HOJA DE DATOS

WatchGuard Patch Management

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

La explotación de vulnerabilidades conocidas sigue siendo uno de los métodos de ataque más comunes. En los informes de la industria, se sigue destacando que los atacantes explotan cada vez más las vulnerabilidades que ya tienen parches disponibles, por lo general, a los pocos días de la divulgación.

Para los MSP que administran muchos entornos diferentes, los parches pasaron de ser una tarea de mantenimiento de rutina a un desafío operativo. Deben actuar rápidamente para reducir la exposición y, al mismo tiempo, garantizar que las actualizaciones no interrumpan las operaciones comerciales.

Vulnerabilidades: Un Riesgo Latente

El desafío actual de la administración de parches no solo implica identificar las actualizaciones que faltan, sino aplicarlas de forma segura a gran escala. Ante tantos entornos de clientes diferentes, los parches deben ejecutarse de una manera que limite la inestabilidad, los momentos sin conectividad o la inconsistencia entre ellos.

Muchas organizaciones tienen dificultades con las herramientas tradicionales de administración de vulnerabilidades por estos motivos:

- La detección de las vulnerabilidades es un proceso largo. Los equipos deben implementar rápidamente parches críticos para reducir la exposición y, si ocurre un incidente, la respuesta debe ser inmediata.
- Debido al trabajo remoto y la infraestructura descentralizada, las herramientas locales dependientes de la red tienen dificultades para garantizar una cobertura completa.
- La administración de flujos de trabajo de prueba y producción separados y de conjuntos de parches inconsistentes aumenta la probabilidad de error humano y la variabilidad de los parches.

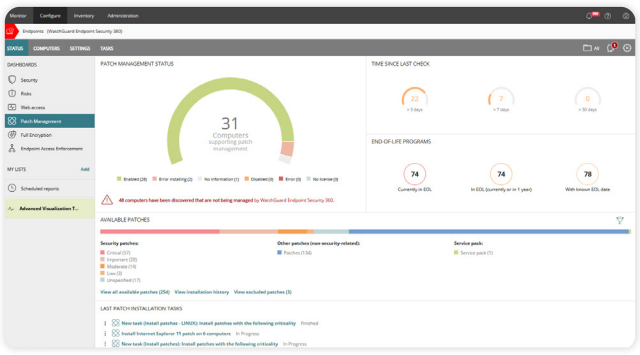

Figura 1: Estado de la organización con Patch Management: panel de control principal

WatchGuard Patch Management

WatchGuard Patch Management simplifica y moderniza la forma en que las organizaciones administran las vulnerabilidades en Windows, macOS y Linux, así como en aplicaciones de terceros.

Esta solución totalmente integrada con WatchGuard Cloud que aprovecha los agentes de endpoints existentes ofrece visibilidad y control centralizados en todo el ciclo de vida del parche, desde la detección y la priorización hasta la implementación y validación.

Patch Management, creada para los MSP y las pymes que estos protegen, permite a los equipos convertir la aplicación de parches de una tarea manual y propensa al riesgo en un proceso controlado y automatizado con el objetivo de que sea más predecible, escalable y seguro.

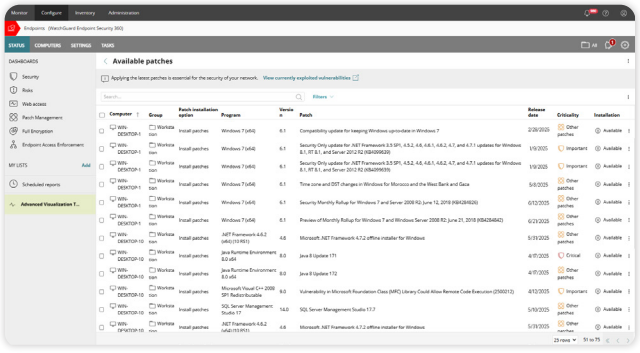

Figura 2: Parches disponibles: administración de Parches

Funcionalidades Clave

Detección y visibilidad

- Visibilidad multiusuario en tiempo real de endpoints vulnerables, parches faltantes y software no compatible (EOL), con estado de corrección.
- Inteligencia detallada de parches, incluidas las referencias de vulnerabilidades y exposiciones comunes (CVE) de los boletines de seguridad asociados.
- Detección de parches continua o programada con intervalos de análisis configurables.
- Notificación de parches pendientes en detecciones de exploits.
- Correlación de detecciones de exploits con parches faltantes para agilizar la corrección.
- Aislamiento, parcheo y reconexión de endpoints remotos desde una sola consola.

