupos, permitiendo seleccionar de forma individual los grupos mediante las casillas de selección.

- **Incluir el siguiente contenido**: permite seleccionar el tipo de información que será incluida en el informe.
  - **Estado de las licencias**: muestra la información de las licencias contratadas y consumidas. Consulta el capítulo 5 Licencias.
  - **Estado de la red**: muestra el funcionamiento de software **Panda Adaptive Defense 360** en los equipos de la red donde ha sido instalado. Incluye los widgets **Equipos desprotegidos** y **Protección desactualizada** del panel de control. Consulta el capítulo 16 Visibilidad del malware y del parque informático para obtener más información.
  - **Detecciones**: muestra las amenazas detectadas en la red. Incluye los widgets **Actividad del malware**, **Actividad de PUPs**, **Amenazas detectadas por el antivirus** y **Filtrado de contenidos en Exchange servers** del panel de control.
  - **Acceso web y Spam**: muestra la actividad web de los usuarios. Incluye los widgets **Accesos a páginas web**, **Categorías más accedidas (Top 10)**, **Categorías más accedidas por equipo (Top 10)**, **Categorías más bloqueadas (Top 10)**, **Categorías más bloqueadas por equipo (Top 10)** y **Spam detectado en Exchange Server**. Consulta el capítulo 16 Visibilidad del malware y del parque informático para obtener más información.

- **Para**: introduce las direcciones de correo separadas por comas que recibirán el informe.
- **CC**
- **CCO:** introduce las direcciones de correo ocultas que recibirán el informe.
- **Asunto:** especifica el campo asunto del correo electrónico**.**
- **Formato**: selecciona el formato (Pdf, Excel, Word) del fichero adjunto al correo electrónico que contendrá el informe.
- **Idioma**: selecciona el idioma en el que se enviará el informe.

22. Control y supervisión de la consola de administración

22.1. Introducción

En este capítulo se detallan los recursos implementados en **Panda Adaptive Defense 360** para controlar y supervisar las acciones realizadas por los administradores de red que acceden a la consola web de gestión.

Esta supervisión y control se implementa en forma de tres recursos, mostrados a continuación:

- Cuenta de usuario
- Roles asignados a las cuentas de usuario
- Registro de la actividad de las cuentas de usuario

22.2. ¿Qué es una cuenta de usuario?

Es un recurso gestionado por **Panda Adaptive Defense 360**, formado por un conjunto de información que el sistema utiliza para regular el acceso de los administradores a la consola web, y establecer las acciones que éstos podrán realizar sobre los equipos de los usuarios.

Las cuentas de usuario son utilizadas únicamente por los administradores de IT que acceden a la consola **Panda Adaptive Defense 360**. Generalmente, cada administrador de IT tiene una única cuenta de usuario personal, pudiéndose crear tantas cuentas de usuario como se considere necesarias.

A diferencia del resto del documento, donde la palabra "usuario" se refiere a la persona que utiliza un equipo o dispositivo, en este capítulo "usuario" se asocia a la cuenta de usuario que el administrador utiliza para acceder a la consola web.

22.2.1 Estructura de una cuenta de usuario

Una cuenta de usuario está formada por los siguientes elementos:

- **Login de la cuenta**: asignada en el momento de la creación de la cuenta, su objetivo es identificar al administrador que accede a la consola.
- **Contraseña de la cuenta**: asignada una vez creada la cuenta, permite regular el acceso a la consola de administración.
- **Rol asignado**: seleccionable una vez creada la cuenta de usuario, permite determinar los equipos sobre los cuales la cuenta tendrá capacidad de administración, y las acciones que podrá ejecutar sobre los mismos.

22.2.2 ¿Qué es el usuario principal?

El usuario principal es la cuenta de usuario suministrada por Panda Security al cliente en el momento de provisionar el servicio **Panda Adaptive Defense 360**. Esta cuenta tiene asignado el rol **Control total** explicado más abajo en este mismo capítulo.

La configuración del usuario principal no se puede editar ni borrar.

22.3. ¿Qué es un rol?

Un rol es una configuración específica de permisos de acceso a la consola, que se aplica a una o más cuentas de usuario. De esta forma, un administrador concreto estará autorizado a ver o modificar determinados recursos de la consola, dependiendo del rol asignado a la cuenta de usuario con la que accedió a **Panda Adaptive Defense 360**.

Una cuenta de usuario solo puede tener un único rol asignado. Sin embargo, un rol puede estar asignado a una o más cuentas de usuario.

22.3.1 Estructura de un rol

Un rol está formado por los siguientes elementos:

- **Nombre del rol**: designado en el momento de la creación del rol, su objetivo es meramente identificativo.
- **Grupos sobre los que tiene permisos**: permite restringir el acceso a determinados equipos de la red. Para configurar esta restricción es necesario especificar las carpetas del árbol de grupos a las cuales la cuenta de usuario tendrá acceso.
- **Juego de permisos**: permite determinar las acciones concretas que las cuentas de usuario podrán ejecutar sobre los equipos que pertenezcan a los grupos definidos con accesibles.

22.3.2 ¿Por qué son necesarios los roles?

En un departamento de IT de tamaño pequeño, todos los técnicos van a acceder a la consola como administradores sin ningún tipo de límite; sin embargo, en departamentos de IT de mediano o gran tamaño con un parque informático grande para administrar, es muy posible que sea necesario organizar o segmentar el acceso a los equipos, aplicando tres criterios:

- **Según la cantidad de equipos a administrar.**

Redes de tamaño medio/grande o redes pertenecientes a delegaciones de una misma empresa pueden requerir distribuir y asignar equipos a técnicos concretos. De esta forma, los dispositivos de una delegación administrados por un técnico en particular serán invisibles para los técnicos que administren los dispositivos de otras delegaciones.

También pueden existir restricciones de acceso a datos delicados de ciertos usuarios. En estos casos se suele requerir una asignación muy precisa de los técnicos que van a poder manipular los dispositivos que los contienen.

- **Según el cometido del equipo a administrar.**

Según la función que desempeñe, un equipo puede asignarse a un técnico experto en ese campo: por ejemplo, los servidores de correo Exchange pueden ser asignados a un grupo de técnicos especialistas, y de la misma forma otros equipos como los dispositivos Android podrían no ser visibles para este grupo.

- **Según los conocimientos o perfil del técnico.**

Según las capacidades del técnico o su función dentro del departamento de IT, puede asignarse únicamente un acceso de monitorización/validación (solo lectura) o, por el contrario, uno más avanzado, como el de modificación de las configuraciones de seguridad de los equipos. Por ejemplo, es frecuente encontrar en compañías grandes un determinado grupo de técnicos dedicados únicamente a desplegar software en los equipos de la red.

Estos tres criterios se pueden solapar, dando lugar a una matriz de configuraciones muy flexible y fácil de establecer y mantener, que permita delimitar perfectamente las funciones de la consola para cada técnico, en función de la cuenta de usuario con la que accedan al sistema.

22.3.3 El rol Control total

Una licencia de uso de **Panda Adaptive Defense 360** viene con un rol de **Control total** predefinido. A este rol pertenece la cuenta de administración creada por defecto, y con ella es posible realizar absolutamente todas las acciones disponibles en la consola.

El rol **Control total** no puede borrarse, modificarse ni visualizarse, y cualquier cuenta de usuario puede pertenecer a este rol previa asignación en la consola.

22.3.4 El rol solo lectura

Está especialmente indicado para aquellos administradores de red encargados de la vigilancia del parque informático, pero que no poseen los permisos suficientes para realizar modificaciones, como por ejemplo editar configuraciones o lanzar análisis bajo demanda.

Los permisos activados son los siguientes:

- Ver configuraciones de seguridad para estaciones y servidores.
- Ver configuraciones de seguridad para dispositivos Android.
- Ver configuraciones de seguimiento de información sensible.
- Ver configuraciones de gestion de parches.
- Visualizar detecciones de amenazas.
- Visualizar accesos a páginas web y spam.
- Acceso a informes avanzados.

22.4. ¿Qué es un permiso?

Un permiso regula el acceso a un aspecto concreto de la consola de administración. Existen 15 permisos que establecen el acceso a otros tantos aspectos de la consola de **Panda Adaptive Defense 360**. Una configuración particular de todos los permisos disponibles genera un rol, que podrá ser asignado a una o más cuentas de usuario.

Los permisos implementados en **Panda Adaptive Defense 360** se listan a continuación:

- Gestionar usuarios y roles
- Asignar licencias
- Modificar el árbol de equipos
- Añadir, descubrir y eliminar equipos
- Configurar proxys e idioma
- Modificar ajustes por equipo (actualizaciones, contraseñas etc)
- Reiniciar equipos
- Configurar seguridad para estaciones y servidores
- Ver configuraciones de seguridad para para estaciones y servidores
- Configurar seguridad para dispositivos Android
- Ver configuraciones de seguridad para dispositivos Android
- Visualizar detecciones y amenazas
- Visualizar accesos a páginas web y spam
- Acceso a Advanced Reporting Tool
- Lanzar análisis y desinfectar
- Excluir temporalmente amenazas (Malware, PUP y Bloqueados)
- Configurar gestión de parches
- Instalar parches
- Visualizar parches disponibles
- Configurar seguimiento de información personal
- Ver configuraciones de seguimiento de información sensible
- Buscar información en los equipos

22.4.1 Significado de los permisos implementados

A continuación, se detallan los permisos existentes, indicando la funcionalidad de cada uno de ellos.

Gestionar usuarios y roles

- **Al activar**: el usuario de la cuenta podrá crear, borrar y editar cuentas de usuario y roles.
- **Al desactivar**: el usuario de la cuenta deja de poder crear, borrar y editar cuentas de usuario y roles. Se permite ver el listado de usuarios dados de alta y los detalles de las

cuentas, pero no el listado de roles creados.

Asignar licencias

- **Al activar**: el usuario de la cuenta podrá asignar y retirar licencias de los equipos gestionados.
- **Al desactivar**: el usuario de la cuenta no podrá asignar y retirar licencias, pero podrá ver si los equipos tienen licencias asignadas.

