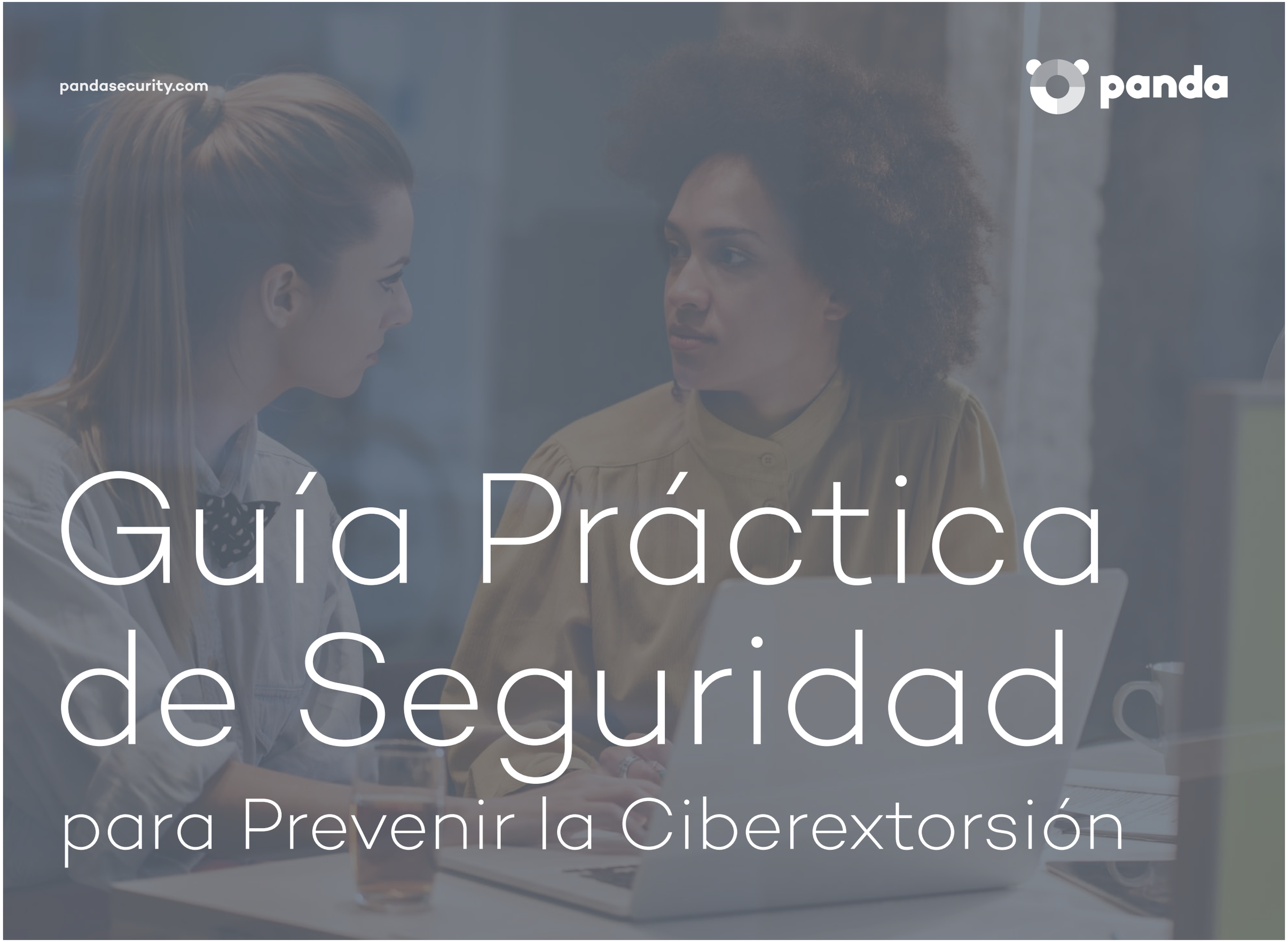
pandasecurity.com

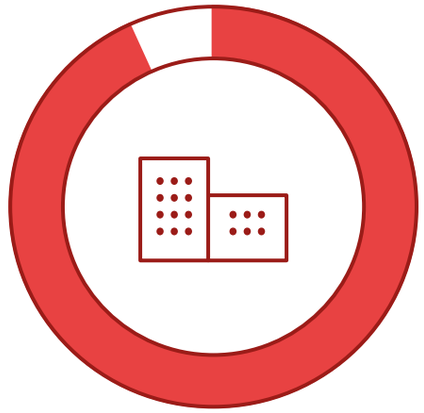


Guía Práctica de Seguridad

para Prevenir la Ciberextorsión

Las organizaciones españolas son las que sufre el mayor número de robo de datos confidenciales de toda Europa.

Y la previsión es que **España** continúe siendo **uno de los países más ciberatacados en 2016**.



El **91%** de las pymes españolas ha sido objetivo de ataques informáticos

Fuente: Shopper Software Seguridad en Pymes. Nielsen, abril 2015.

Ignorar el ataque del malware es un riesgo que no debes asumir.

Panda te descubre las claves para que tu empresa esté protegida y tú estés tranquilo.

¿Qué es la Ciberextorsión?

