HOJA DE DATOS

WATCHGUARD PATCH MANAGEMENT

Reduzca los riesgos y la complejidad de administrar vulnerabilidades en sistemas operativos y aplicaciones de terceros

Según Ponemon Institute[1], el 57% de las víctimas de ataques informáticos afirmó que aplicar un parche hubiera evitado el ataque y el 34% reconoció que conocía la vulnerabilidad antes del ataque.

Los ataques informáticos con ransomware, como WannaCry o Peyta, fueron la tormenta perfecta que azotó a las empresas con políticas deficientes de administración de parches de SO, pero no fueron los únicos. El 86% de las vulnerabilidades se debe a aplicaciones de terceros sin parchear, como Java, Adobe, Firefox, Chrome, Flash y OpenOffice.

VULNERABILIDADES: UN RIESGO LATENTE

En la actualidad, el aprovechamiento de vulnerabilidades es aún la principal causa de la mayoría de las vulneraciones de seguridad. Los casos más famosos, como WannaCry, Petya y BlueKeep, que provocaron estragos a nivel mundial, todavía hoy siguen presentes en nuestra memoria.

Solo un pequeño número de ataques ocurren como resultado de verdaderas vulnerabilidades desconocidas (ataques de día cero), debido a que la mayoría es ocasionada por vulnerabilidades conocidas.

A causa de la transformación digital, es cada vez más difícil reducir la superficie de ataque, debido a la mayor cantidad de usuarios, dispositivos, sistemas y aplicaciones de terceros que requieren actualizaciones.

Como mínimo, tres problemas operativos comunes frustran los programas de administración de vulnerabilidades (VM):

- La detección de las vulnerabilidades es un proceso largo. Sin embargo, el tiempo de respuesta frente a incidentes debe ser inmediato.
- Las empresas están descentralizadas y los empleados no están conectados continuamente a la red corporativa. Las herramientas de VM en las instalaciones no abarcan estos escenarios.
- Otras soluciones de seguridad que ofrecen la administración de parches no correlacionan la detección con endpoints vulnerables para acelerar la respuesta y la mitigación del ataque.

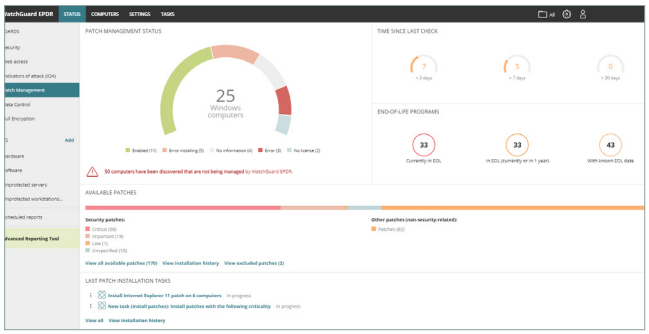


Figura 1: *Estado de la organización con Patch Management: panel de control principal*

WATCHGUARD PATCH MANAGEMENT

WatchGuard Patch Management es una solución fácil de usar que sirve para administrar las vulnerabilidades de los sistemas operativos y las aplicaciones de terceros en estaciones de trabajo y servidores de Windows, macOS y Linux. Permite reducir la superficie de ataque y, al mismo tiempo, fortalecer las capacidades de prevención y contención de su organización.

La solución no requiere nuevos agentes de endpoint ni consolas de administración y se integra completamente con todas las soluciones de endpoint de WatchGuard Security.

Además, proporciona visibilidad centralizada y en tiempo real del estado de seguridad de las vulnerabilidades de software, los parches faltantes, las actualizaciones y el software (EOL[2]) no compatibles, así como herramientas para todo el ciclo de administración de la revisión: desde la detección y la planificación hasta la instalación y la supervisión.

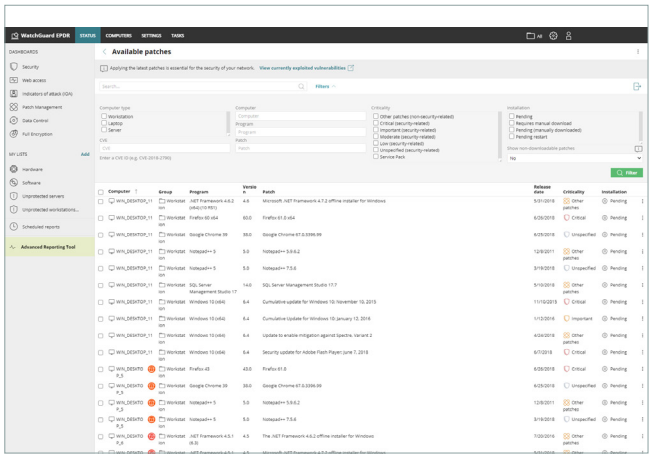


Figura 2: *Parches disponibles: administración de Parches*

[1] Costo y consecuencias de las brechas en la respuesta a las vulnerabilidades (Ponemon).

