Heimdal®

Hunt, Prevent, Detect and Respond

Heimdal Security Threat Prevention

Hunt, Prevent, Detect and Respond to Endpoint Threats.

- Working in tandem, DarkLayer Guard and VectorN Detection are the proactive, code-autonomous tools fine-tuned to layer on top of any existing security solutions.
- Threat intelligence is live from the malware infrastructure to provide a unique level of protection.
- Enhanced with TTPC (Threat To Process Correlation), clients gain the essential threat hunting tools to map out the security-critical points in their environment
- Complete with market-leading Predictive DNS (AI & ML algorithm that is capable of predicting a domain is malicious before it even hosts any malicious content)

DARKLAYER GUARD™

DarkLayer Guard is the essential Host-Based Intrusion Prevention System (HIPS).

- Unique 2-way traffic filtering engine
- Supports fully customisable category-based content filtering
- Block network communication to mitigate Zero Hour exploits, ransomware and data leaks
- Using Heimdal's ground-breaking Threat To Process Correlation technology, an organisation can identify attacking processes and provide HIPS capabilities for endpoints

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

VECTORN DETECTION™

VectorN Detection leads the way with code-autonomous detection to find threats unseen by next-generation anti-virus and code scanners.

- Tracks device-to-infrastructure communication to detect second generation malware strains that no other product can spot
- Uses machine learning to establish compromise patterns and offer indicators of compromise/attack
- Complements and boosts any other endpoint security

By leveraging the unique intelligence gained through blocking threats at the DNS, HTTP and HTTPS level, DarkLayer Guard and VectorN Detection not only give the power to stop active attacks, but they also accelerate the investigation process.

Traditionally, deploying a new security solution has been daunting with potentially a high cost! With Heimdal's Threat Prevention this is not the case.

Heimdal's Threat Prevention is compatible with any existing endpoint security solutions or other Heimdal Security modules.

Available on

3,785
CORPORATE DATA BREACHES

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

- FBI

79%
DNS ATTACKS IN 2020

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

– IDC 2020 Global DNS Threat Report

Contact Brigantia

Suite 2.1, Hurstwood Business Centre, York Road, Thirsk, YO7 3BX

Tel: 020 3358 0090 | Email: partnersupport@brigantia.com | Web: www.brigantia.com