Soluciones de Seguridad del Endpoint de WatchGuard para Empresas

ENDPOINT SECURITY AND MANAGEMENT	WatchGuard EDR Core	WatchGuard EPP	WatchGuard EDR	WatchGuard EPDR	WatchGuard Advanced EPDR
Protección					
Protección contra el malware conocido y de día cero	✓	✓	✓	✓	✓
Protección contra el ransomware conocido y de día cero	✓	✓	✓	✓	✓
Protección contra las vulnerabilidades conocidas y de día cero	✓	✓	✓	✓	✓
Protección contra suplantación de identidad		✓		✓	✓
Protección contra múltiples vectores de ataque *(web, correo electrónico, red, dispositivos)*	✓	✓	✓	✓	✓
Protección tradicional con firmas genéricas y optimizadas		✓		✓	✓
Protección contra amenazas avanzadas persistentes (APTs)	✓		✓	✓	✓
Zero-Trust Application Service			✓	✓	✓
Servicio de Threat Hunting: indicadores de ataque determinados asignados a MITRE ATT&CK			✓	✓	✓
Servicio de Threat Hunting: indicadores de ataque no determinados asignados a MITRE ATT&CK con telemetría contextual.					✓
Consultas a la Inteligencia Colectiva basada en WatchGuard Cloud	✓	✓	✓	✓	✓
Bloqueo de comportamientos	✓	✓	✓	✓	✓
Firewall personal y administrado		✓		✓	✓
IDS / HIPS		✓		✓	✓
Protección contra ataques a la red			✓	✓	✓
Control de dispositivos		✓		✓	✓
Filtrado de URL por categoría *(supervisión de la navegación web)*		✓		✓	✓
Supervisión					
Supervisión de riesgos de los endpoints	✓	✓	✓	✓	✓
Supervisión continua basada en la nube de la actividad de todos los procesos	✓		✓	✓	✓
Retención de datos por un año para la investigación retrospectiva de ataques	✓		✓	✓	✓
Evaluación de vulnerabilidad		✓	✓	✓	✓
Detección					
Detección de las aplicaciones de confianza en peligro			✓	✓	✓
Zero-Trust Application Service			✓	✓	✓
Alertas instantáneas y completamente configurables de riesgos de seguridad	✓	✓	✓	✓	✓
STIX IOCs and YARA rules search					✓
eXtended Detection and Response (XDR)	✓		✓	✓	✓
Contención					
Aislamiento en tiempo real de computadoras desde la consola en la nube	✓		✓	✓	✓
Respuesta y corrección					
Capacidad de revertir y corregir las acciones realizadas por los atacantes		✓	✓	✓	✓
Cuarentena centralizada		✓	✓	✓	✓
Análisis y desinfección automáticos		✓	✓	✓	✓
Copias en la sombra		✓	✓	✓	✓
Capacidad de bloquear las aplicaciones desconocidas y no deseadas			✓	✓	✓
eXtended Detection and Response (XDR)	✓		✓	✓	✓

