



**HEIMDAL™**  
SECURITY



Heimdall™ Security Product Sheet

# Threat Prevention - Network

This unparalleled DNS security solution enhances your protection against APTs, data leaks, ransomware and network malware.

[www.heimdalsecurity.com](http://www.heimdalsecurity.com)

**E:** [sales.inquires@heimdalsecurity.com](mailto:sales.inquires@heimdalsecurity.com)

**P:** +45 7199 9177

2021 Heimdall™ Security. All rights reserved.

Registered trademarks and service marks are the property of their respective owners.

# 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.

## Instantly trace infections to specific users and entry points.

Add an extra layer of protection through advanced Machine Learning and strong, actionable intelligence.

- ✓ Significantly raise your overall security
- ✓ Minimize your costs
- ✓ Don't lose your revenue, intellectual property, and productivity.
- ✓ Protect your infrastructure
- ✓ Free up your internal resources.
- ✓ Access a real-time overview of your current security status

With Heimdal™ Threat 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 learning driven intelligence to instantly identify threats, helping you protect your organization from DNS queries to malicious domains.

### 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



[www.heimdalsecurity.com](http://www.heimdalsecurity.com)

E: [sales.inquires@heimdalsecurity.com](mailto:sales.inquires@heimdalsecurity.com)

P: +45 7199 9177

2021 Heimdal™ Security. All rights reserved.

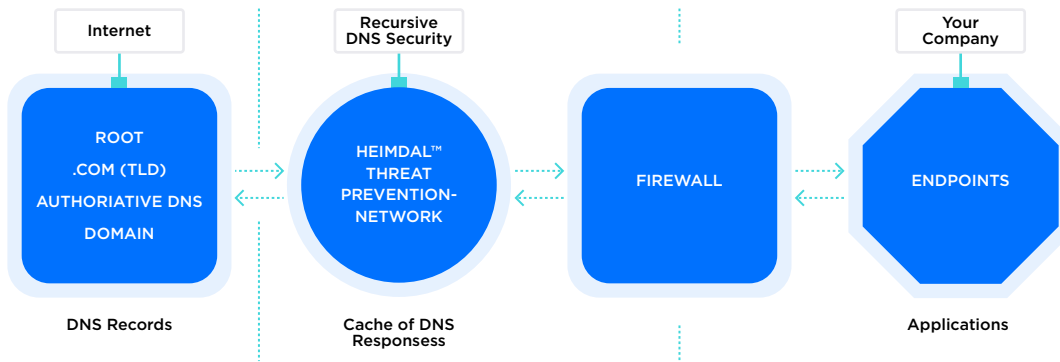
Registered trademarks and service marks are the property of their respective owners.

# 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



## 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)	✓	✗

[Go to Product Page →](#)

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™'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.