HOJA DE DATOS | SOC

WATCHGUARD ADVANCED EPDR

DESAFÍOS DE CIBERSEGURIDAD

Los endpoints son el objetivo principal de la mayoría de los ciberataques. Hoy que la infraestructura tecnológica se vuelve más compleja, las organizaciones luchan por encontrar la experiencia necesaria para monitorear y administrar los riesgos de seguridad de los endpoints. ¿Qué tipos de desafíos enfrentan los equipos de seguridad cuando adoptan soluciones de seguridad de endpoints?

- **Amenazas sofisticadas en constante evolución:** Las prácticas de seguridad proactivas y eficaces pueden marcar la diferencia entre una operación de seguridad menor o ser una víctima. Estas prácticas van desde reducir la superficie de ataque hasta detectar amenazas emergentes antes de un riesgo real.
- **Fatiga por alertas, falta de efectividad:** los equipos de seguridad reciben miles de alertas cada semana, de las cuales solo el 19% se considera confiable y solo el 4% se investiga. Estos equipos dedican dos tercios del tiempo a la administración de las alertas y a la clasificación de archivos sospechosos manualmente.
- **Rendimiento deficiente:** con frecuencia las soluciones de seguridad de endpoints requieren instalar y administrar múltiples agentes en cada computadora de escritorio, servidor y computadora portátil supervisados, lo que genera errores graves, rendimiento deficiente y alto consumo de recursos.

Los equipos que se encargan de la seguridad necesitan **soluciones y armas autónomas de prevención, detección y respuesta para detectar y responder fácilmente** a las amenazas que acechan en los entornos, y para llevar el paquete de seguridad al siguiente nivel para minimizar el tiempo de permanencia de los adversarios.

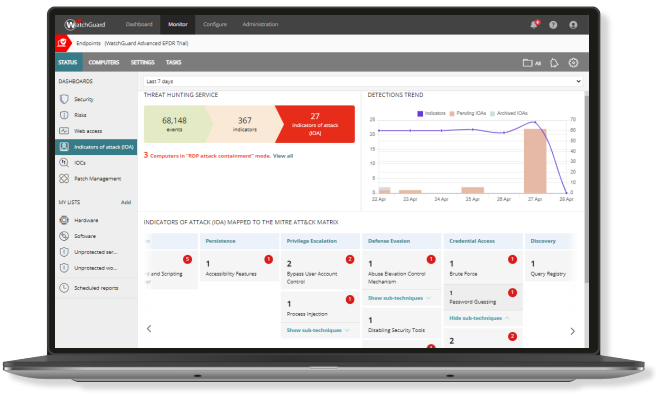
MEJORE SUS SERVICIOS DE CIBERSEGURIDAD

WatchGuard Advanced EPDR es una solución de ciberseguridad de vanguardia que se proporciona desde la nube a computadoras de escritorio, computadoras portátiles y servidores. Esta herramienta automatiza la prevención, detección, contención y respuesta ante cualquier amenaza avanzada, tanto dentro como fuera de la red corporativa.

Combina tecnologías preventivas y de EDR con dos servicios de seguridad:

- **Servicio de Zero-Trust Application:** aprendizaje automático basado en la nube, que clasifica automáticamente todos los archivos
- **Servicio de Threat Hunting:** análisis de comportamiento para descubrir actores de amenazas que utilizan técnicas living-off-the-land (LotL).

WatchGuard Advanced EPDR amplía WatchGuard EPDR: agregar a su paquete de herramientas tecnológicas de detección de amenazas, como el motor de búsqueda de IoC, las detecciones avanzadas de IoA asignadas a MITRE ATT&CK y el acceso remoto a endpoints para una investigación y respuesta rápidas.



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

WatchGuard EPDR integra tecnologías de endpoint tradicionales con tecnologías de EDR en una solución única que permite a los equipos de seguridad hacer frente a las amenazas informáticas avanzadas.

Herramientas de Reducción de Superficie de Ataque

- Detección y puntuación centralizada de riesgos de seguridad de endpoints
- Detección proactiva del endpoint no administrada
- Evaluación de vulnerabilidad de sistemas operativos y de cientos de aplicaciones

Tecnologías Preventivas Tradicionales

- Firewall personal o administrado (IDS)
- Control de dispositivos
- Control de aplicaciones: Lista de rechazos/lista de permisos
- Antimalware permanente multivectorial y análisis a pedido
- Heurística previa a la ejecución
- Filtrado de URL y navegación web
- Protección contra suplantación de identidad y contra alteraciones
- Ataques detectados a través de análisis del tráfico de red
- Corrección automática y capacidad de reversión
- Recuperación de archivos cifrados con copias en la sombra

Tecnologías de Búsqueda y Detección

- Supervisión continua de endpoints con EDR
- Servicios de Zero-Trust Application y servicios de Threat Hunting
- Sandboxing en entornos reales
- Protección antiexploit
- Indicadores de ataque (IoA) asignados a MITRE ATT&CK
- Detección y contención automatizada de ataques RDP
- Búsquedas de indicadores de ataque STIX (IoC) y reglas de YARA
- Rechazo de la ejecución de técnicas de ataque comunes con políticas de seguridad mejoradas

Herramientas de Contención y Corrección

- Aislamiento de computadoras y reinicio de los sistemas
- Shell remoto desde la nube hasta los endpoints

BENEFICIOS

Operaciones Rentables: No Más Tiempo Perdido en Archivos Sospechosos
Como WatchGuard EPDR, el servicio de Zero-Trust Application devuelve a su equipo todo ese tiempo dedicado a la ingeniería inversa de archivos sospechosos sobre los que otras soluciones alertan sin cerrar el ciclo y delegar el último veredicto en usted.

