Endpoint Security LATAM

Heimdal Security - Portafolio de Productos

TABLA DE CONTENIDO

El portafolio de un vistazo

Network Security

- DNS Security - Network

Endpoint Security

- DNS Security - Endpoint
- Next-Gen Antivirus & Firewall
- REP X - Ransomware Encryption Protection

Vulnerability Management

- Patch & Asset Management

Privileged Access Management

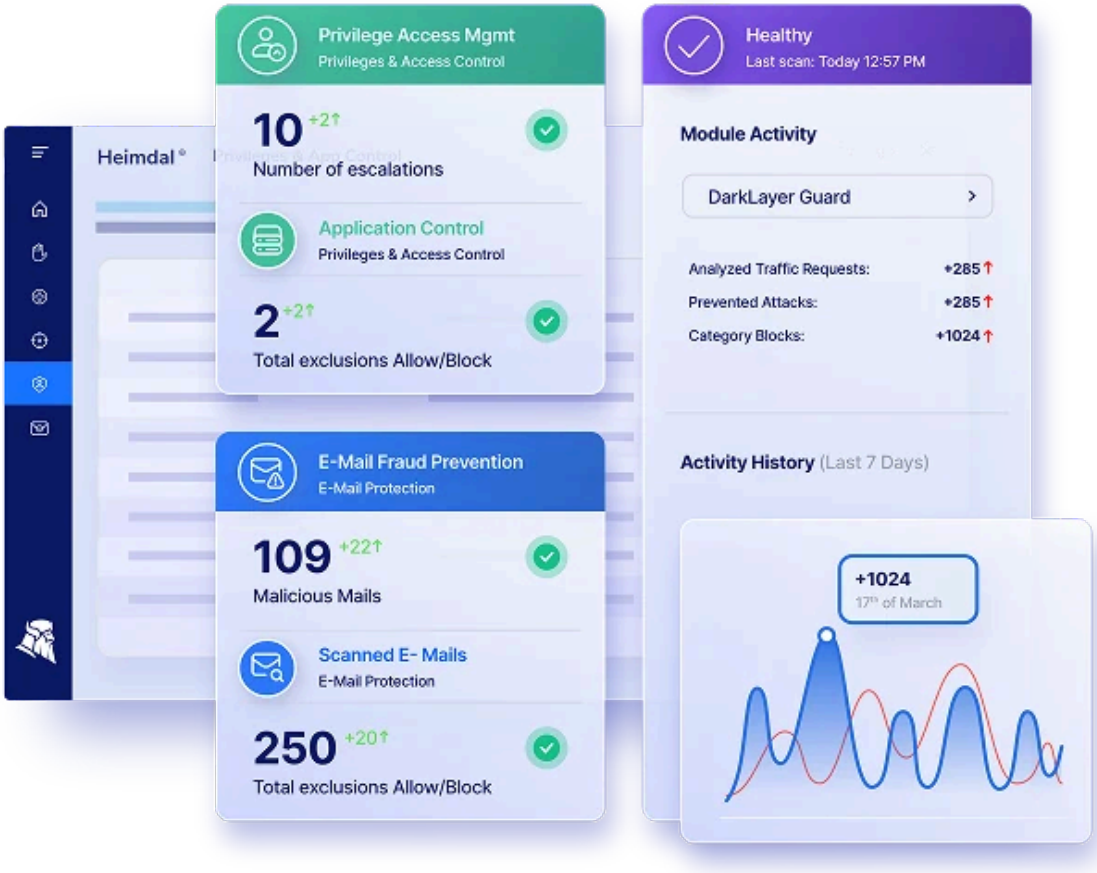
- Heimdal PAM - la suite completa
- Application Control - AppFencing

¿Cómo se combinan los productos?

¿Por dónde empezar?

La ciberseguridad empresarial ya no se compra por piezas. **Heimdal** reúne prevención DNS, antivirus de nueva generación, anti-ransomware, gestión de parches y control de acceso privilegiado en **un solo agente ligero** y **una única consola unificada**, para Windows, macOS y Linux.