Modificar el árbol de equipos

- **Al activar**: el usuario de la cuenta tiene pleno acceso al árbol de grupos, pudiendo crear y eliminar grupos, y mover equipos a grupos ya creados.
- **Al activar con conflicto de permisos**: debido a herencia, modificar el árbol de equipos puede implicar un cambio de configuración para los dispositivos. Si alguno de los permisos que permiten al administrador cambiar las configuraciones están desactivados, solo se permitirá crear grupos, eliminar grupos vacíos y cambiar el nombre de un grupo. Los permisos que permiten cambiar las configuraciones son:
  - Modificar configuración de red (proxys y caché)
  - Modificar ajustes por equipo (actualizaciones, contraseñas, etc.)
  - Configurar seguridad para estaciones y servidores
  - Configurar seguridad para dispositivos Android
  - Lanzar análisis
  - Configurar seguimiento de información personal
- **Al desactivar**: el usuario de la cuenta puede visualizar el árbol de carpetas y las configuraciones asignadas a cada grupo, pero no puede crear nuevos grupos ni mover equipos. Podrá cambiar la configuración de un grupo, ya que esta acción queda regulada con el permiso **Configurar seguridad para estaciones y servidores**, o **Configurar seguridad para dispositivos Android.**

Añadir, descubrir y eliminar equipos

- **Al activar**: el usuario de la cuenta puede distribuir el instalador entre los equipos de la red e integrarlos en la consola, eliminarlos y configurar toda la funcionalidad relativa al descubrimiento de puestos no gestionados: asignar y retirar el rol de descubridor a los equipos, editar las opciones de descubrimiento, lanzar descubrimientos inmediatos e instalar el agente de Panda de forma remota desde los listados de equipos descubiertos.
- **Al desactivar**: el usuario de la cuenta no podrá descargar el instalador, ni por lo tanto distribuirlo entre los equipos de la red. Tampoco podrá eliminar equipos previamente integrados ni gestionar la funcionalidad relativa al descubrimiento de equipos no gestionados.

Configurar proxys e idioma

- **Al activar**: el usuario de la cuenta podrá crear nuevas configuraciones de tipo **Proxy e Idioma**, editar o borrar las existentes y asignarlas a los equipos integrados en la consola.
- **Al desactivar**: el usuario de la cuenta dejará de poder crear nuevas configuraciones de tipo **Proxy e Idioma**, borrar las existentes o cambiar la asignación de los equipos integrados a la consola.

Puesto que un cambio de grupo de un equipo en el árbol de grupos puede provocar un cambio de configuración de Proxy e Idioma asignada, al desactivar Configurar Proxys e idioma se obliga también a desactivar el permiso Modificar el árbol de equipos,

Modificar ajustes por equipo (actualizaciones, contraseñas etc)

- **Al activar**: el usuario de la cuenta podrá crear nuevas configuraciones de tipo **Ajustes por equipo**, editar y borrar las ya creadas y asignar a los equipos integrados en la consola.
- **Al desactivar**: el usuario de la cuenta dejará de poder crear nuevas configuraciones de tipo **Ajustes por equipo**, borrar las existentes o cambiar la asignación de los equipos integrados a la consola.

Puesto que un cambio de carpeta de un equipo en el árbol de carpetas puede provocar un cambio de configuración de Ajustes por equipo asignado, al desactivar Ajustes por equipo se obliga también a desactivar el permiso Modificar el árbol de equipos.

Reiniciar equipos

- **Al activar**: el usuario de la cuenta podrá reiniciar equipos desde el menú superior **Equipos** y seleccionando en el menú de contexto **Reiniciar**, para estaciones y servidores Windows, Linux y macOS.
- **Al desactivar**: el usuario de la cuenta dejará de poder reiniciar equipos.

Aislar equipos

- **Al activar**: el usuario de la cuenta podrá aislar y dejar de aislar equipos desde el menú superior **Equipos** y desde los listados **Licencias** y **Equipos protegidos** seleccionando en el menú de contexto o en barra de acciones **Aislar equipos**, para estaciones y servidores Windows.
- **Al desactivar**: el usuario de la cuenta dejará de poder aislar equipos.

Configurar seguridad para estaciones y servidores

- **Al activar**: el usuario de la cuenta podrá crear, editar, borrar y asignar configuraciones de seguridad para estaciones y servidores Windows, Linux y macOS.
- **Al desactivar**: el usuario de la cuenta dejará de poder crear, editar, borrar y asignar configuraciones de seguridad para estaciones y servidores Windows, Linux y macOS.

Puesto que el cambio de grupo de un equipo en el árbol de grupos puede provocar un cambio de configuración de Estaciones y servidores, al desactivar Configurar seguridad para estaciones y servidores se obliga también a desactivar el permiso Modificar el árbol de equipos,

Al desactivar este permiso se mostrará el permiso Ver configuraciones de seguridad para estaciones y servidores.

Ver configuraciones de seguridad para estaciones y servidores

Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar la seguridad para estaciones y servidores.

- **Al activar**: el usuario de la cuenta podrá únicamente visualizar las configuraciones de seguridad creadas, así como ver la configuración de un equipo o de un grupo.
- **Al desactivar**: el usuario de la cuenta dejará de poder ver las configuraciones de seguridad creadas, y tampoco podrá acceder a las configuraciones asignadas de cada equipo.

Configurar seguridad para dispositivos Android

- **Al activar**: el usuario de la cuenta podrá crear, editar, borrar y asignar configuraciones de dispositivos Android.
- **Al desactivar**: el usuario de la cuenta dejará de poder crear, editar, borrar y asignar configuraciones de dispositivos Android.

Puesto que el cambio de grupo de un equipo en el árbol de grupos puede provocar un cambio de configuración de dispositivos Android, al desactivar Configurar seguridad para dispositivos Android se obliga también a desactivar el permiso Modificar el árbol de equipos.

Al desactivar este permiso se mostrará el permiso **Ver configuraciones de seguridad para dispositivos Android**, explicado a continuación.

Ver configuraciones de seguridad para dispositivos Android

Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar la seguridad para dispositivos Android.

- **Al activar**: el usuario de la cuenta podrá únicamente visualizar las configuraciones dispositivos Android creadas, así como ver la configuración de un dispositivo Android equipo o de un grupo.
- **Al desactivar**: el usuario de la cuenta dejará de poder ver las configuraciones Dispositivos Android creadas, y tampoco podrá acceder a las configuraciones asignadas de cada dispositivo Android.

Visualizar detecciones y amenazas

- **Al activar**: el usuario de la cuenta podrá acceder a los paneles y listados de la sección **Seguridad** en el menú superior **Estado,** y crear nuevos listados con filtros personalizados.
- **Al desactivar**: el usuario de la cuenta no podrá visualizar ni acceder a los paneles y listados de la sección **Seguridad** en el menú superior **Estado,** ni crear nuevos listados con filtros personalizados.

El acceso a la funcionalidad relativa a la exclusión y desbloqueo de amenazas y elementos desconocidos se establece mediante el permiso Excluir temporalmente amenazas (Malware, PUP y Bloqueados).

Visualizar accesos a páginas web y spam

- **Al activar**: el usuario de la cuenta podrá acceder a los paneles y listados de la sección **Accesos web y spam** en el menú superior **Estado.**
- **Al desactivar**: el usuario de la cuenta ya no podrá acceder a los paneles y listados de la sección **Accesos web y spam** en el menú superior **Estado**.

Acceso a Advanced Reporting Tool

- **Al activar**: el usuario de la cuenta podrá acceder a la herramienta **Advanced Reporting Tool** desde el panel de la izquierda en el menú superior **Estado.**
- **Al desactivar**: el acceso a la herramienta **Advanced Reporting Tool** se oculta.

Lanzar análisis y desinfectar

- **Al activar**: el usuario de la cuenta podrá crear editar, modificar y borrar tareas de tipo análisis y desinfección.
- **Al desactivar**: el usuario de la cuenta no podrá crear, editar, modificar ni borrar las tareas ya creadas de tipo análisis. Únicamente podrá listar las tareas y visualizar su configuración.

Excluir temporalmente amenazas (Malware, PUP y Bloqueados)

- **Al activar**: el usuario de la cuenta puede desbloquear, no volver a detectar, bloquear, dejar de permitir y cambiar el comportamiento ante reclasificaciones de malware, PUP y desconocidos en clasificación.
- **Al desactivar**: el usuario de la cuenta no podrá desbloquear, no volver a detectar, bloquear, dejar de permitir y cambiar el comportamiento ante reclasificaciones de malware, PUP y desconocidos en clasificación.

Es necesario activar Visualizar detecciones y amenazas para poder ejercer completamente Excluir temporalmente amenazas (Malware. PUP, Bloqueados).

Configurar gestión de parches

- **Al activar**: el usuario de la cuenta podrá crear, editar, borrar y asignar configuraciones de gestión de parches para estaciones y servidores Windows.
- **Al desactivar**: el usuario de la cuenta dejará de poder crear, editar, borrar y asignar configuraciones de gestión de parches para estaciones y servidores Windows.

Puesto que el cambio de grupo de un equipo en el árbol de grupos puede provocar un cambio de configuración de Gestión de parches, al desactivar Configurar gestión de parches se obliga también a desactivar el permiso Modificar el árbol de equipos,

Al desactivar este permiso se mostrará el permiso **Visualizar configuraciones de gestión de parches**.

Visualizar configuraciones de gestión de parches

Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar gestión de parches.

- **Al activar**: el usuario de la cuenta podrá únicamente visualizar las configuraciones de gestión de parches creadas, así como ver la configuración asignadas a un equipo o a un grupo.
- **Al desactivar**: el usuario de la cuenta dejará de poder ver las configuraciones Gestión de parches creadas, y tampoco podrá acceder a las configuraciones asignadas a cada equipo.

Instalar parches

Puesto que el cambio de grupo de un equipo en el árbol de grupos puede provocar un cambio de configuración de Instalar parches, al desactivar Instalar parches se obliga también a desactivar el permiso Modificar el árbol de equipos.

- **Al activar**: el usuario de la cuenta podrá crear tareas de parcheo y acceder a los listados **Parches disponibles**, **Programas "End of life"** e **Historial de instalaciones**.
- **Al desactivar**: el usuario de la cuenta dejará de poder crear tareas de parcheo.

Visualizar parches disponibles

Este permiso solo es accesible cuando se ha deshabilitado el permiso Instalar parches.

- **Al activar**: el usuario de la cuenta podrá acceder a los listados **Estado de gestión de parches**, **Parches disponibles**, **Programas "End of life"** e **Historial de instalaciones**.
- **Al desactivar**: el usuario de la cuenta dejará de poder acceder a los listados**Parches disponibles**, **Programas "End of life"** e **Historial de instalaciones**.

Configurar seguimiento de información personal

- **Al activar**: el usuario de la cuenta podrá crear, editar, borrar y asignar configuraciones de Seguimiento de información personal en equipos Windows.
- **Al desactivar**: el usuario de la cuenta dejará de poder crear, editar, borrar y asignar configuraciones de Seguimiento de información personal en equipos Windows.

