HOJA DE DATOS

WatchGuard Endpoint Security Elite

EDR Avanzado para Equipos de Seguridad

Visibilidad Profunda e Investigación Avanzada de Amenazas

Para las organizaciones con programas de seguridad maduros o partners que ofrecen servicios de seguridad avanzados, la visibilidad profunda y las capacidades de investigación son fundamentales. Los equipos de seguridad necesitan soluciones de prevención, detección y respuesta para investigar y responder a las amenazas en sus entornos, elevando la pila de seguridad al siguiente nivel y minimizando el tiempo de permanencia de los adversarios.

WatchGuard Endpoint Security Elite proporciona una plataforma de EDR (Endpoint Detection and Response) con todas las funciones, que incluye telemetría enriquecida, herramientas avanzadas de consulta y capacidades de investigación asistidas por IA, para que los equipos de seguridad puedan comprender rápidamente ataques complejos, correlacionar eventos entre endpoints y responder con precisión. Al combinar análisis potentes con respuesta automatizada y visibilidad de datos extendida, Endpoint Security Elite brinda a los equipos de seguridad las herramientas que necesitan para detectar, investigar y detener amenazas sofisticadas a escala empresarial.

EDR Avanzado Diseñado para Operaciones de Seguridad

WatchGuard Endpoint Security Elite está diseñado para organizaciones y proveedores de servicios de seguridad gestionados (MSSP) que requieren una visibilidad de seguridad más profunda y capacidades de investigación avanzadas. A partir de la base de EDR impulsada por IA de WatchGuard, proporciona telemetría enriquecida, visibilidad histórica extendida y herramientas avanzadas de detección de amenazas que permiten a los equipos de seguridad detectar, investigar y responder a ataques sofisticados de manera más efectiva.

Con telemetría detallada de endpoint y datos contextuales de incidentes, los analistas pueden ver los plazos de los ataques, identificar las causas raíz y comprender cómo se mueven los adversarios a través de los sistemas. El mapeo integrado de MITRE ATT&CK y la correlación de comportamiento automatizada proporcionan una visión clara de las tácticas, las técnicas y los procedimientos de los atacantes, lo que ayuda a los equipos de seguridad a priorizar rápidamente las amenazas y responder con confianza.

Las herramientas de investigación avanzadas incluyen la detección de amenazas basada en STIX y Yara y un asistente de IA generativo incorporado que permite a los analistas consultar datos de seguridad utilizando un lenguaje natural. Estas capacidades aceleran drásticamente los flujos de trabajo de investigación, lo que permite a los equipos de seguridad identificar amenazas ocultas, reducir el tiempo de permanencia y fortalecer la postura general de seguridad.

Para los MSP y las organizaciones que ofrecen servicios de seguridad avanzados, WatchGuard Endpoint Security Elite proporciona la profundidad de visibilidad y la potencia analítica necesarias para respaldar las operaciones de seguridad modernas sin la complejidad de las herramientas fragmentadas.

Herramientas Avanzadas de Investigación

- Asistente de IA generativa para consultar la telemetría.
- Búsquedas de indicadores de ataque STIX (IoC) y reglas de YARA.
- Herramienta CAPA: información de archivos (comportamientos, cadenas, importaciones, exportaciones).
- Shell remoto para reducir el MTTR y el tiempo de permanencia

WatchGuard Endpoint Security Elite reúne capacidades avanzadas de investigación y respuesta para los equipos de Operaciones de Seguridad.

Reducción de la Superficie de Ataque

- Panel de control de riesgos de endpoints personalizable
- Detección de endpoints no administrada
- Evaluación de vulnerabilidad.

Tecnologías de Prevención Integradas

- Firewall, IDS y control de dispositivos
- Protección contra múltiples vectores de ataque (web, correo electrónico, red, dispositivos)
- Archivos de firma, heurística previa a la ejecución e inteligencia colectiva
- Detecciones impulsadas por IA que identifican y bloquean instaladores y scripts maliciosos
- Protección contra suplantación de identidad
- URL y filtrado web
- Detección a través del análisis de tráfico de red
- Ejecución de denegación por defecto

Capacidades de Detección y Respuesta

- Supervisión continua del endpoint
- Inteligencia artificial de autoaprendizaje con análisis de comportamiento contextual para detectar y bloquear ataques sin archivos y living-off-the-land (LotL).
- Bloquea automáticamente los intentos de aprovechar las vulnerabilidades en los procesos activos en el dispositivo
- Protección contra ataques de red y vulnerabilidades en servicios expuestos a Internet.
- Detección y prevención automatizadas de los ataques RDP
- Contención del movimiento lateral
- Detección automática y correlación de un ataque, con alertas, asignadas al marco MITRE ATT&CK®
- Vista interactiva de incidentes de múltiples señales para un análisis integral de la causa raíz (RCA)
- Contexto profundo y telemetría forense informática en tiempo real para acelerar las investigaciones
- Integraciones con ThreatSync (XDR) para visibilidad y correcciones
- Aislamiento, escaneo y reinicio de computadoras y redes en tiempo real
- Recuperación de archivos cifrados (copias ocultas)

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

Beneficios Estratégicos

Telemetría Profunda para Investigaciones más Rápidas

Endpoint Security Elite proporciona acceso a telemetría enriquecida y forense, así como a una retención de datos extendida, lo que permite a los analistas analizar la actividad de los ataques a lo largo del tiempo y reconstruir el comportamiento de los atacantes en todos los endpoints.