Menos agentes que mantener, menos consolas que vigilar y una pila de seguridad en la que cada capa comparte inteligencia con las demás: eso es la plataforma Heimdal.



Suite Heimdal Privileged Access Management: módulos PEDM, Application Control y actividad

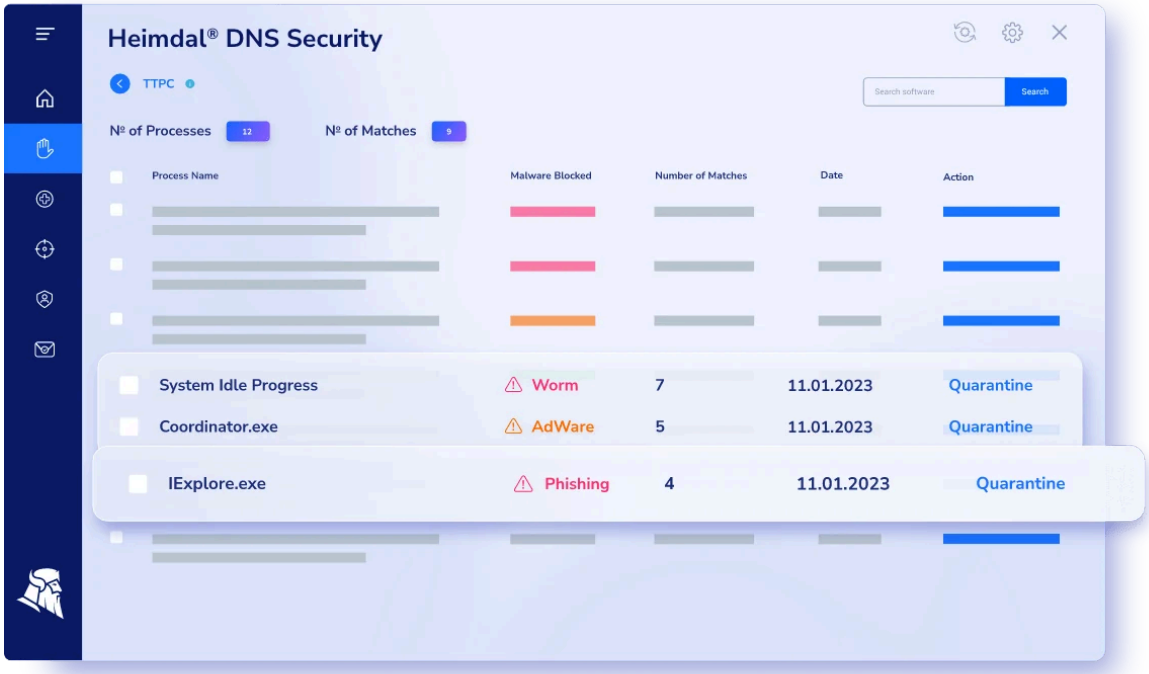
El portafolio de un vistazo

Familia	Producto	En una frase
Network Security	DNS Security - Network	Capa de protección con IA para toda la red: BYOD, IoT y cualquier dispositivo conectado.
Endpoint Security	DNS Security - Endpoint	Filtrado DNS, HTTP y HTTPS en cada equipo, con Predictive DNS™ (96% de precisión).
Endpoint Security	Next-Gen Antivirus & Firewall	AV multicapa con motor XTP mapeado a MITRE ATT&CK y RAP contra accesos remotos maliciosos.
Endpoint Security	REP X	Cuatro motores en tiempo real que detienen el ransomware antes del cifrado.
Vulnerability Mgmt	Patch & Asset Management	Parches automatizados de SO y más de 400 aplicaciones, entregados en menos de 4 horas.
Privileged Access	Heimdal PAM	La suite completa: elevación just-in-time, sesiones privilegiadas y control de aplicaciones.
Privileged Access	Application Control	Ejecución Zero-Trust con AppFencing™: decida exactamente qué corre en sus endpoints.

Network Security

DNS Security - Network

La variante de red protege el ecosistema completo —incluidos BYOD e IoT— con DNS híbrido on-prem/cloud, visibilidad granular del tráfico y threat hunting sin instalar software adicional. Se configura en minutos y cubre automáticamente todos los dispositivos de la red.