Ver seguimiento de información personal

Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar seguimiento de información personal.

- **Al activar**: el usuario de la cuenta podrá únicamente visualizar las configuraciones de Seguimiento de información personal, así como ver la configuración de un equipo o de un grupo.
- **Al desactivar**: el usuario de la cuenta dejará de poder ver las configuraciones de Seguimiento de información personal creadas, y tampoco podrá acceder a las configuraciones asignadas de cada equipo.

Buscar información en los equipos

- **Al activar**: el usuario de la cuenta podrá acceder a los widgets de búsqueda de ficheros por nombre y contenido almacenados en los equipos de los usuarios.
- **Al desactivar**: el usuario de la cuenta dejará de poder acceder a los widgets de búsqueda de ficheros por nombre y contenido almacenados en los equipos de los usuarios.

22.5. Acceso a la configuración de cuentas de usuarios y roles

En el menú superior **Configuración,** y haciendo clic en el panel de la izquierda **Usuarios**, aparecen dos entradas asociadas a la gestión de roles y cuentas de usuario:

- **Usuarios**: permite crear nuevas cuentas de usuario y definir su pertenencia a uno o varios roles.
- **Roles**: permite crear y modificar una nueva configuración de acceso a los recursos de **Panda Adaptive Defense 360**.

Las pestañas de **Usuarios y roles** solo son accesibles si el usuario tiene el permiso **Gestionar usuarios y roles.**

22.6. Creación y configuración de cuentas de usuario

En el menú superior **Configuración**, haciendo clic en el panel de la izquierda **Usuarios** y después en la pestaña **Usuarios,** podrás realizar todas las acciones necesarias relativas a la creación y modificación de cuentas de usuario.

- **Añadir nueva cuenta de usuario**: haz clic en el botón **Añadir** para añadir un nuevo usuario, establecer la cuenta de correo para el acceso, el rol al que pertenecerá y una descripción de la cuenta. El sistema enviará un correo a la cuenta para generar la contraseña de acceso.

- **Editar una cuenta de usuario**: haz clic en el nombre del usuario para mostrar una ventana con todos los datos de la cuenta editables.

- **Borrar o desactivar cuentas de usuarios**: haz clic sobre el icono  de una cuenta de usuario para borrarla. Haz clic en una cuenta de usuario y selecciona el interruptor **Bloquear este usuario para** inhabilitada temporalmente el acceso de la cuenta a la consola web. De esta manera, esa cuenta verá denegado el acceso a la consola de administración, y si ya estuviera logeado será expulsada de forma inmediata. También dejará de recibir alertas por correo en las direcciones de correo especificadas en su configuración.

22.7. Creación y configuración de roles

En el menú superior **Configuración**, haciendo clic en el panel de la izquierda **Usuarios** y después en la pestaña **Roles,** podrás realizar todas las acciones necesarias relativas a la creación y modificación de roles.

- **Añadir nuevo rol**: haz clic en el botón **Añadir**. Se pedirá el nombre del rol, una descripción opcional, una selección sobre los equipos accesibles y una configuración concreta de los permisos.
- **Editar un rol**: haz clic en el nombre del rol para mostrará una ventana con todas sus configuraciones editables.

- **Copiar un rol:** haz clic en el icono  para mostrar una ventana con un nuevo rol configurado de la misma forma que el original.

- **Borrar rol**: haz clic sobre el icono  de un rol para borrarlo. Si al borrar un rol éste ya tiene cuentas de usuario asignadas, se cancelará el proceso de borrado.

22.8. Registro de la actividad de las cuentas de usuario

Panda Adaptive Defense 360 registra todas las acciones efectuadas por los administradores de red en la consola web de gestión. De esta forma es fácil determinar quién realizó un cambio, en que momento y sobre qué objeto.

Para acceder a la sección de actividad haz clic en el menú superior **Configuración** y después en la pestaña **Actividad.**

22.8.1 Registro de acciones

La sección de acciones permite listar todas las acciones ejecutadas por las cuentas de usuario, exportar las acciones a formato csv y filtrar la información.

Campos mostrados en el listado de acciones

Campo	Comentario	Valores
Fecha	Fecha y hora en la que se produjo la acción	Fecha
Usuario	Cuenta de usuario que ejecuto la acción	Cadena de caracteres
Acción	Tipo de operación que se realizó	Acceder Añadir envío Asignar licencia Bloquear Borrar Cambiar 'Ajustes por equipo' Cambiar 'Configuración de Seguridad' Cambiar Grupo Cambiar Grupo-Padre Cambiar 'Proxy e idioma' Cancelar Configurar descubrimiento Crear Desasignar licencia Dejar de permitir Desbloquear Descubrir ahora Designar equipo caché Designar equipo descubridor Designar Proxy Panda Editar Editar descripción Editar envío Editar nombre Eliminar Eliminar envío Heredar 'Ajustes por equipo' Heredar 'Configuración de Seguridad' Heredar 'Proxy e idioma' Instalar Localizar Mover a su ruta de Active Directory Mover equipos a su ruta de Active Directory Ocultar Permitir Publicar Reiniciar Restaurar comunicaciones Revocar equipo caché Revocar equipo descubridor Revocar Proxy Panda Sincronizar grupo Visibilizar
Tipo de elemento	Tipo del objeto de la consola sobre el cual se ejecutó la acción	Amenaza Configuración Dispositivo Android Equipo Equipo no administrado Filtro

		Grupo Grupo de dispositivos Informe ejecutivo Informes avanzados Listado Preferencia para envío emails Rol Tarea - Análisis de seguridad Usuario
Elemento	Objeto de la consola sobre el cual se ejecutó la acción	Cadena de caracteres

Tabla 84: campos del Registro de acciones

Campos mostrados en el fichero exportado

Campo	Comentario	Valores
Fecha	Fecha y hora en la que se produjo la acción	Fecha
Usuario	Cuenta de usuario que ejecuto la acción	Cadena de caracteres
Acciones		Acceder Añadir envío Asignar licencia Bloquear Borrar Cambiar 'Ajustes por equipo' Cambiar 'Configuración de Seguridad' Cambiar Grupo Cambiar Grupo-Padre Cambiar 'Proxy e idioma' Cancelar Configurar descubrimiento Crear Desasignar licencia Dejar de permitir Desbloquear Descubrir ahora Designar equipo caché Designar equipo descubridor Designar Proxy Panda Editar Editar descripción Editar envío Editar nombre Eliminar Eliminar envío Heredar 'Ajustes por equipo' Heredar 'Configuración de Seguridad' Heredar 'Proxy e idioma' Instalar Localizar Mover a su ruta de Active Directory Mover equipos a su ruta de Active Directory Ocultar

Campo	Comentario	Valores
		Permitir Publicar Reiniciar Restaurar comunicaciones Revocar equipo caché Revocar equipo descubridor Revocar Proxy Panda Sincronizar grupo Visibilizar
Tipo de elemento	Tipo del objeto de la consola sobre el cual se ejecutó la acción	Amenaza Configuración Dispositivo Android Equipo Equipo no administrado Filtro Grupo Grupo de dispositivos Informe ejecutivo Informes avanzados Listado Preferencia para envío emails Rol Tarea - Análisis de seguridad Usuario
Elemento	Objeto de la consola sobre el cual se ejecutó la acción	Cadena de caracteres

Tabla 85: campos del fichero exportado Registro de acciones

Herramienta de búsqueda

Campo	Comentario	Valores
Desde		Fecha
Hasta		Fecha
Usuarios		Listado de cuentas de usuario creados en la consola de administración

Tabla 86: campos de filtrado para el Registro de acciones

22.8.2 Registro de sesiones

La sección de sesiones permite listar todos los accesos a la consola de administración, exportarlos a formato csv y filtrar la información.

Campos mostrados en el listado de sesiones

Campo	Comentario	Valores

Fecha	Fecha y hora en la que se produjo el acceso	Fecha
Usuario	Cuenta de usuario que accedió	Cadena de caracteres
Actividad		Iniciar sesión Cerrar sesión
Dirección IP	Dirección IP desde donde se produce el acceso	Cadena de caracteres

Tabla 87: campos del listado sesiones

Campos mostrados en el fichero exportado

Campo	Comentario	Valores
Fecha	Fecha y hora en la que se produjo el acceso	Fecha
Usuario	Cuenta de usuario que accedió	Cadena de caracteres
Actividad		Iniciar sesión Cerrar sesión
Dirección IP	Dirección IP desde donde se produce el acceso	Cadena de caracteres

Tabla 88: campos del fichero exportado sesiones

Herramienta de búsqueda

Campo	Comentario	Valores
Desde		Fecha
Hasta		Fecha
Usuarios		Listado de cuentas de usuario creados en la consola de administración

Tabla 89: campos de filtrado para el listado de sesiones

23. Apéndice I: Requisitos de Panda Adaptive Defense 360

23.1. Requisitos de plataformas Windows

23.1.1 Sistemas operativos soportados

Estaciones de trabajo

- Windows XP SP3 (32 bits)
- Windows Vista (32 y 64-bit)
- Windows 7 (32 y 64-bit)
- Windows 8 (32 y 64-bit)
- Windows 8.1 (32 y 64-bit)
- Windows 10 (32 y 64-bit)

Servidores

- Windows 2003 (32, 64-bit y R2) SP2 y superiors
- Windows 2008 (32 y 64-bit) y 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server Core 2008, 2008 R2, 2012 R2 y 2016

23.1.2 Requisitos hardware

- **Procesador**: Pentium 1 Ghz.
- **Memoria RAM**: 1 Gbyte.
- **Espacio libre en el disco duro para la instalación**: 650 Mbytes.

23.2. Requisitos de plataformas Windows Exchange

23.2.1 Sistemas operativos soportados

- **Exchange 2003**: Windows Server 2003 32 bits SP2+ y Windows Server 2003 R2 32 bits
- **Exchange 2007**: Windows Server 2003 64 bits SP2+, Windows Server 2003 R2 64 bits, Windows 2008 64 bits y Windows 2008 R2
- **Exchange 2010**: Windows 2008 64 bits y Windows 2008 R2
- **Exchange 2013**: Windows Server 2012 y Windows Server 2012 R2
- **Exchange 2016**: Windows Server 2012, Windows Server 2012 R2 y Windows Server 2016.

