Heimdal®

ENDPOINT SECURITY

Next-Gen Antivirus, Firewall & Remote Access Protection

Advanced Endpoint Security for Modern Enterprises and MSPs

Solution Brief

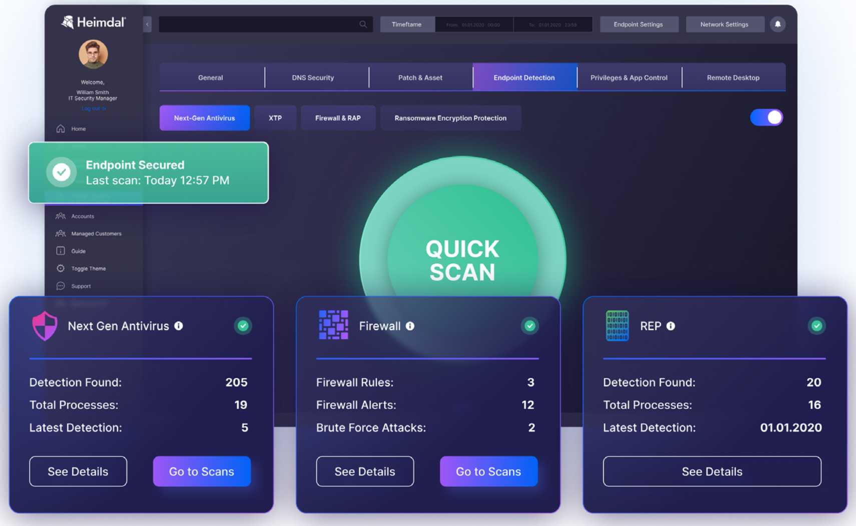
Endpoints Are the #1 Target — for Malware and Remote Access Abuse

Malware is no longer the only threat — **84% of ransomware attacks** start with misused remote access or stolen credentials.

Modern enterprises and MSPs need prevention-first security with real-time detection, response, and visibility.

Protect Endpoints and Block Remote Entry with Layered, Real-Time Defense

In a world of evasive malware, APTs, ransomware, and zero-days, traditional antivirus is no longer enough. **Heimdal's Next-Gen Antivirus (NGAV)**, supercharged by our proprietary **Extended Threat Protection (XTP)** engine, delivers unrivalled threat visibility, remote access control, advanced process monitoring, and real-time mitigation to stop both known and unknown threats in their tracks.



Endpoint Secured
Last scan: Today 12:57 PM

Next Gen Antivirus
Detection Found: 205
Total Processes: 19
Latest Detection: 5

Firewall
Firewall Rules: 3
Firewall Alerts: 12
Brute Force Attacks: 2

REP
Detection Found: 20
Total Processes: 16
Latest Detection: 01.01.2020

Why Choose Heimdal NGAV + XTP?

Built for SecOps Teams, MSPs & Enterprises

Heimdal NGAV + XTP provides your IT and security teams with unparalleled endpoint insight, simplified policy management, and faster response workflows — all managed within the Heimdal Unified Security Platform.

KEY BENEFITS

- ✓ **Comprehensive Attack Coverage**
  Protect against advanced techniques such as Credential Access, Defense Evasion, Exfiltration, and Lateral Movement
- ✓ **MITRE ATT&CK-Based Threat Categorization**
  Utilize MITRE and SIGMA rules, enabling deep threat hunting and forensics.
- ✓ **Real-Time Threat Intelligence**
  Powered by Heimdal Labs and in-house analysts, XTP provides continuous updates with expert-curated Indicators of Compromise (IOCs) and attack techniques.
- ✓ **Remote Access Protection Built In**
  Stops attackers from logging in remotely by blocking all external access unless pre-approved. Enforces controls based on IP, user identity, login risk, and session context.
- ✓ **Lightweight, Low-Impact Deployment**
  Engineered to minimize CPU/memory usage and maximize performance — deployable in minutes.
- ✓ **Built-In Multitenancy for MSPs**
  Manage multiple customer environments from a single pane of glass with isolated policies, reports, and endpoint views — designed for efficient, secure multi-tenant operations.

Key Features & Capabilities:

Features	Description
Multi-Vector Detection	Detects and neutralizes malware, ransomware, APTs, zero-days, fileless attacks, credential theft, and backdoors using both signature-based and signature-less methods.
Extended Threat Protection (XTP)	Delivers 1,400+ curated detection rules, MITRE ATT&CK-aligned classification, and infinite response scenarios for advanced threat categorization and mitigation.
Cloud-Based Threat Analysis	Uses 1,000+ cloud CPU cores and machine learning algorithms to scan unknown files in real time, identifying novel and evasive threats.
Behavioral & Heuristic Process Analysis	Monitors process behavior and execution using heuristic engines to detect anomalies, persistence mechanisms, and potentially malicious actions.
Zero-Trust Execution Protection	Prevents untrusted, unsigned, or unknown applications from executing at runtime by enforcing a Zero-Trust model.
Firewall with Brute-Force Protection	Endpoint firewall with brute-force detection, ransomware isolation, and full control over ports, IPs, and protocols.
Sandboxing & Backdoor Protection	Isolates suspicious files for behavioral inspection and blocks attempts to connect to Command & Control infrastructure or exfiltrate data.
Registry & Persistence Monitoring	Detects unauthorized registry changes commonly used for malware persistence or privilege escalation.
Remote Access Protection (RAP)	Blocks all unsolicited external remote access by default, including RDP and remote tools. Allows only explicitly approved connections with IP/port allowlisting, brute-force login protection, and adaptive access controls via user and session risk scoring.

Get Ahead of the Threat Curve with Heimdal **EDR** or **XDR**

Modern attacks require modern defenses. Heimdal's Next-Gen Antivirus with XTP is your endpoint's first and last line of defense.

It can also be extended into an advanced Endpoint Detection and Response bundle with Heimdal's Ransomware Encryption Protection (REP), or expanded into a full XDR stack with modules like Patch Management, DNS Security, Email Security, and more - for complete prevention, detection, and response across the entire digital estate.

Your endpoints deserve more than basic protection.

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 16k+ 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.

> **"We would recommend Heimdal to our industry peers, as well as any other enterprise looking to streamline and enhance their security operations. The main reason for this is Heimdal's unified All-in-One approach to their suite of products, covering all security needs for an organization."**
>
> - Chief of IT Operations
>
> **Large Construction & Manufacturing Business, Denmark**

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