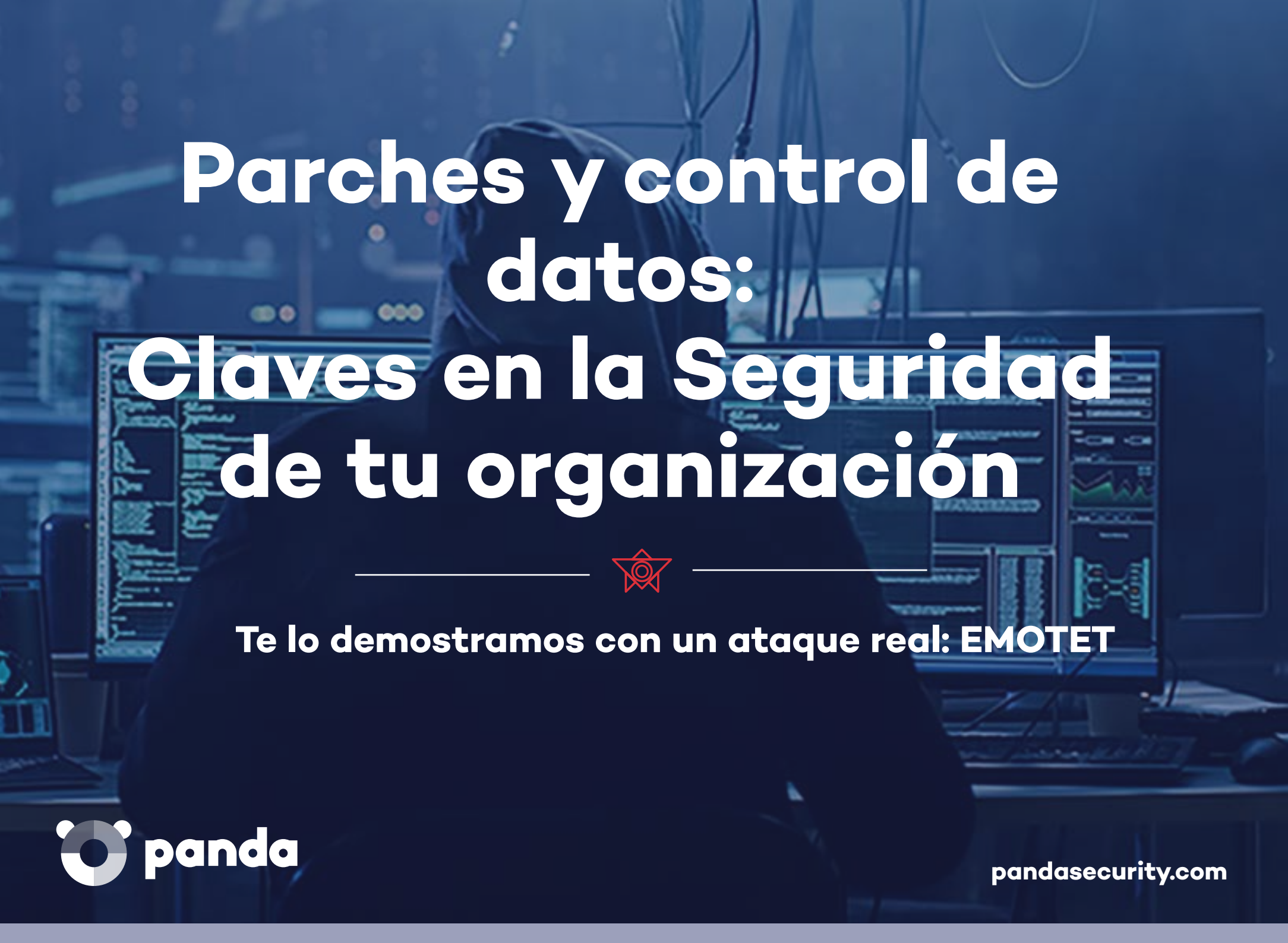


Parches y control de datos: Claves en la Seguridad de tu organización

Te lo demostramos con un ataque real: EMOTET

panda

pandasecurity.com

Introducción

Emotet es un troyano bancario, polimórfico difícil de detectar por las firmas. Su objetivo es robar datos, como las credenciales de usuario almacenadas en el navegador o espiando el tráfico de la red.

Debido a su efectividad en persistencia y propagación de red, Emotet se usa a menudo como un descargador de otro malware, y es un mecanismo de entrega especialmente popular para troyanos bancarios, como Qakbot y TrickBot.
Los sistemas comprometidos se contactan regularmente con los servidores de Comando y Control de Emotet (C&C) para recuperar actualizaciones, enviar información de los equipos comprometidos y hacer ataques fileless con el malware que se descarga.