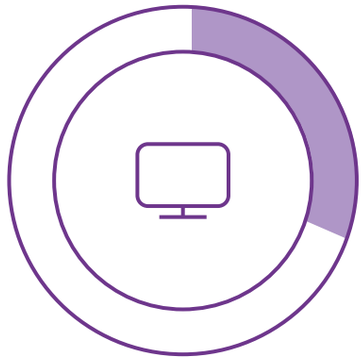
La ciberextorsión es una forma de chantaje que sufre la victima de un ataque informático, mediante el cual se le fuerza a pagar para evitar sus efectos.

Uno de los métodos de ciberextorsión más extendido es el ransomware. Este ataque, cifra los datos de sus víctimas para exigirles a continuación un rescate a cambio de descifrar y recuperar la información.

Una vez se accede al chantaje, pagando el rescate que solicita el cibercriminal, la víctima de una ciberextorsión generalmente recibe un mail con la clave para descifrar sus datos. El método de abono suele ser mediante Bitcoin, una moneda digital con valor de cambio real (1 Bitcoin = 336€). De hecho, suelen recurrir a este método de pago para dificultar su rastreo. Sin embargo, el pago no garantiza que la empresa no pueda ser atacada posteriormente.

Otro tipo de ataques que utilizan esta forma de extorsión son aquellos que, tras infectar tu equipo y acceden a tu webcam, chantajean a la víctima para no difundir los vídeos capturados.

La mayoría de los ataques se inician con emails que incluyen documentos adjuntos, o visitando sitios web comprometidos.



39%

Webs poco seguras o fraudulentas

23%

Descargas de programas de la red

19%

Malware recibido por email

Orígenes de las infecciones
Fuente: Shopper Software Seguridad en Pymes. Nielsen, abril 2015.

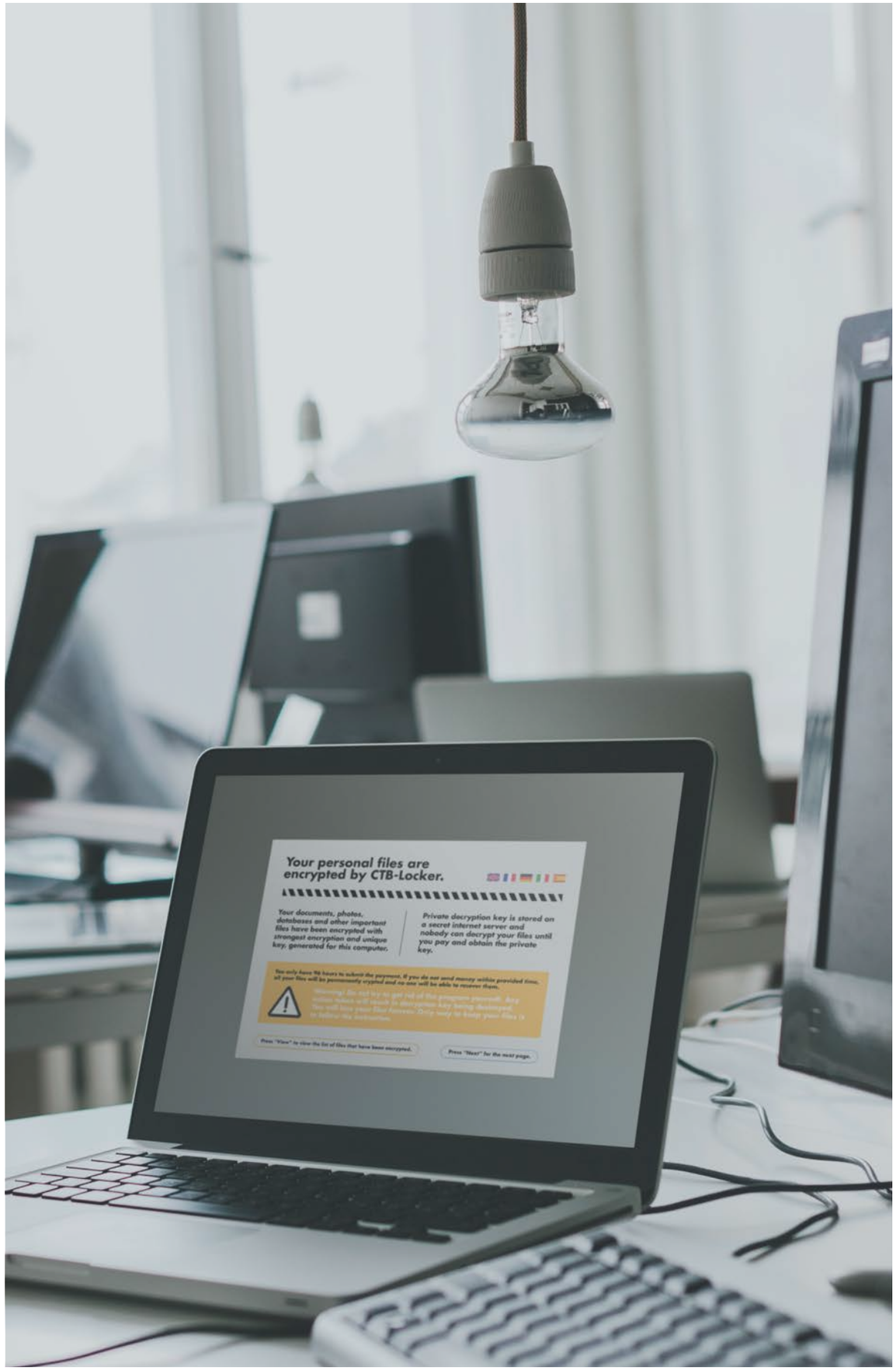
¿Cómo atacan los ciberdelincuentes con ramsonwares?

