Endpoint Security LATAM

Heimdal DNS Security - Endpoint

TABLA DE CONTENIDO

¿Qué es Heimdal DNS Security - Endpoint?

Beneficios clave

Características principales

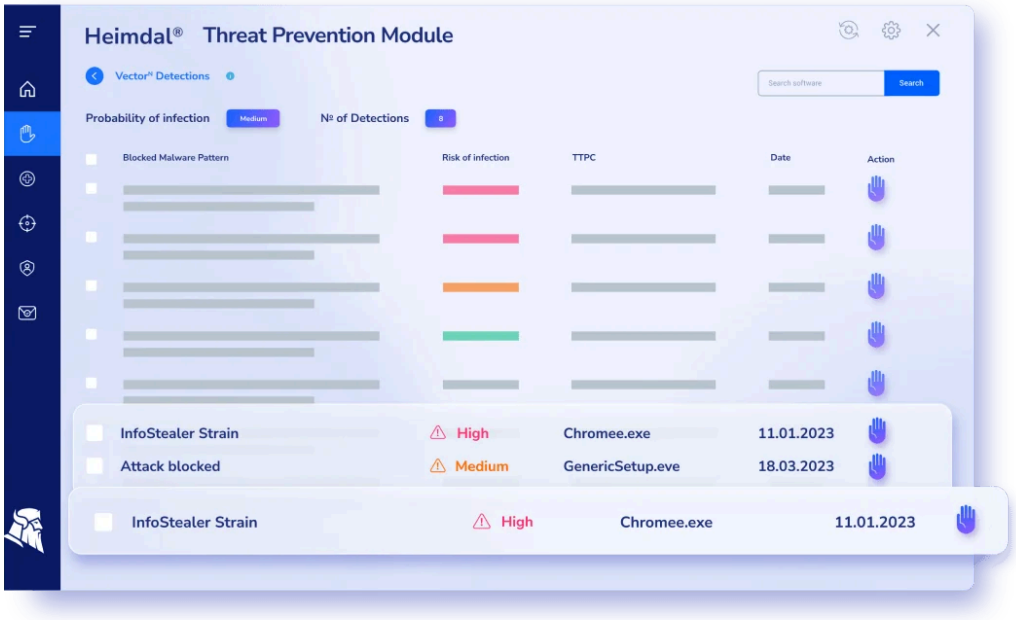
- True DNS over HTTPS Filtering
- Advanced Malware Detection
- Protección proactiva con capacidades CASB
- Compatibilidad cruzada

Tabla completa de funciones

Un solo agente, una plataforma unificada

Heimdal DNS Security - Endpoint (antes DarkLayer Guard Endpoint) es la capa de protección de tráfico a nivel endpoint de la plataforma Heimdal: analiza en tiempo real las comunicaciones DNS, HTTP y HTTPS de cada dispositivo y bloquea dominios infectados y la comunicación con infraestructuras de cibercrimen, con una huella mínima en el sistema.

 © 2026 antivirusthor.com



Panel de Heimdal DNS Security Endpoint: detecciones VectorN en el dashboard

¿Qué es Heimdal DNS Security - Endpoint?

Es una solución de seguridad DNS en la nube y local que combina inteligencia de cibercrimen, machine learning avanzado y prevención basada en IA. Protege a los usuarios —trabajen en la oficina o en remoto— frente a secuestro de DNS (hijacking), suplantación (spoofing), tunelización DNS y dominios maliciosos, sin comprometer el rendimiento del equipo.

Beneficios clave

- **Filtrado DNS, HTTP y HTTPS:** el 91% de las amenazas en línea aprovechan el DNS para explotar vulnerabilidades. La solución identifica amenazas emergentes y ocultas en todos los niveles de conexión, deteniendo ataques que suelen evadir los antivirus tradicionales.
- **Predictive DNS™:** tecnología patentada de Heimdal que predice amenazas futuras con un 96% de precisión mediante modelado con redes neuronales (patente EU P025966EP1 / US 18333620).
- **Threat hunting autónomo:** detecta URLs y procesos maliciosos y permite retroceder hasta el origen del atacante, con visibilidad y control total sobre los endpoints.
- **Despliegue rápido y compatible:** se instala en menos de una hora y funciona junto a cualquier antivirus, firewall o solución de seguridad existente.

Características principales

True DNS over HTTPS Filtering

Heimdal es el primer fabricante del mercado en integrar verdadero filtrado DNS sobre HTTPS en un producto, yendo más allá del simple reencaminamiento de paquetes DNS. Permite cazar amenazas que abusan de herramientas, aplicaciones o servicios cloud legítimos.

Advanced Malware Detection

Control total sobre las comunicaciones DNS, HTTP y HTTPS con inteligencia de amenazas computada por machine learning: pase de una detección antivirus tradicional a una postura de prevención y caza activa, sin necesidad de software de análisis adicional ni más analistas.

Protección proactiva con capacidades CASB

Detecte y erradique instancias de shadow IT, combata amenazas internas (insider threats) y neutralice actividad maliciosa vinculada a cuentas comprometidas.

Compatibilidad cruzada

Inteligencia de amenazas nativa de la nube que se integra con su ecosistema de seguridad actual y protege desde errores humanos simples hasta campañas de malware sofisticadas.

Tabla completa de funciones

Función	Descripción
Filtrado DNS, HTTP y HTTPS	Motor de filtrado de tráfico bidireccional (DarkLayer Guard®) con listas blancas/negras personalizables que bloquea exploits de hora cero, servidores C&C de ransomware y fugas de datos.
True DNS over HTTPS (DoH)	Primer producto del mercado con filtrado DoH real: cifra las consultas DNS dentro de la sesión HTTPS, mitigando ataques Man-in-the-Middle y DNS spoofing sin coste de rendimiento.
VectorN Detection®	Detección code-autonomous que rastrea la comunicación dispositivo-infraestructura y descubre malware de segunda generación invisible para antivirus y escáneres de código, con indicadores IOA/IOC.
Predictive DNS™	Algoritmo de IA y ML que predice que un dominio es malicioso antes de que aloje contenido, mediante redes neuronales y análisis lingüístico (96% de precisión; tecnología patentada).
Threat To Process Correlation (TTPC)	Correlaciona amenazas con procesos para identificar qué proceso del endpoint ha sido comprometido por el atacante.
Capacidades CASB	Detección de shadow IT, amenazas internas y actividad maliciosa vinculada a cuentas comprometidas.
Compatibilidad universal	100% compatible con las soluciones de seguridad existentes; se despliega en menos de una hora.

Un solo agente, una plataforma unificada

DNS Security - Endpoint se suma a cualquier antivirus o firewall y se combina con los demás módulos de Heimdal para conformar una postura completa de Endpoint Detection and Response (EDR): un solo agente ligero y una única consola de gestión para Windows, macOS y Linux.

¿Quiere verlo en funcionamiento? Solicite una demo o cotización de DNS Security - Endpoint a través de Sogyo.