Detección de Amenazas Avanzada

Los equipos de seguridad pueden buscar proactivamente amenazas emergentes con herramientas avanzadas que analizan la telemetría de endpoints en busca de indicadores de compromiso y comportamiento sospechoso. Con soporte para marcos de detección estructurados como STIX y YARA, los equipos de seguridad pueden descubrir amenazas ocultas e investigar la actividad en todo el entorno.

Contexto de Ataque Visual Enriquecido

Las líneas de tiempo interactivas, los árboles de procesos y los mapas de movimiento lateral proporcionan un contexto visual claro para comprender cómo se desarrollan los ataques en los endpoints. Esto permite a los equipos de seguridad identificar rápidamente la causa raíz, comprender el comportamiento de los atacantes y acelerar las investigaciones.

Análisis de Seguridad Asistido por IA

Un asistente de IA generativo incorporado permite a los analistas consultar datos de seguridad utilizando un lenguaje natural, acelerando las investigaciones y reduciendo el tiempo necesario para comprender los incidentes, sin necesidad de consultas complejas.

Controles de Políticas Granulares

Endpoint Security Elite permite a los administradores aplicar políticas de seguridad detalladas que controlan la ejecución de aplicaciones, el acceso a dispositivos y el comportamiento del sistema en todos los endpoints. Estos controles granulares reducen la superficie de ataque al tiempo que garantizan una aplicación de seguridad coherente en todos los usuarios, dispositivos y entornos.

Creado para los Servicios de Seguridad Administrada

Endpoint Security Elite proporciona la telemetría profunda, las herramientas de investigación y la automatización necesarias para que los MSP brinden servicios de seguridad de alto valor. Con una administración centralizada de múltiples usuarios y capacidades avanzadas de investigación, los socios pueden monitorear, investigar y responder de manera eficiente a las amenazas en múltiples entornos de clientes.

Modelo de Zero Trust: Una Protección en Capas

La plataforma Endpoint Security de WatchGuard no depende de una única tecnología. Implementamos varias capas de herramientas simultáneamente para reducir las posibilidades de éxito de los agentes de amenaza. Al trabajar en conjunto, estas tecnologías utilizan los recursos del endpoint para minimizar el riesgo de vulneración.

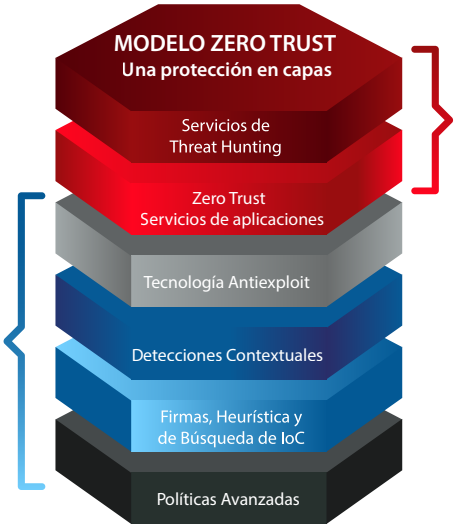
Capas de Endpoints:

Capa 1: Políticas de Seguridad Mejoradas
Detecte o bloquee la ejecución de técnicas de ataque comunes.

Capa 2: Archivos de Firma, Tecnologías Heurísticas y Motor de Búsqueda de IoC de STIX Buscan ataques recientemente revelados por hash, nombre de archivo, ruta, dominio C2, IP y reglas de YARA.

Capa 3: Detecciones de Contacto
Identifica ataques malintencionados que abusan de herramientas legítimas como PowerShell, WMI y navegadores web

Capa 4: Tecnología antiexploit
Detecta ataques sin archivos diseñados para aprovechar vulnerabilidades



Capas de Endpoints:

Capa 5: Servicio de Zero-Trust Application
Clasifica el 100% de los procesos antes de ejecutarlos y prohíbe cualquier ejecución hasta que esté certificada como confiable

Capa 6 /Servicio integrado de búsqueda de amenazas
Detecta endpoints comprometidos, IoA, ataques en etapa inicial y actividades sospechosas. Los IoA se contextualizan en la consola basada en la nube con la telemetría asociada, lo que permite a los analistas de seguridad investigar posibles intentos de ataque

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 5347-6063 VENTAS ESPAÑA +34 911 410 918 WEB www.watchguard.com/es WatchGuard Technologies, Inc.