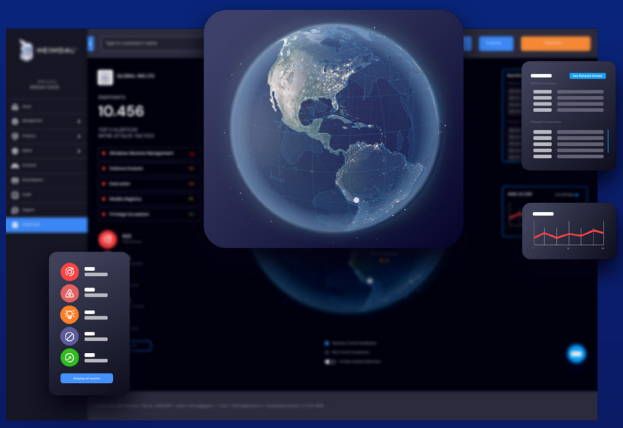
Heimdal®

Threat-hunting & Action Center

Product Sheet

Revolutionary / Unified / AI Cybersecurity



AT FIRST SIGHT:

VISUALIZE
Provides an advanced threat-centric view of the digital estate

HUNT
Empowers SecOps leaders and teams at all levels

REMEDIATE
Hunt and neutralize stealthy adversaries swiftly

ACTION
Mitigate enterprise risks from a single pane of glass

DID YOU KNOW THAT....

- **56% of large companies struggle with 1,000+ daily security alerts ***
- **Security staff spend 30 minutes on average for each alert that requires action ****
- **32 minutes are wasted every day chasing false positive alerts ****
- **27% critical alerts go unnoticed in companies with 500-1,500 employees ****
- **The figure reaches 30% in companies that have up to 5,000 employees ****

Visualize incidents with ease and achieve true action with unified data and risk prioritization

The Heimdal Threat-hunting and Action Center is a revolutionary platform that is fully integrated with the Heimdal solution suite. Designed to provide security teams with an advanced threat-centric view of their IT landscape, the solution employs granular telemetry to enable swift decision-making, using built-in hunting, remediation, and actioning capabilities – all managed from the Heimdal Unified Security Platform.

The Threat-hunting and Action Center leverages the industry-renowned MITRE ATT&CK techniques to help security teams proactively classify and prioritize security risks, hunt anomalies, and neutralize threats in a secure environment. This takes place behind the scenes, without disrupting users or impacting productivity and while adding the power of actionability to the suite.

Supercharge traditional ATP with our XTP Engine

The XTP Engine is Heimdal's amplified take on Advanced Threat Protection (ATP) solutions, which are known for providing enhanced cyber-defenses with a variety of next-gen tools that identify infiltration attempts in their early stages.

Heimdal's XTP Engine analyzes system audit events to detect and classify infinite threats with greater ease and higher accuracy, achieving a stunning 95% coverage of Windows Specific techniques in MITRE ATT&CK.

Hunt for advanced threats with the detection powers of the Heimdal® XTP Engine

The Threat-hunting and Action Center is powered by Heimdal's state-of-the-art eXtended Threat Protection (XTP) Engine, leveraging its detection powers to provide real-time visibility, rich threat intel, and contextual attack data. This empowers in-house teams to protect critical company infrastructures and react to sophisticated threats without the need for external expertise or augmentations.

Heimdal®

Features

Threat Telemetry Visualizer
An interactable globe and map view of organizational locations & endpoints

Threat Hunting & Analysis
Pinpoint groups and hosts that have IOCs across the network and track down their location with completely visualized endpoint-level intel

Enterprise Risk Reporting
Easy-to-digest organizational risk scores and recommendations for senior stakeholders to present in the board room

MITRE Risk Alerts & Visualizer
Pre-computed top 5 alerts by MITRE ATT&CK tactics for SecOps

Threat Detection & Classification
Via the XTP Engine which analyses logs using 2k+ rules and classifies risks and threats based on threat type

Action Controls
A handy hot action widget control panel that spans across detection, remediation action log, audit trails, and recommendations

Risk Remediation
Deep intel to review, resolve, or action a response straight from the console

Categorized Events
Classified by severity for analysts and hunters (critical, high, med, low)

Risk Scoring
Pre-computed risk trends and analysis filtered by day/month

Benefits

Single Pane of Glass
Fully integrated and consolidated with the Heimdal suite, XTP Engine, and MITRE ATT&CK techniques

Cybersecurity at the Forefront
Giving back the power of cybersecurity to employees with real-time insights and risk scoring to align security leaders, SecOps, and IT admins

Proactive Threat Hunting
Complete insight into what to look for and where with forensics view

The Tool for Incident Management Teams
Helps incident responders with investigating and closing down security gaps with actionable controls

No Alert Fatigue
Cut down on legacy and manual tools & aid stretched IT teams with contextualized and actionable intel

Painless Mitigation
Easy to switch to investigation and action mode

Who is the Heimdal® Threat-hunting & Action Center for?

Strategic

Security Leaders

- Enterprise-level risk reporting and prioritization
- Brings security posture into the boardroom
- Complete threat-centric view of the company's digital risk appetite
- Helps balance budget & skill gaps within the security department

Tactical

Security Practitioners

- Boosted hunting capabilities
- Reduced time and resource consumption on SecOps
- Adds supercharged detection and action capabilities to the standard suite
- Reduces alert fatigue through unification

Operational

MSSPs

- Fully adaptable multi-tenant architecture
- Visibility into the customer environment by risk and alerts to action
- Game changer for versatile and global customer environment management
- Efficient for all enterprise clients, regardless of seat size

Morten Kjaersgaard

CEO Heimdal®

"I am extremely pleased to announce that Heimdal is launching a product that will reshape cybersecurity as we know it. Our new Threat-hunting and Action Center will supercharge SecOps and leapfrog the effectiveness of any cybersecurity strategy. Heimdal is continuing its commitment to drive ground breaking changes to the industry, and we are certain that this new tool will evolve threat-hunting by mitigating risks faster with less effort, as well as drive a change in productivity for mid-market and enterprise customers, as well as MSP and MSSPs."

Sources

* https://techbeacon.com/security/35-stats-matter-your-security-operations-team

** https://www.criticalstart.com/resources/in-cybersecurity-every-alert-matters/

About Heimdal®

Gartner peerinsights. ★★★★★

SOURCEFORGE ★★★★★

G2 CROWD ★★★★½

Trustpilot ★★★★½

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.**