Heimdal®

Threat Prevention - Endpoint

Product Sheet

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^{N} DETECTION®

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

By tracking device-to-infrastructure communication, Vector^{N} 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 patters and offering indicators of compromise/ attack (IOA/IOC), this is a unique add-on that will boost any other type of endpoint security.

World's First Solution on the Market to Support True DNS over HTTPS

With the introduction of this groundbreaking feature, Threat Prevention – Endpoint becomes the world's first cybersecurity product on the market to support true DNS over HTTPS filtering, evolving beyond the standard rerouting of DNS packages. The functionality encrypts domain name system traffic by passing all DNS queries through a Hypertext Transfer Protocol Secure encrypted session.

Through bona fide DNS over HTTPS, Threat Prevention – Endpoint helps enterprises mitigate the ever-increasing risks of Man-in-the-middle (MitM) attacks and DNS spoofing that can infiltrate their infrastructure by encrypting the session info between a user's browser and the DNS server it communicates with.

As a result, your organization will benefit from increased user privacy without any toll on system performance, saving essential time and resources in the process as well. Heimdal's response to the growing threat of spoofing and MiTM attacks, DNS over HTTPS is an addition to our base Threat Prevention – Endpoint product that makes a difference.

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.

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.

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

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.

Advanced Malware Obfuscation Techniques can Circumvent Traditional Detection

With DarkLayer Guard and Vector^{N} 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^{N} 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^{N} Detection are the code-autonomous solution to combat next-gen malware, ransomware and other enterprise threats.

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.

> "In terms of preventing attacks, we have already seen a clear value in the first couple of months that we have used HeimdalTM 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**

About Heimdal®

Gartner peerinsights. ★★★★★
SOURCEFORGE ★★★★★
G2 CROWD ★★★★★
Trustpilot ★★★★★

HEIMDALSECURITY.COM

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.**