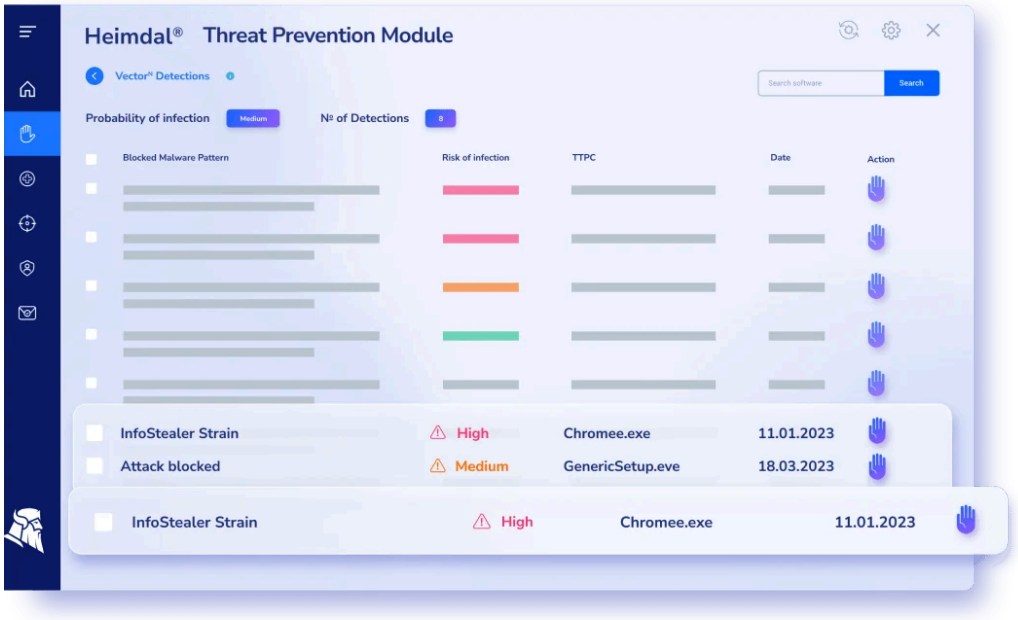
Consola Heimdal DNS Security: tráfico TTPC y acciones de cuarentena

→ [Ficha técnica de DNS Security - Network]

Endpoint Security

DNS Security - Endpoint

El motor DarkLayer Guard® en cada dispositivo: filtrado DNS, HTTP y HTTPS en tiempo real, verdadero DNS over HTTPS, correlación amenaza-proceso (TTPC) y Predictive DNS™, la tecnología patentada que predice dominios maliciosos antes de que alojen contenido.

