Panda Data Control

Supervisa los datos sensibles en el endpoint

Seguridad, visibilidad y control de los datos personales en tiempo real. Simplifica el cumplimiento de la GDPR.

Desde la entrada en vigor del Reglamento General de Protección de Datos de la Unión Europea (GDPR), todas las empresas, se ven forzadas a proteger **la información personal identificable (PII)** que almacenan y/o procesan, especialmente la que reside, se opera y transita en los **equipos de empleados y colaboradores.**

¿POR QUÉ DEBES PROTEGER LOS DATOS PERSONALES Y SENSIBLES DE LA EMPRESA?

La entrada en vigor de la GDPR[1] en Mayo del 2018 acarrea severas multas, pudiendo llegar a los 20M€ o al 4% de la facturación anual, por incumplir sus disposiciones.

La GDPR impacta a todas las empresas, incluso a aquellas fuera de la UE, que recopilan y almacenan datos de carácter personal de ciudadanos de la UE.

Los problemas de fuga de datos causan pérdidas de reputación frente a clientes actuales y futuros o incluso a sus propios empleados.

Las empresas se enfrentan a múltiples retos para poder cumplir con dicha regulación, dos de estos grandes retos son:

- **Controlar los datos que proliferan de forma descontrolada en los puestos de trabajo.** Los datos no estructurados dispersos en servidores, dispositivos y portátiles de empleados y colaboradores (partners, consultores, etc...) representan aproximadamente el 80% de los datos relacionados con la empresa[2]. Al igual que el crecimiento de estos datos desestructurados, el riesgo para su negocio se duplica cada año.
- **Bloquear el incremento exponencial de casos de Exfiltración.** Cada día son más los casos de robo de datos personales, gestionados con un nivel de seguridad y control bajo, que se hacen públicos y muchos otros que permanecen ocultos sin que las empresas sean conscientes de su existencia. Además estas filtraciones de información son ejecutadas tanto por atacantes externos como por insiders, trabajadores negligentes o malintencionados con objetivos lucrativos o como venganza.

LA SOLUCIÓN: PANDA DATA CONTROL

Panda Data Control es un módulo de seguridad, integrado en la plataforma de Panda Adaptive Defense, diseñado para ayudarte a cumplir con las regulaciones, proteger y dar visibilidad sobre los **datos de carácter personal** y sensible de tu organización, tanto en tiempo real como durante todo su ciclo de vida cuando éstos residen en los servidores y puestos de trabajo.

Panda Data Control descubre, audita y monitoriza los **datos de carácter personal desestructurados[3]** en los equipos: desde el dato en reposo (data at rest), hasta las operaciones sobre ellos (data in use) y su tránsito (data in motion).

Dispone de un potente **motor de búsqueda personalizada** capaz de localizar ficheros con datos de una persona en concreto y cualquier concepto de información personal sensible (salud, religión, afiliaciones políticas,etc)

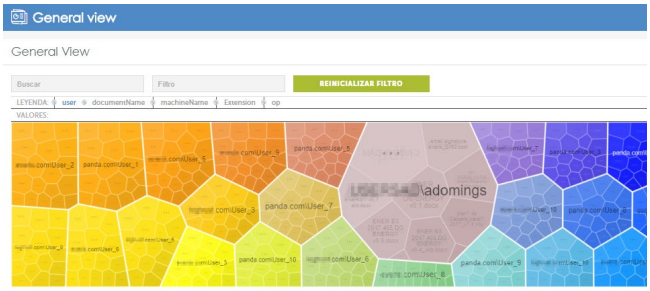


Figura 1 – Vista general de las máquinas con información de carácter personal.

PRINCIPALES BENEFICIOS

Descubre y Audita

Identifica automáticamente los ficheros con datos de carácter personal (PII[4]) de tu empresa además de los usuarios, empleados o colaboradores, y equipos o servidores que acceden a ella.

Monitoriza y Detecta

Los informes y alertas en tiempo real de filtraciones y uso sospechoso y no autorizado de archivos con datos de carácter personal, que Panda Data Control ofrece, ayudan a implementar medidas proactivas de acceso y operación sobre estos.

Realiza búsquedas personalizadas de información personal que la empresa desee gestionar.

