HOJA DE DATOS

WATCHGUARD EPDR

Protección, Detección y Respuesta para Endpoints

DESAFÍOS DE SEGURIDAD CIBERNÉTICA DE LA ORGANIZACIÓN

Los endpoints son el principal objetivo de la mayoría de los ataques cibernéticos y a medida que la infraestructura de la tecnología se vuelve más compleja, las organizaciones se esfuerzan por conseguir los conocimientos y los recursos necesarios para supervisar y administrar los riesgos de seguridad de endpoints. Entonces, ¿qué tipos de desafíos enfrentan las empresas cuando adoptan soluciones de seguridad para los endpoint?

- **Numerosas alertas:** Las organizaciones reciben miles de alertas de malware cada semana, de las cuales solo el 19% se considera confiable y solo el 4% se investiga. Dos tercios del tiempo de un administrador de seguridad cibernética se dedica a la administración de las alertas de malware.
- **Complejidad:** Demasiadas herramientas de seguridad cibernética, desconectadas entre si, pueden ser difíciles de administrar para por los profesionales de la seguridad, debido a la cantidad de tecnologías habilitadoras, la falta de habilidades internas y el tiempo requerido para identificar amenazas.
- **Rendimiento deficiente:** Con frecuencia las soluciones de seguridad para endpoints requieren la instalación y la administración de múltiples agentes en cada computadora de escritorio, servidor y computadora portátil supervisada, lo que genera errores graves, rendimiento deficiente y alto consumo de recursos.

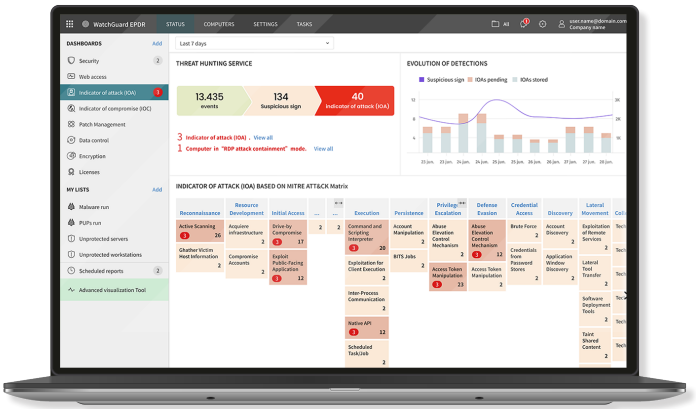
Las técnicas tradicionales de protección de endpoints, enfocadas en la prevención, son válidas para amenazas conocidas y comportamientos maliciosos, pero no son suficientes contra las amenazas cibernéticas avanzadas.

DE LA PREVENCIÓN A LA RESPUESTA - SEGURIDAD DE ENDPOINTS AUTOMATIZADA

WatchGuard EPDR es una solución de seguridad cibernética innovadora para computadoras de escritorio, computadoras portátiles y servidores, que se ofrece desde la nube. Automatiza la prevención, la detección, la contención y la respuesta relacionadas con cualquier amenaza avanzada, malware de día cero, ransomware, suplantación de identidad, vulnerabilidad en la memoria o ataque sin malware y sin archivo, dentro y fuera de la red corporativa.

A diferencia de otras soluciones, combina la más amplia variedad de tecnologías de protección de endpoints (EPP) con capacidades automatizadas de detección y respuesta (EDR). También cuenta con dos servicios administrados por expertos de WatchGuard, que se brindan como una funcionalidad de la solución:

- **Servicio Zero-Trust de Aplicaciones:** clasificación del 100% de las aplicaciones
- **Servicio de Threat Hunting:** detección de hackers e intrusos



WatchGuard EPDR integra antivirus de última generación con protección innovadora, adaptable y tecnologías de EDR en una solución única, que permite a los profesionales de TI hacer frente a las ciberamenazas avanzadas.

Tecnologías antivirus de última generación

- Firewall personal o administrado (IDS)
- Control de dispositivos
- Inteligencia colectiva y heurística previa a la ejecución
- Antimalware permanente multivectorial y análisis a pedido
- Filtrado de URL y navegación web
- Filtrado de URL, navegación web y protección contra suplantación de identidad
- Protección contra alteraciones
- Corrección automática y capacidad de reversión
- Recupere archivos cifrados con Shadow copies
- Evaluación de vulnerabilidad

Tecnologías de Seguridad Avanzadas

- Supervisión continua de endpoints con EDR
- Aprendizaje basado en la nube que clasifica el 100% de los procesos (APT, ransomware, rootkits, etc.)
- Sandboxing en entornos reales
- Protección antiexploit
- Protección contra ataques de red: evite que los ataques exploten vulnerabilidades en servicios expuestos en Internet
- Threat Hunting: análisis del comportamiento y detección de Indicadores de Ataques (IoA) para detectar los ataques del tipo Living-off-the-Land (LotL).
- Indicadores de ataques asociados al marco de MITRE ATT&CK
- Detección y prevención de ataques de RDP
- Capacidades de contención y corrección, como el aislamiento de computadoras y el bloqueo de programas por hash o nombre del programa

BENEFICIOS

Simplifica y Maximiza la Seguridad

- Sus servicios automatizados reducen los costos de personal especializado. No hay necesidad de administrar falsas alertas, no se pierde tiempo en configuraciones manuales y no se delegan responsabilidades.
- El rendimiento del endpoint no se ve afectado, ya que se basa en un agente único y en arquitectura nativa de la nube.

