HOJA DE DATOS

WatchGuard Endpoint Security Basic

Protección de EDR Moderna. Sin Complicaciones.

Hoy en día, es fundamental que las organizaciones cuenten con una sólida protección de los endpoints. Las herramientas antivirus tradicionales ya no son suficientes para detener los ciberataques modernos, sin embargo, muchas plataformas avanzadas de detección y respuesta de endpoints (EDR) son complejas, requieren muchos recursos y son difíciles de administrar.

WatchGuard Endpoint Security Basic cambia eso al ofrecer una protección de EDR moderna impulsada por IA con una administración mínima. Creado para organizaciones que necesitan protección confiable con baja complejidad, combina la detección de comportamiento, la protección contra ransomware y la reducción de la superficie de ataque en una solución ligera y administrada en la nube.

Con clasificación automatizada, bajo nivel de ruido de alerta y administración centralizada de la nube, Endpoint Security Basic protege a los usuarios, dispositivos y datos sin necesidad de un ajuste constante o experiencia en seguridad dedicada.

Protección Fuerte sin Complejidad

WatchGuard entiende que muchas organizaciones simplemente necesitan una seguridad confiable que proteja a los usuarios y dispositivos sin necesidad de un equipo de seguridad dedicado.

Diseñado para organizaciones que necesitan una protección sólida sin gastos operativos, Endpoint Security Basic combina la prevención inteligente de malware, la protección contra ransomware y los controles de reducción de la superficie de ataque en una solución ligera y gestionada en la nube. Con monitoreo de seguridad en tiempo real y menor ruido operativo, detiene los ataques temprano sin ajuste constante o intervención manual.

Endpoint Security Basic ofrece protección moderna para endpoints mediante tecnologías de prevención impulsadas por IA que identifican y bloquean automáticamente el malware, el ransomware, los scripts maliciosos y las amenazas emergentes, así como los ataques sin archivos y las técnicas living-off-the-land. La protección antiphishing incorporada, el control de dispositivos y el filtrado de URL ayudan a reducir los puntos de entrada de ataques comunes antes de que las amenazas puedan afianzarse.

Debido a que la solución se entrega a través de una plataforma centralizada nativa de la nube, los equipos pueden implementar fácilmente políticas, monitorear la postura de seguridad y administrar la protección en todos los endpoints desde una sola consola. El resultado es una protección confiable que detiene las amenazas temprano mientras mantiene bajos los gastos operativos.

Endpoint Security Basic incluye capacidades modernas de prevención y detección diseñadas para detener los ataques de manera temprana.

Reducción de la Superficie de Ataque

- Panel de control de riesgos de endpoints personalizable
- Detección de endpoints no administrada
- Evaluación de vulnerabilidad

Tecnologías de Prevención Integradas

- Firewall, IDS y control de dispositivos
- Protección contra múltiples vectores de ataque (web, correo electrónico, red, dispositivos)
- Inteligencia Colectiva
- Detecciones impulsadas por IA que identifican y bloquean instaladores y scripts maliciosos
- Protección contra suplantación de identidad
- Antimalware y análisis a pedido
- Filtrado de URL y navegación web

Capacidades de Detección y Respuesta

- Supervisión continua del endpoint
- Detecciones impulsadas por IA
- Detección contextualizada de comportamiento
- Bloquea automáticamente los intentos de aprovechar las vulnerabilidades en los procesos activos en el dispositivo
- Supervisión de riesgos de los endpoints
- Integración de ThreatSync (XDR) para mayor visibilidad
- Historia de ataque de incidente automatizado
- Recuperación de archivos cifrados (copias ocultas).

Protección Confiable.
Operaciones Silenciosas.

Seguridad que se Configura Una Sola Vez

Endpoint Security Basic está diseñado para funcionar silenciosamente en segundo plano. La clasificación impulsada por IA analiza automáticamente la actividad y determina si es segura o maliciosa, eliminando la necesidad de ajuste o investigación constantes.

Este enfoque «de diseño silencioso" reduce drásticamente la fatiga de alerta y los gastos operativos, lo que permite a los equipos mantener una fuerte protección sin dedicar tiempo a la supervisión continua.

Control Centralizado de Dispositivos

Detiene el malware y las filtraciones de información, ya que bloquea categorías completas de dispositivos (unidades flash, módems USB, cámaras web, DVD/CD, etc.), clasifica dispositivos en listas blancas o configura permisos de acceso de solo lectura, solo escritura y lectura y escritura.

Supervisión de Riesgos de los Endpoints

Administre y supervise los endpoints desprotegidos, las configuraciones incorrectas de seguridad, los sistemas operativos y las vulnerabilidades de software de terceros, y los parches faltantes para proteger proactivamente su red antes de que se presente una vulneración.

Protección contra Malware y Ransomware

Endpoint Security Basic analiza comportamientos y técnicas de hacking para detectar y bloquear malware conocido y desconocido, incluyendo ransomware, troyanos y phishing.

Supervisión y Reportes en Tiempo Real

Ofrece supervisión de seguridad detallada y en tiempo real a través de paneles de control integrales y gráficos fáciles de interpretar. Se generan y entregan de manera automática reportes sobre el estado de protección, las detecciones y el uso inadecuado de dispositivos.

Reducción de la Superficie de Ataque Integrada

Muchas infracciones exitosas comienzan con vulnerabilidades sin parches, aplicaciones no autorizadas o acceso web inseguro.

Endpoint Security Basic ayuda a reducir estos riesgos a través de la evaluación integrada de vulnerabilidades, el control de dispositivos y las políticas de filtrado de URL que limitan de forma proactiva la exposición a técnicas de ataque comunes.

Evaluación de Vulnerabilidad

La evaluación de vulnerabilidad es un proceso crítico que ayuda a los equipos de TI a identificar, evaluar y priorizar las debilidades y vulnerabilidades de seguridad en aplicaciones y sistemas. Comprenda e identifique posibles amenazas, y tome medidas proactivas para mitigarlas antes de que los atacantes las aprovechen.

Simplicidad Nativa de la Nube

Endpoint Security Basic se administra a través de la plataforma de administración nativa de la nube de WatchGuard, que proporciona políticas centralizadas, paneles e informes en todos los endpoints. Esta consola unificada simplifica las operaciones, reduce los gastos generales de administración y permite a las organizaciones proteger a las fuerzas de trabajo distribuidas desde cualquier lugar.

Acerca de WatchGuard

WatchGuard Technologies es líder mundial en ciberseguridad unificada y diseñada para proveedores de servicios administrados (MSP). Desde hace más de 30 años, WatchGuard define la manera en que los MSP ofrecen seguridad a escala e innova continuamente para mantenerse a la vanguardia de cada cambio importante en el panorama de las amenazas. La Unified Security Platform® de WatchGuard, impulsada por IA, ofrece protección de identidades, endpoints y redes alineada con Zero Trust en una plataforma única e integrada, lo que permite a los MSP reducir la complejidad operativa, mejorar los resultados de seguridad y hacer crecer sus negocios de manera más eficiente. Gracias a la confianza de más de 25.000 MSP que protegen a más de 1,5 millones de clientes en todo el mundo, WatchGuard permite a los partners ofrecer resultados de seguridad sólidos y medibles para clientes de todo el mundo. Obtenga más información en WatchGuard.com/es.

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