HOJA DE DATOS

WATCHGUARD EPDR

Endpoint Protection, Detection and Response.

CIBERSEGURIDAD DE LA ORGANIZACIÓN

La movilidad, el procesamiento y el trabajo remoto han revolucionado el entorno empresarial. Los endpoints son el objetivo principal de la mayoría de los ataques cibernéticos. Es por eso que las soluciones de seguridad de endpoints deben ser avanzadas, adaptables y automáticas, con los máximos niveles posibles de prevención, detección y respuesta.

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.

LA SOFISTICACIÓN DE LOS ATAQUES INFORMÁTICOS

Defensa Cibernética Contra Amenazas Avanzadas

Los ataques cibernéticos de avanzada están diseñados para evadir la protección que proporcionan las soluciones de seguridad tradicionales. Estos ataques se están volviendo más frecuentes y más sofisticados a medida que los hackers se vuelven más profesionales. También son el resultado de la falta de enfoque en la corrección de las vulnerabilidades de seguridad en los sistemas.

En este contexto, las plataformas de protección tradicionales (EPP) no son suficientes. Esto se debe a que no proporcionan suficiente visibilidad detallada de los procesos y las aplicaciones que se ejecutan en las redes corporativas. Además, algunas soluciones de EDR, lejos de resolver los problemas, generan mayor estrés y aumentan la carga de trabajo de los administradores de seguridad, ya que delegan la responsabilidad de administrar alertas y los obligan a clasificar las amenazas manualmente.

WATCHGUARD EPDR

Detección y Búsqueda Proactivas de Amenazas

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, tanto presentes como futuros, dentro y fuera de la red corporativa.

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

- Servicio de Confianza Cero de Aplicaciones: clasificación del 100% de las aplicaciones
- Servicio de Búsqueda de Amenazas: detección de hackers e intrusos

Gracias a su arquitectura basada en la nube, el agente es liviano y tiene poco impacto en los endpoints, que se administran a través de WatchGuard Cloud. WatchGuard Cloud le permite administrar todo el portafolio desde una vista única, reducir los costos de infraestructura y minimizar el tiempo invertido en la generación de reportes y en tareas operativas.

BENEFICIOS

Simplifica y Minimiza los Costos de Seguridad

- Sus servicios administrados reducen los costos de personal especializado. No hay falsas alertas que administrar y no se delegan responsabilidades.
- Los servicios administrados aprenden sobre las amenazas de manera automática. No se pierde tiempo en configuraciones manuales.
- No es necesario instalar, configurar ni mantener ninguna infraestructura de administración.
- El rendimiento del endpoint no se ve afectado, ya que se basa en un agente liviano y en arquitectura nativa de la nube.

Automatiza y Reduce el Tiempo de Detección

- Bloquea aplicaciones que representan un riesgo de seguridad (por hash o nombre de proceso).
- Bloquea la ejecución de amenazas, malware de día cero, ataques sin archivos/sin malware, ransomware y suplantación de identidad.
- Detecta y bloquea la actividad maliciosa en la memoria (vulnerabilidades) antes de que pueda causar daño.
- Detecta y bloquea técnicas, tácticas y procedimientos de ataque.

Automatiza y Reduce el Tiempo de Respuesta e Investigación

- 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.
- Mejora y ajuste de políticas de seguridad gracias a las conclusiones del análisis forense.

SEGURIDAD AVANZADA Y AUTOMATIZADA DE ENDPOINTS

Las técnicas de protección tradicional (EPP), enfocadas en la prevención, son medidas de bajo costo que resultan válidas para amenazas conocidas y comportamientos maliciosos, pero no son suficientes. Para defender correctamente una organización y lograr que las amenazas cibernéticas lleguen a su fin, es necesario alejarse de la prevención tradicional y virar hacia la prevención, la detección y la respuesta continuas, asumiendo en todo momento que la organización está en peligro y que todos los endpoints sufren la amenaza constante de los atacantes.

