HOJA DE DATOS

WATCHGUARD EPP

Solida Plataforma de protección de Endpoint

DESAFÍOS DE SEGURIDAD CIBERSEGURIDAD

En la lucha constante por defender su organización, el endpoint es uno de los blancos favoritos de los criminales cibernéticos. Esto significa que es más importante que nunca proteger y supervisar a todos los endpoints que manejan información confidencial y que se conectan a sistemas, tanto dentro como fuera de la red corporativa.

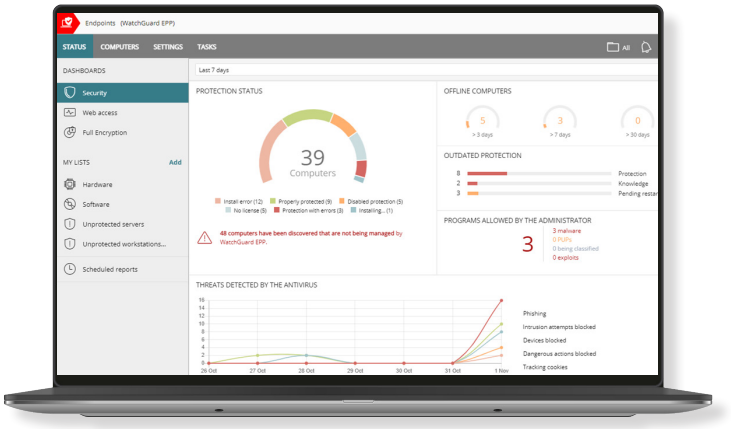
De hecho, el año pasado se registraron más de 350.000 programas maliciosos por día. Los hackers apuntan a los endpoints vulnerables, donde las empresas almacenan sus activos más valiosos. ¿Con qué fin? Como suele suceder, el motivo es obtener beneficios económicos. El malware y el ransomware se convirtieron en una de las principales amenazas, aunque paradójicamente, los costos directos no son el problema principal, sino los momentos sin conectividad que provocan. Por lo tanto, las empresas deben tomar medidas para mejorar su posición de seguridad.

PROTEJA SU EMPRESA CONTRA EL MALWARE Y EL RANSOMWARE

La creciente exposición de las empresas a nuevos tipos de malware y amenazas pone en peligro su seguridad, por lo que se necesitan nuevos enfoques para ayudar a reducir el impacto de los posibles ataques.

WatchGuard EPP es una efectiva solución de seguridad nativa de la nube que centraliza el antivirus de última generación para todas las computadoras de escritorio, computadoras portátiles y servidores con Windows, macOS, iOS y Linux, además de los dispositivos Android y los sistemas de virtualización líderes.

Incluye un conjunto de tecnologías de EPP para evitar el malware, el ransomware y las últimas amenazas. Una de estas tecnologías controla en tiempo real la Inteligencia sobre Amenazas de WatchGuard, un enorme repositorio que recibe los últimos algoritmos de aprendizaje automático para detectar ataques maliciosos con más rapidez.



BENEFICIOS

Seguridad de Múltiples Plataformas

- Seguridad contra amenazas avanzadas desconocidas: detecta y bloquea malware, troyanos, suplantación de identidad y ransomware.
- Análisis y desinfección automáticos de computadoras. Análisis de comportamiento para detectar malware conocido y desconocido.
- Seguridad de plataforma cruzada: Sistemas Windows, Linux, macOS, iOS, Android y entornos virtuales (VMware, Virtual PC, MS Hyper-V, Citrix). Administración de licencias que pertenecen a infraestructura de virtualización (VDI) tanto persistente como no persistente.

Administración Simplificada

- Fácil de mantener: no se requiere infraestructura específica para hospedar la solución, por lo que el departamento de TI puede concentrarse en tareas más importantes.
- Fácil de implementar: varios métodos de implementación, que incluyen desinstaladores automáticos para los productos de la competencia con el fin de facilitar una rápida migración de soluciones de terceros.
- Curva de aprendizaje fluida: interfaz de administración basada en la web, intuitiva y sencilla; las opciones de uso más frecuente están disponibles con solo hacer un clic.

Menor Impacto en el Rendimiento

- El agente tiene un uso mínimo de red, memoria y CPU, ya que todas las operaciones se realizan en la nube.
- WatchGuard EPP no requiere instalación y su agente ligero no afecta el rendimiento de endpoints, lo que simplifica el mantenimiento de seguridad y aumenta la eficiencia operativa.