Los ramsonware como Criptolocker, Cryptowall o CoinVault amenazan la integridad de los archivos, que se encuentran en el equipo o en unidades de red a las que éste tiene acceso.

El malware cifra los datos para que únicamente puedan ser descifrados a través de una clave que los ciberdelicuentes solo proporcionan si la empresa paga el rescate solicitado.

Si te ofrecen una fecha límite posterior y el pago no ha sido realizado, es posible que borren la clave de descifrado y por tanto sería imposible poder recuperar los archivos de tu empresa.

Incluso en el caso de que se efectúe el pago, no existe seguridad de que tus datos vayan a ser liberados. Porque es posible que el software desarrollado por los ciberdelicuentes contenga bugs que provoquen un funcionamiento corrupto que interrumpan el proceso de descifrado.



¿Qué hacer si eres víctima de una ciberextorsión?

No cedas al chantaje de los cibercriminales.

Pues no hay ninguna garantía de que se resuelva el problema.

De hecho, en muchas ocasiones la víctima del chantaje que ha pagado el rescate, no recibe la clave de descifrado o recibe una corrupta. En ningún caso recuperaría el acceso a la información.

También son frecuentes los casos de chantajes sucesivos. Una vez devuelto el acceso a la información, los ciberdelincuentes instalan procesos recurrentes que vuelven a cifrar los datos de la empresa al poco tiempo.

Y en otras ocasiones, el cibercriminal negocia al alza las cantidades exigidas, según el grado de desesperación o de la situación financiera de la víctima.

Limpia todo rastro de malware en los equipos afectados.

Para limpiar completamente los vestigios del malware, Panda Security recomienda **Cloud Cleaner**, una solución especializada en retirar todo rastro de virus avanzados en los equipos ya infectados.

Recupera todos los archivos cifrados.

Para ello es necesario que previamente tuvieses activada la función “Historial de archivos” (en Windows 8.1 y 10) o “Protección del sistema” (en Windows 7 y Vista), que permitirá revertir los cambios efectuados por el malware.

La importancia de mantener actualizadas las copias de seguridad de tus archivos es vital porque, en una situación así, poder utilizarlas puede salvar tu negocio.

Y si has hecho una copia de seguridad poco antes de que notases la infección, te recomendamos que analices todos los archivos antes de que las pases a tu equipo para asegurarte de que no guarda remanentes del malware.

Hay que tener presente que éste tipo de amenazas se ha vuelto muy popular.

De hecho, la industria del malware mueve billones de euros cada año. Como ejemplo, se estima que solo una clase de ransomware, el Cryptowall 3.0, ha generado más de 325$ millones durante 2015 solo en Estados Unidos.

Además, el elevado número de mutaciones y nuevas cepas de ransomware que aparecen de forma constante, impide a los antivirus tradicionales basados en ficheros de firmas detectarlos a tiempo.

Por esta razón es fundamental contar con una solución de seguridad avanzada que detecte y proteja los equipos de ataques dirigidos, zero-day y de las nuevas versiones de ransomware.

¿Qué es y cuáles son los tipos más comunes de malware?

Lo primero es tener claro que “malware” es cualquier programa o código informático malicioso cuyo objetivo es infiltrarse en las redes y en los equipos para provocar daños, espiar o robar información. Y los especies más comunes y peligrosas son:

RANSOMWARE

Bloquea el PC, te quita el control, cifra tus archivos y te pide rescate económico para liberarlos.

APT (AMENAZA PERSISTENTE AVANZADA)

Se filtra en tu seguridad para controlarla y monitorizarla, y poder extraer datos de forma continua con fines de negocio o políticos.

EXPLOIT

Aprovecha un fallo de seguridad o una vulnerabilidad en los protocolos de comunicaciones para entrar en tus equipos.

PHISHING

Crea una url falsa para obtener tus datos y suplantar tu identidad para robar en tus cuentas bancarias.

TROYANO

Instala varias aplicaciones para que los hackers controlen tu equipo, accedan a tus archivos y roben tu información.

GUSANO

Es capaz de infectar a todos tus equipos, ralentiza tu conexión de red e incluso bloquea las comunicaciones.

SCAM

Te engaña con promociones de viajes o lotería y te piden dinero para acceder al “premio”.

BOT

Este programa puede controlar tu equipo de forma remota.

BACKDOOR

Abre una puerta trasera y toma el control del sistema.

