RESUMEN DEL SERVICIO

WatchGuard Total MDR

WatchGuard Total MDR es un servicio de detección y respuesta de amenazas totalmente administrado las 24 horas del día, los 7 días de la semana, que unifica la pila de seguridad de WatchGuard (punto final, firewall, identidad y red), además de entornos de nube de terceros seleccionados como Microsoft 365, Azure, AWS CloudTrail y Google Workspace. Cuenta con la tecnología de automatización impulsada por IA y con detectores de amenazas expertos, por lo que ofrece una detección más rápida, menos falsos positivos y una respuesta coordinada desde un solo portal.

¿Por qué Debería Considerar MDR?

Las organizaciones se ven abrumadas por tantas herramientas, tanto ruido y tan poco personal para administrar todo. Las amenazas impactan más rápido en entornos híbridos y la mayoría de las empresas más pequeñas no cuentan con los recursos necesarios para operar su propio SOC 24/7. Como resultado, la fatiga de alerta se establece, las señales se pierden y las infracciones se vuelven más probables y más costosas. WatchGuard Total MDR reúne todo para que pueda ofrecer una protección completa y siempre activa sin la carga de construir o dotar de personal a un SOC.

La detección y respuesta total de amenazas de MDR incluye:

Criterios de valoración:
WatchGuard EDR, EPDR, AEPDR

Firewall:
WatchGuard Firebox

Identidad:
AuthPoint

Red:
ThreatSync+ NDR

Nube:
Microsoft 365/Azure, AWS CloudTrail, Google Workspace

Beneficios de las Funciones Clave

Visibilidad unificada de amenazas

> Obtenga una vista completa de su postura de seguridad en un solo lugar. WatchGuard Total MDR reúne datos de entornos de punto final, firewall, identidad, red y nube en un portal único y fácil de usar. No más saltos entre herramientas o perder el panorama general, solo una visión clara y centralizada para detectar y actuar más rápido ante las amenazas.

Cobertura SOC 24/7

> Nuestros analistas de seguridad expertos supervisan, investigan y responden a las amenazas las 24 horas del día, para que usted no tenga que hacerlo. Ya sea a las 2 p.m. o a las 2 a.m., el SOC de WatchGuard está trabajando activamente para proteger a las organizaciones sin el costo o la complejidad de crear un SOC interno.

Detección impulsada por IA

> El aprendizaje automático analiza constantemente miles de señales para detectar actividades sospechosas en tiempo real. Elimina el ruido de alerta, detecta anomalías y se adapta a las nuevas amenazas más rápido que las herramientas tradicionales basadas en reglas, lo que brinda una mejor protección con menos esfuerzo manual.

Respuesta activa rápida

> Con un tiempo de respuesta promedio de menos de seis minutos, las amenazas se detienen antes de que se propaguen. WatchGuard Total MDR aísla los dispositivos comprometidos, contiene archivos maliciosos y escala los incidentes solo cuando es necesario para que los equipos se centren en lo que importa, no en las alertas.

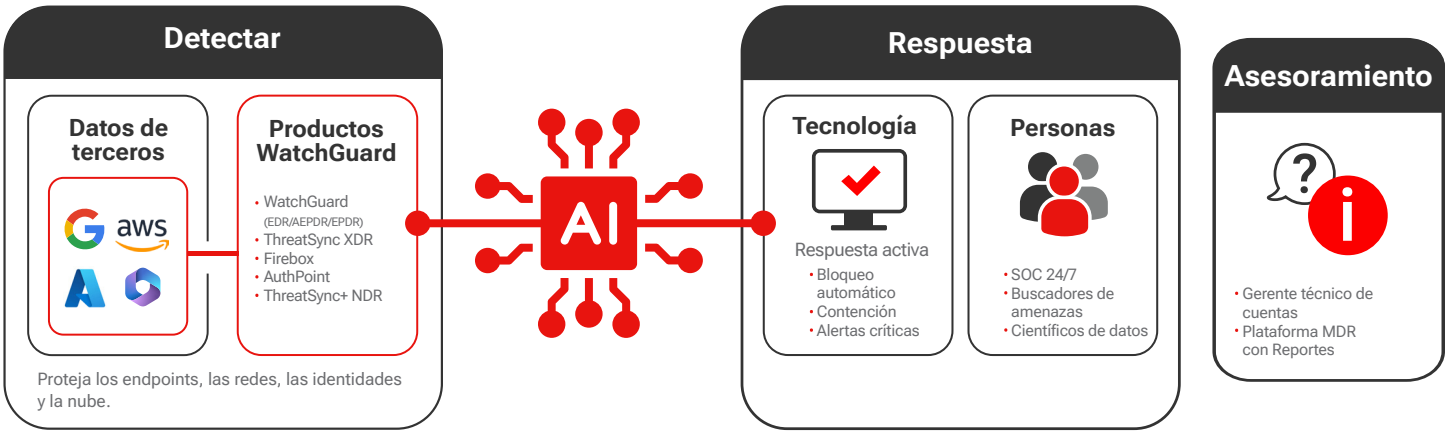
Alta fidelidad, bajo nivel de ruido

> WatchGuard Total MDR entrega menos de un falso positivo por mes en promedio. Eso significa que recibe alertas de alta confianza con planes de acción claros, lo que reduce la fatiga de las alertas, genera confianza y le ayuda a responder de manera decisiva cuando es importante.

Equipo de asistencia experto

> Los gerentes técnicos de cuentas (TAM) brindan orientación continua sobre seguridad, información sobre amenazas y soporte para la escalada. Ayudan a dar sentido a la actividad compleja, las tendencias de la superficie y recomiendan mejoras para fortalecer la protección a lo largo del tiempo.

Información General del Servicio Total MDR



Asegure la superficie de ataque completa

Protección de punto final
Los puntos finales son un objetivo principal para el ransomware, la suplantación de identidad y los ataques sin archivos. Total MDR utiliza WatchGuard EDR, EPDR, AEPDR para detectar comportamientos como el robo de credenciales y la escalada de privilegios, luego aísla los dispositivos comprometidos, detiene los procesos maliciosos y permite la respuesta en vivo de los analistas antes de que el malware pueda propagarse lateralmente y escalar.

Protección de identidad
Total MDR se integra con AuthPoint de WatchGuard para detectar y responder a actividades sospechosas, como anomalías en el inicio de sesión, tormentas de inicio de sesión fallidas o creación de cuentas fraudulentas. Al deshabilitar las cuentas comprometidas en tiempo real, impide que los atacantes se hagan pasar por usuarios o accedan a plataformas en la nube sin ser detectados.

Protección de redes
Los ataques que eluden los puntos finales, como el movimiento lateral, los escaneos de puertos o el tráfico C2, se identifican a través de Firebox y NDR. Total MDR responde instantáneamente bloqueando IP maliciosas, cerrando puertos o deteniendo la exfiltración de datos, protegiendo los sistemas internos de amenazas furtivas.

Protección en la nube
Total MDR monitorea Microsoft 365 y otras plataformas en la nube en busca de signos de compromiso, incluidos inicios de sesión sospechosos, cambios de permisos y acceso a buzones de correo.

Métricas que importan

<1 falso positivo al mes

Promedio de 6 alertas por mes

6 minutos de tiempo medio para la primera respuesta

10 milisegundos para contener automáticamente las amenazas

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