23.2.2 Requisitos hardware y software

Los requisitos de hardware para instalar la protección de Servidores Exchange son los que marca el propio Exchange Server:

- Exchange 2003:

http://technet.microsoft.com/es-es/library/cc164322(v=exchg.65).aspx

- Exchange 2007:

http://technet.microsoft.com/es-es/library/aa996719(v=exchg.80).aspx

- Exchange 2010:

http://technet.microsoft.com/es-es/library/aa996719(v=exchg.141).aspx

- Exchange 2013

http://technet.microsoft.com/es-es/library/aa996719(v=exchg.150).aspx

- Exchange 2016

https://technet.microsoft.com/es-es/library/aa996719(v=exchg.160).aspx

23.2.3 Versiones Exchange soportadas

- Microsoft Exchange Server 2003 Standard y Enterprise (SP1 / SP2)
- Microsoft Exchange Server 2007 Standard y Enterprise (SP0 / SP1 / SP2 / SP3)
- Microsoft Exchange Server 2007 incluido en Windows SBS 2008
- Microsoft Exchange Server 2010 Standard y Enterprise (SP0 / SP1 / SP2)
- Microsoft Exchange Server 2010 incluido en Windows SBS 2011
- Microsoft Exchange Server 2013 Standard y Enterprise
- Microsoft Exchange Server 2016 Standard y Enterprise

23.3. Requisitos de plataformas macOS

23.3.1 Sistemas operativos soportados

- macOS 10.10 Yosemite
- macOS 10.11 El Capitan
- macOS 10.12 Sierra
- macOS 10.13 High Sierra

23.3.2 Requisitos hardware

- **Procesador**: Intel Core 2 Duo
- **Memoria RAM**: 2 Gbyte
- **Espacio libre en el disco duro para la instalación**: 400 Mbytes
- **Puertos:** se requieren los puertos 3127, 3128, 3129 y 8310 libres para el funcionamiento del filtrado web y la detección web de malware.

23.4. Requisitos de plataformas Linux

23.4.1 Distribuciones de 64 bits soportadas

- Ubuntu 14.04 LTS, 14.10, 15.04, 15.10, 16.0.4 LTS y 16.10
- Fedora 23, 24 y 25

23.4.2 Versión de kernel soportada

- **Versión mínima soportada**: 3.13
- **Versión máxima soportada**: 4.10

23.4.3 Gestores de ficheros soportados

- Nautilus
- Pcmanfm
- dolphin

23.4.4 Requisitos hardware

- **Procesador**: Pentium 1 Ghz
- **Memoria RAM**: 1.5 Gbytes
- **Espacio libre en el disco duro para la instalación**: 100 Mbytes
- **Puertos:** se requieren los puertos 3127, 3128, 3129 y 8310 libres para el funcionamiento del filtrado web y la detección web de malware.

23.4.5 Dependencias del paquete de instalación

debconf (>= 0.5) | debconf-2.0	libfreetype6 (>= 2.3.5)	libpng12-0 (>= 1.2.13-4)	libxcb1
dkms (>= 1.95)	libgcc1 (>= 1:4.1.1)	libsm6, libssl1.0.0 (>= 1.0.0)	libxrender1
libc6 (>= 2.17)	libgl1-mesa-glx | libgl1	libstdc++6 (>= 4.6)	make
libc6-dev	libice6 (>= 1:1.0.0)	libstdc++6:i386	notify-osd
libcurl3:i386	libltdl7 (>= 2.4.2)	libuuid1 (>= 2.16)	notification-daemon
libcups2	libnl-3-200 (>= 3.2.7)	libuuid1:i386	python-nautilus (>= 1.1-4)
libdbus-1-3 (>= 1.1.1)	libnl-genl-3-200 (>= 3.2.7)	libx11-6	zlib1g (>= 1:1.1.4)
libfontconfig1 (>= 2.9.0)	libnotify-bin (>= 0.7.6)	libx11-xcb1	

Tabla 90: librerías necesarias para la instalación

23.5. Requisitos de plataformas Android

23.5.1 Sistemas operativos soportados

- Ice Cream Sandwich 4.0
- Jelly Bean 4.1 - 4.2 - 4.3
- KitKat 4.4
- Lollipop 5.0/5.1
- Marshmallow 6.0
- Nougat 7.0 - 7.1
- Oreo 8.0

23.5.2 Requisitos hardware

Se requiere un mínimo de 10 megabytes de espacio en la memoria interna del dispositivo. Dependiendo del modelo es posible que el espacio requerido sea superior.

23.5.3 Requisitos de red

Para que las notificaciones push funcionen correctamente desde la red de la empresa es necesario abrir los puertos 5228, 5229 y 5230 a todo el bloque de IPs ASN 15169 correspondientes a Google.

23.6. Acceso a la consola web

La consola de administración es accesible con la última versión de los navegadores compatibles mostrados a continuación:

- Chrome
- Internet Explorer
- Microsoft Edge
- Firefox
- Opera

23.7. Acceso a URLs del servicio

Para el correcto funcionamiento de **Panda Adaptive Defense 360** es necesario que las URL mostradas a continuación sean accesibles desde los equipos protegidos de la red.

- https://*.pandasecurity.com
- http://*.pandasecurity.com
- https://*.windows.net

- https://pandasecurity.logtrust.com
- http://*.pandasoftware.com

Tráfico de entrada y salida (Antispam y filtrado URL)

- http://*.pand.ctmail.com
- http://download.ctmail.com

Puertos

- Port 80 (HTTP, websocket)
- Port 443 (HTTPS)

Descarga de parches y actualizaciones (Panda Patch Management)

Consulta la pagina de soporte https://www.pandasecurity.com/spain/support/card?id=700044 para obtener un listado completo de las urls accesibles desde los equipos de la red que recibirán los parches o desde los equipos con rol de caché / repositorio.

24. Apéndice II: Creación y gestión de cuentas Panda

Creación de una Cuenta Panda
Activación de la Cuenta Panda

24.1. Introducción

La Cuenta Panda ofrece al administrador un mecanismo de creación y acceso seguro a los servicios contratados con Panda Security, frente al método estándar de recepción de credenciales por correo electrónico.

Con una Cuenta panda es el propio administrador quien crea y activa el método de acceso a la consola Web de **Panda Adaptive Defense 360**.

24.2. Creación de una Cuenta Panda

Para crear una nueva Cuenta Panda es necesario seguir el procedimiento descrito a continuación.

Recepción del mensaje de correo

- Al adquirir **Panda Adaptive Defense 360** recibirás un mensaje de correo electrónico procedente de Panda Security.
- Haz clic en el vínculo que contiene el mensaje para acceder a la Web desde la que podrás crear la Cuenta Panda.

Rellena el formulario

- Rellena con tus datos el formulario mostrado.
- Utiliza el desplegable situado en la esquina inferior derecha si deseas que la página se muestre en otro idioma.
- Accede al acuerdo de licencia y la política de privacidad haciendo clic en el vínculo correspondiente.
- Haz clic en **Crear** cuando hayas terminado para recibir un mensaje de correo electrónico en la dirección especificada en el formulario. Utilizando ese mensaje podrás activar la cuenta.

24.3. Activación de la Cuenta Panda

Una vez creada la Cuenta Panda es necesario activarla. Para ello hay que utilizar el mensaje de correo electrónico que has recibido en la bandeja de entrada de la dirección mail utilizada para crear la Cuenta Panda.

- Ve a la bandeja de entrada y localiza el mensaje.
- Haz clic en el botón de activación. Al hacerlo, se confirmará como válida la dirección proporcionada al crear la Cuenta Panda. En caso de que el botón no funcione, copia en el navegador el enlace que se muestra en el mensaje.
- La primera vez que se acceda a la Cuenta Panda se solicitará una confirmación de contraseña. Después, haz clic en el botón **Activar cuenta**.

- Introduce los datos necesarios y haz clic en **Guardar datos**. Si prefieres facilitar los datos en otra ocasión, utiliza la opción **Ahora no**.
- Acepta el acuerdo de licencias y haz clic en **Aceptar**.

Una vez finalizado con éxito el proceso de activación de la Cuenta Panda te encontrarás en la página principal de Panda Cloud. Desde aquí puedes acceder a la consola Web de **Panda Adaptive Defense 360**. Para ello, utiliza el icono de acceso directo que encontrarás en **Mis servicios**.

25. Apéndice III: Listado de des instaladores

Al lanzar la instalación del producto **Panda Adaptive Defense 360** es posible que se detecten otros productos de seguridad instalados en el equipo. En este caso, antes de instalar la protección, **Panda Adaptive Defense 360** desinstalará automáticamente los productos que aparecen en la Tabla 91:

Fabricante	Nombre del producto
Computer Associates	eTrust AntiVirus 8.1.655, 8.1.660, 7.1* eTrust 8.0
Avast	Avast! Free Antivirus 2014 Avast! 8.x Free Antivirus Avast! 7.x Free Antivirus Avast! 6.x Free Antivirus Avast! 5.x Free Antivirus Avast! 4 Free Antivirus Avast! 4 Small Business Server Edition Avast! 4 Windows Home Server Edition 4.8
AVG	AVG Internet Security 2013 (32bit- Edition) AVG Internet Security 2013 (64bit- Edition) AVG AntiVirus Business Edition 2013 (32bit- Edition) AVG AntiVirus Business Edition 2013 (64bit- Edition) AVG CloudCare 2.x AVG Anti-Virus Business Edition 2012 AVG Internet Security 2011 AVG Internet Security Business Edition 2011 32bits* AVG Internet Security Business Edition 2011 64bits (10.0.1375)* AVG Anti-Virus Network Edition 8.5* AVG Internet Security SBS Edition 8 Anti-Virus SBS Edition 8.0 AVGFree v8.5, v8, v7.5, v7.0
Avira	Avira AntiVir PersonalEdition Classic 7.x, 6.x Avira AntiVir Personal Edition 8.x Avira Antivir Personal - Free Antivirus 10.x, 9.x Avira Free Antivirus 2012, 2013 Avira AntiVir PersonalEdition Premium 8.x, 7.x, 6.x Avira Antivirus Premium 2013, 2012, 10.x, 9.x Avira Antivirus 15.x
CA	CA Total Defense for Business Client V14 (32bit- Edition) CA Total Defense for Business Client V14 (64bit- Edition) CA Total Defense R12 Client (32bit- Edition) CA Total Defense R12 Client (64bit- Edition)
Bitdefender	BitDefender Panda Endpoint Protection 6.x BitDefender Business Client 11.0.22 BitDefender Free Edition 2009 12.0.12.0* Bit Defender Standard 9.9.0.082
Check Point	Check Point Endpoint Security 8.x (32 bits) Check Point Endpoint Security 8.x (64 bits)
Eset	ESET NOD32 Antivirus 3.0.XX (2008)*, 2.70.39*, 2.7* ESET Smart Security 3.0* ESET Smart Security 5 (32 bits) ESET NOD32 Antivirus 4.X (32 bits) ESET NOD32 Antivirus 4.X (64 bits) ESET NOD32 Antivirus 5 (32 bits) ESET NOD32 Antivirus 5 (64 bits) ESET NOD32 Antivirus 6 (32 bits)