ENDPOINT SECURITY AND MANAGEMENT	WatchGuard EDR Core	WatchGuard EPP	WatchGuard EDR	WatchGuard EPDR	WatchGuard Advanced EPDR
Investigación					
Servicio de Threat Hunting: indicadores de ataque determinados asignados a MITRE ATT&CK			✓	✓	✓
Servicio de Threat Hunting: indicadores de ataque no determinados asignados a MITRE ATT&CK con telemetría contextual.					✓
Gráficos de incidentes e información del ciclo de vida disponibles desde la consola web	✓		✓	✓	✓
Capacidad de exportar información del ciclo de vida para el análisis local	✓		✓	✓	✓
Advanced Reporting Tool (complementaria)			✓	✓	✓
Detección y supervisión de datos personales no estructurados en endpoints *(complemento)*			✓	✓	✓
Investigación de ataques avanzada (Jupyter Notebooks)			✓	✓	✓
Shell remoto para administrar procesos y servicios, transferencias de archivos, herramientas de línea de comandos, obtener volcados, pcap, etc.					✓
Reducción de la superficie de ataque					
Modo de bloqueo en la protección avanzada			✓	✓	✓
Tecnología anti-exploit	✓		✓	✓	✓
Bloqueo de programas por hash o nombre (p. ej., PowerShell)			✓	✓	✓
Control de dispositivos		✓		✓	✓
Protección web		✓		✓	✓
Actualizaciones automáticas	✓	✓	✓	✓	✓
Detección automática de endpoints desprotegidos	✓	✓	✓	✓	✓
Administración de parches para SO y aplicaciones de terceros		✓	✓	✓	✓
Seguridad para conexiones de VPN (se necesita Firebox)	✓	✓	✓	✓	✓
Acceso seguro a la red Wi-Fi a través de puntos de acceso	✓	✓	✓	✓	✓
Políticas de seguridad avanzadas					✓
Administración de la seguridad de endpoints					
Consola centralizada basada en la nube	✓	✓	✓	✓	✓
Herencia de la configuración entre grupos y endpoints	✓	✓	✓	✓	✓
Riesgo (seguimiento continuo)	✓	✓	✓	✓	✓
Capacidad de establecer y aplicar la configuración por grupos	✓	✓	✓	✓	✓
Capacidad de establecer y aplicar la configuración por endpoints	✓	✓	✓	✓	✓
Implementación en tiempo real de configuración de la consola a los endpoints	✓	✓	✓	✓	✓
Administración de la seguridad según vistas del endpoint y filtros dinámicos		✓	✓	✓	✓
Capacidad de asignar permisos personalizados a usuarios de la consola	✓	✓	✓	✓	✓
Habilidad para personalizar las alertas locales	✓	✓	✓	✓	✓
Auditoría de actividades de los usuarios	✓	✓	✓	✓	✓
Instalación mediante paquetes de MSI, URL de descarga y correos electrónicos enviados a usuarios	✓	✓	✓	✓	✓
Reportes a pedido y programados en diferentes niveles con múltiples opciones de granularidad	✓	✓	✓	✓	✓
KPI de seguridad y paneles de control de administración	✓	✓	✓	✓	✓
Disponibilidad de API	✓	✓	✓	✓	✓

ENDPOINT SECURITY AND MANAGEMENT	WatchGuard EDR Core	WatchGuard EPP	WatchGuard EDR	WatchGuard EPDR	WatchGuard Advanced EPDR
Integraciones de Supervisión y Administración Remotas (RMM)					
ConnectWise Automate	✓	✓	✓	✓	✓
Kaseya VSA	✓	✓	✓	✓	✓
N-able N-central	✓	✓	✓	✓	✓
N-able N-sight	✓	✓	✓	✓	✓
NinjaOne (Script de instalación automatizado)	✓	✓	✓	✓	✓
Modules					
WatchGuard Data Control*			✓	✓	✓
WatchGuard Advanced Reporting Tool			✓	✓	✓
WatchGuard Patch Management		✓	✓	✓	✓
WatchGuard Full Encryption		✓	✓	✓	✓
WatchGuard SIEMFeeder			✓	✓	✓
Servicio de alta disponibilidad	✓	✓	✓	✓	✓
Certificaciones de la plataforma host	✓	✓	✓	✓	✓
Sistemas operativos compatibles					
Compatible con Windows Intel	✓	✓	✓	✓	✓
Compatibilidad con Windows ARM	✓	✓	✓	✓	✓
Compatibilidad con macOS ARM	✓	✓	✓	✓	✓
Compatible con macOS	✓	✓	✓	✓	✓
Compatible con Linux	✓	✓	✓	✓	✓
Compatible con Android		✓		✓	✓
Compatible con iOS		✓		✓	✓
Compatibilidad para entornos virtuales persistentes y no persistentes (VDI)**	✓	✓	✓	✓	✓

✓ Solo la funcionalidad básica

✓ Funcionalidad completa

* Data Control está disponible en los siguientes países: España, Alemania, Reino Unido, Suecia, Francia, Italia, Portugal, Holanda, Finlandia, Dinamarca, Suiza, Noruega, Austria, Bélgica, Hungría e Irlanda.

