TOSHIBA

Threat Prevention

- Predict tomorrow's threats today with advanced endpoint and network DNS security
- DNS, HTTP and HTTPS filtering for your perimeter and endpoints
- Raise you security level with minimal impact on your existing IT setup
- Automatically cover all devices in your network

Powerful endpoint and network DNS security.
Stay one step ahead of cybercriminals and stop threats before they damage your organisation with Heimdal Security's Threat Prevention*.

Stop threats at the Perimeter-level and experience complete DNS protection. Stay in control of your network traffic and identify hidden threats.

Hunt, prevent, detect and block threats at the Endpoint-level, and detect DNS hijacking and stop exploits, ransomware, data leaks and more.

*Delivered in conjunction with Heimdal Security and Brigantia.

TOGETHER INFORMATION

Hunt, Prevent, Detect and Respond

Heimdal Security Threat Prevention will help you 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 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

VectorN Detection leads the way with code-autonomous detection to find threats unseen by next-generation antivirus 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. Accepts any MSI/EXE installer and offers command lines for scripting.

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

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

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

Safeguard your business with Threat Prevention

Contact our Managed IT Services team to take the next step.

Toshiba Tec UK Imaging Systems Ltd.

T 020 7735 9992 | **E** managed.itservices@toshibatec.co.uk | **W** www.toshibatec.co.uk

Toshiba Tec UK deliver these services in conjunction with Heimdal Security and Brigantia.
www.brigantia.com | heimdalsecurity.com

Copyright ©2021 Toshiba Tec. DS_ThreatPrevention_0821