Heimdal®

ENDPOINT & CLOUD SECURITY

Ransomware Encryption Protection X (REP X)

Four engines. One solution. Near-zero ransomware encryption risk.

Solution Brief

Get a Demo →

Why Ransomware Protection Requires Multiple Layers

Most organizations have a strong security foundation, including comprehensive Endpoint Detection and Response (EDR) solutions. These tools play a critical role in **blocking known malware, stopping exploits, and preventing data breaches**. However, ransomware threats are evolving—leveraging **fileless techniques, living-off-the-land tactics, and relying heavily on credential** theft to bypass traditional defenses.

Heimdal Ransomware Encryption Protection (REP) is engineered to enhance your existing EDR security stack—delivering real-time prevention against the encryption processes that ransomware depends on.

Why Having a Solution is Critical:

Without Heimdal REP, organizations remain exposed to:

Gaps in Detection	EDR stops early-stage malware, but **encryption-based attacks** often begin after the initial compromise.
False Sense of Backup Security	**Less than 14% of businesses** relying only on backups are able to fully restore data after a ransomware incident.
The Financial Impact	**60% of SMBs** hit by ransomware attacks reportedly shut down within six months of the attack.

Compliance and resilience are no longer optional. Regulatory frameworks like NIS2, GDPR, HIPAA, and CIS mandate ransomware protection and monitoring. REP X provides multi-engine defense and detailed reporting that simplifies audit readiness and strengthens organizational resilience.

Advanced Defense: REP X

The Next Generation of Ransomware Encryption Protection

Heimdal REP X is our next generation ransomware protection module, rebuilt with four complementary detection engines — encryption, rename, shadow copy, and canary. Validated against more than 800 ransomware samples, REP X minimizes encryption risk to near zero while remaining lightweight and seamless to deploy.

Fully compatible with existing antivirus and EDR stacks, or integrated into Heimdal's unified security platform, REP X ensures operational continuity by neutralizing ransomware before it can encrypt files or disrupt business.

KEY BENEFITS

For Security Leaders:

- ✓ **Proactive Threat Mitigation:** Stops ransomware encryption attempts in real time using four complementary detection engines.
- ✓ **Enhanced Compliance:** Simplifies audit readiness with detailed attack chain visibility and reporting.
- ✓ **Broad Compatibility:** Seamlessly integrates with existing security solutions, enhancing your cybersecurity stack.

For IT Teams:

- ✓ **Instant Isolation:** Automatically isolates infected endpoints to prevent lateral movement and contain threats.
- ✓ **Actionable Insights:** Visualize attack paths and origins with comprehensive graphical reports.
- ✓ **Ease of Deployment:** Works alongside any Next-Gen AV and EDR solution, reducing operational complexity.

For MSPs:

- ✓ **Multi-Tenant Efficiency:** Manage ransomware defense across multiple clients from a unified dashboard.
- ✓ **Real-Time Response:** Detect, analyze, and block ransomware activity within seconds.
- ✓ **Service Differentiation:** Showcase advanced ransomware defense to clients for stronger retention.

ENDPOINT & CLOUD SECURITY

Ransomware Encryption Protection X (REP X)

Heimdal®

Key Features & Capabilities:

Features	Description
Encryption Engine	Detect and block real-time encryption attempts.
Rename Engine	Stop malicious file renaming and tampering.
Shadow Copy Engine	Protect system recovery and resilience.
Canary Engine (Honeypots)	Early detection via planted decoy files.
Signatureless Detection	Neutralize zero-day and fileless ransomware using advanced analytics.
Advanced Event Logging	Capture granular details (hashes, callbacks, signatures) for forensic analysis.
Comprehensive Attack Visibility	Visualize ransomware incidents with attack chain mapping.
Automatic Isolation	Quarantine infected devices to stop lateral spread.
Cloud Workload Protection	Safeguard Microsoft Teams, OneDrive, and SharePoint in real time.
File System Monitoring	Track file and directory changes to detect ransomware behavior.
Encryption Blocking	Prevent unauthorized file encryption locally and in the cloud.

REP X – Standalone Power, Unified by Heimdal XDR

Heimdal Ransomware Encryption Protection X (REP X) is built on four complementary detection engines to deliver real-time ransomware prevention, stopping encryption threats before they impact your business. REP X can operate as a powerful standalone solution, or integrate seamlessly into Heimdal's cybersecurity ecosystem—allowing organizations to unify detection, response, and containment through the Threat-Hunting & Action Center (TAC), DNS Security, Privileged Access Management (PAM), and NGAV.

Ready to safeguard your organization against ransomware?

- **Unified Management:** Centralized visibility and control for endpoints, users, and cloud environments.
- **Compliance-Ready Reporting:** Generate detailed audit trails to meet GDPR, ISO 27001, NIS2, and NIST requirements.
- **Rapid Response Workflows:** Real-time alerts and automated containment reduce downtime and impact.

Get a Demo ⟶

Why choose Heimdal as your security partner?

Heimdal is an industry-leading, unified, and AI-powered cybersecurity solutions provider established in Copenhagen in 2014. With an integrated approach to cybersecurity, Heimdal has dramatically boosted operational efficiency and security effectiveness for over 17k+ customers globally.

Heimdal empowers CISOs, Security Teams, and IT admins to enhance their SecOps, reduce alert fatigue, and be proactive using one seamless XDR security platform.

Our award-winning line-up of 10+ fully integrated cybersecurity solutions span the entire IT estate, allowing organizations to be proactive, whether remote or onsite.

> **"The Heimdal Endpoint Detection and Response (EDR) system has proven highly effective and received praise from the security company that recently conducted a network security audit. Although they were unfamiliar with Heimdal, it successfully blocked their attempts to install hacking tools, all while quickly notifying our IT staff of their actions."**
>
> **- Chris Stebbins,**
> **Assistant Director of Technology**
>
> SAU 67

heimdalsecurity.com

Gartner peerinsights ★★★★★ SOURCEFORGE ★★★★★ Capterra ★★★★★ Expert Insights ★★★★★