KEYLOGGER

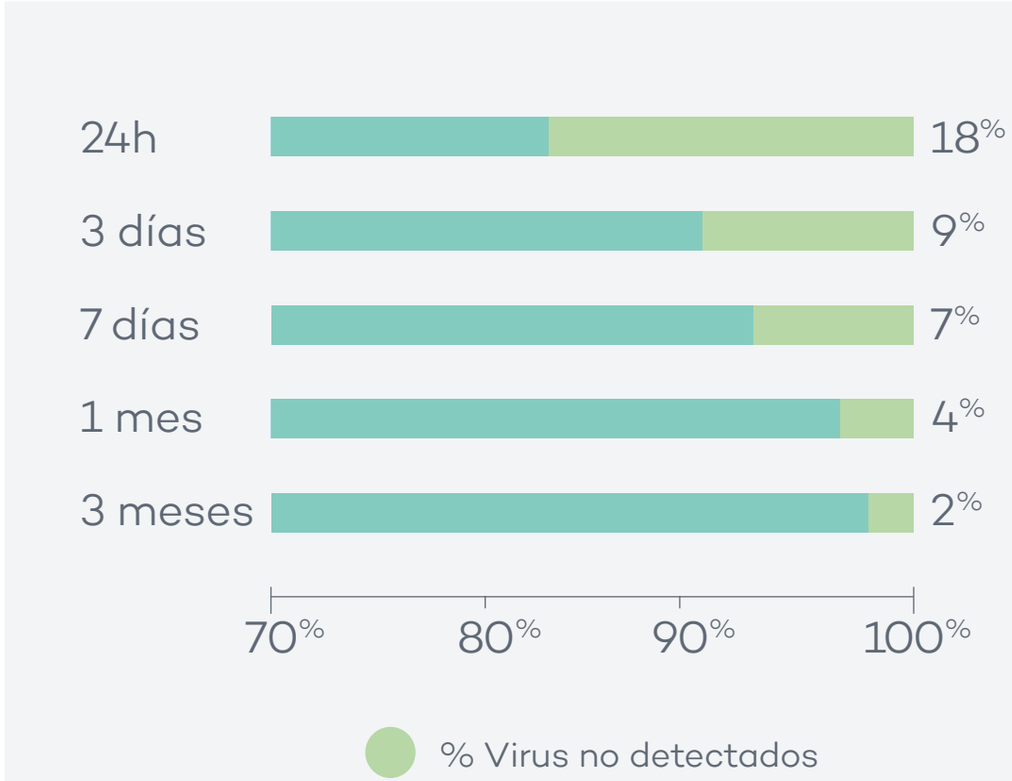
Recoge, guarda y envía cada tecleo que haga el usuario.

SPYWARE

Recoge nombres, cuentas de acceso, claves y, en general, cualquier dato de tu organización.

Evolución del malware, complejidad y sofisticación.

Las tecnologías usadas por los antivirus tradicionales (fichero de firmas, heurísticas) son reactivas. De ahí que **los antivirus tradicionales son incapaces de detectar un 18% del nuevo malware durante las 24 primeras horas**, y un 2% sigue sin ser detectado 3 meses después.



Antivirus tradicionales contra amenazas avanzadas.

Ningún antivirus tradicional puede detenerlas. De hecho, existen webs que permiten comprobar si un determinado malware puede ser detectado por la batería de antivirus. Y los hackers lanzan su código malicioso una vez han comprobado en este tipo de webs que **NO son detectados por ningún antivirus**.

Las 5 recomendaciones de Panda para prevenir los Ciberataques

1. Conciencia a tus usuarios

para que conozcan los riesgos y para que no descarguen aplicaciones desconocidas o que no hayan sido proporcionadas por la compañía, y para que eviten las webs no confiables.

2. Define políticas de navegación

reglas de navegación web que controlen la reputación de los sitios a los que se accede.

3. Una solución a tu medida

asegúrate de que tienes la solución de seguridad que necesita tu empresa y mantenla actualizada.

Una solución con varias capas de seguridad capaz de detectar y parar amenazas avanzadas.