Fabricante	Nombre del producto
	ESET NOD32 Antivirus 6 (64 bits) ESET NOD32 Antivirus 7 (32 bits) ESET NOD32 Antivirus 7 (64 bits)
eScan	eScan Anti-Virus (AV) Edition for Windows 14.x eScan Internet Security for SMB 14.x eScan Corporate for Windows 14.x
Frisk	F-Prot Antivirus 6.0.9.1
F- Secure	F-secure PSB Workstation Security 10.x F-Secure PSB for Workstations 9.00* F-Secure Antivirus for Workstation 9 F-Secure PSB Workstation Security 7.21 F-Secure Protection Service for Business 8.0, 7.1 F-Secure Internet Security 2009 F-Secure Internet Security 2008 F-Secure Internet Security 2007 F-Secure Internet Security 2006 F-Secure Client Security 9.x F-Secure Client Security 8.x Antivirus Client Security 7.1 F-Secure Antivirus for Workstation 8
iSheriff	iSheriff Endpoint Security 5.x
Kaspersky	Kaspersky Endpoint Security 10 for Windows (32bit- Edition) Kaspersky Endpoint Security 10 for Windows (64bit- Edition) Kaspersky Endpoint Security 8 for Windows (32bit- Edition) Kaspersky Endpoint Security 8 for Windows (64bit- Edition) Kaspersky Anti-Virus 2010 9.0.0.459* Kaspersky® Business Space Security Kaspersky® Work Space Security Kaspersky Internet Security 8.0, 7.0, 6.0 (con Windows Vista+UAC, es necesario desactivar UAC) Kaspersky Anti-Virus 8* Kaspersky® Anti-virus 7.0 (con Windows Vista+UAC, es necesario desactivar UAC) Kaspersky Anti-Virus 6.0 for Windows Workstations*
McAfee	McAfee LiveSafe 2016 x86 / x64 McAfee SaaS Panda Endpoint Protection 6.x, 5.X, 10.5.X (64 y 32 bits) McAfee VirusScan Enterprise 8.8, 8.7i, 8.5i, 8.0i, 7.1.0 McAfee Internet Security Suite 2007 McAfee Total Protection Service 4.7* McAfee Total Protection 2008
Norman	Norman Security Suite 10.x (32bit- Edition) Norman Security Suite 10.x (64bit- Edition) Norman Security Suite 9.x (32bit- Edition) Norman Security Suite 9.x (64bit- Edition) Norman Panda Endpoint Protection 8.x/9.x Norman Virus Control v5.99
Norton	Norton Antivirus Internet Security 2008* Norton Antivirus Internet Security 2007 Norton Antivirus Internet Security 2006
Microsoft	Microsoft Security Essentials 1.x Microsoft Forefront Panda Endpoint Protection 2010 Microsoft Security Essentials 4.x Microsoft Security Essentials 2.0 Microsoft Live OneCare

Fabricante	Nombre del producto
	Microsoft Live OneCare 2.5*
MicroWorld Technologies	eScan Corporate for Windows 9.0.824.205
PC Tools	Spyware Doctor with AntiVirus 9.x
Sophos	Sophos Anti-virus 9.5 Sophos Endpoint Security and Control 10.2 Sophos Endpoint Security and Control 9.5 Sophos Anti-virus 7.6 Sophos Anti-virus SBE 2.5* Sophos Security Suite
Symantec	Symantect.cloud - Panda Endpoint Protection.cloud 22.x Symantec.cloud - Panda Endpoint Protection.cloud 21.x (32bits) Symantec.cloud - Panda Endpoint Protection.cloud 21.x (64bits) Symantec Panda Endpoint Protection 14.x (32bits) Symantec Panda Endpoint Protection 14.x (64bits) Symantec Panda Endpoint Protection 12.x (32bits) Symantec Panda Endpoint Protection 12.x (64bits) Symantec Panda Endpoint Protection 11.x (32bits) Symantec Panda Endpoint Protection 11.x (64bits) Symantec Antivirus 10.1 Symantec Antivirus Corporate Edition 10.0, 9.x, 8.x
Trend Micro	Trend Micro Worry-Free Business Security 8.x (32bit- Edition) Trend Micro Worry-Free Business Security 8.x (64bit- Edition) Trend Micro Worry-Free Business Security 7.x (32bit- Edition) Trend Micro Worry-Free Business Security 7.x (64bit- Edition) Trend Micro Worry-Free Business Security 6.x (32bit- Edition) Trend Micro Worry-Free Business Security 6.x (64bit- Edition) Trend Micro Worry-Free Business Security 5.x PC-Cillin Internet Security 2006 PC-Cillin Internet Security 2007* PC-Cillin Internet Security 2008* Trend Micro OfficeScan Antivirus 8.0 Trend Micro OfficeScan 7.x Trend Micro OfficeScan 8.x Trend Micro OfficeScan 10.x Trend Micro OfficeScan 11.x
Comodo AntiVirus	Comodo Antivirus V 4.1 32bits
Panda Security	Panda Cloud Antivirus 3.x Panda Cloud Antivirus 2.X Panda Cloud Antivirus 1.X
	Panda for Desktops 4.50.XX Panda for Desktops 4.07.XX Panda for Desktops 4.05.XX Panda for Desktops 4.04.10 Panda for Desktops 4.03.XX y anteriores
	Panda for File Servers 8.50.XX Panda for File Servers 8.05.XX Panda for File Servers 8.04.10 Panda for File Servers 8.03.XX y anteriores

Fabricante	Nombre del producto
	Panda Global Protection 2017* Panda Internet Security 2017* Panda Antivirus Pro 2017* Panda Gold Protection 2017*
	Panda Global Protection 2016* Panda Internet Security 2016* Panda Antivirus Pro 2016* Panda Gold Protection 2016*
	Panda Global Protection 2015* Panda Internet Security 2015* Panda Antivirus Pro 2015* Panda Gold Protection* Panda Free Antivirus
	Panda Global Protection 2014* Panda Internet Security 2014* Panda Antivirus Pro 2014* Panda Gold Protection*
	Panda Global Protection 2013* Panda Internet Security 2013* Panda Antivirus Pro 2013*
	Panda Global Protection 2012* Panda Internet Security 2012* Panda Antivirus Pro 2012*
	Panda Global Protection 2011* Panda Internet Security 2011* Panda Antivirus Pro 2011* Panda Antivirus for Netbooks (2011)*
	Panda Global Protection 2010 Panda Internet Security 2010 Panda Antivirus Pro 2010 Panda Antivirus for Netbooks
	Panda Global Protection 2009 Panda Internet Security 2009 Panda Antivirus Pro 2009
	Panda Internet Security 2008 Panda Antivirus+Firewall 2008 Panda Antivirus 2008
	Panda Internet Security 2007 Panda Antivirus + Firewall 2007 Panda Antivirus 2007
Webroot	Webroot SecureAnywhere 9

Tabla 91: listado de desinstaladores

*Productos Panda 2015, 2014, 2013, 2012 necesitan un reinicio para completar la desinstalación.

*Comodo AntiVirus V 4.1 32 bits - En sistemas con UAC activado, durante el proceso de desinstalación el usuario debe intervenir seleccionando en la ventana del UAC la opción Permitir.

F-Secure PSB for Workstations 9.00 - Durante el proceso de instalación del agente de Panda Endpoint Protection en Windows 7 y Windows Vista, el usuario debe intervenir seleccionando la opción Permitir.

* AVG Internet Security Business Edition 2011 32 bits - Durante el proceso de instalación del agente de Panda Endpoint Protection, el usuario debe intervenir seleccionando en varias ventanas la opción Permitir.

** AVG Internet Security Business Edition 2011 64 bits (10.0.1375) - Durante el proceso de instalación del agente de Panda Endpoint Protection, el usuario debe intervenir seleccionando en varias ventanas la opción Permitir.

* Kaspersky Anti-Virus 6.0 for Windows Workstations: Durante el proceso de instalación del agente de Panda Endpoint Protection en sistemas operativos de 64 bits el usuario debe intervenir seleccionando en varias ventanas la opción Permitir. Para poder hacer la desinstalación, la protección de Kaspersky no debe tener password. En sistemas con UAC activado, durante el proceso de desinstalación el usuario debe intervenir seleccionando en la ventana del UAC la opción Permitir.

* F-Secure PSB for Workstations 9.00 - Durante el proceso de instalación del agente de Panda Endpoint Protection, el usuario debe intervenir seleccionando la opción Permitir en dos ventanas de F-Secure PSB for Workstations 9.00.

* AVG Anti-Virus Network Edition 8.5 - Durante el proceso de instalación del agente de PCOP el usuario debe intervenir seleccionando en dos ventanas de AVG Anti-Virus Network Edition 8.5 la opción Permitir.

* Productos Panda Antivirus 2011 - No se desinstalan en Windows Vista x64. En sistemas con UAC activado, durante el proceso de desinstalación el usuario debe intervenir seleccionando en la ventana del UAC la opción de permitir.

* Panda Cloud Antivirus 1.4 Pro y Panda Cloud Antivirus 1.4 Free - En sistemas con UAC activado, durante el proceso de desinstalación el usuario debe intervenir seleccionando en la ventana del UAC la opción de permitir.

* Trend Micro - PC-Cillin Internet Security 2007 y 2008 no se puede desinstalar automáticamente en Windows Vista x64.

* Trend Micro - PC-Cillin Internet Security 2007 y 2008 no se pueden desinstalar automáticamente en Windows Vista x86 teniendo UAC activado.

* ESET NOD32 Antivirus 3.0.XX (2008) no se desinstala automáticamente en plataformas de 64 bits.

* ESET Smart Security 3.0 no se desinstala automáticamente en plataformas de 64 bits.

* ESET NOD32 Antivirus 2.7 tras la instalación de agente de Panda Endpoint Protection el equipo se reiniciará automaticamente sin mostrar ningún aviso, ni pedir confirmación al usuario.

* ESET NOD32 Antivirus 2.70.39 tras la instalación de agente de Panda Endpoint Protection el equipo se reiniciará automaticamente sin mostrar ningún aviso, ni pedir confirmación al usuario.

* Sophos Anti-virus SBE 2.5 no se desinstala correctamente en Windows 2008.

