Endpoint Security LATAM

Heimdal REP X - Ransomware Encryption Protection

TABLA DE CONTENIDO

¿Qué es Heimdal REP X?

Beneficios clave

Características principales

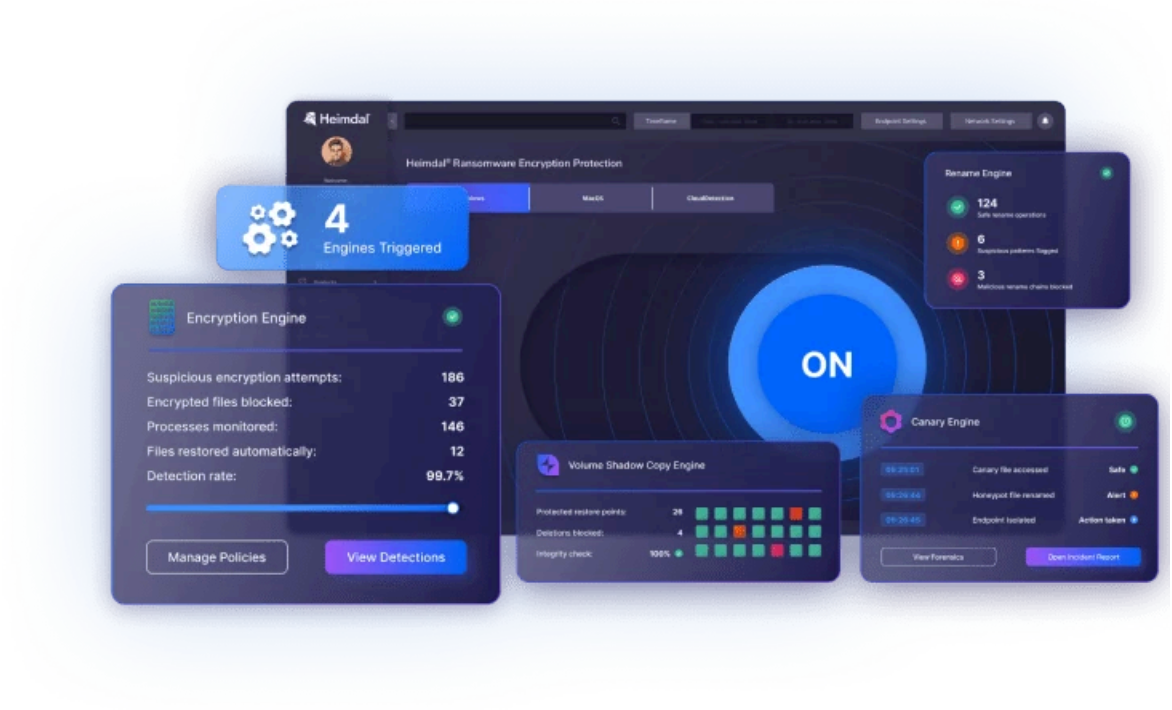
- Encryption Engine - detección del cifrado malicioso en curso
- Rename & Canary Engines - trampa temprana contra el ransomware
- Shadow Copy Engine - protección de la recuperación
- Protección en tiempo real para entornos cloud

Tabla completa de funciones

Potencie cualquier antivirus con REP X

Heimdal REP X es la nueva generación del módulo Ransomware Encryption Protection: cuatro motores de detección en tiempo real que detienen el ransomware antes de que comience el cifrado, validado contra más de 800 muestras de ransomware y con un riesgo de cifrado cercano a cero en ataques reales.

 © 2026 antivirusthor.com



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

¿Qué es Heimdal REP X?

Es una solución anti-ransomware reconstruida para las tácticas modernas: combina múltiples métodos de detección en tiempo real y ofrece a empresas y MSPs una protección fiable por capas, tanto on-prem como en la nube. Prevenir y proteger, no solo mitigar. Además, es ligera y se despliega sin fricción.

Beneficios clave

- **Protección multi-motor:** cuatro motores complementarios —encryption, rename, shadow copy y canary— que detectan y bloquean el ransomware en varias fases del ataque, reduciendo el riesgo de cifrado a casi cero.
- **Integración y visibilidad totales:** funciona junto a cualquier antivirus o como parte de la plataforma unificada Heimdal, con reporting avanzado y dashboards que ayudan a los equipos de seguridad y cumplimiento a responder con rapidez.
- **Resiliencia frente al ransomware moderno:** bloquea los intentos de alterar las shadow copies y las herramientas de recuperación, garantizando la continuidad del negocio incluso bajo ataques avanzados.

Características principales

Encryption Engine - detección del cifrado malicioso en curso

La lógica central monitoriza operaciones de archivo sospechosas (lecturas, escrituras, renombrados y borrados), detectando patrones de cifrado de forma temprana e impidiendo que el ransomware complete su payload con un margen de detección mínimo.