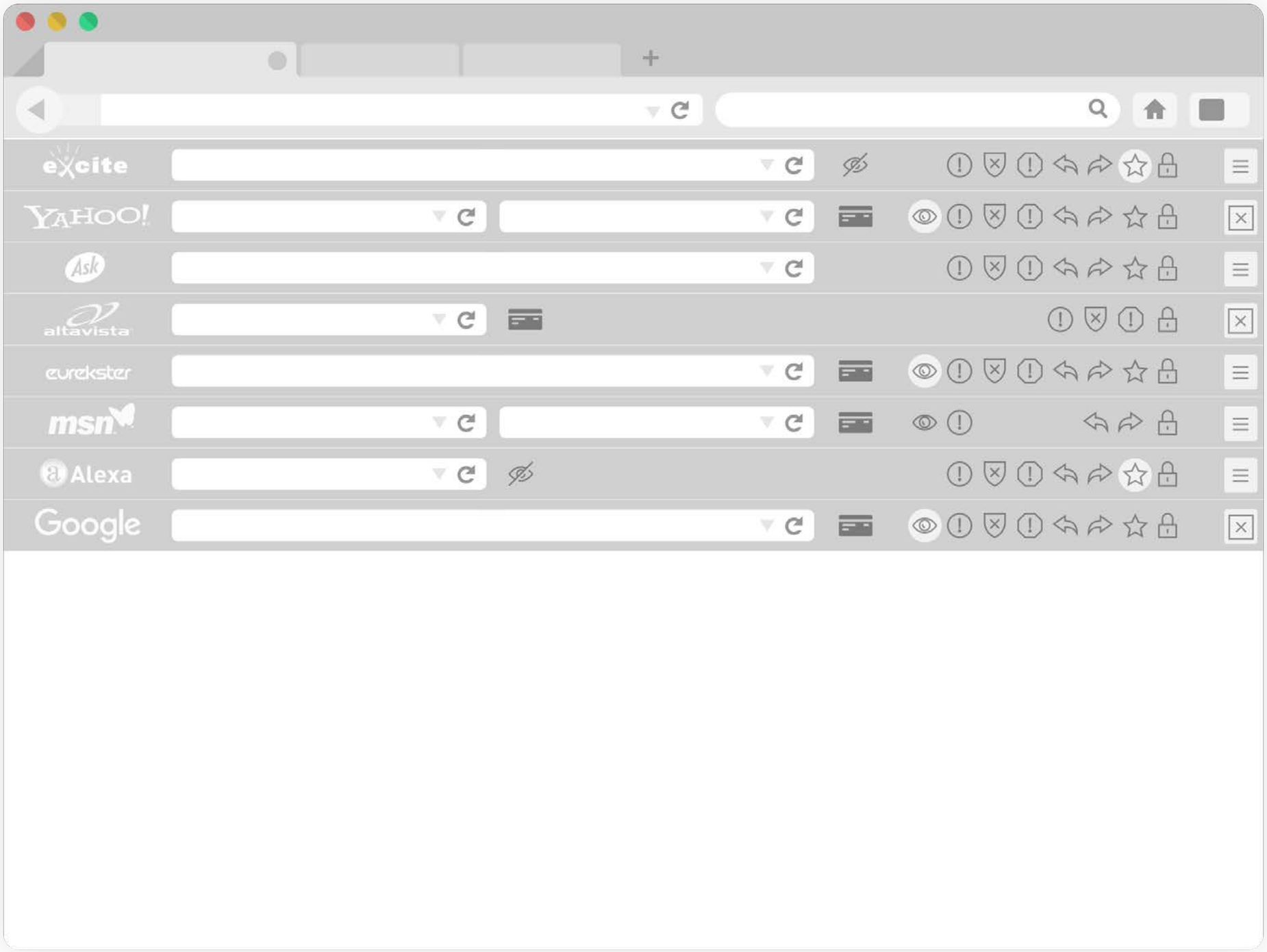
4. Establece protocolos

y medidas de seguridad para controlar la instalación y ejecución del software. Examina el inventariado de tus aplicaciones con cierta frecuencia.

5. Mantente actualizado

Determina una política de actualización de tus aplicaciones y de bloqueo/eliminación si no son necesarias para el negocio.

Es muy importante que te protejas de aplicaciones que, aun siendo confiables (como Java, Office, Chrome, Mozilla o Adobe), pueden tener vulnerabilidades o agujeros de seguridad que pueden ser aprovechadas por los ciberdelincuentes.



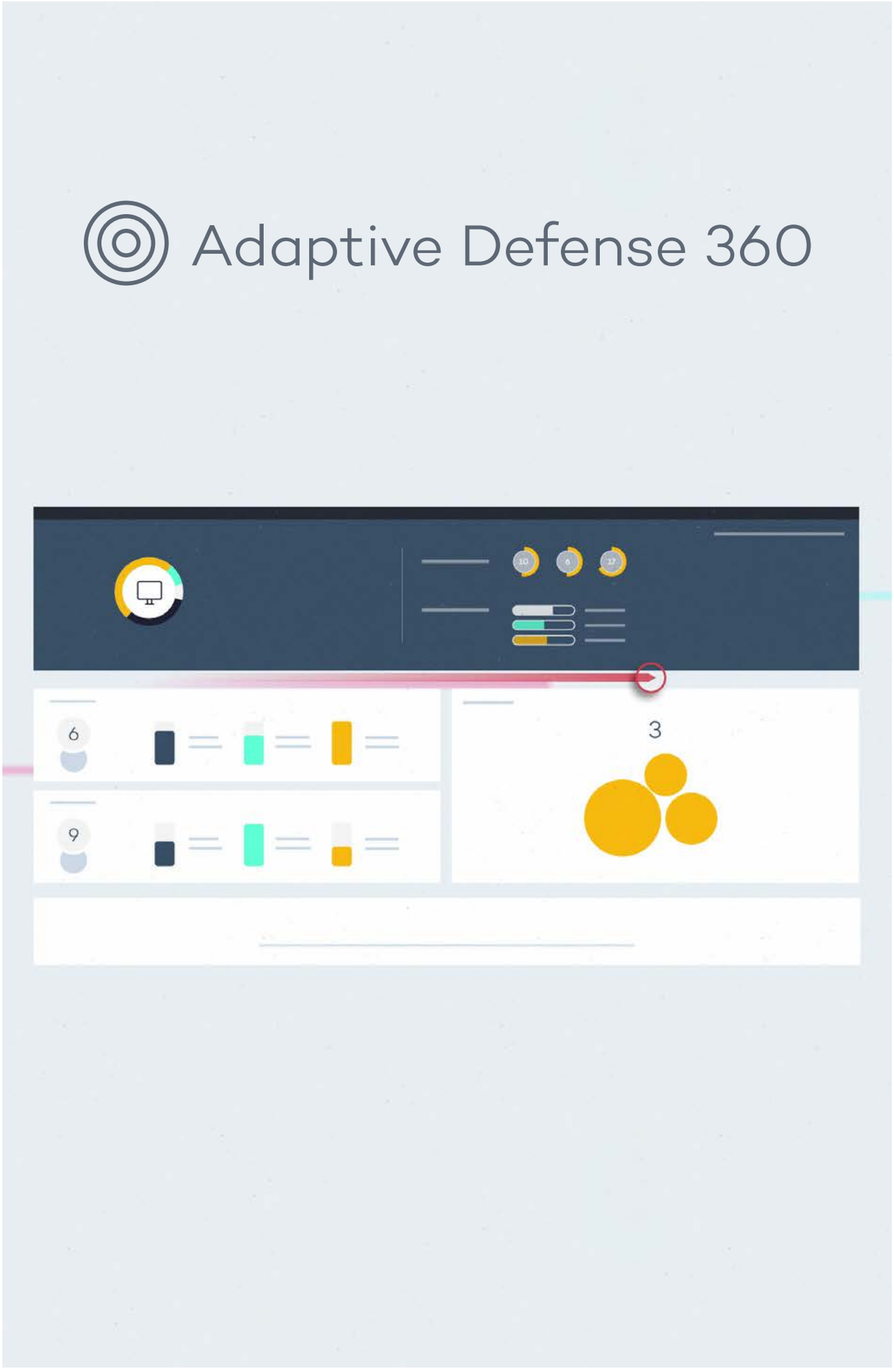
Las toolbars (barras de herramientas de navegadores) presentan grandes problemas de vulnerabilidades.

