HEIMDAL ™ SECURITY

DarkLayer Guard ™ – Vector^{N} Detection ™

The next-gen EDR and HIPS capabilities your organization needs to combat evolving threats.

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

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.

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

Malware obfuscation techniques are getting more advanced and capable of evading 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.

"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

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.

10,975 MALICIOUS DOMAINS

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

– 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.

– FBI

3,785 CORPORATE DATA BREACHES

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

– FBI

85%

of MSPs reported that ransomware victims had antivirus software installed.

- Datto, Inc: Global State of the Channel Ransomware Report, 2018

65%

of MSPs reported that ransomware victims had email/spam filters installed.

- Datto, Inc: Global State of the Channel Ransomware Report, 2018

29%

of MSPs victims had pop-up blockers.

- Datto, Inc: Global State of the Channel Ransomware Report, 2018

2018 Computing Security Awards WINNER

Anti Malware Solution of the Year

Get in touch today to discover how they enhance your environment.

HEIMDAL™ SECURITY

Contact us at

+45 7199 9177

or

corpsupport@heimdalsecurity.com