Protección de Endpoints

¿HA DESAPARECIDO EMOTET PARA SIEMRPE?

Vamos a ver un caso real para mostrarle los riesgos: EMOTET

Introducción

Emotet es un troyano bancario, polimórfico y difícil de detectar con el uso de firmas. Su objetivo es robar datos, lo que incluye las credenciales de usuario almacenadas en navegadores o espiar el tráfico de Internet.

Dada su efectividad en cuanto a persistencia y propagación de red, Emotet se utiliza con frecuencia para descargar otro tipo de malware y es conocido en particular como una herramienta que esparce troyanos bancarios, como Qakbot y TrickBot.

Los sistemas comprometidos a menudo entran en contacto con servidores de comando y control (C&C) de Emotet para buscar actualizaciones, enviar información desde las computadoras comprometidas y ejecutar ataques sin archivo con el malware descargado.

Una vez que Emotet infecta la computadora de una red, se aprovecha de la vulnerabilidad de EternalBlue para esparcirse y vulnerar los endpoints con sistemas sin parches.

Emotet: ¿Cómo se esparce y persiste?

Propagación

Por lo general, Emotet **se esparce a través del correo electrónico, en adjuntos infectados o URL incrustadas.**

Puede parecer que los correos electrónicos tienen un origen confiable, ya que Emotet toma control de las cuentas de correo electrónico de sus víctimas. Esto ayuda a engañar a otros usuarios para que descarguen el troyano en su sistema.

Dada la manera en que Emotet se esparce por la red corporativa, cualquiera de las computadoras infectadas en una red reinfectará a otras que estaban limpias en el momento de unirse a la red.

Persistencia

Emotet está diseñado para garantizar su permanencia en el sistema infectado y activarse incluso aunque el sistema se reinicie o se cierre la sesión, etc. Con este fin, crea:

- Copias de sí mismo
- Claves de registro con nombres aleatorios
- Servicios para permanecer activo

Daño

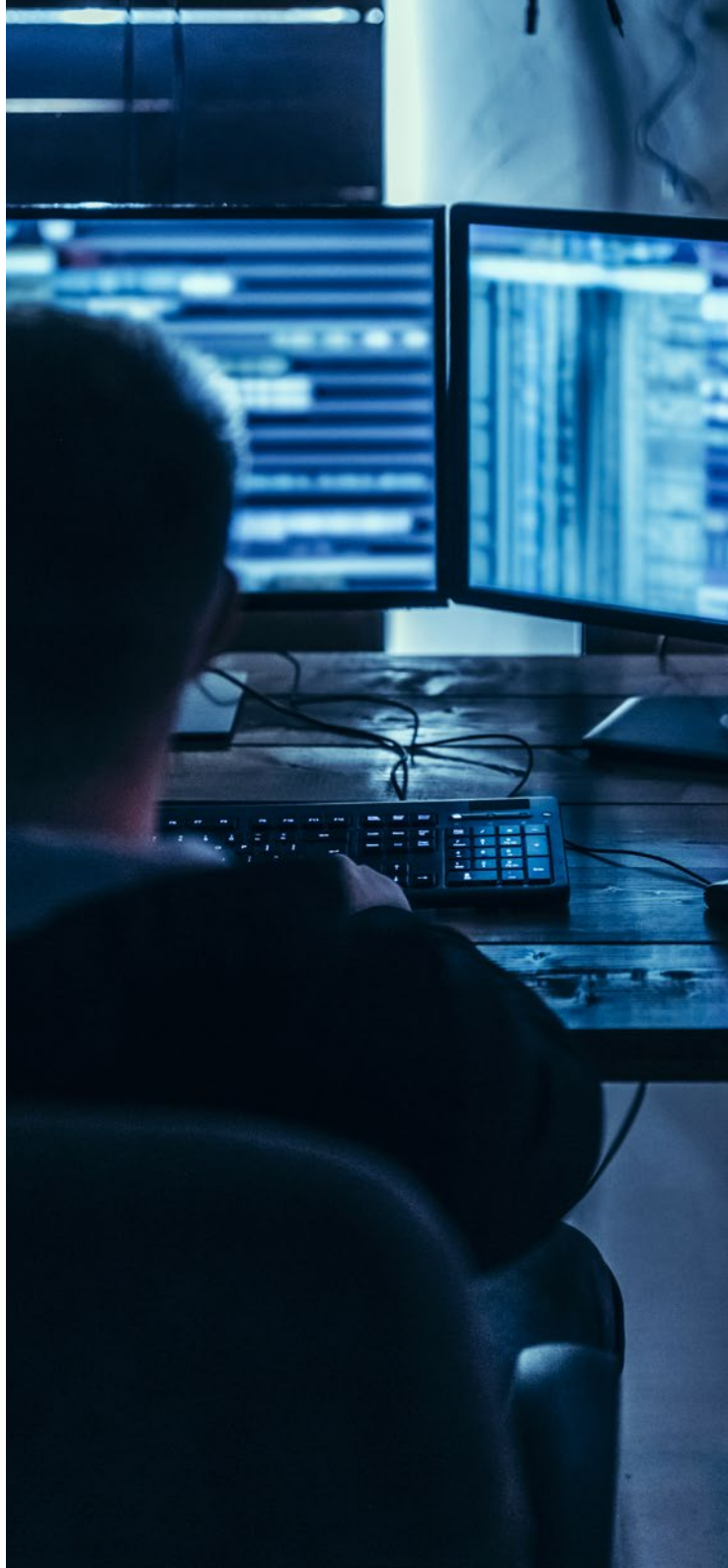
Emotet es peligroso no solo por su capacidad ilimitada de esparcirse aprovechando la vulnerabilidad de EternalBlue, sino que además descarga e instala otros malware, lo cual deja la puerta abierta a cualquier tipo de troyano, spyware o incluso ransomware.