¿Cómo puedes proteger de forma efectiva tu empresa?

Panda Security ha desarrollado la primera solución que garantiza la monitorización de todos los procesos activos.

Panda Security ha desarrollado la única solución de ciberseguridad capaz de proteger a tu empresa de ataques dirigidos, virus zero-days o cualquier otra amenaza avanzada, incluido Cryptolocker.

Es el primer producto del mercado que garantiza la monitorización continua del 100% de los procesos de todos los equipos y servidores de tu red corporativa.

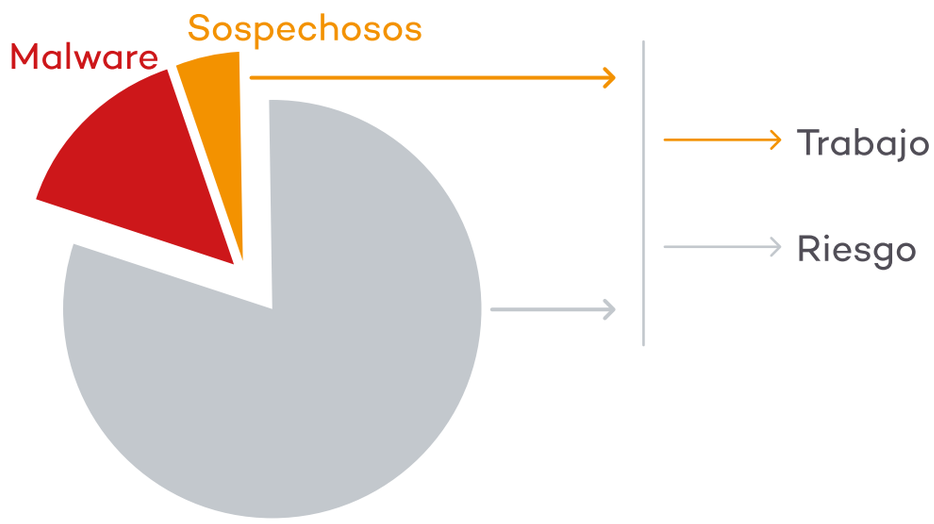


Adaptive Defense 360 ofrece la capa más elevada de seguridad, por encima de cualquier antivirus del mercado.

Adaptive Defense 360 monitoriza, registra y clasifica el 100% de las aplicaciones en ejecución que, combinado con las funcionalidades EDR, nos permite detectar y bloquear el malware que otros sistemas de protección ni siquiera ven.

Antivirus tradicionales

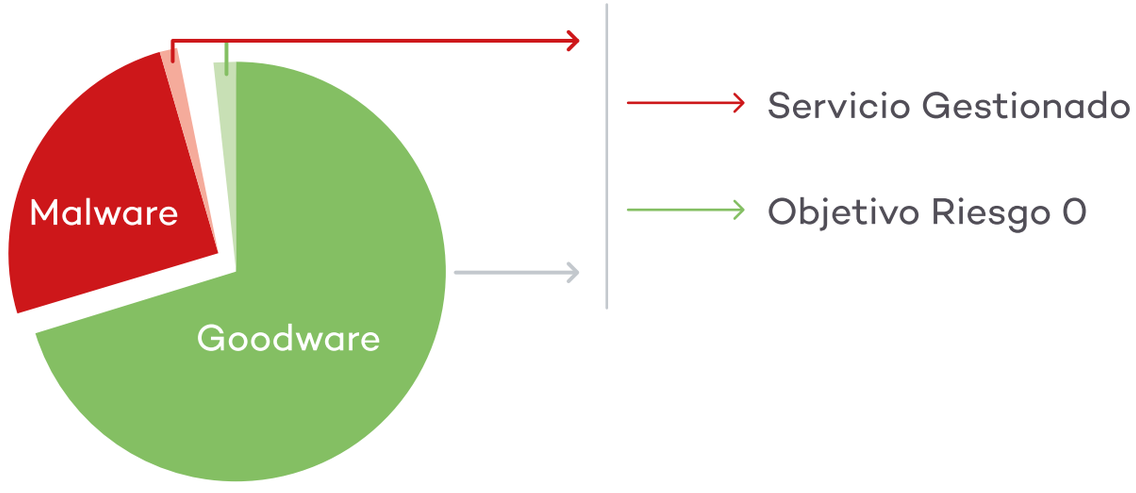
Conocen el malware pero desconocen todo lo demás.