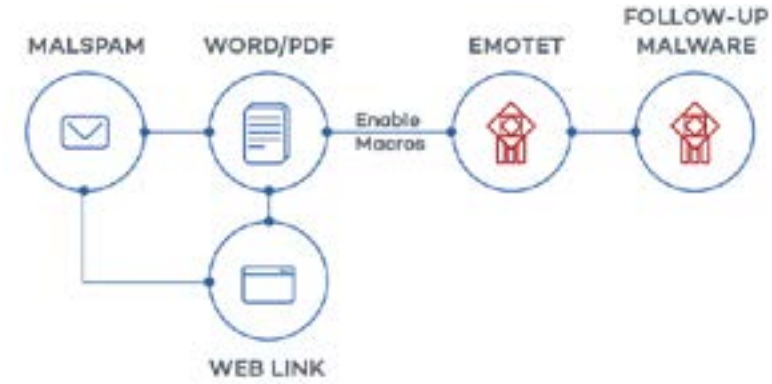
Una vez que Emotet ha infectado una máquina en red, se propagará utilizando la vulnerabilidad EternalBlue para explotar los endpoints con los sistemas no parcheados.

Emotet: ¿Cómo se propaga y gana persistencia?

Propagación

Emotet se suele difundir por correo electrónico, utilizando archivos adjuntos infectados, así como URL incrustadas.

Puede parecer que estos correos electrónicos provienen de fuentes confiables, ya que Emotet se hace cargo de las cuentas de correo electrónico de sus víctimas. **Esto ayuda a engañar a los usuarios para que descarguen el troyano en su máquina.**



Debido a la forma en que Emotet se propaga a través de la red de una empresa, cualquier máquina infectada en la red **volverá a infectar las máquinas** que se limpiaron previamente cuando se unen a la red.

Persistencia

Esta diseñado para asegurar su persistencia en el sistema y volver a estar activo incluso después de reiniciar/reiniciar/cerrar sesión, etc., para ello crea:

- Copias de sí mismo.
- Claves de registro con nombres aleatorios.
- Servicios para estar siempre activo.

Daño

Emotet es peligroso no solo por su capacidad de propagarse sin límites, al utilizar la vulnerabilidad EternalBlue, sino también porque descarga e instala malware adicional, lo que deja la puerta abierta a cualquier tipo de troyanos, software espía o el temido ransomware.

Las posibles consecuencias son:

- **Robo** de información de **identificación personal (PII)**
- **Robo** de Información **financiera** y **propietaria**, que luego puede llevar a la extorsión.
- **Robo de credenciales**, lo que significa que otras cuentas serán vulneradas
- **Tiempos de remediación prolongados** para administradores de red
- **Pérdida de productividad para los trabajadores** cuyos endpoints deben se aislados de la red.

panda

Protección en el Endpoint

Mantenerse a salvo de la campaña de Emotet no es particularmente difícil, ya que se propaga a través de **spam malicioso**. Sin embargo, los usuarios de tu organización pueden ser víctimas de las técnicas **phishing** e **ingeniería social**, que se suelen utilizar.

Lo que hace realmente peligroso a este troyano es su **capacidad de cambiar automáticamente el código** que tiene, y eso hace más difícil que un antivirus tradicional sea capaz de detectarlo.

Por suerte para las empresas protegidas por Panda Security, incluso si los empleados abren el correo electrónico y descargan el documento, están protegidas de este troyano.

Pero además, las organizaciones protegidas con **Panda Adaptive Defense** y **Panda Adaptive Defense 360**, lo estarán también para cualquier variante, troyano o malware conocido o desconocido que se aproveche de la vulnerabilidad de **Eternal Blue**.

Panda Adaptive Defense 360 es sin duda, la mejor protección preventiva contra cualquier tipo de malware conocido y sobre todo desconocido ya que impide su ejecución.

Su servicio gestionado de clasificación del 100% de las aplicaciones y procesos impide su ejecución hasta que no lo cataloga como confiable.

Más información sobre **Panda Adaptive Defense 360,** en su **hoja de producto** y sobre las soluciones de seguridad avanzadas de Panda Security en nuestra web

https://www.pandasecurity.com/business/

La respuesta al incidente y su remediación

Remediación

La limpieza de una red afectada por Emotet requiere seguir unos **pasos claves** en el menor tiempo posible:

1. Identificar las **máquinas afectadas** por Emotet.
2. Eliminar los **ejecutables** maliciosos y hacer rollback de los **cambios en el sistema.**
3. Determinar o solicitar al equipo de operaciones de IT, la lista de los **equipos vulnerables a Eternal Blue.**
4. **Aislar** los equipos vulnerables.
5. Volver a **conectar** los equipos a la red.