WatchGuard EPDR integra tecnologías preventivas tradicionales con tecnologías innovadoras y adaptativas de prevención, detección y respuesta en una solución única a fin de lidiar con las amenazas cibernéticas avanzadas, tanto presentes como futuras:

Tecnologías Preventivas Tradicionales

- Firewall personal o administrado (IDS)
- Control de dispositivos
- Antimalware permanente multivectorial y análisis a pedido
- Lista de denegación/lista de permitidos administradas
- Inteligencia colectiva
- Heurística previa a la ejecución
- Filtrado de URL y navegación web
- Protección contra suplantación de identidad
- Protección contra alteraciones
- Corrección y reversión

Tecnologías de Seguridad Avanzadas

- Supervisión continua de endpoints con EDR
- Prevención de la ejecución de procesos desconocidos
- Aprendizaje basado en la nube que clasifica el 100% de los procesos (APT, ransomware, rootkits, etc.)
- Sandboxing en entornos reales
- Análisis del comportamiento y detección de indicadores de ataques (IoA), como scripts, macros, etc.
- Búsqueda de amenazas
- Aislamiento de computadoras
- Bloqueo de programa por hash o nombre
- Vista de gráficos de actividad de ataques

MODELO DE CONFIANZA CERO

El Servicio de Confianza Cero de Aplicaciones clasifica el 100% de los procesos, supervisa la actividad de endpoints y bloquea la ejecución de aplicaciones y procesos maliciosos. Para cada ejecución, se envía en tiempo real un veredicto de clasificación de "malicioso" o "legítimo", sin incertidumbre y sin delegar al cliente, lo que evita procesos manuales. Todo esto es posible gracias a la capacidad, la velocidad, la capacidad de adaptación y la escalabilidad de la IA y el procesamiento en la nube.

El servicio unifica tecnología de big data y técnicas de aprendizaje automático multinivel, como el aprendizaje profundo, los resultados de la supervisión continua y la automatización de la experiencia y del conocimiento acumulados por el equipo de amenazas de WatchGuard.

El servicio de búsqueda de amenazas administrado está a cargo de un equipo de expertos que usan herramientas de correlación de eventos de análisis y elaboración de perfiles para detectar de manera proactiva nuevas técnicas de ataques y evasión. Los cazadores de WatchGuard trabajan con la premisa de que las organizaciones están en constante peligro.

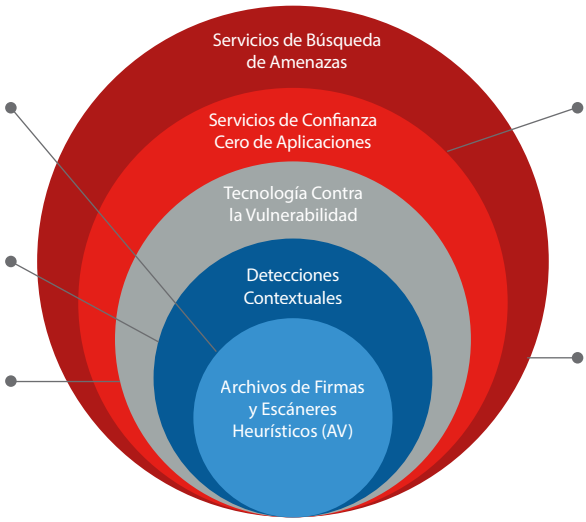
Modelo de Confianza Cero: una protección en capas

CAPAS DE 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 Contra Vulnerabilidades
Nos permite detectar ataques sin archivos diseñados para aprovechar vulnerabilidades



CAPAS NATIVAS DE LA NUBE

Capa 4 - Servicio de Confianza Cero 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 Búsqueda de Amenazas
Nos permite detectar endpoints comprometidos, ataques en etapas iniciales y actividades sospechosas

Requisitos de plataformas y sistemas compatibles con WatchGuard EPDR

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

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