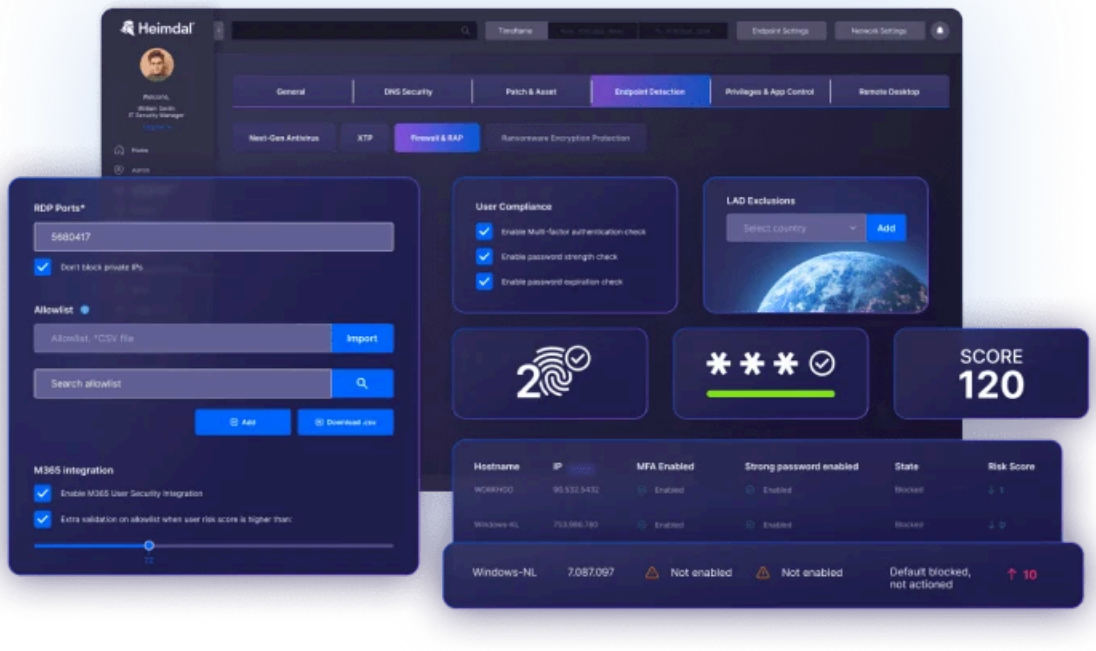


Panel de Heimdal DNS Security Endpoint: detecciones VectorN en el dashboard

→ [Ficha técnica de DNS Security - Endpoint]

Next-Gen Antivirus & Firewall

Escaneo multicapa —local, en la nube y en sandbox—, el motor propietario XTP mapeado a las tácticas y técnicas de MITRE ATT&CK, y RAP: la capa que frena la fuerza bruta, las credenciales robadas y las sesiones remotas no autorizadas antes de que empiece la brecha.

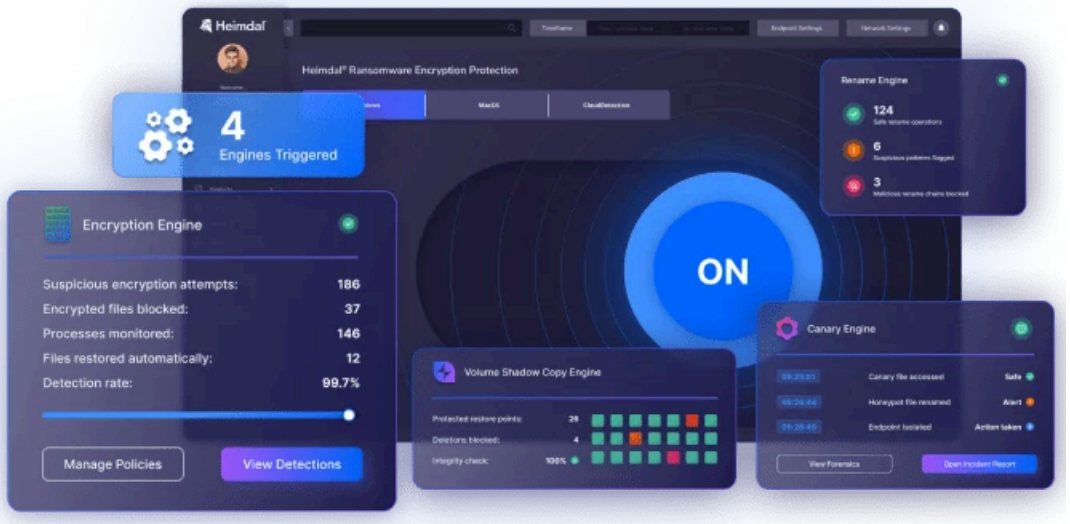


Configuración de Firewall y RAP en Heimdal Next-Gen Antivirus & Firewall

→ [Ficha técnica de Next-Gen Antivirus & Firewall]

REP X - Ransomware Encryption Protection

Cuatro motores complementarios —encryption, rename, shadow copy y canary— validados contra más de 800 muestras de ransomware, con aislamiento automático del equipo infectado, análisis forense y protección en tiempo real de las cargas de trabajo en Microsoft 365.