Al no poder clasificar los sospechosos, estos ataques representan un grave problema de seguridad para los antivirus tradicionales (sobre todo los ataques dirigidos y zero-day).

Adaptive Defense 360

Monitoriza absolutamente todos los procesos en ejecución.



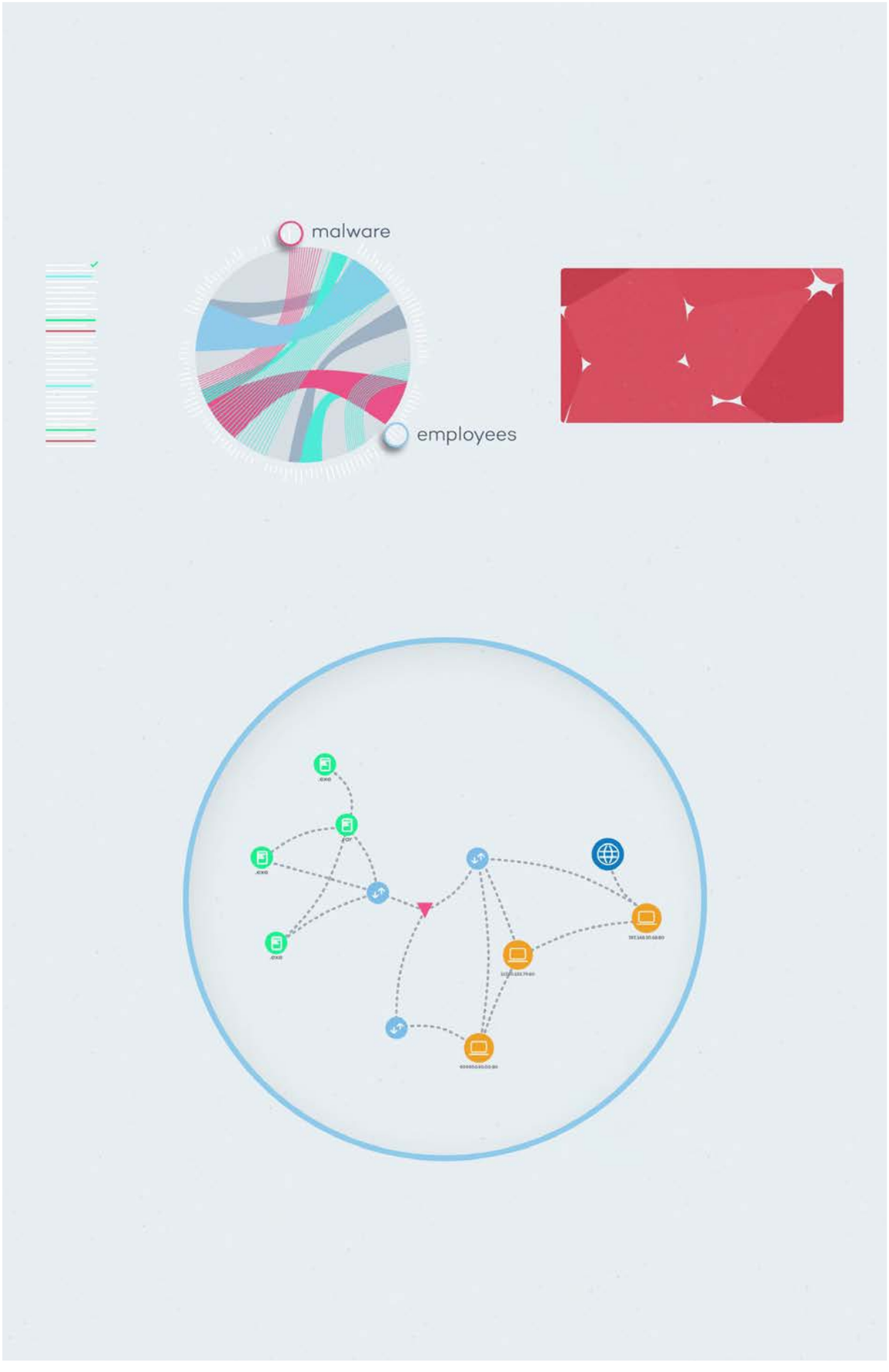
Adaptive Defense 360 sabe con certeza si un proceso es bueno o malo, clasifica absolutamente todo para que no haya sospechas.

Poder controlar absolutamente todo lo que ocurre en tus equipos nos permite:

Detectar fuga de información, tanto si viene del malware como de tus empleados y para cualquier tipo de archivo de datos (pdf, word, excel, txt,...).