Rename & Canary Engines - trampa temprana contra el ransomware

Combina la detección de renombrado con archivos canario (honeypot) colocados en ubicaciones estratégicas: atrapa el ransomware antes de que se propague y aporta telemetría clara para la investigación, reforzando los flujos de respuesta de SecOps y MSPs.

Shadow Copy Engine - protección de la recuperación

Muchas familias de ransomware intentan borrar o alterar las Volume Shadow Copies de Windows para impedir la recuperación. REP X bloquea esos intentos automáticamente, asegurando resiliencia y continuidad incluso frente a cepas avanzadas o desconocidas.

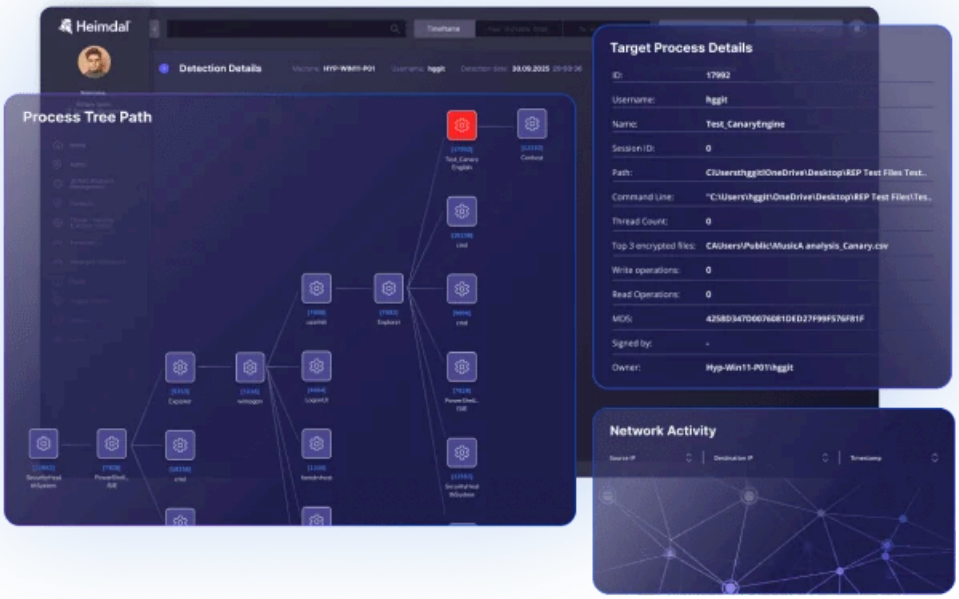
Protección en tiempo real para entornos cloud

Extiende la defensa anti-ransomware a Microsoft 365, SharePoint, OneDrive y Teams, monitorizando modificaciones de archivos, extensiones y operaciones de lectura/escritura en tiempo real para proteger los datos en la nube frente a variantes conocidas y emergentes.

Tabla completa de funciones

Función	Descripción
Encryption Engine	Detecta y bloquea los intentos de cifrado en tiempo real.
Rename Engine	Detiene el renombrado malicioso y la manipulación de archivos.
Canary Engine (Honeypots)	Detección temprana mediante archivos señuelo plantados en ubicaciones estratégicas.
Shadow Copy Engine	Protege las copias de seguridad del sistema (Volume Shadow Copies) y garantiza la recuperación.
Signatureless Detection	Neutraliza ransomware de día cero y sin archivo (fileless) mediante analítica avanzada, sin depender de firmas.
File System Monitoring	Seguimiento de cambios en archivos y directorios para detectar comportamiento de ransomware.
Encryption Blocking	Impide el cifrado no autorizado de archivos tanto en local como en la nube.
Cloud Workload Protection	Protección en tiempo real de Microsoft Teams, OneDrive y SharePoint.
Automatic Isolation	Aislamiento automático de los dispositivos infectados para frenar la propagación lateral.
Comprehensive Attack Visibility	Visualización de los incidentes de ransomware con mapeo de la cadena de ataque.
Advanced Event Logging	Captura de detalles granulares (hashes, callbacks, firmas) para el análisis forense.

Por qué es crítico: menos del 14% de las empresas que dependen solo de backups logran restaurar todos sus datos tras un ataque, y el 60% de las pymes atacadas cierra en los seis meses siguientes. REP X funciona como solución independiente o unificada con Threat-Hunting & Action Center (TAC), DNS Security, PAM y NGAV.



Análisis forense de REP X: árbol de procesos y actividad de red

Potencie cualquier antivirus con REP X

REP X amplía la protección de cualquier antivirus tradicional añadiendo la defensa anti-ransomware que los AV por sí solos no pueden ofrecer. Úselo junto a su AV actual o combínelo con Next-Gen Antivirus, Firewall y Threat Hunting de Heimdal para una defensa unificada: un solo agente y una sola consola.

¿Quiere verlo en funcionamiento? Solicite una demo o cotización de REP X a través de Sogyo.