Entre las posibles consecuencias se incluyen las siguientes:

- Robo de información personal identificable (PII)
- Filtración de información financiera y confidencial, que puede utilizarse para extorsionar
- Robo de credenciales de inicio de sesión que genera otras cuentas vulnerables
- Largos períodos de corrección para los administradores de red
- Pérdida de productividad para empleados cuyos endpoints deben ser aislados de la red

Observe la infografía del flujo de ataques de Emotet >

WatchGuard



Adaptive Defense 360 automatiza la defensa de múltiples capas contra el **flujo de ataques de Emotet**

1 ATTACKER

2 Victim receives a spam with **WORD attachment**

3 Victim opens **the email and the attachment**

4 Victim **clicks away protected view** and **macro warnings**

5 Macro downloads **EMOTET** from compromised website

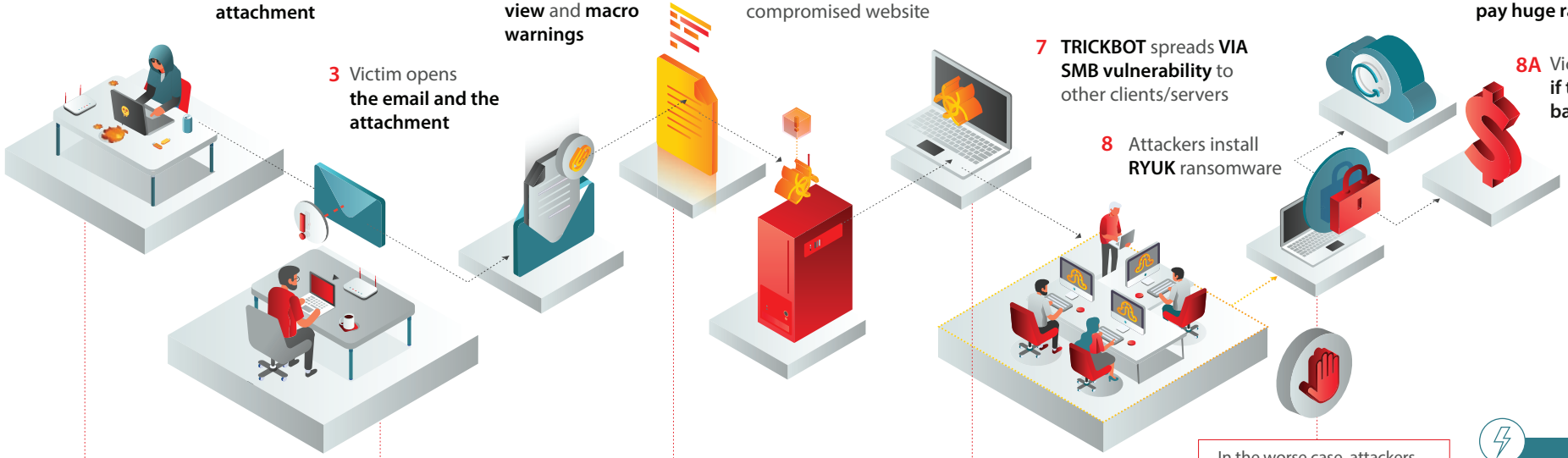
6 EMOTET drops TRICKBOT

7 TRICKBOT spreads **VIA SMB vulnerability** to other clients/servers

8 Attackers install **RYUK** ransomware

8A Victim can restore files **if they have offline backups**

8B If all backups are encrypted, **victim might pay huge ransom**



AD360 approach to defense:

Blocks malicious **email with antispam.**

Prevents access to known malicious URLs with URL filtering.

80%

AD360 approach to defense:

Blocks script execution with **macro detection and context-based detection**.

70%

AD360 approach to defense:

Blocks threats after lookup to the **Collective Intelligence** – the WatchGuard Cloud-based repository of malware and legitimate apps.

Blocks known/unknown threats with **generalist signatures & heuristics.**

60%

AD360 approach to defense:

Blocks known browser exploitation with **anti-exploit technology.**

Blocks unknown exploitation with **in-memory anti-exploit technology.**

50%

In the worse case, attackers are stopped here.

AD360 approach to defense:

The zero-trust model blocks any unknown binary coming from "outside" (email, web, network, device) until classified.

The Zero-Trust Application Service automatically classifies the payload **in a Cloud-based machine-learning system.**

0%

Ransomware begins process of encrypting files on the endpoint.

Message displayed confirms the presence on the endpoint and **provides intructions for paying the ransom.**

0% chance of success

WatchGuard

Emotet: ¿Cómo se esparce y persiste?

Protegerse contra la campaña de Emotet no es especialmente difícil ya que se esparce a través del **correo no deseado malicioso.** Sin embargo, los usuarios de su organización pueden convertirse en víctimas fáciles de las técnicas de **suplantación de identidad e ingeniería social** que se utilizan con frecuencia.

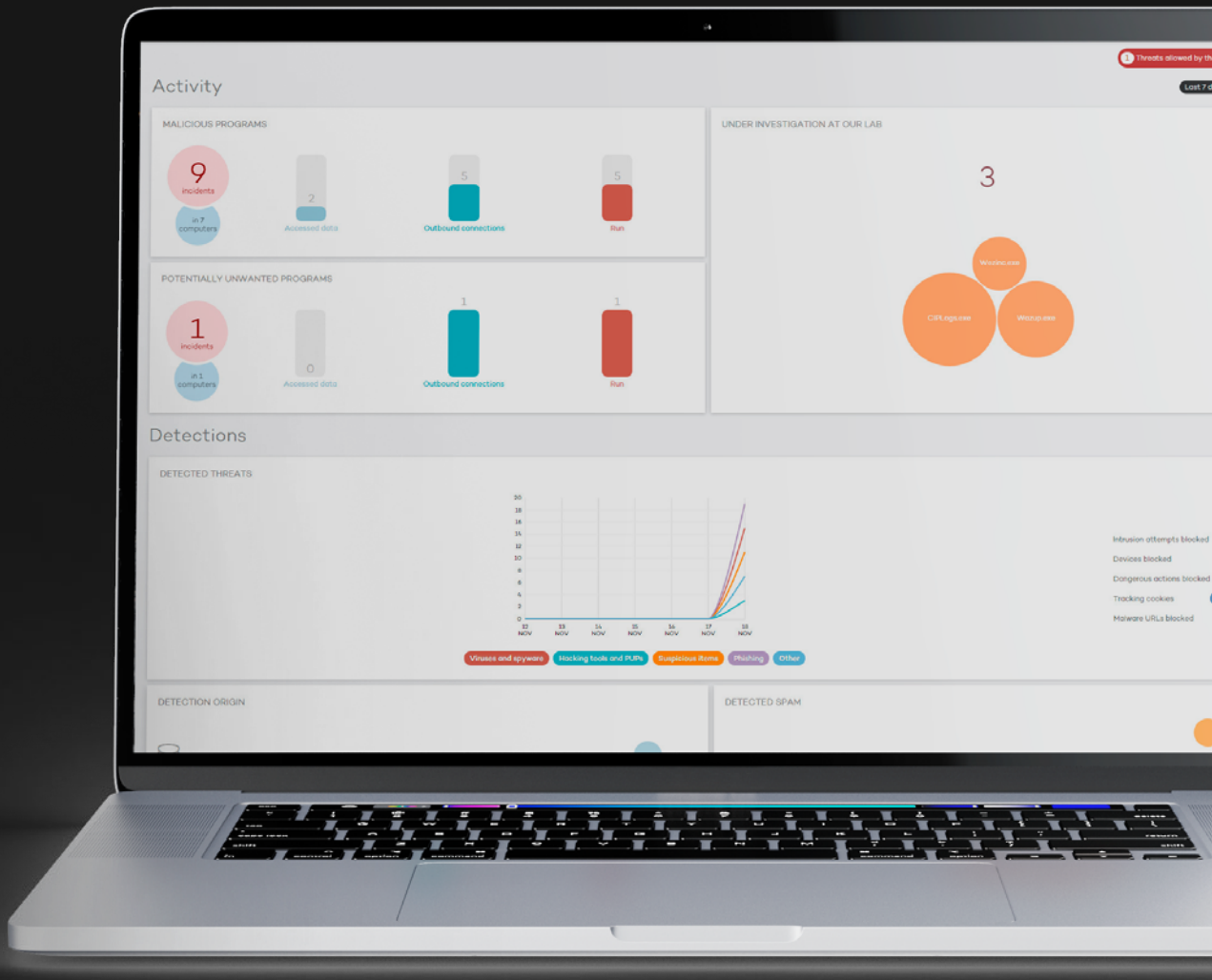
Lo que vuelve a este troyano en verdad peligroso es su capacidad de cambiar de manera automática su propio código; esto hace que sea mucho más difícil que un antivirus tradicional lo detecte.

