

# Threat Prevention - Network

Product Sheet

## Hunt, Prevent, Detect and Respond to Endpoint Threats.

Heimdal Threat Prevention - Network uses Machine Learning on device-to-infrastructure communication to spot and stop attacks that firewalls can't see, offering you an essential threat hunting tool to prevent attacks on your network.

Now enhanced with Predictive DNS, a truly revolutionary AI & ML algorithm that is capable of predicting a domain is malicious before it will host any malicious content. The advanced neural networks and AI linguistic analysis are capable of achieving an unprecedented level of truly intelligent prevention.



### Block malicious web content

Over 22% of all new domains are created for illegal purposes. And it would be impossible for your users to know exactly which websites are completely safe.

For instance, malicious code can be often found in banners on entirely legitimate websites. But Heimdal Threat Prevention - Network blocks access to websites containing malicious code and to servers controlled by cybercriminals. Every day, we evaluate over 300,000 domains.



### Prevent data leakage

Heimdal Threat Prevention - Network also stops communications from any existing malware intrusions, avoiding data leaks by detecting and blocking malicious traffic initiated by threats such as APTs and ransomware.



### Detect advanced malware

If Heimdal Threat Prevention - Network ever identifies an infection, we send you alerts for every type of device that's been infected, including PCs, Macs, Androids and iOS devices.

With HeimdalThreat Prevention - Network, your network is protected against:

- ✓ Ransomware
- ✓ Data Exfiltration
- ✓ APTs
- ✓ Malware

**79%** DNS ATTACKS  
IN 2020

Nearly 4 out of 5 organizations (79%) have experienced a DNS attack in 2020.

**9.5** ATTACKS  
PER YEAR

Organizations across all industries suffered an average of 9.5 attacks per year in 2020.

**\$924** THOUSAND  
IN DAMAGE COST

The average cost of a DNS attack in 2020 on organizations is \$924,000 globally

**\$1** MILLION  
IN DAMAGE COST

The average cost of a DNS attack in 2020 on organizations is \$1,082,710 in the USA.

DNS is commonly used in data breaches as a pathway for data exfiltration, since traditional security products don't know how to address this issue.

But Heimdal Threat Prevention - Network is based upon a technology that reveals and stops data leakages through DNS. It also employs machine learningdriven intelligence to instantly identify threats, helping you protect your organization from DNS queries to malicious domains.

## Filter traffic locally in any environment

A revolutionary solution, the Hybrid DNS module included in Threat Prevention – Network adds advanced filtering capabilities onto any local DNS server, allowing customers to secure DNS traffic in their internal networks without needing to forward the DNS queries to Heimdal’s TPN resolvers.

This feature empowers users to use any DNS forwarder of their choice, plus the ability to have a dynamic IP on the local DNS resolver. Due to this, Threat Prevention – Network is a perfect fit for both on-prem and cloud-based DNS environments.

### Customer voice

“ It used to take days between knowledge of a threat to actual protection against it. We now use Heimdal Threat Prevention - Network to make that process a whole lot faster. ”