Seguridad de Endpoints Integral para Adaptar a Sus Servicios
WatchGuard Advanced EPDR proporciona una amplia gama de capacidades para fortalecer los programas de seguridad de endpoints, incluida la reducción de la superficie de ataque; la prevención, detección y respuesta a amenazas; las herramientas de caza proactiva; y la conexión remota de endpoint para una respuesta rápida.

Búsqueda y Respuesta Mejoradas al Alcance de la Mano
Gracias a las búsquedas centralizadas de IoC, WatchGuard Advanced EPDR permite a los equipos de seguridad descubrir amenazas sin tener que lidiar con consultas complejas. Su servicio de Threat Hunting ofrece IoA contextualizados con telemetría para continuar con la investigación.

Servicios de Seguridad Administrada Escalables para Crecer a su Ritmo

La arquitectura de Unified Security Platform de WatchGuard
brinda seguridad integral desde la red hasta el endpoint, Wi-Fi e identidad, con características de plataforma sin precedentes y sin costo adicional. Cuantos más servicios adopte, mayores serán sus beneficios operativos y comerciales.

MODELO ZERO TRUST: UNA PROTECCIÓN EN CAPAS

La plataforma de Seguridad de Endpoints de WatchGuard no depende de una única tecnología. Implementamos varias 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: Los Archivos de Firma, las Tecnologías Heurísticas y el Motor de Búsqueda de IoC de STIX permiten a los equipos de seguridad buscar ataques recientemente revelados por hash, nombre de archivo, ruta, dominio C2, IP y reglas de YARA.

Capa 3: Detecciones Contextuales de ataques sin malware utilizando herramientas del sistema operativo, como PowerShell, WMI, navegadores web y otras aplicaciones comúnmente dirigidas, como Java, Adobe y más.

Capa 4: Tecnología Antiexploit
Nos permite detectar ataques sin archivos diseñados para aprovechar vulnerabilidades.

CAPAS NATIVAS DE LA NUBE

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 de Threat Hunting
Nos permite detectar endpoints comprometidos, ataques en etapas iniciales, actividades sospechosas y la detección de IoA. Los IoA no deterministas se contextualizan en la consola basada en la nube con los eventos asociados, lo que permite a los analistas de seguridad investigar posibles intentos de ataque.

IMPLEMENTE UNA SEGURIDAD PODEROSA Y SIMPLIFICADA CON UNIFIED SECURITY PLATFORM DE WATCHGUARD

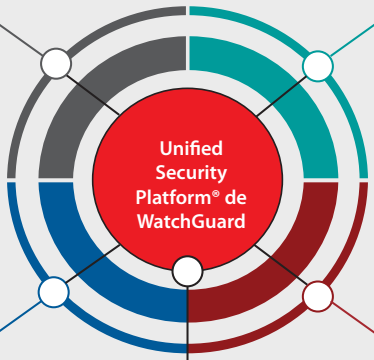
La arquitectura de Unified Security Platform de WatchGuard es una plataforma única que permite mejorar la seguridad moderna.

Nuestro enfoque de plataforma lo ayuda a ofrecer servicios de seguridad poderosos para cada vector de amenazas con mayor escala y velocidad, a la vez que respalda eficiencias operativas y una mayor rentabilidad. Obtenga más información aquí.

Una plataforma única y escalable para aumentar la entrega de seguridad moderna.

SEGURIDAD INTEGRAL
Un portafolio completo de **productos y servicios de** endpoints, autenticación multifactor **y seguridad de red** para proteger entornos, usuarios y dispositivos.

CLARIDAD Y CONTROL
Administración de seguridad centralizada, visibilidad y generación de reportes avanzados a través de **WatchGuard Cloud**.



ALINEACIÓN OPERATIVA
Operaciones comerciales simplificadas con **acceso directo de API,** un variado ecosistema de **integraciones listas para usar** y soporte para todos los modelos de pago y uso a través de **FlexPay.**

CONOCIMIENTO COMPARTIDO
Una plataforma completamente integrada para adoptar una posición de seguridad Zero Trust a través de **Identity Framework** de WatchGuard y para implementar un verdadero enfoque basado en XDR para la detección y corrección de amenazas a través de **ThreatSync®**.

AUTOMATIZACIÓN
Automation Core® de WatchGuard ofrece simplificación y escala para todos los aspectos de uso, prestación de servicios y administración de seguridad.

VENTAS EN MÉXICO: +52 55 5347-6063 VENTAS ESPAÑA: +34 911 410 918 WEB: www.watchguard.com/es
WatchGuard Technologies, Inc.