No obstante, afortunadamente, las empresas protegidas por Panda Security tienen protección contra este troyano, aunque los empleados abran el correo electrónico y descarguen el documento.

Además, las organizaciones protegidas con **Panda Adaptive Defense y Panda Adaptive Defense 360** también tienen protección contra cualquier variante conocida o desconocida, troyano o malware que se aproveche de la **vulnerabilidad de EternalBlue.**

Su servicio de atestación administrado para clasificar el 100% de las aplicaciones y los procesos impide que se ejecuten hasta ser clasificados como confiables.

Para obtener más información sobre Panda Adaptive Defense 360 descargue la hoja de datos del producto.



WatchGuard

Respuesta a incidentes y corrección

Corrección

Limpiar una red infectada con Emotet **implica seguir algunos pasos fundamentales lo más rápido posible.**

Implementar estos pasos **sin las herramientas adecuadas,** automatizadas e integradas en la solución de seguridad, es un procedimiento arriesgado y extenso, que puede prolongarse durante meses. En este período, **una organización corre el grave riesgo de ser víctima de este o cualquier otro ataque cibernético.**

Persistencia

Además de protegerlo contra Emotet y todas sus variantes, Panda Adaptive Defense 360, le ofrece otras herramientas que facilitan y aceleran la respuesta a un potencial incidente:

- **Corrección automatizada que destruye todos los rastros de Emotet.**
- **Para cada detección, puede acceder a un cronograma de las medidas que se han tomado durante el incidente. Este cronograma le permite identificar dónde y cuándo tuvo lugar el ataque, cómo ingresó y qué hizo el malware o el atacante mientras estuvo activo en los endpoints.**

Pasos fundamentales >

1. Identificar las computadoras afectadas por Emotet.
2. Eliminar archivos ejecutables maliciosos y revertir los cambios realizados en el sistema.
3. Buscar (o solicitar al equipo de TI) la lista de computadoras vulnerables a EternalBlue.
4. Aislar las computadoras vulnerables.
5. Volver a conectar las computadoras a la red.

