Heimdal®

# Threat-hunting & Action Center

## Leverage the power of unity

Solutions Brief

## Real-time threat hunting without the alert-fatigue and complexity is now a reality.

The **Heimdal® Threat-hunting and Action Center** is a powerful threat intel and hunting toolkit that equips security leaders, operations teams, and managed solution providers with the ability to detect and respond to next-gen threats using a visual storyboard across their entire IT landscape or customer base.

The platform provides granular **telemetry** into IT environments, endpoints, networks, and beyond to help teams proactively **classify** security risks, **hunt** detected anomalies, and **neutralize** persistent threats in a secure environment without risking the spread of attacks, disrupting end-users, or affecting organizational productivity.

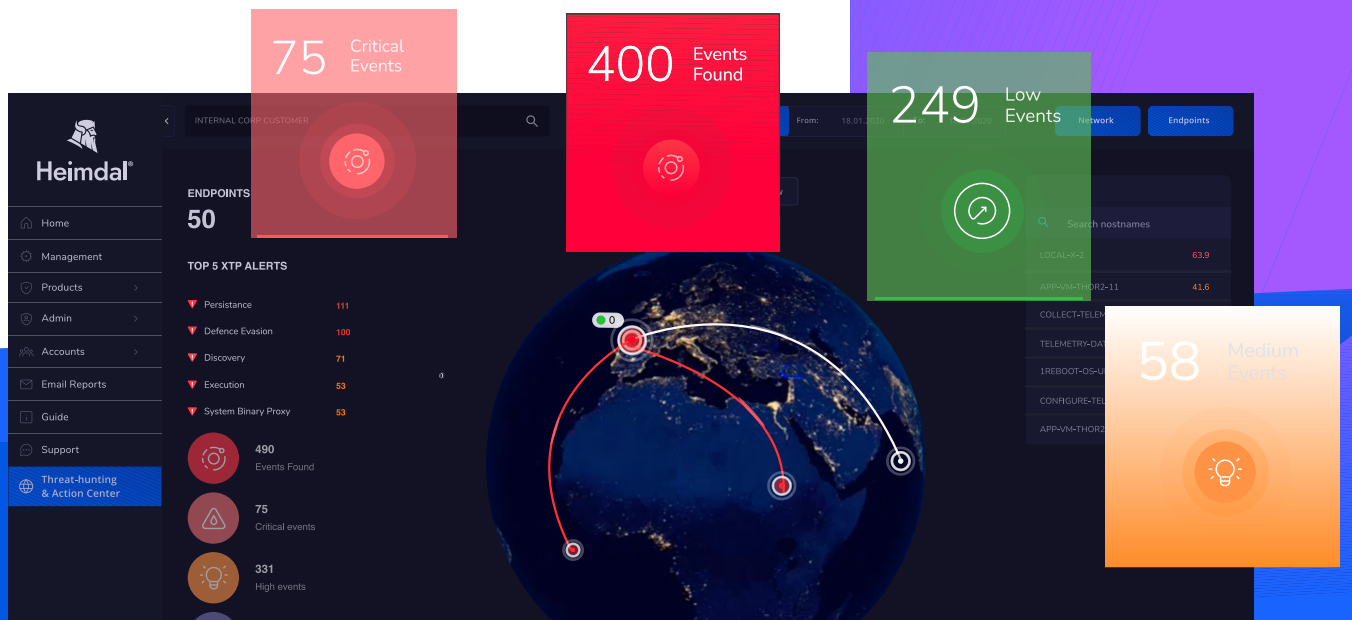
Our pioneering **action center** allows your security teams to make critical decisions on the-go with the ability to run and execute commands such as file scans, malware quarantines, software patches, machine isolation, and more with **1-click resolutions** while further investigating incidents or threats using the platform's deep analysis reporting modules.

Engineered and designed by Heimdal's security experts from the ground up, the platform features a **unified**, intuitive, and user-friendly **console.**

Say goodbye to manual and time-consuming security operations - the Heimdal Threat-hunting and Action Center jumpstarts a new era in security.