El motor de búsqueda, permite localizar ficheros de forma precisa y dirigida por el usuario estableciendo sus propios criterios de búsqueda.

Simplifica la Gestión

El módulo de Panda Data Control, es nativo en Panda Adaptive Defense y Panda Adaptive Defense 360, no requiere ningún despliegue adicional a la protección, ni configuraciones engorrosas y todo ello gestionado desde la nube.

Demuestra a tus responsables, al DPO[5], y al resto de empleados de tu organización, que la empresa tiene un control exhaustivo de los datos de carácter personal.

[1] GDPR: General Data Protection Regulation – Regulación General de Protección de Datos.
[2] Carla Arend. IDC Opinion - Marzo 2017.
[3] Información no estructurada son los datos que no están en una base de datos o están contenidos en algún otro tipo de estructura de datos. Los datos no estructurados pueden ser textuales o no textuales. Panda Data Control se centra en datos desestructurados textuales en los dispositivos y servidores.
[4] PII: Personally Identifiable Information.
[5] DPO – Data Protection Officer: Es la figura, obligada por la regulación, responsable de la protección de datos en la empresa.

SEGURIDAD Y GOBERNANZA DE DATOS DE CARÁCTER PERSONAL

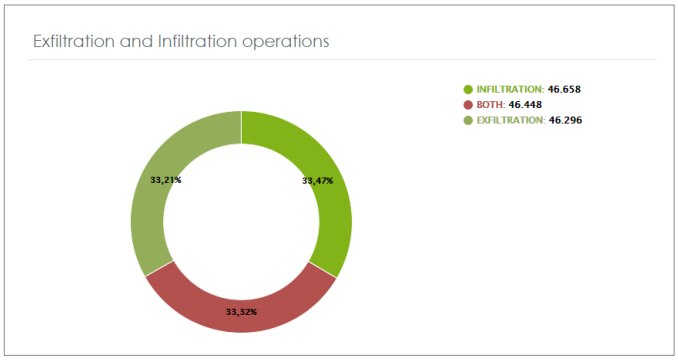
Las organizaciones protegidas con **Panda Adaptive Defense** pueden estar seguras de que sus puestos de trabajo no se verán comprometidos con programas maliciosos utilizados por atacantes externos para exfiltrar sus datos.

El servicio de clasificación del 100% de las aplicaciones que corren en los puestos y servidores protegidos, da un veredicto sobre su confiabilidad o naturaleza maliciosa mediante técnicas de **machine learning** supervisado por expertos en malware de Panda Security. Como resultado, sólo se ejecutarán las **aplicaciones clasificadas como confiables,** evitando así el robo de información.

El **módulo de Panda Data Control** se basa en la capacidad EDR (Endpoint Detection and Response) de monitorización continua de los puestos protegidos de los empleados, pero orientado a custodiar los datos desestructurados de carácter personal que almacenan.

Los informes y las alertas preconfiguradas pueden ser además personalizadas para adaptarse a las necesidades específicas de cada empresa.

Figura 2 - Operaciones en ficheros con riesgos de Exfiltración e Infiltración: Estos gráficos permiten monitorizar el control sobre las operaciones realizadas por los usuarios y averiguar el riesgo que entrañan. Como consecuencia, Panda Data Control nos ayuda a adoptar medidas para su prevención y control.



FUNCIONALIDADES

Data Discovery:

Crea un inventario indexado de todos los ficheros donde se han encontrado datos personales desestructurados, con el número de ocurrencias por cada tipo mediante una clasificación automática de los mismos (data at rest).

La clasificación combina diferentes técnicas y algoritmos de machine learning que optimizan los resultados tanto para minimizar falsos positivos, como para disminuir el consumo de recursos en los dispositivos.

Data Search:

Realiza búsquedas libres personalizadas para identificar ficheros con cualquier tipo de información personal. Ofrece un listado de todos los ficheros donde se encuentra dicha información y permite su exportación para un sencillo manejo.

