



**HEIMDAL™**  
SECURITY



Heimdall™ Security Product Sheet

# Threat Prevention - Endpoint

Working in tandem, DarkLayer Guard™ and VectorN Detection™ are the proactive, code-autonomous tools fine-tuned to layer on top of other protective, code-detection based technologies.

[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.

Enhanced with TTPC (Threat To Process Correlation), your organization gains the essential threat hunting tools to map out the security-critical points in your environment.

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.



## DARKLAYER GUARD™

### The essential Host-Based Intrusion Prevention System (HIPS)

The DarkLayer Guard™ is a unique 2-way traffic filtering engine that supports fully customizable white/black listing.

With it, your organization can block network communication to mitigate Zero Hour exploits, Ransomware C&C's, next-gen attacks and data leakages.

Using our ground-breaking Threat To Process Correlation technology, we can identify attacking processes and provide HIPS capabilities for endpoints.



## VECTOR<sup>N</sup> DETECTION™

### Code-autonomous detection to find threats unseen by NGAV and code scanners

By tracking device-to-infrastructure communication, Vector<sup>N</sup> Detection™ will detect 2nd generation malware strains that no other product can see, effectively delivering a HIDS at the machine traffic layer.

Using machine learning to establish compromise patterns and offering indicators of compromise/ attack (IOA/IOC), this is a unique add-on that will boost any other type of endpoint security.

## Advanced Malware Obfuscation Techniques can Circumvent Traditional Detection

With DarkLayer Guard™ and Vector<sup>N</sup> Detection™, malware is blocked at a traffic level, stopping its communications with criminal infrastructure.

By leveraging the unique intelligence gained through blocking threats at the DNS, HTTP and HTTPS level, DarkLayer Guard™ and Vector<sup>N</sup> Detection™ not only give you the power to stop active attacks, but they also accelerate your investigation process. This way, vulnerable endpoints can be pinpointed and reinforced against future threats, ensuring a proactive approach to security.

The cost of deploying a new solution, including a security one, has long been an intimidating proposition for businesses, especially smaller, more resource-constrained ones.

That's not the case here.

100% compatible with your existing solutions and other Heimdal Security modules, DarkLayer Guard™ and Vector<sup>N</sup> Detection™ are the code-autonomous solution to combat next-gen malware, ransomware and other enterprise threats.

**10,975** MALICIOUS DOMAINS

The number of malicious domains removed monthly in the UK, by one agency alone.

Source: NCSC.gov.uk

**1,783** RANSOMWARE COMPLAINTS

The number of complaints filed to The Internet Crime Complaint Center(IC3), with an average of 5 victims daily.

Source: FBI

**3,785** CORPORATE DATA BREACHES

In 2017, as recorded in The Internet Crime Complaint Center (IC3). On average, 10 data breaches happen daily.

Source: FBI

**79%** DNS ATTACKS IN 2020

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

Source: IDC 2020 Global DNS Threat Report

**9.5** ATTACKS PER YEAR

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

Source: IDC 2020 Global DNS Threat Report

**\$924** THOUSAND IN DAMAGE COST

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

Source: IDC 2020 Global DNS Threat Report

**\$1** MILLION IN DAMAGE COST

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

Source: IDC 2020 Global DNS Threat Report



[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.

# Going the extra mile in keeping cyberthreats away from your endpoints

Besides its unique threat hunting capabilities, Heimdal™'s Threat Prevention Endpoint is remarkable through its added potential of integrations with the rest of our Endpoint Prevention, Detection and Response suite, allowing you to cover all fronts of cybersecurity defenses from the same unified interface.

Furthermore, the individual solutions which converge into the EPDR suite empower one

another, and can also be chosen and combined according to your custom organizational needs.

Flexible, easily scalable and perfectly suited for a mixed of remote and on-site teams, Heimdal™'s Threat Prevention Endpoint and its complementary solutions provide you with true security against tomorrow's threats today.

Criminals can easily bypass behavior and code scanners like Antivirus, as well as firewalls, unleashing devastating ransomware attacks or creating data breaches that will damage your organization.

“ In terms of preventing attacks, we have already seen a clear value in the first couple of months that we have used Heimdal™ Security, with even having a couple of ransomware attacks blocked. The way it spots malware that the antivirus doesn't see is just so special. Heimdal is a simply and fast way to improve our core security and it helps us prevent attacks before they even happen.”

- Kifaf General Trading, key Sony Entertainment distributor in the UAE Region

“ Even though our network is very well protected we knew that we had to add an extra layer of security on our clients. Simply because the most part are laptops. When these clients left the building it was clear that the antivirus was not enough according to the modern scape of cyber threats.”

- Schultz Information

[Go to Product Page →](#)



[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.