WatchGuard

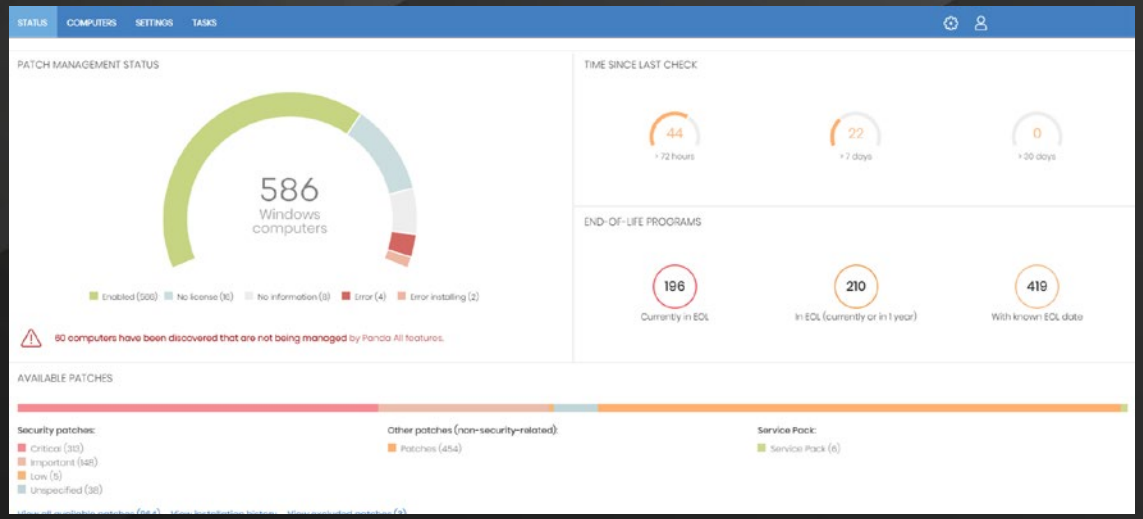
No permita que su organización sea la próxima en la lista

Parcheo y actualización simples desde una única consola de administración

Además, **Panda Patch Management**, completamente integrada con la consola de administración de Panda Adaptive Defense 360, identifica de manera automática todas las computadoras vulnerables a EternalBlue o a cualquier otra vulnerabilidad del sistema operativo o del programa y los parchea en tiempo real desde la consola solo con un clic.

No hay dudas de que Panda Patch Management facilita y acelera esta tarea tanto para el equipo de Operaciones de TI como para el equipo de seguridad, quienes deben garantizar que esta medida para reducir la superficie de ataque se implemente de manera sistemática.

Video: Panda Patch Management



Para obtener más información sobre Panda Patch Management, descargue la hoja de datos del producto.

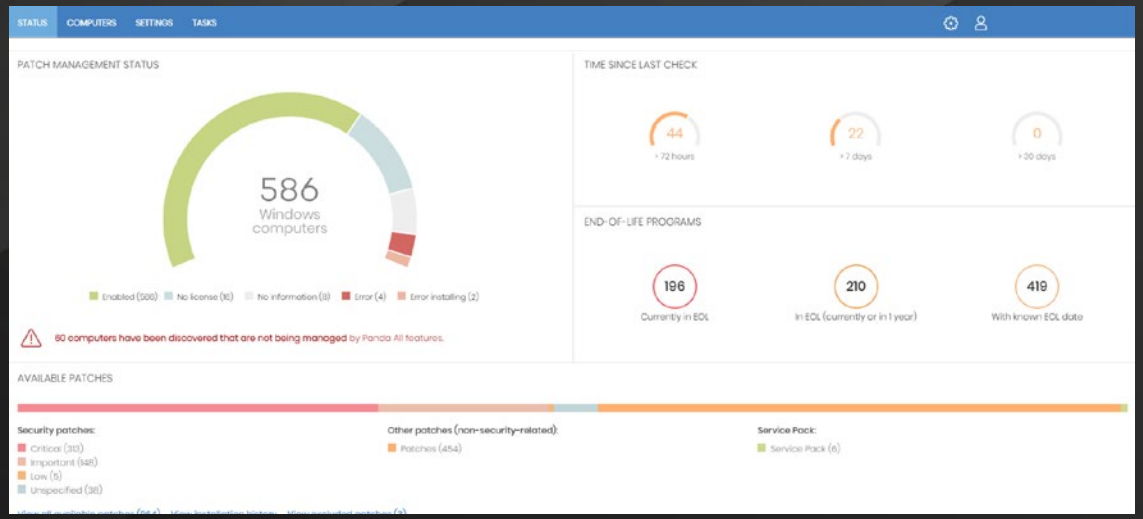
Panda Data Control

Por último, la presencia de **información personal identificable (PII) o de datos confidenciales que podría atraer a los atacantes,** como información financiera o confidencial, sobre los endpoints de usuarios representa un riesgo de seguridad latente para su organización.