Data Monitoring:

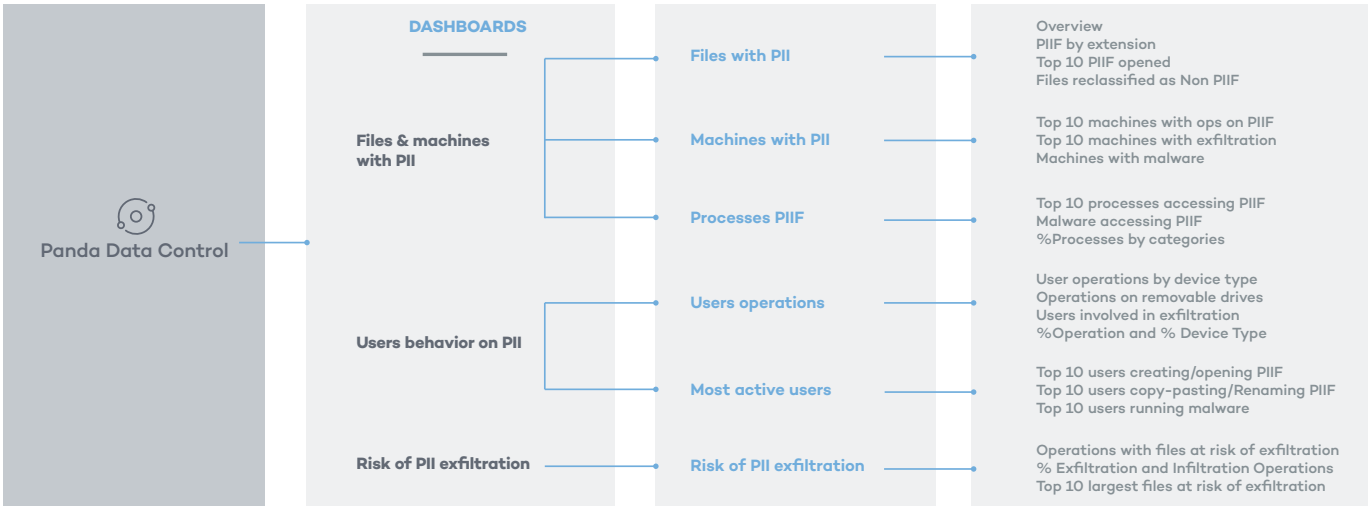
Se monitorizan las diferentes operaciones sobre los ficheros desestructurados manteniendo actualizado el inventario de ficheros con datos personales (data in use). Cuando estos ficheros van a ser copiados o movidos desde el dispositivo, se registra la operación de exfiltración sobre los clientes de correo, navegadores, FTP, etc (data in motion).

Data Visualization:

El resultado del descubrimiento y la monitorización continua se sincroniza constantemente en la Plataforma de Adaptive Defense y su módulo de Advanced Visualization Tool. En él se dispone de herramientas de explotación de los eventos sobre los datos personales en reposo, uso y tránsito, tanto en tiempo real como retrospectivo, a lo largo de su ciclo de vida en los dispositivos.

Los Paneles de control, los informes y las alertas pre-configuradas ayudan a cubrir los casos de uso para una correcta gobernanza de la seguridad de los datos personales desestructurados.

Figura 3 – Panda Data Control – Paneles de Control, secciones, gráficos y consultas predefinidas.