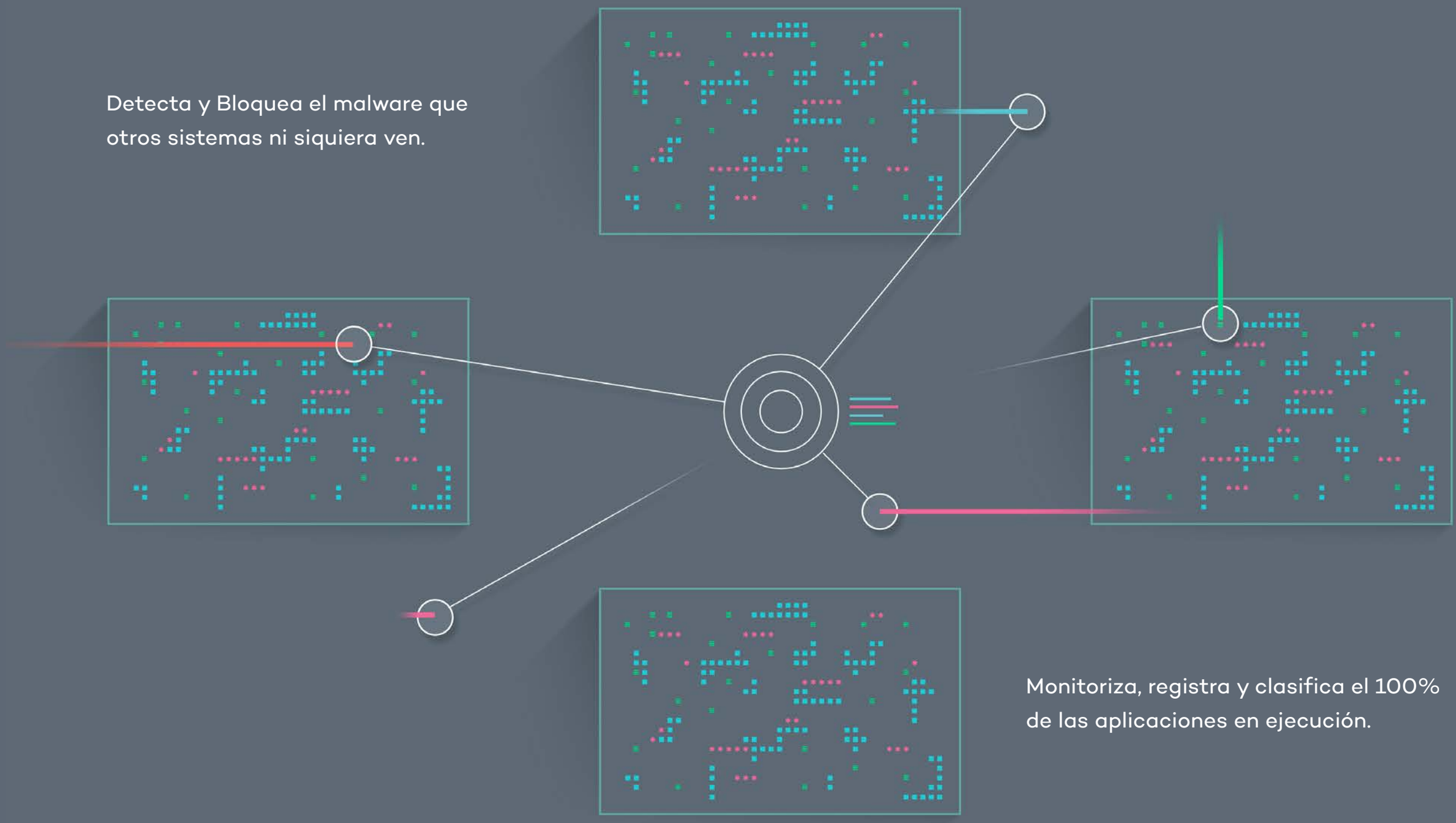
Descubrir y solucionar vulnerabilidades de tus sistemas y aplicaciones, y prevenir el uso de programas no deseados.

Y **detectar ataques dirigidos** contra tus sistemas.



Visibilidad sin Límites, Control Absoluto

Detecta y Bloquea el malware que otros sistemas ni siquiera ven.



Monitoriza, registra y clasifica el 100% de las aplicaciones en ejecución.

Adaptive Defense 360 en cifras

500K

Protege a más de 500.000 endpoints y servidores en todo el mundo.

1,5M

Ha categorizado ya más de 1,5 mil millones de aplicaciones.

1,1M

Ha mitigado más de 1.100.000 brechas de seguridad sólo en el último año.

550K

Ha ahorrado más de 550.000 horas de recursos IT, lo que supone una reducción del coste estimado en 34,8M€.

100%

Ha detectado malware en el 100% de los escenarios donde ha sido implantado, independientemente de los mecanismos de protección existentes.

Datos relativos a 2015.

Además cuenta con el respaldo de los **25 años de experiencia de Panda**, que nos acredita como pionera en detección del malware y en implementar soluciones innovadoras en el sector de seguridad.

Además de los **más de 30 millones de endpoints que son protegidos por Panda en todo el mundo**.

Más información en el teléfono gratuito:

900 90 70 80

o en comercialpanda@pandasecurity.com

panda

pandasecurity.com