Panda Data Control ayuda a las organizaciones y al administrador de datos a identificar esta información en archivos no estructurados en los endpoints en toda la organización.

Esta evaluación es el primer paso en el programa de administración de riesgos de vulneración de datos. **La clasificación automatizada** de información personal, la búsqueda de información confidencial en endpoints y **el análisis de inventario y de la evolución de datos son herramientas que ayudan a mitigar este riesgo.**

Video: Panda Data Control



Para obtener más información sobre Panda Data Control, descargue la hoja de datos del producto.

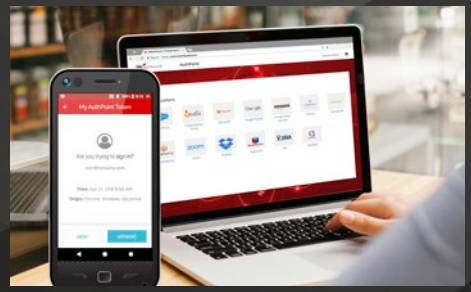
WatchGuard Unified Security Platform™

Seguridad de Red

Las soluciones de Seguridad de Red de WatchGuard están diseñadas desde el inicio para ser fáciles de implementar, usar y administrar, además de brindar la mayor seguridad posible. Nuestra propuesta única para la seguridad de redes se concentra en brindar la mejor seguridad de tipo empresarial de su clase a cualquier organización, independientemente del tamaño o la capacidad técnica.

Secure Wi-Fi

La solución Secure Wi-Fi de WatchGuard, una verdadera innovación en el mercado actual, está diseñada para proporcionar un espacio aéreo seguro y protegido para los entornos de Wi-Fi a la vez que elimina los problemas administrativos y reduce los costos en gran medida. Cuenta con herramientas de interacción amplias y visibilidad de análisis empresariales y proporciona la ventaja competitiva que su empresa necesita para triunfar.



Autenticación Multifactor

WatchGuard AuthPoint® es la solución correcta para abordar la brecha de seguridad basada en contraseñas con la autenticación multifactor en una plataforma de nube fácil de usar. El enfoque exclusivo de WatchGuard agrega el "ADN del teléfono móvil" como factor de identificación para garantizar que solo las personas correctas tengan acceso a las redes confidenciales y a las aplicaciones en la nube.

Seguridad de Endpoints

La Seguridad de Endpoints de WatchGuard es un portafolio avanzado de seguridad de endpoints, nativo de la nube, que protege las empresas contra cualquier tipo de ataque cibernético presente y futuro. Su principal solución, Panda Adaptive Defense 360, impulsada por la inteligencia artificial, mejora de inmediato la posición de seguridad de las organizaciones. Combina las capacidades de protección de endpoints (EPP) y de detección y respuesta de endpoints (EDR) con los servicios de aplicaciones de confianza cero y de búsqueda de amenazas.

Acerca de WatchGuard

WatchGuard® Technologies, Inc. es un líder mundial en seguridad de red, seguridad de endpoint, Wi-Fi seguro, autenticación multifactor y servicios de inteligencia de red. Más de 18.000 revendedores de seguridad y proveedores de servicios de todo el mundo confían en los productos y los premiados servicios de la empresa para proteger a más de 250.000 clientes. La misión de WatchGuard es lograr que empresas de todos los tipos y tamaños accedan de manera sencilla a una seguridad de calidad empresarial. Por ello, WatchGuard es una solución ideal para medianas empresas y también para empresas distribuidas. La empresa tiene su oficina central en Seattle, Washington, y posee oficinas en Norteamérica, Europa, Asia-Pacífico y Latinoamérica.

VENTAS EN NORTEAMÉRICA 1.800.734.9905 VENTAS INTERNACIONALES 1.206.613.0895 SITIO WEB www.watchguard.com