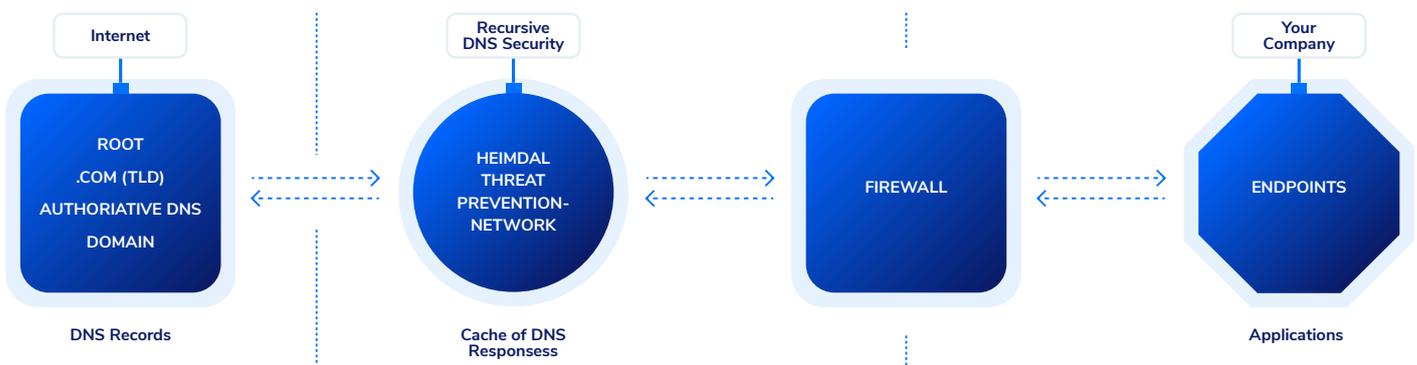
- Thomas Kaaber  
IT Manager at Bang & Olufsen

## Fully secure your network at perimeter level with Heimdal® Threat Prevention - Network.

Next-gen network security with added HIPS capabilities to stop threats before they infect your organization.

In recent years, traditional security products turned out to be highly inefficient in an ever-changing threat environment.

## Heimdal® Threat Prevention - Network in the network



Stop threats before they damage your organization!

- ✓ Implementation takes less than 15 minutes.
- ✓ Perimeter Recursive DNS
- ✓ Hunt and detect advanced network threats.
- ✓ Run it in Active and Passive Modes.
- ✓ Benefit from machine learning-driven intelligence.
- ✓ See exactly where attacks are coming from.
- ✓ Malicious links and attachments.
- ✓ Using ITILv3 standard for security incidents helps you comply with ISO27001/2.
- ✓ Spot hidden threats using Vector<sup>N</sup> Detection<sup>TM</sup>'s Machine Learning.
- ✓ Best protection/investment ratio.

With Heimdal Threat Prevention - Network, you can now significantly raise your security level with minimal impact on your existing IT setup.

- ✓ Subscription model, no initial investment needed.
- ✓ Continuous updates with no administration or maintenance.
- ✓ Fully hosted: experience zero downtime or service interruptions.
- ✓ No configuration changes or server reboots needed.
- ✓ Automatically covers all devices in your network.

# Don't leave your network vulnerable!

Cybercriminals won't stop exploiting the existing security holes in the Internet's infrastructure. Be one step ahead of them and secure your network at DNS-level!

Features	Heimdal Threat Prevention - Network	Regular Firewall
Detect & block web-based threats	✓	✗
C&C callback blocker	✓	✗
Network based malware & APT detection	✓	✗
Data leakage prevention	✓	✓
Hosted service - no servers or client software	✓	✗
Supports all servers, desktops & mobile devices	✓	✗
Custom block and allow list	✓	✓
Basic statistics	✓	✗
Advanced statistics & forensics, with internal IP-addresses and hostnames	✓	✗
Run it in passive/IDS mode	✓	✗
Customized block page (OPTIONAL)	✓	✗

## About Heimdal®



★★★★★



★★★★★



★★★★★



★★★★★

Founded in 2014 in Copenhagen, Denmark, Heimdal® is a leading European provider of cloud-based cybersecurity solutions.

The company offers a multi-layered security suite that combines threat prevention, patch and asset management, endpoint rights management, and antivirus and e-mail security which together secure customers against cyberattacks and keep critical information and intellectual property safe.

Heimdal has been recognized as a **thought leader in the**

**industry** and has won multiple awards both for its solutions and for its educational content.

Currently, Heimdal's cybersecurity solutions are deployed in **more than 50 countries** and supported regionally from offices in 15+ countries, by 175+ highly qualified specialists. Heimdal is ISAE 3000 certified and secures **more than 3 million endpoints** for over 11,000 companies.

The company supports its partners without concessions on the basis of predictability and scalability, creating sustainable ecosystems and **strategic partnerships**.