



HEIMDAL™
SECURITY



OPSWAT.
CERTIFIED

 **Capterra**
★★★★★ 4.5/5

2021
Computing
Security
Awards
WINNER




AWARDS 2021
★ WINNER ★
CLOUD DELIVERED SECURITY
SOLUTION OF THE YEAR



 **Gartner
peerinsights..**
★★★★★ 4.8/5

Heimdal™ Security Product Sheet

Unified Threat Dashboard

Heimdal™ Unified Threat Dashboard (UTD) is a dynamic platform that constantly detects and tracks potential and existing security holes in your environment.

www.heimdalsecurity.com

E: 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.

Featuring either a single, stand-alone Heimdal™ module, or our full range of state-of-the-art security tools, it holds unlimited potential for thorough cyber risk evaluations.



A holistic security approach. Real-time data. Clear, structured, and enhanced reporting.

Securely log in using 2FA and get accurate data and reports delivered in the intervals of your choosing.

Choose your desired timeframe or get access to your complete lifetime history. Data is graphed and scaled daily, weekly or monthly and can be integrated into SIEM via API.

The Heimdal™ UTD stores the entire history as long as you are our customer and will help you perform compliance audits and risk assessments. Coupled with weekly reports, data exports, email alerts and data drill down built in, Heimdal™ UTD offers a powerful and simple way to manage your environment.



The Heimdal™ Dashboard

Helps you get a customizable visual depiction of your data and it allows you to understand exactly what happens in your network and supports you to easily detect, avoid, and anticipate cyber threats.

By finding trends, recognizing patterns, and keeping track of essential details, the Heimdal™ UTD enables you to make perfect sense of your data. It reduces the time spent with reviewing details, decreases the possibility of overlooking crucial aspects, and supports you to take immediate action.

With Heimdal™, visualizing data is easy and flexible. You can filter it as needed, so you can view essential information in a manner that works best for you.

The Heimdal™ UTD Essential Features

Get an integrated view of the Heimdal™ cybersecurity controls of your choosing, all in a single place. Gain a rapid and accurate assessment of your cybersecurity posture, in real-time.

Choose exactly what you need or benefit from our entire product line-up, intelligently connected and talking together using AI.

Why choose Heimdal™'s Unified Threat Dashboard:

✓ Intelligently Connected

Heimdal™'s offering has been designed and perfected with a "one-agent- for-all" strategy in mind. This ensures that the more you plug in, the smarter they become.

✓ Overarching

Evaluates and measures your ability to prevent, detect and respond to threats and checks the networks, systems, processes, and users in your organization on an ongoing basis.

✓ Adaptive

It can be fully customized to suit a wide range of business requirements. It enables you to view accurate metrics and reports for everything of interest.

✓ Real-time

Get actual, live data from your environment. Heimdal™ UTD features continuous data aggregation and real-time alerts and reports, so you can continuously keep your organization secure.

✓ Fast

Benefit from quick setup and implementation, even in highly complex environments. Once configured, the Heimdal™ deployment is simple and easy and can happen through any MSI deployment tool.

Use the Heimdal™ dashboard and:

- ✓ Get actionable insights.
- ✓ Have lifetime history storage for auditing and compliance.
- ✓ Manage Group Policies and get Active Directory integration.
- ✓ Create policies which apply to your exact needs across the Active Directory groups in your organization.
- ✓ Define policies for each component in detail.
- ✓ Refine blacklisting of websites, files and processes or patches per Active Directory group.

Threat Prevention	Vulnerability Management	Endpoint Detection and Response	
<p>Next-Gen malware prevention, with HIPS</p> <p>Data leakage prevention and Forensics</p> <p>Quick response to hidden threats (Threat to Process Correlation)</p> <p>Hidden threat detection, with HIDS for what AV can't see</p>	<p>3rd Party Updates with Zero user interruption & Silent software installation.</p> <p>Automatic deployment/re- deployment of 3rd party and Microsoft patches.</p> <p>Deploy custom software (with optional add-on).</p> <p>Delay, version manage and rollback any update.</p> <p>Vulnerability inventory and CVSS scores included.</p> <p>Un-install supported software.</p> <p>Schedule of updates according PC clock</p> <p>Schedule and force reboots.</p>	Next-Gen Antivirus and MDM	Ransomware Encryption Protection
		<p>Next-Gen AV - Automated and Enhanced Threat Mitigation</p> <p>Firewall - block Brute Force Ransomware attacks from hitting Servers and Desktops. Full management of the Windows Firewall and device Isolation in case of major outbreaks.</p> <p>MDM solution - offers Threat Prevention and Next-Gen AV for mobile to locate, wipe, or lock remote devices.</p>	<p>Works with any Antivirus product and detects all processes trying to encrypt your files.</p> <p>Allows you to see the attack path through a process tree.</p> <p>Views attacker origins and file connections.</p>

Privileges & Application Control		Privileges & Application Control		Remote Desktop
PAM	Application Control	Email Security	Email Fraud Prevention	
<p>Elevate users or files</p> <p>Approval of escalation via dashboard or mobile app</p> <p>Pre-approve escalations (Auto- pilot mode)</p> <p>Prevent/De-escalate on infected machines*</p> <p>Ability to select period of escalation</p> <p>Pending escalation overview on Email and Email approval</p> <p>Ability to cancel pending usage rights</p> <p>Option to remove existing local admin rights (NIST AC-1,6)</p> <p>Option to block elevation of system files</p> <p>Individual rights per AD group (NIST AC-5)</p> <p>Can integrate with our Access Control</p> <p>Full audit trail.</p>	<p>Allow or Block execution of applications</p> <p>Allow or Block based on File Path, MD5, Publisher, Certificate or Software Name</p> <p>Passive Mode for system indexing</p> <p>Integrates with Privilege Access Management to allow Privileged users execution of files even where they are blocked</p> <p>Individual rights per AD group</p> <p>Full audit trail</p>	<p>Threat tracing & Full Audit Log</p> <p>Personal Quarantine Emails to users</p> <p>Greylisting and e-mail tagging</p> <p>Scanning of even Whitelisted senders</p> <p>Tagging of Emails from new senders</p> <p>Advanced Malware Filtering & Protection against ransomware</p> <p>Deep content inspection</p> <p>Full Forensic Data logging of the Email</p> <p>Customizable threat alerts</p>	<p>Monitoring of all Emails alongside existing email filtering solutions.</p> <p>Detection of BEC, CEO Fraud, Phishing and advanced malware.</p> <p>Find Imposter Threats (Modified invoices)</p> <p>Alerts you if historic emails are detected as malicious afterwards.</p> <p>Top 5 vectors include:</p> <ul style="list-style-type: none"> - Phraseology changes, IBAN/Account number scanning, attachment modification, link execution and scanning and man-in-the-email detection. - Can be connected to external invoice approval systems using API's. 	<p>Supports connections from:</p> <ul style="list-style-type: none"> - Dashboard-to-agent - Agent-to-agent - Dashboard-to-NO agent <p>Works via Application or via Web</p> <p>Secure connections with 2FA</p> <p>Attended/Unattended Access i.e. End-user request or IT accessed</p> <p>Transfer Remote Session to other supporters</p> <p>Invite other supporters to a session</p> <p>Multiple sessions at once are supported</p> <p>Clipboard Sharing, Content Sharing and File Sharing supported</p> <p>Works with our Privilege Access Management tool to raise elevations during sessions</p> <p>Video Recording and Audit Log option</p>