Endpoint Security LATAM

Heimdal DNS Security - Network

TABLA DE CONTENIDO

¿Qué es Heimdal DNS Security - Network?

Beneficios clave

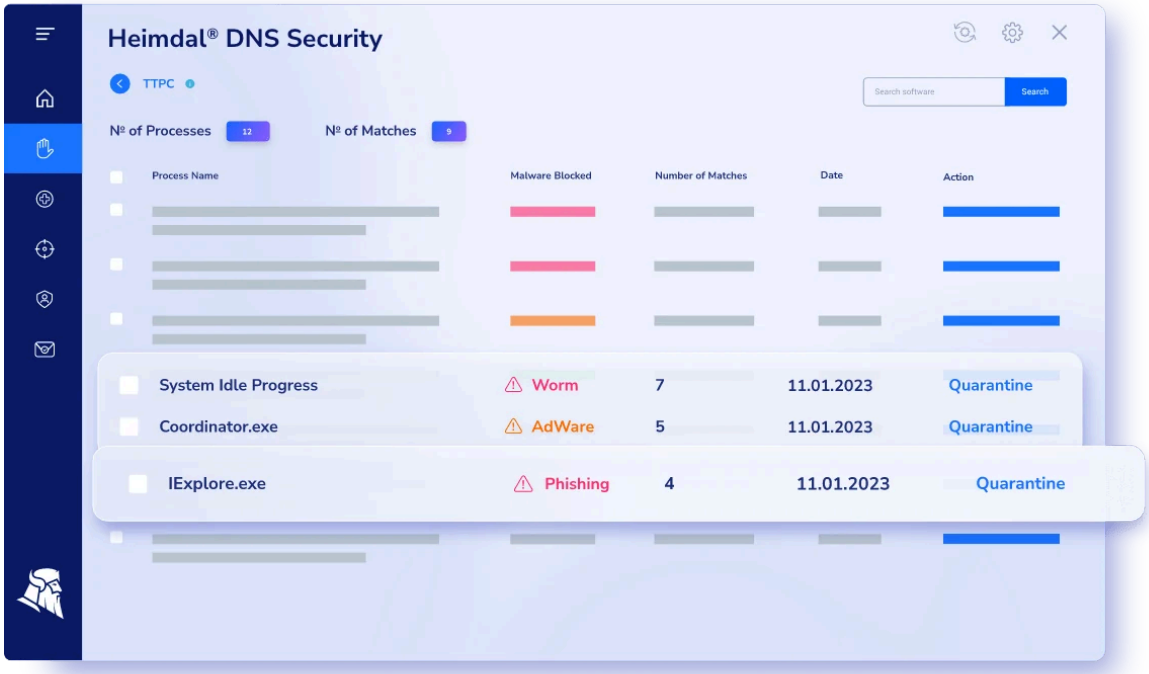
Características principales

- Capacidades completas de threat hunting
- Cobertura híbrida para cualquier entorno
- Detección y respuesta ilimitadas
- Predictive DNS™ para prevención avanzada

Tabla completa de funciones

Un solo agente, una plataforma unificada

Heimdal DNS Security - Network (antes DarkLayer Guard Network) añade una capa de protección con inteligencia artificial a toda la red de la empresa, permitiendo cazar, prevenir, detectar y responder a cualquier amenaza —por avanzada que sea— bajo una misma consola unificada.



Consola Heimdal DNS Security: tráfico TTPC y acciones de cuarentena

¿Qué es Heimdal DNS Security - Network?

Es la variante de DNS Security que protege el ecosistema completo, más allá de los endpoints gestionados: dispositivos BYOD, IoT y cualquier equipo conectado a la red corporativa. Su DNS híbrido permite securizar el tráfico localmente en cualquier servidor DNS, sin necesidad de reencaminar a los resolvers de Heimdal, ideal tanto para entornos on-prem como cloud.

Beneficios clave

- **Cobertura completa de dispositivos:** proteja y mantenga BYOD, IoT y todo el equipamiento vinculado a la red de su empresa.
- **Visibilidad granular de la red:** registro de tráfico (traffic logging) para saber qué hace cada dispositivo y prevenir ataques antes de que lleguen a los endpoints.
- **Threat hunting sin fricción:** se configura en segundos y no requiere instalación de software adicional.
- **Predictive DNS™:** 96% de precisión en la prevención de amenazas, anticipando ataques antes de que se materialicen (tecnología patentada).

Características principales

Capacidades completas de threat hunting

Potente sistema HIPS (Host-Based Intrusion Prevention System) aumentado con detección de amenazas inteligente basada en IA: análisis de comportamiento con machine learning combinado con filtrado de tráfico para un enfoque integrado de la seguridad de red.

Cobertura híbrida para cualquier entorno

Elimina el intermediario: añade capacidades de filtrado directamente a su red local y securiza el tráfico DNS entrante y saliente, tanto en entornos cloud como on-prem.

Detección y respuesta ilimitadas

Utiliza CASB (Cloud Access Security Brokerage) para aumentar la seguridad frente a actividades maliciosas, con granularidad ampliada sobre aplicaciones en la nube: identifique, clasifique y elimine aplicaciones no autorizadas de su entorno cloud.

Predictive DNS™ para prevención avanzada

Anticipación proactiva frente a amenazas de red e IoT con una precisión del 96%: cace, detecte y responda a ataques potenciales antes de que ocurran.

Tabla completa de funciones

Función	Descripción
Hybrid DNS	Añade filtrado avanzado a cualquier servidor DNS local sin reencaminar las consultas a los resolvers de Heimdal; admite cualquier forwarder DNS e IP dinámica, para entornos on-prem y cloud.
DNS recursivo de perímetro	Caza y detección de amenazas de red avanzadas, ejecutable en modos Activo y Pasivo (IDS).
Detección y bloqueo de amenazas web	Evaluación de más de 300.000 dominios al día; bloqueo de sitios con código malicioso y de servidores controlados por cibercrimen.
Bloqueo de callbacks C&C	Detección de malware y APT a nivel de red y corte de la comunicación con servidores de comando y control.
Prevención de fuga de datos	Detiene la exfiltración de datos a través de consultas DNS a dominios maliciosos (ransomware, APT).
VectorN Detection™	Machine learning aplicado a la comunicación dispositivo-infraestructura para revelar amenazas ocultas.
Listas personalizadas	Listas de bloqueo y permiso (block/allow) propias, con página de bloqueo personalizable opcional.
Estadísticas y forense avanzada	Estadísticas detalladas con direcciones IP internas y hostnames; estándar ITILv3 para incidentes que facilita el cumplimiento de ISO 27001/2.
Alertas multi-dispositivo	Alertas de infección por cada tipo de dispositivo: PCs, Macs, Android e iOS.
Servicio 100% alojado	Sin servidores ni software cliente; implementación en menos de 15 minutos, sin cambios de configuración ni reinicios; cobertura automática de todos los dispositivos de la red.

Un solo agente, una plataforma unificada

DNS Security - Network se suma a cualquier antivirus, firewall, IDS o IPS y se combina con otros productos Heimdal para ofrecer una auténtica postura de Endpoint Detection and Response (EDR), todo desde un agente y una plataforma unificados.

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