CÓMO PANDA DATA CONTROL AYUDA AL CUMPLIMIENTO DE LA GDPR

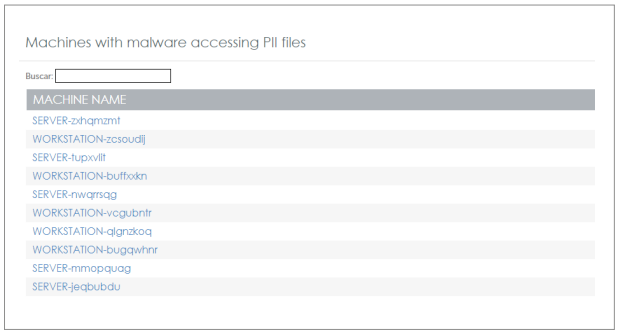
Artículo de la GDPR	Capacidad de Panda Data Control
Art. 17: Derecho de supresión («el derecho al olvido») *«El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales…»*	Panda Data Control permite configurar búsquedas personalizas encaminadas a localizar los ficheros donde aparecen los datos de una persona que desee ejercitar su Derecho de supresión.
Art. 32: Seguridad del tratamiento. *«El responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros, un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.»*	Panda Data Control ofrece herramientas para validar en tiempo real y retrospectivamente si la PII es accedida solamente por las personas adecuadas para su tratamiento y si las políticas establecidas por la compañía son las correctas. Entre otros, los siguientes informes: • Machines with PII, PII files, Machines with most operations on PII files, Malware processes accessing PII files del Panel: Files and machines with PII. • Distribution of types of operation on PII, Users involved in Personal Data operations, Users running malware del Panel: User operations on PII files.
Art. 33: Notificación de una violación de la seguridad de los datos personales a la autoridad de control *«En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente, a más tardar, 72 horas después de que haya tenido constancia de ella y deberá describir la naturaleza de la violación de la seguridad de los datos personales, las categorías y el número de registros de datos personales afectados.»*	Panda Data Control ofrece, adicionalmente a todos los gráficos detallados para el artículo 32, una serie de informes especialmente enfocados a exfiltración de PII: • Operations with files at risk of exfiltration and infiltration. • Largest files at risk of exfiltration. • Users/machines involved in exfiltration operations del Panel: Risk of PII exfiltration.
Art. 35: Evaluación de impacto relativa a la protección de datos *«Cuando sea probable que un tipo de tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas, El artículo pide realizar una evaluación del impacto relativa a la protección de datos.»*	El módulo de Panda Data Control está orientado a identificar los ficheros en los que hay información personal así como monitorizar las operaciones que se realizan sobre los mismos y los usuarios involucrados. Con esta información es posible conocer la cantidad, tipología, volumen y uso de la información personal, de tal manera que se pueda realizar una evaluación de impacto y de riesgo en el tratamiento de la información. Los informes y paneles de los apartados anteriores, también aplican a este artículo.
Art. 39: Funciones del delegado de protección de datos (DPO) *«El DPO, tiene entre otras, las siguientes funciones:* *· Supervisar el cumplimiento de lo dispuesto en el reglamento.* *· Ofrecer asesoramiento acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35.»*	Los informes y paneles expuestos en los apartados anteriores, especialmente los del artículo 35, son herramientas fundamentales para el buen desempeño de las funciones del DPO.

PANDA DATA CONTROL DASHBOARDS

Art. 32: Seguridad del tratamiento.

Files and machines with PII Panda Data Control Dashboard - Machines with malware accessing PII files:

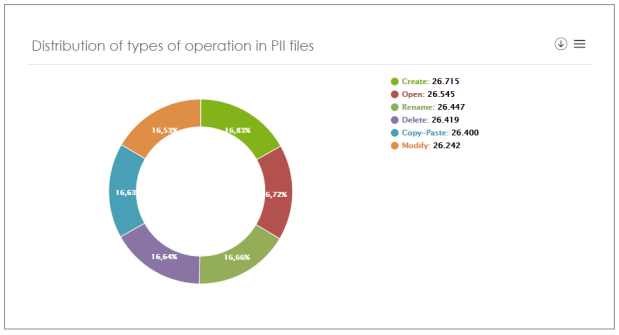
Este Dashboard, muestra el top 10 de máquinas en las que se han detectado procesos maliciosos accediendo a información personal. Esto proporciona al administrador de la seguridad la capacidad para detectar infecciones recurrentes de malware o amenazas persistentes presentes en determinados equipos, además de posibilitar el dimensionamiento de estos incidentes sobre información personal según requiere la GDPR.



Art. 33: Notificación de una violación de la seguridad de los datos personales a la autoridad de control.