Planificación e implementación

- Defina las políticas de parches por gravedad, software y entorno.
- Programe parches para ejecutarlos de forma inmediata, única o recurrente.
- Automatice las implementaciones por etapas probando los parches en los endpoints designados antes de pasar a producción.
- Garantice la coherencia implementando exactamente los mismos parches validados en todos los entornos.
- Configure el comportamiento de reinicio y las excepciones para minimizar las interrupciones que experimenta el usuario.
- Realice una reversión para resolver rápidamente los problemas de compatibilidad.

Supervisión y generación de informes

- Paneles centralizados con visibilidad en tiempo real del estado del parche en todos los endpoints.
- Vistas procesables del estado de la actualización, incluidos los parches pendientes o con error.
- Resúmenes de alto nivel e informes detallados para el seguimiento y el cumplimiento operativos.

Control y administración de acceso

- Control de acceso basado en roles con permisos detallados por usuario, grupo o inquilino.
- Visibilidad ajustada de las vulnerabilidades, los parches y el estado de actualización en función de los roles asignados.

Control de parches centralizado

- Control total de las actualizaciones del sistema operativo, incluida la capacidad de desactivar los servicios de actualización nativos (por ejemplo, Windows Update).
- Excluya parches específicos por versión, tipo o conflictos conocidos.
- Excluya aplicaciones específicas de los parches según sea necesario.
- Almacenamiento en caché local de los parches descargados para optimizar el ancho de banda y el rendimiento de la implementación.

Beneficios

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

Reducir la superficie de ataque
Adelántese a las amenazas creando implementaciones automáticas de parches, incluso de parches críticos, para reducir los puntos de entrada de los atacantes.

Priorizar la respuesta a las vulnerabilidades
Identifique, priorice y corrija rápidamente las exposiciones en los sistemas operativos y las aplicaciones de terceros.

Reducir el riesgo con parches validados
Pruebe los parches antes de la implementación y asegúrese de que solo las actualizaciones probadas lleguen a los sistemas de producción.

Obtener visibilidad en todos los entornos
Obtenga una vista total de las vulnerabilidades, el estado de los parches y las actualizaciones pendientes para comprobar rápidamente el estado de seguridad de los clientes.

Mejorar la eficacia de los parches
Reduzca los retrasos con las funcionalidades de secuenciación automatizada, control centralizado y visibilidad en tiempo real.

Controlar de forma única los entornos multiusuario
Aplique políticas que reconozcan a los suscriptores y criterios de éxito adaptados al entorno de cada cliente.

Requisitos de plataformas y sistemas soportados por WatchGuard Patch Management

Es compatible con WatchGuard EDR, Seguridad de Endpoints Basic, Prime, 360 y Elite.

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

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

Patch Management para vulnerabilidades:
https://www.watchguard.com/wgrd-resource-center/vulnerabilities

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

Acerca de WatchGuard

WatchGuard Technologies es líder mundial en ciberseguridad unificada y diseñada para proveedores de servicios administrados (MSP). Desde hace más de 30 años, WatchGuard define la manera en que los MSP ofrecen seguridad a escala e innova continuamente para mantenerse a la vanguardia de cada cambio importante en el panorama de las amenazas. La Unified Security Platform® de WatchGuard, impulsada por IA, ofrece protección de identidades, endpoints y redes alineada con Zero Trust en una plataforma única e integrada, lo que permite a los MSP reducir la complejidad operativa, mejorar los resultados de seguridad y hacer crecer sus negocios de manera más eficiente. Gracias a la confianza de más de 25.000 MSP que protegen a más de 1,5 millones de clientes en todo el mundo, WatchGuard permite a los partners ofrecer resultados de seguridad sólidos y medibles para clientes de todo el mundo. Obtenga más información en WatchGuard.com/es.

VENTAS EN MÉXICO: +52 55 5347-606 VENTAS ESPAÑA: +34 911 410 918 WEB www.watchguard.com/es WatchGuard Technologies, Inc.

No. de pieza WGCE67518_051526