* eTrust Antivirus 7.1. no se desinstala en sistemas operativos de 64bits (Windows 2003 64bits y Windows XP 64bits).

* Norton Antivirus Internet Security 2008 no se puede desinstalar en Windows Vista con UAC activado.

* Kaspersky Anti-Virus 2010 9.0.0.459. En sistemas con UAC activado, durante el proceso de desinstalación el usuario debe intervenir seleccionando en la ventana del UAC la opción de permitir.

* Kaspersky Anti-Virus 8. En Windows Vista con UAC activado, durante el proceso de desinstalación el usuario debe intervenir seleccionando en la ventana del UAC la opción de permitir.

* BitDefender Free Edition 2009 12.0.12.0. En Windows Vista con UAC activado, durante el proceso de desinstalación el usuario debe intervenir seleccionando en la ventana del UAC la opción de permitir.

*McAfee Total Protection Service 4.7. El desinstalador no funciona en sistemas con UAC activado. Además, en sistemas de 32 bits es necesaria la intervención del usuario.

* Microsoft Live OneCare 2.5. No desinstala en Windows Small Business Server 2008.

En caso de tener instalado un programa que no se encuentra incluido en el listado, consulte con el proveedor correspondiente cómo desinstalarlo antes de instalar la protección de Panda Endpoint Protection.

26. Apéndice IV: Conceptos Clave

100% Attestation Service

Servicio de **Panda Adaptive Defense 360** incluido en la licencia básica que clasifica el 100% de los procesos ejecutados en los equipos de usuario y servidores para emitir una valoración sin ambigüedades (goodware o malware, sin sospechosos).

Adaptador de red

Hardware que permite la comunicación entre diferentes equipos conectados a través de una red de datos. Un equipo puede tener más de un adaptador de red instalado y es identificado en el sistema mediante un número de identificación único.

Advanced Reporting Tool (ART)

Servicio avanzado de explotación del conocimiento generado en tiempo real por los productos Panda Adaptive Defense y Panda Adaptive Defense 360. Facilita el descubrimiento de amenazas desconocidas, ataques dirigidos y APTs, representando los datos de actividad de los procesos ejecutados por los usuarios, poniendo el énfasis en los eventos relacionados con la seguridad y la extracción de información.

Adware

Programa que, una vez instalado o mientras se está instalando, ejecuta, muestra o descarga automáticamente publicidad en el equipo.

Agente Panda

Uno de los dos módulos del software Panda Adaptive Defense 360, se encarga de las comunicaciones entre los equipos de la red y los servidores en la nube de Panda Security, además de la gestión de los procesos locales.

Alerta

Ver Incidencia.

Análisis forense

Conjunto de técnicas y procesos ejecutados por el administrador de la red con herramientas especializadas para seguir la ejecución de un programa malicioso y determinar las consecuencias de la infección.

Análisis heurístico

Análisis estático formado por un conjunto de técnicas que inspeccionan el programa sospechoso en base a cientos de características del archivo para determinar la probabilidad de que pueda llevar a cabo acciones maliciosas o dañinas cuando se ejecute en el equipo del usuario.

Anti-tamper

Conjunto de tecnologías que evitan la manipulación de los procesos de **Panda Adaptive Defense 360** por parte de amenazas avanzadas y APT que buscan sortear las capacidades de protección de la herramienta de seguridad instalada.

Anti Spam

Tecnología que busca correos no deseados en función de su contenido.

Antivirus

Módulo de protección basado en tecnologías tradicionales (fichero de firmas, análisis heurístico, anti exploit etc), que detecta y elimina virus informáticos y otras amenazas.

APT (Advanced Persistent Threat)

Conjunto de estrategias emprendidas por hackers orientadas a infectar la red del cliente, utilizando múltiples vectores de infección de forma simultánea para pasar inadvertidos a los antivirus tradicionales durante largos periodos de tiempo. Su objetivo principal es económico (robo de información confidencial de la empresa para chantaje, robo de propiedad intelectual etc).

ASLR (Address Space Layout Randomization)

Técnica implementada por el sistema operativo para mitigar los efectos de ataques de tipo exploit basados en desbordamiento de buffer. Mediante ASLR el sistema operativo introduce aleatoriedad a la hora de asignar direcciones de memoria para reservar espacio destinado a la pila, el heap y las librerías cargadas por los procesos. De esta forma, se dificulta la utilización ilegítima de llamadas a funciones del sistema por desconocer la dirección física de memoria donde residen.

Árbol de carpetas

Estructura jerárquica formada por agrupaciones estáticas, utilizada para organizar el parque de equipos y facilitar la asignación de configuraciones.

Árbol de filtros

Colección de filtros agrupados en carpetas que facilitan la organización del parque de equipos y la asignación de configuraciones.

Archivo de identificadores / fichero de firmas

Fichero que contiene los patrones que el antivirus utiliza para detectar las amenazas.

ARP (Address Resolution Protocol)

Protocolo utilizado para resolver direcciones del nivel de red a direcciones del nivel de enlace. En redes IP traduce las direcciones IP a direcciones físicas MAC

Asignación automática de configuraciones

Ver Herencia.

Asignación indirecta de configuraciones

Ver Herencia.

Asignación manual de configuraciones

Asignación de una configuración a un grupo de forma directa, en contraposición al establecimiento de configuraciones automático o indirecto, que utiliza el recurso de la herencia para fijar configuraciones sin intervención del administrador.

Audit

Modo de configuración de **Panda Adaptive Defense 360** para visualizar la actividad de los procesos ejecutados en los equipos protegidos de la red sin desencadenar ninguna acción de protección (desinfección o bloqueo).

Backup

Área de almacenamiento de ficheros maliciosos no desinfectables, así como de spyware y herramientas de hacking detectadas. Todos los programas eliminados del sistema por ser clasificados como amenazas se copian de forma temporal en el área de backup / cuarentena durante un periodo de entre 7 y 30 días según el tipo.

Bloquear

Acción de la protección avanzada que impide la ejecución de los programas clasificados como amenaza o de aquellos programas que son desconocidos para **Panda Adaptive Defense 360**.

Bloqueado (elemento)

Dependiendo de la configuración de la protección avanzada, **Panda Adaptive Defense 360** impedirá tanto la ejecución de los programas desconocidos, hasta que sea completado su análisis y emitida una clasificación, como de los programas clasificados como malware o PUP.

Broadcast

Transmisión de paquetes en redes de datos a todos los nodos de la subred: un paquete de datos llegará a todos los equipos dentro de la misma subred sin necesidad de enviarlo de forma individual a cada nodo. Los paquetes de broadcast no atraviesan encaminadores y utilizan un direccionamiento distinto para diferenciarlos de los paquetes unicast.

Cache / Repositorio (rol)

Equipos que descargan y almacenan de forma automática todos los ficheros necesarios para que otros equipos con **Panda Adaptive Defense 360** instalado puedan actualizar el archivo de identificadores, el agente y el motor de protección sin necesidad de acceder a Internet. De esta manera se produce un ahorro de ancho de banda, ya que cada equipo no descargará de forma independiente las actualizaciones, sino que se hará una única vez de forma centralizada.

Cambio de comportamiento

Al clasificar como malware o goodware un programa que el administrador permitió su ejecución cuando todavía era desconocido, **Panda Adaptive Defense 360** se puede comportar de dos maneras:

- Eliminarlo de la lista de Programas permitidos: si se ha clasificado como goodware seguirá pudiéndose ejecutar, si se ha clasificado como malware, se impedirá su ejecución.
- Mantener en la lista de Programas permitidos: se seguirá permitiendo su ejecución independientemente de que se trate de malware o goodware.

Ciclo de protección adaptativa

Nuevo enfoque de seguridad basado en la integración de un conjunto de servicios de protección, detección, monitorización, análisis forense y resolución, todos ellos centralizados en una única consola de administración accesible desde cualquier lugar y en cualquier momento.

Ciclo de vida del malware

Detalle de todas las acciones desencadenadas por un programa malicioso, desde que fue visto por primera vez en un equipo del cliente hasta su clasificación como malware y posterior desinfección.

Configuración

Ver Perfil de configuración.

Control de dispositivos

Módulo que permite definir el comportamiento del equipo protegido al conectar dispositivos extraíbles o de almacenamiento masivo, para minimizar la superficie de exposición del equipo.

Control de acceso a páginas web

Tecnología que permite controlar y filtrar las URLs solicitadas por los navegadores de la red con el propósito de denegar o permitir su acceso, tomando como referencia una base de datos de URLs dividida en categorías o temas.

Consola Web

Herramienta de gestión del servicio de seguridad avanzada **Panda Adaptive Defense 360**, accesible desde cualquier lugar y en cualquier momento mediante un navegador web compatible. Con la consola web el administrador podrá desplegar el software de protección, establecer las configuraciones de seguridad y visualizar el estado de la protección. También permite utilizar las herramientas de análisis forense, para determinar el alcance de los problemas de seguridad.

Cuarentena

Ver Backup.

Cuenta de usuario

Ver Usuario.

CVE (Common Vulnerabilities and Exposures)

Lista de información definida y mantenida por The MITRE Corporation sobre vulnerabilidades conocidas de seguridad. Cada referencia tiene un número de identificación único, ofreciendo una nomenclatura común para el conocimiento público de este tipo de problemas y así facilitar la compartición de datos sobre dichas vulnerabilidades.

Desbloqueado (programa)

Son programas inicialmente bloqueados por no haber obtenido todavía una clasificación, pero que el administrador de la red permite su ejecución de forma selectiva y temporal para minimizar las molestias a los usuarios de la red.

Desbordamiento de buffer

Fallo en la gestión de los buffers de entrada de un proceso. En estos casos, si el volumen de datos recibido es mayor que el tamaño del buffer reservado, los datos sobrantes no se descartan, sino que se escriben en zonas de memoria adyacentes al buffer. Estas zonas de memoria pueden ser interpretadas como código ejecutable en sistemas anteriores a la aparición de la tecnología DEP.

Descubridor (rol)

Equipos capaces descubrir puestos de usuario y servidores no administrados para iniciar una instalación remota del agente **Panda Adaptive Defense 360.**

DEP

Característica de los sistemas operativos que impide la ejecución de páginas de memoria destinadas a datos y marcadas como no ejecutables. Esta característica se diseñó para prevenir la explotación de fallos por desbordamiento de buffer.

Desinfectable

Fichero infectado por malware del cual se conoce el algoritmo necesario para poder revertirlo a su estado original.

DHCP

Servicio que asigna direcciones IP a los nuevos equipos conectados a la red.