User operations on PII files Panda Data Control Dashboard – Distribution of types of operation in PII Files:

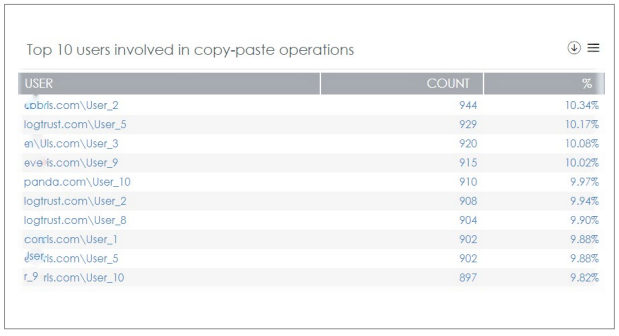
Ofrece información sobre las tipologías de operación que se realizan sobre los ficheros que contienen datos de carácter sensible o personal (PIIFs) dentro de la organización. El aumento o reducción drástica en el porcentaje de sucesos de algún tipo de operación sirve como indicador de algún evento o incidente relacionado con IP.



Art. 35: Evaluación de impacto relativa a la protección de datos

User operations on PII Files Panda Data Control Dashboard – Top 10 users involved in copy-paste operations:

En lo relativo al control de los usuarios que realizan operaciones sobre ficheros con datos de carácter personal (PIIFs), este widget ayuda a monitorizar quiénes son los usuarios que realizan con mayor frecuencia operaciones de copiado y pegado de contenido en PIIFs. Aunque pueden ser monitorizadas otras operaciones como: Acceso, Crear, Abrir, Renombrar, Borrar ficheros, etc...

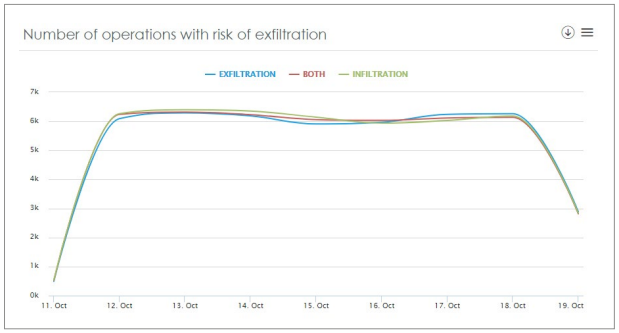


Art. 39: Funciones del Delegado de Protección de Datos (DPO).

Risk of PII Exfiltration Panda Data Control Dashboard - Number of operations with files at risk of exfiltration and infiltration:

Con el fin de monitorizar los flujos de información que contienen datos personales, conviene controlar el volumen de operaciones realizadas sobre ficheros que contengan información sensible en los Endpoints y que estén involucrados en operaciones de exfiltración.

Esta información permite identificar cuál es el volumen habitual de operaciones de exfiltración, pudiendo ser monitorizadas para detectar posibles desviaciones provocadas por incidentes.



PLATAFORMA CLOUD DE GESTIÓN

Aether Platform

La plataforma cloud Aether y su consola de gestión, común para todas las soluciones endpoint de Panda Secrutiy, optimiza la gestión de la seguridad avanzada y adaptativa, dentro y fuera de la red. Diseñada para minimizar la complejidad y maximizando la flexibilidad, granularidad y escalabilidad.

Genera más valor en menos tiempo. Facilita la implementación

- Despliegue, instalación y configuración en minutos. Valor desde el primer día.
- Agente único ligero multi-producto y multi-sistemas (Windows, MAC, Linux y Android).
- Descubrimiento automático de endpoints no protegidos. Instalación remota.
- Tecnología propia proxy y Repositorio/Caché. Comunicación optimizada incluso con los endpoints sin conexión a internet.

Simplifica la operativa. Se adapta a tu organización

- Consola web intuitiva. Gestión flexible y modular que reduce el coste total de la solución.
- Usuarios con capacidad y visibilidad total o restringida y Auditoría de acciones.
- Políticas de seguridad por grupos y endpoint. Roles predefinidos o personalizados.
- Inventario de hardware, software y changelog.

Facilita la implantación de capacidades de seguridad y gestión a lo largo del tiempo

- Los módulos se despliegan sin infraestructura nueva a o costes de despliegue.
- Comunicación en tiempo real con los endpoints desde la consola única de gestión web.
- Paneles de control e Indicadores por cada módulo.

Soluciones compatibles sobre la plataforma Aether:

Panda Adaptive Defense Panda Adaptive Defense 360

Plataformas Soportadas y Requisitos del Sistema para Panda Data Control:

http://go.pandasecurity.com/data-control/requisitos