La ejecución de todos estos pasos **sin las herramientas adecuadas**, automatizadas e integradas en la solución de seguridad, es un procedimiento que conlleva **riesgo**, y mucho **tiempo**, a veces incluso meses. Tiempo en el que la organización está en alto riesgo de ser víctima de esto o de cualquier otro ciber ataque.

Panda Adaptive Defense 360, además de proteger contra Emotet y todas sus variantes, te ofrece otras herramientas que facilitan y aceleran las acciones de Respuesta a un potencial incidente[1]:

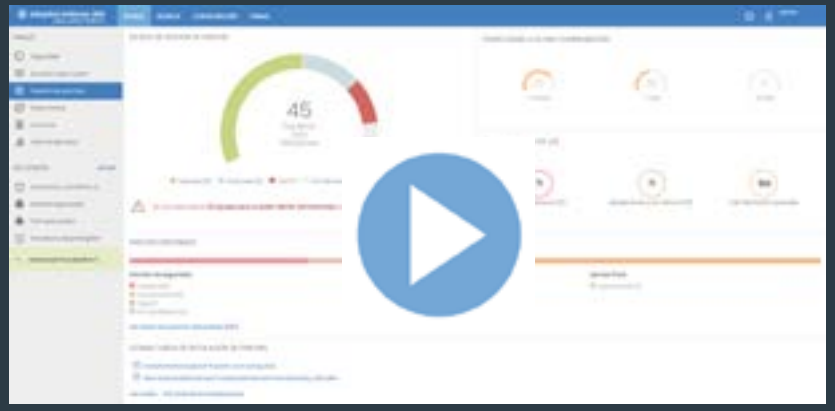
- **Remediación automatizada** que destruye todas las trazas que Emotet deja.
- Por cada detección, podrás acceder al **historial de las acciones** realizadas durante el incidente. El historial, o la **timeline**, permite identificar por donde se produjo el ataque y cuando, como y que hizo el malware o el atacante mientras estaba activo en los endpoints.

[1] Por ejemplo, en el caso de que el equipo se encuentre ya infectado con anterioridad

Evita que tu organización sea la próxima

Parchea y actualiza fácilmente desde una única consola de gestión

Pero además, **Panda Patch Management**, integrado totalmente en la **consola de gestión única de Panda Adaptive Defense 360**, identifica automáticamente todos los equipos vulnerables a Eternal Blue, o cualquier otra vulnerabilidad del **sistema y de aplicaciones de terceros** y parchear todas ellas en tiempo real y desde la consola unificada, es un simple clic.



Video de Panda Patch Management

Aconsejamos a todas las organizaciones a que no esperen a ser víctimas de este o cualquier otro ataque y que mantengan siempre sus endpoints actualizados.

Panda Patch Management, sin duda, facilita y acelera esta tarea tanto en el equipo de Operaciones IT como en el equipo de Seguridad que debe garantizar que esta medida de reducción de la superficie de ataque se lleva a cabo de forma sistemática.

*M*ás información sobre **Panda Patch Management** en su hoja de producto y en nuestra web

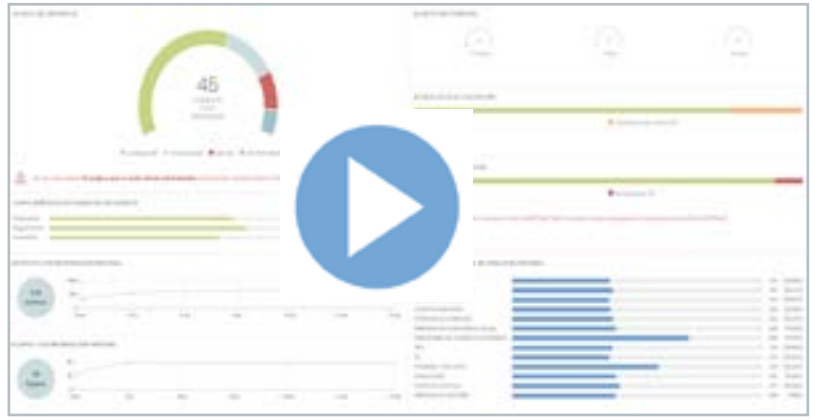
https://www.pandasecurity.com/business/solutions/#patchmanagement

Controla los datos sensibles de tu organización

Panda Data Control

Por último, la **presencia de Información de carácter personal (PII) o datos sensibles y atractivos para los atacantes**, como información financiera o propietaria, en los endpoints de los usuarios es un riesgo de seguridad latente en su organización.

Panda Data Control, ayuda a las organizaciones y al responsable de la custodia de los datos (data steward) a la identificación de esta información en los ficheros no estructurados en los endpoints de su organización.