Dialer

Programa que marca un número de tarificación adicional (NTA), utilizando para ello el módem. Los NTA son números cuyo coste es superior al de una llamada nacional.

Dirección IP

Número que identifica de manera lógica y jerárquica la interfaz de red de un dispositivo (habitualmente un ordenador) dentro de una red que utilice el protocolo IP.

Dirección MAC

Identificador hexadecimal de 48 bits que corresponde de forma única a una tarjeta o interfaz de red.

Directorio Activo

Implementación propietaria de servicios LDAP (Lightweight Directory Access Protocol, Protocolo Ligero/Simplificado de Acceso a Directorios) para máquinas Microsoft Windows. Permite el acceso a un servicio de directorio para buscar información diversa en entornos de red.

Distribución Linux

Conjunto de paquetes de software y bibliotecas que conforman un sistema operativo basado en el núcleo Linux.

DNS (Domain Name System)

Servicio que traduce nombres de dominio con información de diversos tipos, generalmente direcciones IP.

Dominio

Arquitectura de redes Windows donde la gestión de los recursos compartidos, permisos y usuarios está centralizada en un servidor llamado Controlador Principal de Dominio (PDC) o Directorio Activo (AD).

Entidad

Predicado o complemento incluido en las tablas de acciones del módulo análisis forense.

Entidad (Panda Data Control)

Conjunto de datos que tomados como una unidad adquieren un significado propio.

EoL (End Of Life)

Término utilizado para indicar el final del ciclo de vida de un producto. A partir de la fecha indicada el producto ya no recibirá actualizaciones ni parches que corrijan sus defectos, convirtiéndose en un objetivo claro para los hackers.

Equipos sin licencia

Equipos cuya licencia ha caducado o no ha sido posible asignar una licencia valida por haberse superado el número máximo permitido de instalaciones de la protección. Estos equipos no están protegidos, pero son visibles en la consola web de administración.

Excluido (programa)

Son programas inicialmente bloqueados por haber sido clasificados como malware o PUP, pero que el administrador de la red permite su ejecución de forma selectiva y temporal excluyéndolos del análisis.

Exploit

De forma general un exploit es una secuencia de datos especialmente diseñada para provocar un fallo controlado en la ejecución de un programa vulnerable. Después de provocar el fallo, el proceso comprometido interpretará por error parte de la secuencia de datos como código ejecutable, desencadenando acciones peligrosas para la seguridad del equipo.

Firewall

También conocido como cortafuegos. Tecnología que bloquea el tráfico de red que coincide con patrones definidos por el administrador mediante reglas. De esta manera se limita o impide la comunicación de ciertas aplicaciones que se ejecutan en los equipos, restringiéndose la superficie de exposición del equipo.

Filtro

Contenedor de equipos de tipo dinámico que agrupa de forma automática aquellos elementos que cumplen con todas las condiciones definidas por el administrador. Los filtros simplifican la asignación de configuraciones de seguridad y facilitan la administración de los equipos del parque informático.

Fragmentación

En redes de transmisión de datos, cuando la MTU del protocolo subyacente es menor que el tamaño del paquete a transmitir, los encaminadores dividen el paquete en piezas más pequeñas (fragmentos) que se encaminan de forma independiente y se ensamblan en el destino en el orden apropiado.

Funcionalidad Peer To Peer (P2P)

Modo de transferencia de información utilizando el ancho de banda de la red de forma más eficiente entre nodos que adoptan el rol de cliente y servidor de forma simultánea, estableciendo comunicaciones bidireccionales directas.

En **Panda Adaptive Defense 360** los equipos con el archivo de identificadores ya actualizado aplican funcionalidades Peer To Peer para reducir el consumo de ancho de la conexión a Internet, compartiéndolo a nivel local con otros equipos que también necesitan actualizarlo.

Funcionalidad Proxy

Esta funcionalidad permite el funcionamiento de **Panda Adaptive Defense 360** en equipos sin acceso a Internet, ejecutando los accesos a través de otro agente instalado en una máquina de su misma subred.

GDPR (General Data Protection Regulation)

Normativa que regula la protección de los datos de los ciudadanos que viven en la Unión Europea.

Geolocalizar

Posicionar en un mapa un dispositivo en función de sus coordenadas.

Goodware

Fichero clasificado como legítimo y seguro tras su estudio.

Grafo de actividad / grafo de ejecución

Representación visual de las acciones ejecutadas por las amenazas, poniendo énfasis en el enfoque temporal.

Grupo

Contenedor de tipo estático que agrupa a uno o más equipos de la red. La pertenencia de un equipo a un grupo se establece de forma manual. Los grupos se utilizan para simplificar la asignación de configuraciones de seguridad y para facilitar la administración de los equipos del parque informático.

Grupo de trabajo

Arquitectura de redes Windows donde la gestión de los recursos compartidos, permisos y usuarios residen en cada uno de los equipos de forma independiente.

Hardening

Modo de configuración de **Panda Adaptive Defense 360** que bloquea los programas desconocidos descargados de Internet, así como todos los ficheros clasificados como malware.

Heap Spraying

Head Spray es una técnica utilizada para facilitar la explotación de vulnerabilidades por parte de un proceso malicioso independiente.

Debido a la constante mejora de los sistemas operativos, la explotación de vulnerabilidades se ha convertido es un proceso muy aleatorio. Debido a que el comienzo de la región de memoria heap de un proceso es predecible, y las posteriores reservas de espacio son secuenciales, Head Spray aporta predictibilidad a los ataques, sobrescribiendo porciones de la región de memoria heap del proceso objetivo. Estas porciones de memoria serán referenciadas más adelante por un proceso malicioso para ejecutar el ataque.

Esta técnica es muy empleada para explotar vulnerabilidades de navegadores y sus plugins correspondientes.

Herencia

Método de asignación automática de configuraciones sobre todos los grupos descendientes de un grupo padre, ahorrando tiempo de gestión. También llamado Asignación automática de configuraciones o Asignación indirecta de configuraciones.

Herramienta de hacking

Programa utilizado por hackers para causar perjuicios a los usuarios de un ordenador, pudiendo provocar el control del ordenador afectado, obtención de información confidencial, chequeo de puertos de comunicaciones, etc.

Hoaxes

Falsos mensajes de alarma sobre amenazas que no existen y que llegan normalmente a través del correo electrónico.

ICMP (Internet Control Message Protocol)

Protocolo de control y notificación de errores utilizado por el protocolo IP en Internet.

Identificador

Palabra clave utilizada en las búsquedas de **Panda Data Control** que permite seleccionar un tipo de entidad.

IDP (Identity Provider)

Servicio centralizado responsable de gestionar las identidades de los usuarios.

IFilter

Librería del sistema operativo que permite el acceso al contenido de ficheros ofimáticos.

Incidencia

Mensaje relativo a la protección avanzada de **Panda Adaptive Defense 360,** susceptible de requerir la intervención del administrador. Las incidencias se reciben mediante la consola de administración y el correo electrónico (alertas), y el usuario del equipo protegido mediante mensajes generados por el agente que se visualizan en el escritorio de su dispositivo.

Indexar

Proceso que analiza el contenido de los ficheros y lo almacena en una base de datos de rápido acceso para acelerar su búsqueda.

Informes avanzados

Ver Advanced Reporting Tool (ART).

IP (Internet Protocol)

Principal protocolo de comunicación en Internet para el envío y recepción de los datagramas generados en el nivel de enlace subyacente.

IP feeds

Servicio de entrega de bloques de direcciones IP utilizadas por las redes de bots descubiertas y analizadas por Panda Security.

Joke

Broma con el objetivo de hacer pensar a los usuarios que han sido afectados por un virus.

Malware

Término general utilizado para referirse a programas que contienen código malicioso (MALicious softWARE), ya sean virus, troyanos, gusanos o cualquier otra amenaza que afecta a la seguridad e integridad de los sistemas informáticos. El malware se infiltra y daña un ordenador sin el conocimiento de su dueño, con finalidades muy diversas.

Lock

Modo de configuración de **Panda Adaptive Defense 360** que bloquea los programas desconocidos y los ya clasificados como amenazas.

Machine learning

Es una rama de la inteligencia artificial cuyo objetivo es desarrollar técnicas para capaces de generalizar comportamientos a partir de una información no estructurada suministrada en forma de ejemplos.

Malware freezer

Comportamiento del backup / cuarentena cuyo objetivo es evitar la pérdida de datos por falsos positivos. Todos los ficheros clasificados como malware o sospechosos son enviados a la zona de backup / cuarentena, evitando su borrado completo en previsión de un fallo en la clasificación que derive en pérdida de datos.

MD5 (Message-Digest Algorithm 5)

Algoritmo de reducción criptográfico que obtiene una firma (hash o digest) de 128 bits que representa de forma única una serie o cadena de entrada. El hash MD5 calculado sobre un fichero sirve para su identificación unívoca o para comprobar que no fue manipulado / cambiado.

Microsoft Filter Pack

Paquete de librerias IFilter que abarca todos los formatos de fichero generados por la suite de ofimática Microsoft Office.

MTU (Maximun transmission unit)

Tamaño máximo del paquete que el protocolo subyacente puede transportar.

Normalización

En **Panda Data Control**, es una tarea que forma parte del proceso de indexación de textos, y que consiste en eliminar todos los caracteres innecesarios (generalmente caracteres separadores o delimitadores) antes de almacenarlos en la base de datos.

Nube (Cloud Computing)

Tecnología que permite ofrecer servicios a través de Internet. En este sentido, la nube es un término que se suele utilizar como una metáfora de Internet en ámbitos informáticos.

OU (Organizational Unit)

Forma jerárquica de clasificar y agrupar objetos almacenados en directorios.

Panda Advanced Reporting Tool

Modulo compatible con Panda Adaptive Defense 360 que almacena toda la telemetría generada por los procesos ejecutados en los equipos de usuario y servidores, y la presenta de forma gráfica para generar inteligencia de seguridad.

Panda Data Control

Modulo compatible con **Panda Adaptive Defense 360** que descubre ficheros PII en la red de la empresa y monitoriza su acceso para cumplir con las regulaciones de almacenamiento de datos vigentes, tales como la GDRP.

Panda Patch Management

Módulo compatible con **Panda Adaptive Defense 360** que parchea y actualizar los programas instalados en los equipos de usuario y servidores para eliminar las vulnerabilidades producidas por fallos de programación, minimizando asi su superficie de ataque.

Panda SIEMFeeder

Modulo compatible con **Panda Adaptive Defense 360** que envía al servidor SIEM de la empresa toda la telemetría generada por los procesos ejecutado en los equipos de usuario y servidores.

