Endpoint Security LATAM

Heimdal Next-Gen Antivirus & Firewall

TABLA DE CONTENIDO

¿Qué es Heimdal Next-Gen Antivirus & Firewall?

Beneficios clave

Características principales

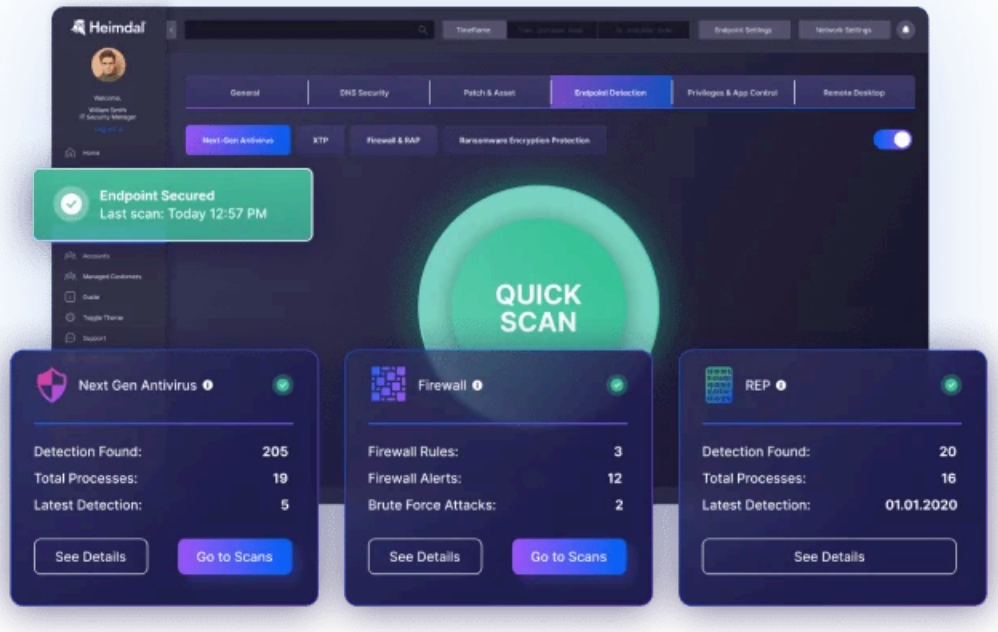
- Motor de escaneo multi-etapa
- Extended Threat Protection (XTP)
- Remote Access Protection (RAP)
- Prevención y contención autónomas

Tabla completa de funciones

Unifique su stack de seguridad

Heimdal Next-Gen Antivirus & Firewall (antes Next-Gen Antivirus & MDM) es la protección endpoint avanzada de Heimdal: antivirus multicapa, prevención de exploits y análisis de comportamiento, combinados con protección inteligente del acceso remoto, en un solo agente ligero.

 © 2026 antivirusthor.com



Dashboard del agente Heimdal: Next-Gen Antivirus, Firewall y REP

¿Qué es Heimdal Next-Gen Antivirus & Firewall?

Es una defensa 24x7 en todas las capas del endpoint: detección avanzada, bloqueo en tiempo real y visibilidad profunda sobre las amenazas, protegiendo la infraestructura frente a malware, ransomware y ataques fileless.

Beneficios clave

- **Protección avanzada contra amenazas:** defensas potentes frente a malware, ransomware y ataques sin archivos (fileless), diseñada para las amenazas actuales.
- **Mitigación de precisión con XTP:** la capa Extended Threat Protection, enriquecida con telemetría, detecta comportamiento sigiloso, analiza el riesgo entre usuarios y dispositivos y bloquea las amenazas antes de que escalen.
- **Remote Access Protection (RAP):** la mayoría de las brechas empiezan con un inicio de sesión, no con un archivo. RAP protege frente a fuerza bruta, credenciales robadas y sesiones remotas no autorizadas.

Características principales

Motor de escaneo multi-etapa

Detecta y bloquea amenazas conocidas, desconocidas y emergentes mediante tres capas de escaneo:

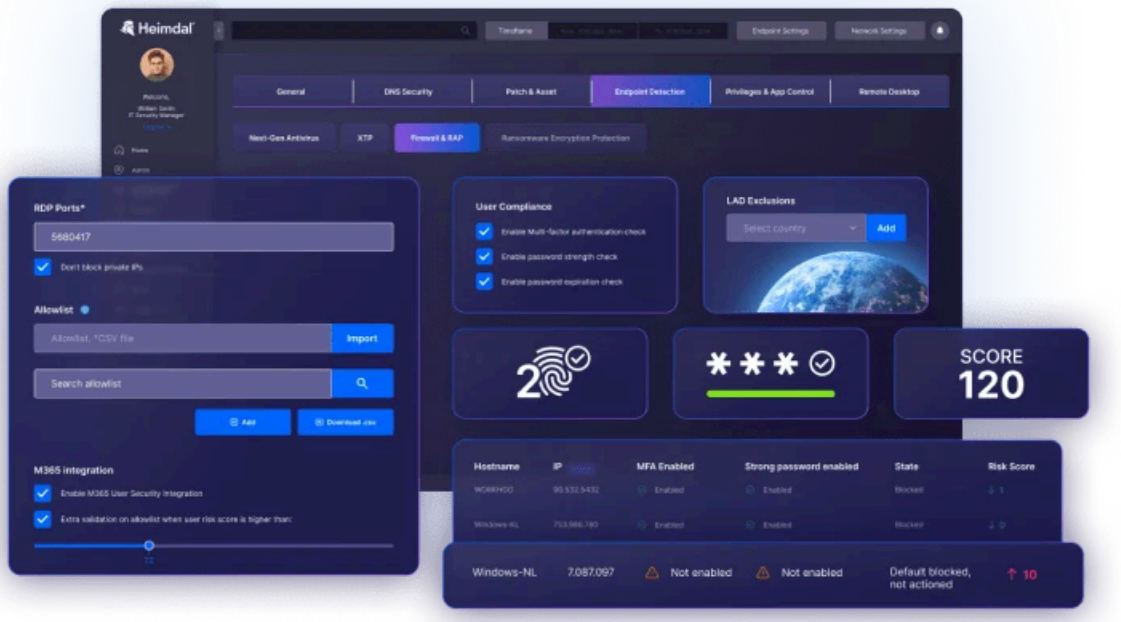
- Análisis estático para amenazas basadas en firmas
- Escaneo de comportamiento para anomalías en tiempo real
- Consulta en la nube (cloud lookup) para veredictos instantáneos con telemetría global

Extended Threat Protection (XTP)

El motor XTP refuerza la defensa del endpoint detectando amenazas según el comportamiento real de los ataques. Mapeado a las técnicas de MITRE ATT&CK, descubre acciones sospechosas como credential dumping, movimiento lateral y ejecución remota, rastreando anomalías entre usuarios, dispositivos y aplicaciones para una respuesta rápida y precisa.

Remote Access Protection (RAP)

Frena el abuso del acceso remoto antes de que empiece: inspecciona cada intento de inicio de sesión en tiempo real y bloquea los accesos no autorizados según ubicación, anomalías de sesión y riesgo del usuario, tanto si la amenaza viene de puertos expuestos como de consolas remotas o aplicaciones mal utilizadas.



Configuración de Firewall y RAP en Heimdal Next-Gen Antivirus & Firewall

Prevención y contención autónomas

Neutraliza las amenazas automáticamente, sin intervención manual: desde detectar payloads maliciosos hasta aislar sistemas infectados y detener sesiones remotas, actuando al instante en cada fase del ataque. Cada endpoint se convierte en un activo que se defiende solo.

Tabla completa de funciones

Función	Descripción
Escaneo local de archivos, firmas y registro	Escaneo de archivos y firmas en memoria, de bajo impacto y en tiempo real, junto a monitorización activa de cambios en el registro.
Escaneo en la nube en tiempo real	Los archivos desconocidos se envían a la nube de Heimdal para un escaneo adicional con algoritmos de machine learning sobre 1.000 núcleos de CPU.
Inspección en sandbox y backdoor	Los archivos que no figuran como malware se aíslan en el sandbox y se examinan en busca de comportamiento malicioso, cortando de raíz cualquier contacto con servidores C&C.
Escaneo de procesos basado en comportamiento	Motores heurísticos de IA que monitorizan los procesos en ejecución y detectan cambios de código a todos los niveles.
Extended Threat Protection (XTP)	Motor propietario que identifica ciberataques en fases tempranas mapeado a tácticas y técnicas MITRE ATT&CK, con árboles de proceso, mecanismos de ataque e inteligencia basada en evidencia; más de 2.000 reglas de detección curadas y 95% de cobertura de las técnicas específicas de Windows.
Remote Access Protection (RAP)	Bloqueo de ataques de fuerza bruta, credenciales robadas y herramientas remotas maliciosas, inspeccionando cada inicio de sesión en tiempo real según ubicación, anomalías de sesión y riesgo.
Prevención y contención autónomas	Neutralización automática de amenazas: detección de payloads, aislamiento de sistemas infectados y corte de sesiones remotas sin intervención manual.
Integración con Firewall y MDM	Motor antivirus con integración de firewall y capacidades de gestión de dispositivos móviles (MDM) en el mismo agente.

Unifique su stack de seguridad

NGAV, impulsado por el motor XTP, se integra con el resto de módulos Heimdal para conformar una solución robusta de Endpoint Detection and Response (EDR): detección, mitigación y defensa de

vanguardia gestionadas desde una plataforma unificada y un único agente para Windows, macOS y Linux.

¿Quiere verlo en funcionamiento? Solicite una demo o cotización de Next-Gen Antivirus & Firewall a través de Sogyo.