** Sistemas compatibles con los siguientes tipos de máquinas virtuales: VMWare Desktop, VMware Server, VMware ESX, VMware ESXi, Citrix XenDesktop, XenApp, XenServer, MS Virtual Desktop y MS Virtual Servers. Las soluciones de WatchGuard EPDR son compatibles con Citrix Virtual Apps, Citrix Desktops 1906 y Citrix Workspace App para Windows.

Requisitos de plataformas y sistemas compatibles con WatchGuard Endpoint Security

Sistemas operativos compatibles: Windows (Intel & ARM), macOS (Intel & ARM), Linux, iOS y Android.

Soporte para sistemas heredados que empieza con Windows XP SP3 y Server 2003.

Las capacidades de EDR están disponibles en Windows, macOS y Linux; Windows es la plataforma que proporciona todas las capacidades en su totalidad.

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

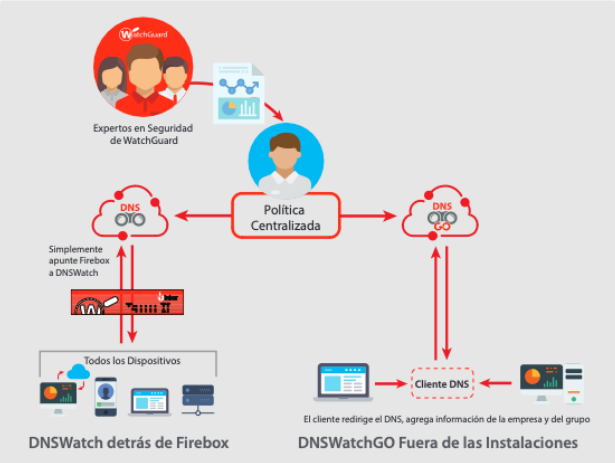
MÓDULOS Y PRODUCTOS ADICIONALES DE SEGURIDAD DE ENDPOINT DE WATCHGUARD

DNSWatchGO

DNSWatchGO es un servicio basado en la nube que ofrece protección en el nivel de dominio, filtrado de contenido y entrenamiento de conocimiento sobre seguridad integrado

para mantener a sus usuarios protegidos cuando salen del su perímetro seguro de red. Cuando se detectan alertas críticas, el equipo de expertos en seguridad de WatchGuard realiza un análisis personalizado de la posible amenaza y ofrece un seguimiento con explicaciones sencillas que incluyen insights detallados de la potencial infección. Cuando un usuario hace clic en un enlace malicioso, DNSWatchGO lo redirige de manera automática a una página segura y ofrece recursos para reforzar la educación sobre seguridad.

Más información



Advanced Reporting Tool

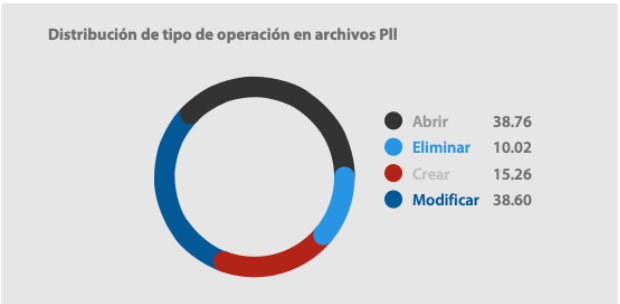
The Advanced Reporting Tool almacena y correlaciona la información relativa a la ejecución de procesos y su contexto extraído por WatchGuard EPDR de endpoints. Genera inteligencia de seguridad de manera automática y proporciona herramientas que permiten a las organizaciones detectar no solo ataques y comportamientos inusuales, sino también el uso indebido interno de los sistemas corporativos y de la red para realizar una investigación de seguridad más profunda.