Partner

Empresa que ofrece productos y servicios de Panda Security.

Payload

En informática y telecomunicaciones es el conjunto de datos transmitidos útiles, que se obtienen de excluir cabeceras, metadatos, información de control y otros datos que son enviados para facilitar la entrega del mensaje.

En seguridad informática referida a amenazas de tipo exploit, payload es la parte del código del malware que realiza la acción maliciosa en el sistema, como borrar los ficheros o enviar datos al exterior, frente a la parte del encargado de aprovechar una vulnerabilidad (el exploit) que permite ejecutar el payload.

PDC (Primary Domain Controller)

Es un rol adoptado por servidores en redes Microsoft de tipo Dominio, que gestiona de forma centralizada la asignación y validación de las credenciales de los usuarios para el acceso a los recursos de red. En la actualidad el Directorio Activo cumple esta función.

Perfil de configuración

Un perfil es una configuración específica de la protección o de otro aspecto del equipo administrado. Este perfil es posteriormente asignado a un grupo o grupos y aplicado a todos los equipos que lo forman.

Phishing

Intento de conseguir de forma fraudulenta información confidencial de un usuario mediante el engaño. Normalmente la información que se trata de lograr tiene que ver con contraseñas, tarjetas de crédito o cuentas bancarias.

Parche

Pequeños programas publicados por los proveedores de software que modifican sus programas corrigiendo fallos y añadiendo nuevas funcionalidades.

PII (Personally Identifiable Information)

Ficheros que contienen datos que pueden ser utilizados para identificar o localizar a personas concretas.

Proceso comprometido

Son aquellos procesos vulnerables que han sido afectados por un exploit y pueden comprometer la seguridad del equipo de usuario.

Proceso vulnerable

Son programas que, debido a fallos de programación, no son capaces de interpretar correctamente los datos recibidos de otros procesos. Al recibir una secuencia de datos especialmente diseñada (exploit), los hackers pueden provocar un mal funcionamiento del proceso, induciendo la ejecución de código que compromete la seguridad del equipo del usuario.

Programas potencialmente no deseados (PUP)

Son programas que se introducen de forma invisible o poco clara en el equipo aprovechando la instalación de otro programa que es el que realmente el usuario desea instalar.

Protección (módulo)

Una de las dos partes que componen el software Panda Adaptive Defense 360 que se instala en los equipos. Contiene las tecnologías encargadas de proteger el parque informático y las herramientas de resolución para desinfectar los equipos comprometidos y determinar el alcance de los intentos de intrusión en la red del cliente.

Protección avanzada

Tecnología de monitorización continua y recogida de información de los procesos ejecutados en los equipos Windows de la red para su posterior envío de a la nube de Panda Security. Allí, se analiza mediante técnicas de Machine Learning en entornos Big Data para emitir una clasificación (goodware o malware) precisa.

Protocolo

Conjunto de normas y especificaciones utilizadas para el intercambio de datos entre ordenadores. Uno de los más habituales es el protocolo TCP- IP.

Proxy

Software que hace de intermediario de las comunicaciones establecidas entre dos equipos, un cliente situado en una red interna (por ejemplo, una intranet) y un servidor en una extranet o en internet.

Proxy (rol)

Equipo que hace la funciona de pasarela, conectando a otros puestos de usuario y servidores sin salida directa a internet con la nube de **Panda Adaptive Defense 360.**

Puerto

Identificador numérico asignado a un canal de datos abierto por un proceso en un dispositivo a través del cual tienen lugar las transferencias de información (entradas / salidas) con el exterior.

QR (Quick Response), código

Representación gráfica en forma de matriz de puntos que almacena de forma compacta información.

Reclasificación de elementos

Ver Cambio de comportamiento.

Red pública

Redes desplegadas en locales abiertos al público como cafeterías, aeropuertos, etc. Debido a su naturaleza publica se recomienda establecer límites en el nivel de visibilidad de los equipos que se conectan a este tipo de redes ellas, y en su utilización, sobre todo a la hora de compartir archivos, recursos y directorios.

Red de confianza

Redes desplegadas en locales privados, tales como oficinas y domicilios. Los equipos conectados son generalmente visibles por sus vecinos y no es necesario establecer limitaciones al compartir archivos, recursos y directorios.

Responsive / Adaptable (RWD, Responsive Web Design)

Conjunto de técnicas que permiten desarrollar páginas Web que se adaptan de forma automática al tamaño y resolución del dispositivo utilizado para visualizarlas.

RIR (Regional Internet Registry)

Organización que supervisa la asignación y el registro de direcciones IP y de sistemas autónomos (AS, Autonomous System) dentro de una región particular del mundo.

Rol

Configuración específica de permisos que se aplica a una o más cuentas de usuario y autoriza a ver o modificar determinados recursos de la consola.

Rootkits

Programa diseñado para ocultar objetos como procesos, archivos o entradas del Registro de Windows (incluyendo los suyos propios). Este tipo de software es utilizado esconder evidencias y utilidades en sistemas previamente comprometidos.

ROP

ROP es una técnica de ejecución de exploits que permite a un atacante ejecutar código arbitrario en presencia de defensas como DEP o ASLR.

Los ataques tradicionales basados en desbordamiento de pila consistían en sobrescribir regiones de memoria enviando bloques de datos a la entrada de programas que no controlaban debidamente el tamaño de los datos recibidos. Estos ataques dejaron de funcionar cuando técnicas como DEP fueron implementadas de forma masiva en los sistemas operativos: en esta nueva situación el sistema operativo impide la ejecución del "código desbordado" ya que reside en regiones de memoria marcadas como de no ejecución (datos). ROP sobrescribe la pila de llamadas (call stack) de un proceso para ejecutar zonas de código del propio proceso, conocidas como "gadgets". Así, el atacante puede "armar" un flujo de ejecución alternativo al del proceso original, formado por partes de código del proceso atacado.

Samples feed

Servicio de entrega de malware normalizado y automatizaciones mediante una API REST para empresas con laboratorio propio de estudio de malware.

SCL (Spam Confidence Level)

Valor normalizado asignado a un mensaje que refleja la probabilidad de que sea Spam, evaluando características tales como su contenido, cabeceras y otros.

Servidor Exchange

Servidor de correo desarrollado por Microsoft. El servidor Exchange almacena los correos electrónicos entrantes y/o salientes y gestiona la distribución de los mismos en las bandejas de entrada configuradas para ello.

Servidor SMTP

Servidor que utiliza el protocolo SMTP -o protocolo simple de transferencia de correo- para el intercambio de mensajes de correo electrónicos entre los equipos.

SIEM (Security Information and Event Management)

Software que ofrece almacenamiento y análisis en tiempo real de las alertas generadas por los dispositivos de red.

Software Panda Adaptive Defense 360

Programa que se instala en los equipos a proteger. Se compone de dos módulos: el agente Panda y la protección.

Sospechoso

Programa que, tras un análisis de su comportamiento realizado en el equipo del usuario por la protección de **Panda Adaptive Defense 360**, tiene una alta probabilidad de ser considerado malware.

Spam

El término correo basura hace referencia a mensajes no solicitados, habitualmente de tipo publicitario y generalmente enviados en grandes cantidades, que perjudican de alguna manera al receptor.

SSL (Secure Sockets Layer)

Protocolo criptográfico diseñado para la transmisión segura de datos por red.

Spyware

Programa que acompaña a otro y se instala automáticamente en un ordenador (generalmente sin permiso de su propietario y sin que éste sea consciente de ello) para recoger información personal y utilizarla posteriormente.

SYN

Bandera (flag) en el campo TOS (Type Of Service) de los paquetes TCP que los identifican como paquetes de inicio de conexión.

Tarea

Conjunto de acciones programadas para ejecutarse con una frecuencia y en un intervalo de tiempo configurables.

TCO (Total Cost of Ownership, Coste total de Propiedad)

Estimación financiera que mide los costes directos e indirectos de un producto o sistema.

Threat hunting

Conjunto de tecnologías y recursos humanos especializados que permiten detectar los movimientos laterales y otros indicadores tempranos de las amenazas, antes de que ejecuten acciones nocivas para la empresa.

Tiempo de exposición (dwell time)

Tiempo que una amenaza ha permanecido sin ser detectada en un equipo de la red.

TLS (Transport Layer Security)

Nueva versión del protocolo SSL 3.0.

Topología de red

Mapa físico o lógico de los nodos que conforman una red para comunicarse.

Troyanos

Programa que llega al ordenador de manera encubierta, aparentando ser inofensivo, se instala y realiza determinadas acciones que afectan a la confidencialidad del usuario.

TCP (Transmission Control Protocol)

Principal protocolo del nivel de transporte dentro de la pila de protocolos de Internet, orientado a la conexión para el envío y recepción de paquetes IP.

UDP (User Datagram Protocol)

Protocolo del nivel de transporte dentro de la pila de protocolos de Internet, no confiable y no orientado a la conexión para el envío y recepción de paquetes IP.

Usuario (consola)

Recurso formado por un conjunto de información que Panda Adaptive Defense 360 utiliza para regular el acceso de los administradores a la consola web y establecer las acciones que éstos podrán realizar sobre los equipos de la red.

Usuario (red)

Trabajadores de la empresa que utilizan equipos informáticos para desarrollar su trabajo.

Variable de entorno

Cadena compuesta por información del entorno, como la unidad, la ruta de acceso o el nombre de archivo, asociada a un nombre simbólico que pueda utilizar Windows. La opción Sistema del Panel de control o el comando set del símbolo del sistema permiten definir variables de entorno.

Vector de infección

Puerta de entrada o procedimiento utilizado por el malware para infectar el equipo del usuario. Los vectores de infección más conocidos son la navegación web, el correo electrónico y los pendrives.

Ventana de oportunidad

Tiempo que transcurre desde que el primer equipo fue infectado a nivel mundial por una muestra de malware de reciente aparición hasta su estudio e incorporación a los ficheros de firmas de los antivirus para proteger a los equipos de su infección. Durante este periodo de tiempo el malware puede infectar equipos sin que los antivirus tradicionales sean conscientes de su existencia.

Virus

Programa que se introduce en los ordenadores y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.

VPN (Virtual Private Network)

Tecnología de red que permite interconectar redes privadas (LAN) utilizando un medio público, como puede ser Internet.

Widget (Panel)

Panel que contiene un gráfico configurable y que representa un aspecto concreto de la seguridad de la red del cliente. El conjunto de widgets forma el Dasboard o panel de control de **Panda Adaptive Defense 360.**

Panda Adaptive Defense 360