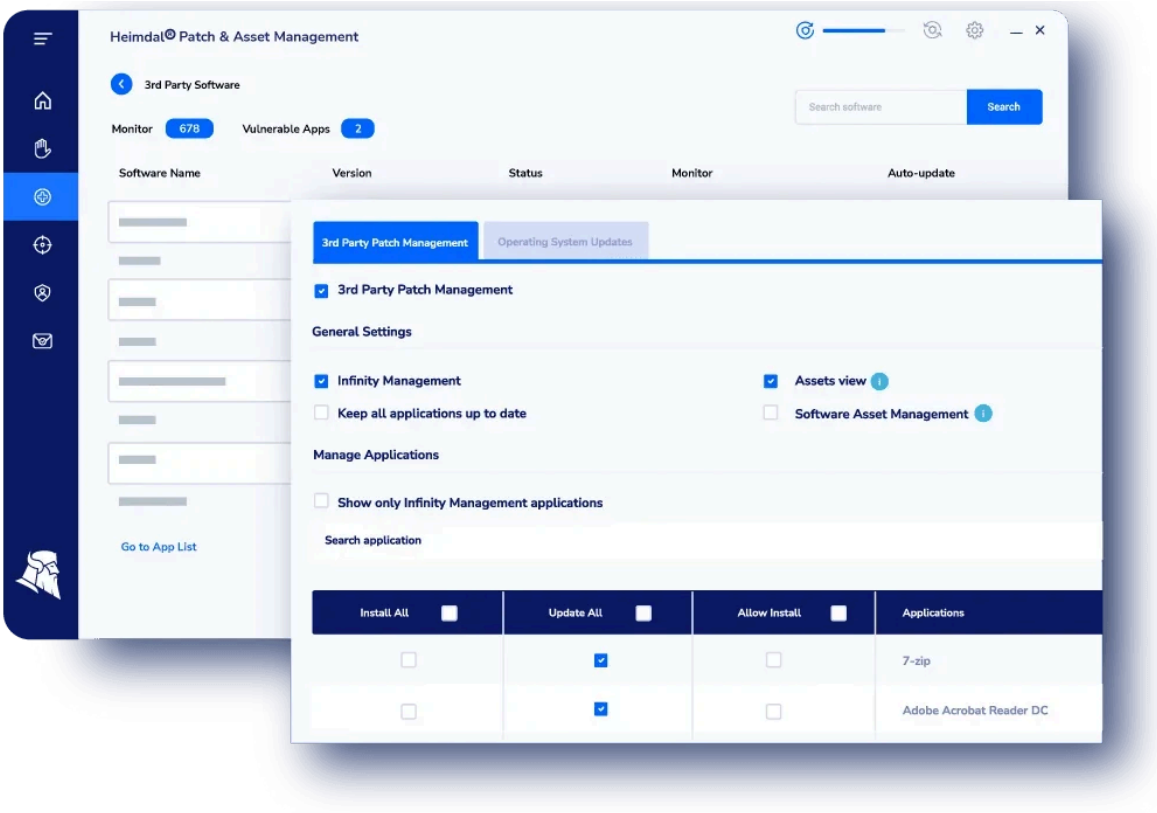
REP X en acción: los cuatro motores de detección de ransomware activados

→ [Ficha técnica de REP X]

Vulnerability Management

Patch & Asset Management

Automatización de parches de Windows, macOS, Linux y más de 400 aplicaciones de terceros: del fabricante al endpoint en menos de 4 horas —frente a los 16 días del parcheo tradicional—, con inventario de activos, cumplimiento continuo y el add-on Infinity Management para el software propio de su empresa.



Configuración de Patch & Asset Management e Infinity Management en el dashboard Heimdal

→ [Ficha técnica de Patch & Asset Management]

Privileged Access Management

Heimdal PAM - la suite completa

Tres módulos que trabajan juntos: **PEDM** (elevación de privilegios just-in-time, sin derechos de administrador permanentes), **PASM** (vault de credenciales con MFA y grabación de sesiones RDP/SSH) y **Application Control**. Una suite PAM que se despliega en horas, no en meses, sin la complejidad ni el coste de las soluciones empresariales tradicionales.