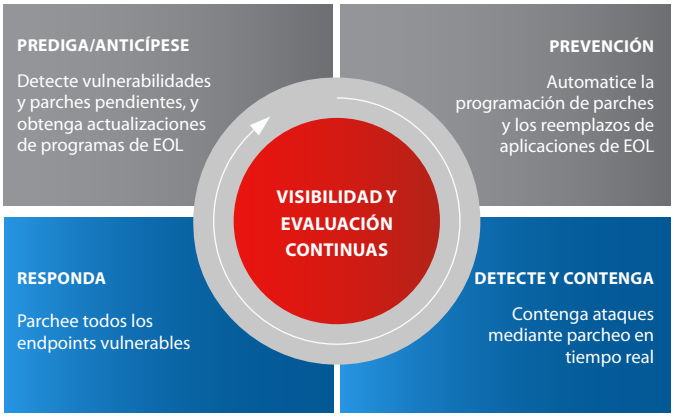
[2] EOL (fin de ciclo de vida): Un producto que está al final de su vida útil y que es posible que ya no reciba actualizaciones de seguridad

BENEFICIOS

Con una única solución fácil de usar, WatchGuard Patch Management le permite realizar lo siguiente:

- Auditar, supervisar y priorizar las actualizaciones del sistema operativo y las aplicaciones. La vista desde un solo panel ofrece visibilidad centralizada, actualizada y completa del estado de seguridad de la organización con respecto a las vulnerabilidades, los parches y las actualizaciones pendientes de los sistemas y cientos de aplicaciones.
- Reducir sistemáticamente la superficie de ataque creada por las vulnerabilidades del software con el objetivo de evitar incidentes. Esto se logra controlando los parches y las actualizaciones con herramientas de administración en tiempo real y fáciles de usar, que permiten a las organizaciones adelantarse a los ataques de aprovechamiento de vulnerabilidades.
- Contener y corregir ataques de aprovechamiento de vulnerabilidades enviando de manera inmediata actualizaciones o parches desde la consola. Las computadoras afectadas pueden aislarse del resto de la red, lo que evita que el ataque se esparza.
- Reducir el costo operativo:
  - Simplifica la administración, ya que no es necesario implementar nuevos agentes de endpoint ni actualizar agentes existentes.
  - Minimiza los esfuerzos de parcheo, ya que las actualizaciones se inician de manera remota desde la consola basada en la nube.
  - Proporciona visibilidad inmediata y completa de todas las vulnerabilidades, las actualizaciones pendientes y las aplicaciones de EOL instantáneamente después de la activación.
- Cumplir con el principio de responsabilidad, que forma parte de muchas regulaciones. Esto obliga a las organizaciones a adoptar las medidas técnicas y organizativas correspondientes para garantizar la protección adecuada de los datos confidenciales bajo su control.

WATCHGUARD PATCH MANAGEMENT
ARQUITECTURA DE SEGURIDAD ADAPTABLE



"Designing an Adaptive Security Architecture for Protection from Advanced Attacks" ("Cómo diseñar una arquitectura de seguridad adaptable para la protección contra los ataques avanzados"), Gartner

FUNCIONALIDADES CLAVE

Detección:

- Vista desde un solo panel con información en tiempo real de todas las computadoras vulnerables, los parches pendientes y el software no compatible (EOL), junto con su estado de corrección.
- Información detallada sobre parches y actualizaciones pendientes, detalles de boletines de seguridad relevantes (CVE).
- Búsqueda automática de parches disponibles en tiempo real o en intervalos periódicos (3, 6, 12 o 24 horas).
- Notificación de parches pendientes en detecciones de vulnerabilidades.
- Capacidad de aislar, parchear y anular el aislamiento de computadoras y servidores.

Planificación y tareas de instalación de parches y actualizaciones:

- Configuración según la importancia y el software que se debe parchear.
- Programación de ejecución inmediata, única o repetida en intervalos regulares (fecha/hora).
- Capacidad de controlar los reinicios de la computadora y configurar excepciones.
- Reversión para desinstalar un parche que pueda provocar un conflicto inesperado con una configuración existente.

Supervisión del estado de actualizaciones y el endpoint mediante:

- Panel de control y listas prácticas. Reportes de alto nivel y detallados.
- Listas de computadoras actualizadas y computadoras con actualizaciones pendientes con errores.

Administración granular basada en grupos y roles con diferentes permisos:

- Visibilidad basada en roles de las computadoras vulnerables, los parches y los paquetes de servicio.

Control centralizado de actualizaciones, parches y software:

- Capacidad de desactivar Windows Update y administrar las actualizaciones del sistema operativo de manera centralizada.
- Capacidad de excluir parches específicos por versión y tipo.
- Capacidad de excluir software (p. ej., Java).
- Capacidad de guardar en caché los parches descargados.

Requisitos de plataformas y sistemas compatibles con WatchGuard Patch Management

Compatible con WatchGuard EPDR, WatchGuard Advanced EPDR, WatchGuard EDR y WatchGuard EPP

Sistemas operativos compatibles: Windows, macOS (Catalina o superior) y Linux (RedHat, CentOS y SUSE).

Lista de navegadores compatibles: Google Chrome, Mozilla Firefox, Microsoft Edge y Safari.

Administración de Parches para Vulnerabilidades: https://www.watchguard.com/wgrd-resource-center/vulnerabilities

Aplicaciones de terceros compatibles: https://www.watchguard.com/wgrd-resource-center/patch-management