Más información

Data Control

Data Control es un módulo de seguridad de datos no estructurados, diseñado para ayudar a las organizaciones en el cumplimiento de las regulaciones de protección de datos, así como en la detección y la protección de datos confidenciales, tanto en tiempo real como durante su ciclo de vida en endpoints y servidores. Data Control detecta, audita y supervisa datos personales no estructurados en endpoints: desde datos en reposo hasta datos en uso y en movimiento.

Más información

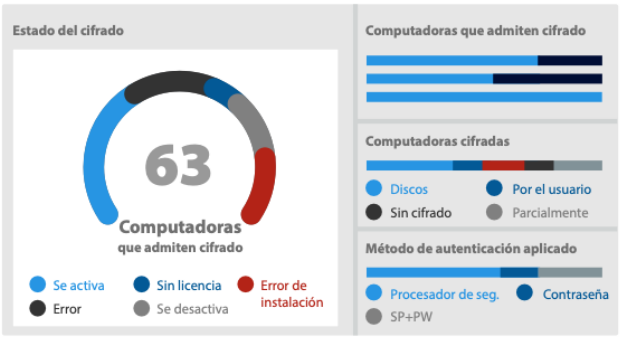


**Data Control está disponible en los siguientes países: España, Alemania, Reino Unido, Suecia, Francia, Italia, Portugal, Holanda, Finlandia, Dinamarca, Suiza, Noruega, Austria, Bélgica, Hungría e Irlanda.*

Full Encryption

Full Encryption es un módulo adicional de las soluciones de seguridad adaptables avanzadas y de protección de endpoints de WatchGuard, diseñado para administrar de manera centralizada el cifrado completo de disco y ofrecer las siguientes funcionalidades: Cifrado y descifrado completos de unidades, administración y recuperación centralizadas de claves de cifrado, listas y reportes y aplicación centralizada de políticas.

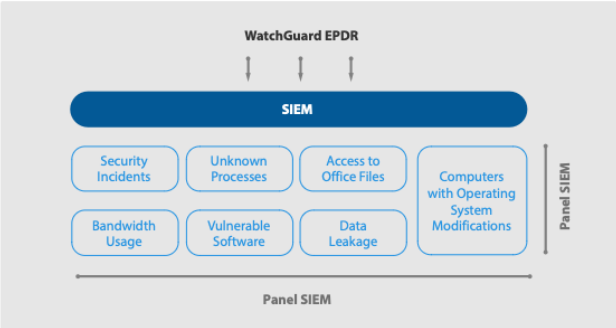
Más información



SIEM Feeder

SIEM Feeder. WatchGuard EDR y WatchGuard EPDR integran sin problemas los eventos recopilados de endpoints protegidos con soluciones corporativas de SIEM existentes sin implementaciones adicionales en dispositivos de usuarios. Los eventos monitoreados se envían de manera segura con los formatos LEEF/CEF compatibles con la mayoría de los sistemas de SIEM del mercado, ya sea en forma directa o indirecta a través de complementos.

Más información



Distribución de WatchGuard. La compra y la configuración requieren la asistencia del personal de WatchGuard.

Patch Management

Patch Management es un módulo para administrar las vulnerabilidades de los sistemas operativos y las aplicaciones de terceros en estaciones de trabajo y servidores de Windows.

No requiere la implementación de nuevos agentes de endpoint ni consolas de administración, ya que se integra completamente con todas las soluciones de endpoint de WatchGuard. Además, proporciona visibilidad centralizada y en tiempo real del estado de seguridad de las vulnerabilidades de software, las revisiones faltantes, las actualizaciones y el software en fin del ciclo de vida útil (EOL) sin soporte, así como herramientas fáciles de usar y en tiempo real para instalar y supervisar actualizaciones.

Más información