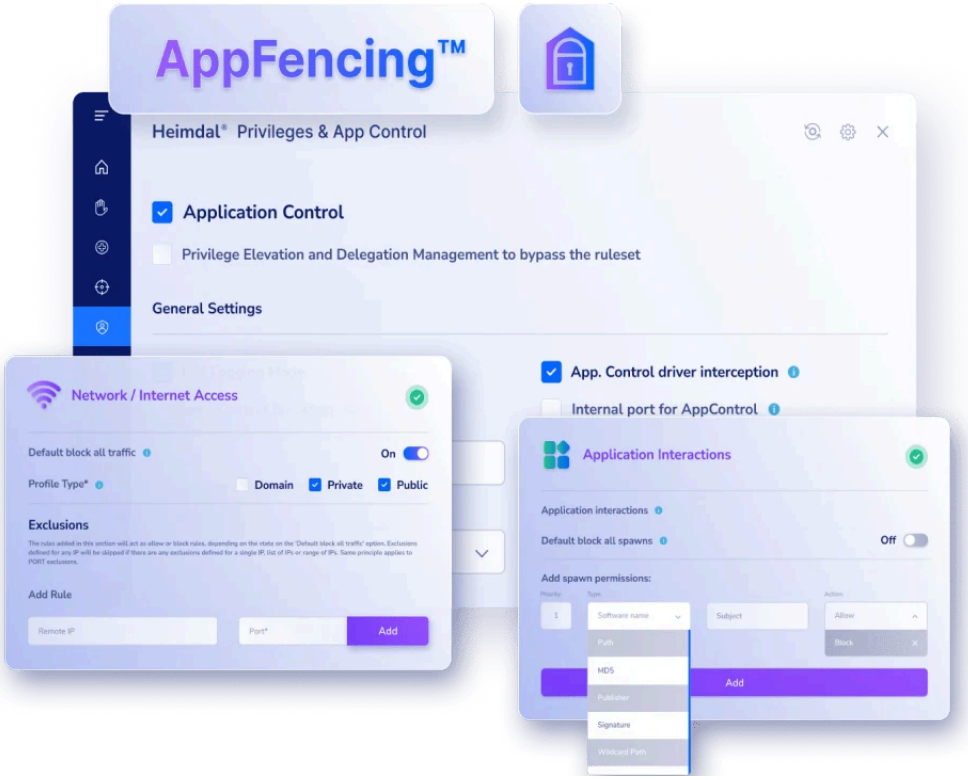


Heimdal PASM: monitorización, grabación y conexión de sesiones privilegiadas RDP/SSH

→ **Ficha técnica de Heimdal PAM**

Application Control - AppFencing

Disponible dentro de la suite PAM o como módulo independiente: ejecución Zero-Trust con políticas por ruta de archivo, hash MD5, publisher o certificado, flujos de aprobación automáticos, modo pasivo de monitorización y logs auditables de 90 días.



Heimdal Application Control con AppFencing: acceso a red, interacciones y permisos de ejecución

→ [Ficha técnica de Application Control]

¿Cómo se combinan los productos?

Todos los módulos se licencian por separado o en bundles. El bundle **EDR** reúne Next-Gen Antivirus & Firewall, DNS Security (Network y Endpoint), Patch & Asset Management, Infinity Management y REP X. Sobre esa base, **XDR** suma la suite Privileged Access Management completa, Email Security y Threat Hunting. En cualquier combinación, todo sigue gestionándose desde el mismo agente y la misma consola.

¿Por dónde empezar?

- Si su prioridad es **detener el ransomware** → REP X junto a Next-Gen Antivirus & Firewall.
- Si necesita **parcheo y cumplimiento** (NIS2, ISO 27001, Cyber Essentials) → Patch & Asset Management.
- Si quiere **cortar phishing, C&C y exfiltración en la capa DNS** → DNS Security Endpoint + Network.
- Si el problema son los **administradores locales y las sesiones sin auditar** → Heimdal PAM.

Cada ficha de producto incluye su tabla completa de funciones extraída del Solution Brief oficial del fabricante. Para ver la plataforma en vivo, solicitar una demo o una cotización, **contacte con Sogyo**.