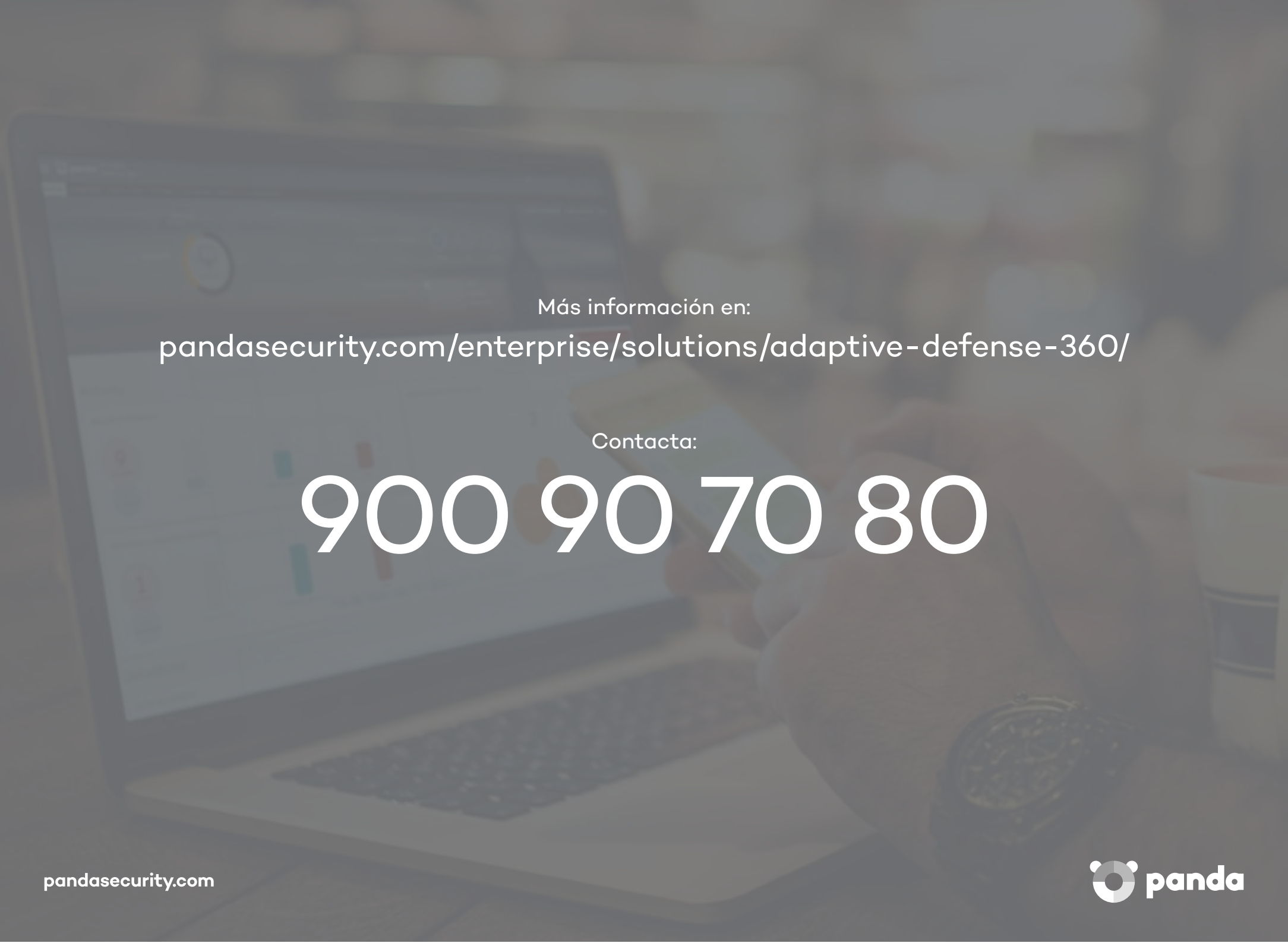
Video Inventario de ficheros con Datos Personales y Sensibles en Panda Data Control

Este Assessment es el primer paso para un programa de gestión del riesgo de violación de datos. La **clasificación automatizada** de la información personal, la **búsqueda** de información sensible en los endpoints, el **inventariado** y análisis de **evolución en el tiempo** son herramientas que facilitan la operativa para mitigar este riesgo.

Más información en:

- La hoja de producto de **Panda Data Control**
- En nuestra web ***https://www.pandasecurity.com/business/modules/#datacontrol***

panda



Más información en:

pandasecurity.com/enterprise/solutions/adaptive-defense-360/

Contacta:

900 90 70 80