

WATCHGUARD ADVANCED EPDR



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. ¿Qué tipos de desafíos enfrentan los equipos de seguridad cuando adoptan soluciones de seguridad de endpoint?

- **Amenazas sofisticadas de evolución constante:** Las prácticas de seguridad proactivas efectivas 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. La automatización de la seguridad aumenta la efectividad.
- **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.

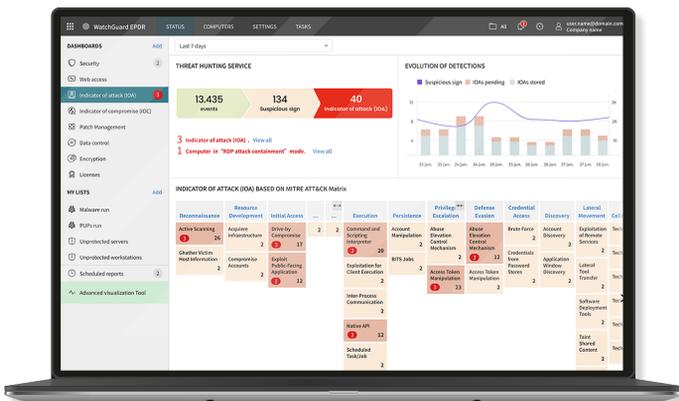
Las técnicas tradicionales de protección de endpoints, enfocadas en la prevención, son válidas para amenazas conocidas y comportamientos maliciosos, pero no son suficientes contra las amenazas cibernéticas sofisticadas y desconocidas.

CIBERSEGURIDAD PROACTIVA COMPLETA CONTRA AMENAZAS EN CONSTANTE EVOLUCIÓN

WatchGuard Advanced 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 Advanced 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.

Tecnologías Preventivas Tradicionales

- Firewall personal o administrado (IDS)
- Control de dispositivos
- Inteligencia colectiva
- 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 (Anti-phishing)
- Protección contra alteraciones
- Corrección automática y capacidad de reversión
- Recupere archivos cifrados con Shadow copies

Tecnologías de Seguridad Avanzadas

- Supervisión continua de endpoints con EDR
- Monitorización continua del riesgo en los endpoints
- Aprendizaje basado en la nube que clasifica el 100% de los procesos (APT, ransomware, rootkits, etc.)
- Sandboxing en entornos reales
- Threat hunting, con análisis de comportamiento para la detección de LotL (técnicas living-off-the-land)
- Indicadores de ataques asociados al marco de MITRE ATT&CK
- Antiexploit. Detección y prevención de ataques de RDP
- Contención y corrección: aislamiento y bloqueo de programas
- Investigación y respuesta: acceso remoto a los endpoints
- Búsqueda de Indicadores de Compromiso (IoCs) con STIX 2.0
- Las políticas de seguridad mejoradas permiten proteger a los endpoints contra la ejecución de técnicas de ataque comunes

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.
- No es necesario instalar, configurar ni mantener ninguna infraestructura de administración.
- Reduce el riesgo de seguridad prohibiendo la ejecución de técnicas LotL comunes.

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.
- Ofrece un diseño de interfaz de usuario nuevo y visible que puede dominarse rápidamente.
- Administración centralizada de búsqueda de IoC en todos los endpoints.

Funcionalidades de EDR Automatizadas

- Detecta y bloquea técnicas, tácticas y procedimientos de ataques informáticos y la actividad maliciosa en la memoria (exploits) antes de que puedan causar daño.
- Resolución y respuesta: información forense para investigar a fondo cada intento de ataque y herramientas para mitigar sus efectos (desinfección).
- Capacidad de rastrear cada acción: funcionalidades prácticas de visibilidad del atacante y su actividad, lo que facilita la investigación forense.

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.

CAPAS PARA ENDPOINTS:

Capa 1/ Políticas de Seguridad Mejoradas

Tecnología efectiva y optimizada para detectar ataques conocidos

Capa 2 / Archivos de Firmas, Tecnologías Heurísticas y Búsquedas de IoC

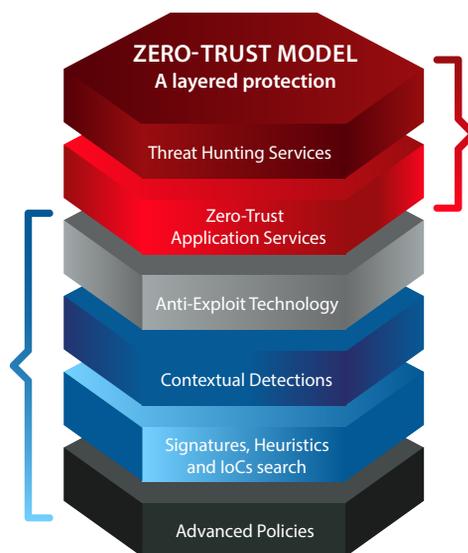
Tecnología efectiva y optimizada para detectar ataques conocidos

Capa 3 - Detecciones Contextuales

Nos permiten detectar ataques sin malware y sin archivos

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 de Aplicaciones

Clasifica el 100% de los procesos antes de que se ejecuten, denegando cualquier ejecución hasta que se certifique como de confianza

Capa 6 / Servicio de Threat Hunting

Nos permite detectar endpoints comprometidos, ataques en etapas iniciales, actividades sospechosas y la detección de IoA

Las **Políticas de Seguridad Mejoradas** permiten a los profesionales de seguridad supervisar o proteger endpoints contra la ejecución de scripts sospechosos y técnicas de ataque comunes utilizadas por amenazas sofisticadas (PowerShell, scripts desconocidos, documentos con macros, etc.)

Los **archivos de firmas y las tecnologías heurísticas**, conocidas como protección de endpoint tradicional (EPP), conforman una capa de tecnología de antivirus de última generación que ha probado ser efectiva contra muchas amenazas comunes de bajo nivel y bloqueos de URL maliciosos.

La **detección contextual** es muy eficaz contra ataques basados en scripts, ataques con uso de herramientas de sistema operativo de goodware, como PowerShell, WMI, etc.; vulnerabilidades de navegadores web, y otras aplicaciones a las que se dirigen los ataques con frecuencia, como Java, Adobe, entre otras.

La **capacidad de búsqueda de IoC** permite a los equipos de seguridad detectar rápidamente incidentes divulgados de manera reciente, así como encontrar endpoints afectados en un análisis

forense. Compatibilidad con diferentes tipos de indicadores: MD5/SHA256, nombre de archivo/ruta, dominio/IPv6/IPv4 y reglas de Yara.

La **tecnología antiexploit** permite buscar y detectar comportamientos anómalos. Cumple una función crítica en endpoints sin revisión o con revisiones por implementar y en endpoints con sistemas operativos que ya no son compatibles.

El **Servicio de Zero-Trust Application** clasifica el 100% de los procesos y prohíbe de manera predeterminada cualquier ejecución hasta que esté certificada como confiable. No hay necesidad de clasificar manualmente las amenazas ni de delegarlas a administradores de seguridad.

El **Servicio de Threat Hunting** se basa en un conjunto de reglas de búsqueda de amenazas, creado por especialistas en ciberseguridad, que se procesan de manera automática en todos los datos recolectados a partir de la telemetría, lo que identifica indicadores de ataque (IoA) que minimizan el tiempo de detección y respuesta (MTTD y el MTTR).

Requisitos de plataformas y sistemas compatibles con la plataforma de seguridad de endpoints de WatchGuard:

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](#), [Internet Explorer](#), [Microsoft Edge](#) y [Opera](#)