Fácil de Usar y Mantener

- El portafolio de seguridad de endpoints maneja todas las necesidades de protección de sus endpoints con una notable simplicidad desde una consola web única.
- Fácil de configurar. Plataforma cruzada de administración de endpoints desde una vista unificada.

Funcionalidades EDR únicas

- Doce meses de retención de datos y sandboxing físico en tiempo real para evitar acciones de hackers inadvertidas.
- Servicio de Zero-Trust Application: cada proceso se clasifica en función del comportamiento dinámico. Servicio de Threat Hunting: detección de hackers e intrusos.

MODELO ZERO-TRUST: UNA PROTECCIÓN EN CAPAS

La plataforma de seguridad de endpoints de WatchGuard no utiliza una única tecnología. Implementamos varias tecnologías juntas para reducir las posibilidades de que una amenaza se convierta en un ataque. Al trabajar de manera conjunta, estas tecnologías utilizan recursos del endpoint para minimizar el riesgo de una vulneración.

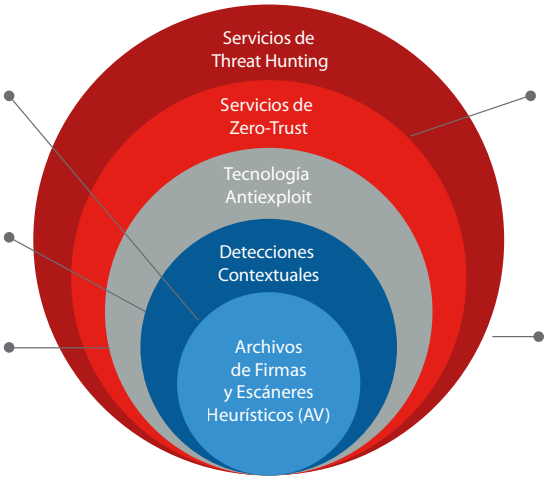
Modelo Zero-Trust: una protección en capas

CAPAS PARA ENDPOINTS:

Capa 1 - Archivos de Firmas y Tecnologías Heurísticas
Tecnología efectiva y optimizada para detectar ataques conocidos

Capa 2 - Detecciones Contextuales
Nos permiten detectar ataques sin malware y sin archivos

Capa 3 - Tecnología Antiexploit
Nos permite detectar ataques sin archivos diseñados para aprovechar vulnerabilidades



CAPAS NATIVAS DE LA NUBE

Capa 4 - Servicio de Zero-Trust de Aplicaciones
Ofrece detección en caso de que una capa anterior sea una vulnerabilidad, detiene los ataques a computadoras ya infectadas y los ataques de movimiento lateral dentro de la red

Capa 5 - Servicio de Threat Hunting
Detecte endpoints comprometidos, ataques en etapa inicial y actividades sospechosas, e identifique IoA que minimicen el tiempo de detección y respuesta (MTTD y MTTR).

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

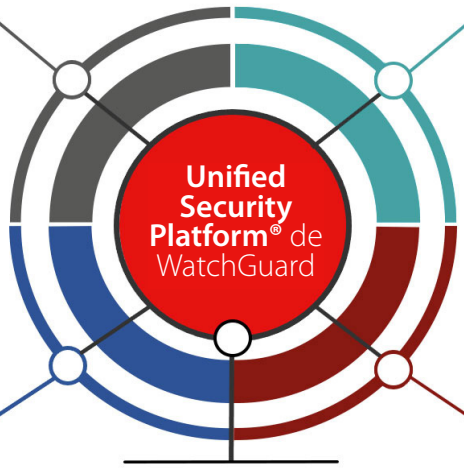
Unified Security Platform® de WatchGuard es una plataforma única que permite mejorar la seguridad moderna. Nuestro enfoque de plataforma lo ayuda a ofrecer servicios de seguridad poderosos para cada vector de amenazas con mayor escala y velocidad, a la vez que respalda eficiencias operativas y una mayor rentabilidad.

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

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

Requisitos de plataformas y sistemas compatibles con WatchGuard EPDR

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, Safari y Microsoft Edge.

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