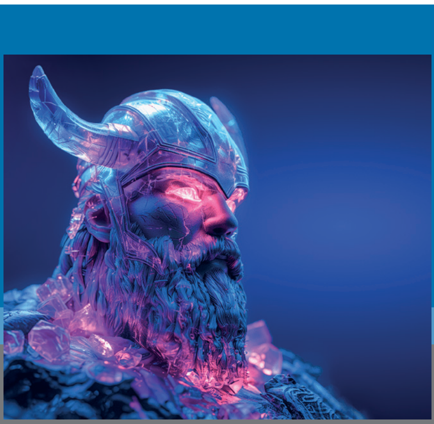
Heimdal®

DNS Security Endpoint

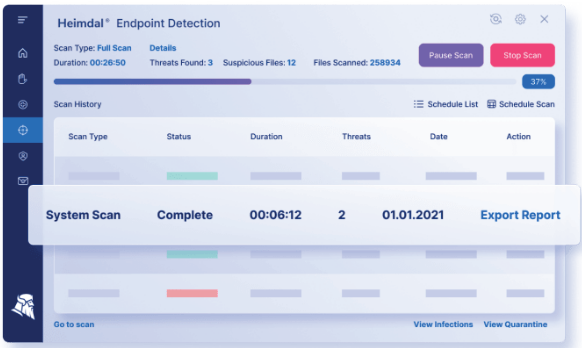


Heimdal offers an end-to-end, proactive, unified cybersecurity suite built to defend against next-gen threats. Its unique, multi-layered approach provides comprehensive protection through a fully integrated network and endpoint protection suite.

Key features

- **Real-time traffic scanning monitors and blocks infected domains instantly**
- **The first solution to integrate true DNS over HTTPS filtering**
- **Predictive DNS with machine learning detects and blocks malicious domains before they become harmful**
- **Identifies and stops attacking processes on endpoints**
- **Two-way traffic filtering allows customisable content filtering and control over incoming and outgoing traffic**
- **Compatible with existing security solutions and other Heimdal modules**

Heimdal is the only vendor in the market with an offering that combines next-generation antivirus, DNS-level traffic filtering on the endpoint, silent, automated third-party patch management, privileged access management, email security, and a managed service in one platform.



Heimdal® Endpoint Detection

Scan Type: Full Scan
Duration: 00:26:50

Details
Threats Found: 3 Suspicious Files: 12 Files Scanned: 258934

Scan Type	Status	Duration	Threats	Date	Action
System Scan	Complete	00:06:12	2	01.01.2021	Export Report

Why Heimdal DNS Security Endpoint?

Heimdal DNS Security Endpoint provides real-time traffic scanning to block infected domains and disrupt cybercriminal communication. It ensures secure browsing without impacting performance, prioritising DNS over HTTPS filtering to stop hidden malware and threats. Leveraging machine learning, Heimdal detects potential threats based on traffic patterns from previously blocked domains, enhancing predictive accuracy. It's also the first solution to offer true DNS over HTTPS, advancing threat hunting beyond traditional antivirus detection.

Challenges Heimdal DNS Security Endpoint solves

Heimdal's DNS Security Endpoint blocks zero-hour exploits, ransomware, and data leaks by filtering DNS, HTTP, and HTTPS traffic in real time. It uses machine learning to detect advanced threats that evade traditional tools, preventing malware from communicating with criminal infrastructures. The solution includes cloud-based security policy enforcement capabilities to address insider threats, shadow IT, and compromised accounts.