SEGURIDAD DE DISPOSITIVOS CENTRALIZADA

Administración centralizada de actualizaciones de seguridad y productos para todas las estaciones de trabajo y los servidores de la red corporativa. Administra la protección de los dispositivos Windows, Linux, macOS, iOS y Android desde una consola de administración única basada en la web.

PROTECCIÓN CONTRA MALWARE Y RANSOMWARE

WatchGuard EPP analiza los comportamientos y las técnicas de los ataques informáticos para detectar y bloquear tanto el malware conocido como el desconocido, y además, los ataques de ransomware, los troyanos y la suplantación de identidad.

DESINFECCIÓN AVANZADA

En el caso de que se produzca una vulnerabilidad de seguridad, WatchGuard EPP permite a las empresas restaurar rápidamente las computadoras afectadas al estado en que estaban antes de la infección, gracias a las herramientas avanzadas de desinfección y la cuarentena, que almacenan los elementos sospechosos y eliminados.

Además, permite a los administradores reiniciar de manera remota estaciones de trabajo y servidores para garantizar que queden instaladas las últimas actualizaciones de los productos.

SUPERVISIÓN Y REPORTES EN TIEMPO REAL

Ofrece supervisión de seguridad detallada y en tiempo real a través de paneles de control integrales y gráficos fáciles de interpretar.

Se generan y entregan de manera automática reportes sobre el estado de protección, las detecciones y el uso inadecuado de dispositivos.

CONFIGURACIÓN GRANULAR DE PERFILES

Asigna políticas específicas de protección por perfiles de usuario, lo que garantiza la implementación de la política más apropiada para cada grupo de usuarios.

CONTROL CENTRALIZADO DE DISPOSITIVOS

Detiene el malware y las filtraciones de información, ya que bloquea categorías completas de dispositivos (unidades flash, módems USB, cámaras web, DVD/CD, etc.), clasifica dispositivos en listas blancas o configura permisos de acceso de solo lectura, solo escritura y lectura y escritura.

INSTALACIÓN RÁPIDA Y FLEXIBLE

Implemente la protección a través del correo electrónico con una URL de descarga o la implementa silenciosamente en endpoints seleccionados con la herramienta de distribución de la solución. El instalador de MSI es compatible con herramientas de terceros (Active Directory, Tivoli, SMS, etc.).

MALWARE FREEZER

La solución Malware Freezer pone al malware detectado en cuarentena durante siete días y, en caso de detectar un falso positivo, restablece de manera automática el archivo afectado al sistema.

SUPERVISIÓN DE RIESGOS DE LOS ENDPOINTS

Administre y supervise los endpoints desprotegidos, los indicadores de ataque, las configuraciones incorrectas de seguridad, los sistemas operativos y las vulnerabilidades de software de terceros, y los parches faltantes para proteger proactivamente su red antes de que se presente una vulneración

EVALUACIÓN DE VULNERABILIDAD

La evaluación de vulnerabilidad es un proceso crítico que ayuda a los equipos de TI a identificar, evaluar y priorizar las debilidades y vulnerabilidades de seguridad en aplicaciones y sistemas. Comprenda e identifique posibles amenazas, y tome medidas proactivas para mitigarlas antes de que los atacantes exploten las vulnerabilidades.

CORRECCIÓN Y RECUPERACIÓN ANTE ATAQUES DE RANSOMWARE

Para evitar la recuperación de un sistema dañado, además de cifrar archivos, los atacantes intentan eliminar los archivos de copia de seguridad y VSS creados por los administradores y desactivar los servicios designados para impulsar la recuperación

Con la función de copias en la sombra, se aprovecha la tecnología del sistema operativo y se protege a estos archivos mediante tecnología contra alteraciones a fin de que los usuarios puedan recuperar la información después de un ataque de ransomware.

Los profesionales de TI utilizan copias en la sombra con el fin de recuperar archivos de fallas críticas del sistema, pero esta es también una tecnología genial para recuperar archivos cifrados por ransomware.

Requisitos de plataformas y sistemas compatibles con 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.

VENTAS EN EE. UU. 1.800.734.9905 VENTAS INTERNACIONALES +1.206.613.0895 SITIO WEB www.watchguard.com/es WatchGuard Technologies, Inc.