## KEY FEATURES

- Deploys **Out-of-the Box**
- Single **Unified** Platform
- **Integrated** with the Heimdal Suite
- Interactable **Threat Visualizer**
- Centralized **Data & Intel**
- **Pre-computed** Risk Scores & Event Categorization
- **MITRE ATT&CK** Catalogued
- Detailed **Forensics** Reports
- Dedicated **Action & Resolution Center**



Heimdal®

# Threat-hunting & Action Center

Leverage the power of unity

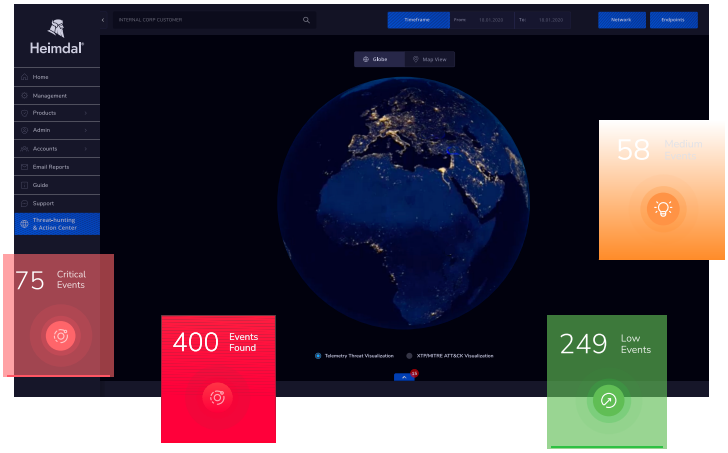
## VISUALIZE

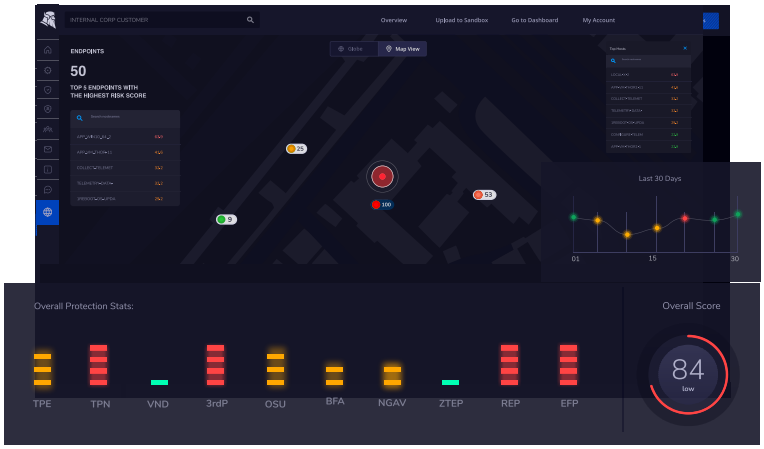
### Threat Telemetry Visualizer

An interactive globe and map view of the organizational locations and endpoints for an aerial view.

### XTP/MITRE ATT&CK Classified Risk & Events

Pre-computed top 5 alerts and events by severity and attack types are provided for SecOps teams to action.




## HUNT

### Track Weak Spots

Pinpoint groups and hosts that have IOCs across the network, and track down their location with completely visualized endpoint-level intel.

### Analyse & Enforce

Understand the complete process and pathways for high-risk accounts and systems, then jump in and provide corrective recommendations to stay ahead of vulnerabilities.

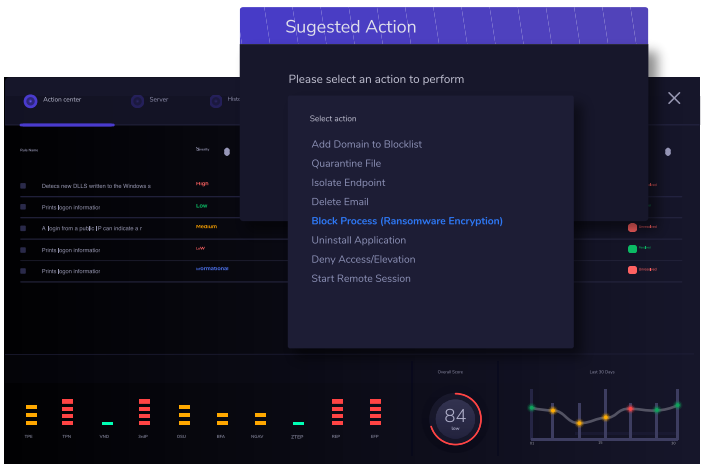
## ACTION

### Always-on Action Pane

The hot action widget spans across various areas, including detection, remediation, action logging, audit trails, and recommendations.

### Single Click Remediations

You can perform corrective actions, such as quarantine, isolate, scan, block, and more, against indicators of risk using just one command.



Heimdal®

# Threat-hunting & Action Center

Leverage the power of unity

## One Platform. Many Benefits.

### Empower teams at all levels.

#### CIOs, CISOs and Heads of Security

The stakes are high for security leaders to maintain reputation & compliance

- Enables enterprise-level risk reporting & prioritization in a single view
- Brings security posture into the boardroom with computed trends & scores
- Real-time threat-centric view of the company's digital risk appetite
- Helps balance budget & skill gaps within the security department

#### Security Ops and IT Admins

Bring back focus to things that matter to tactical teams

- Light-weight platform to monitor all digital artefacts globally
- Beat multiple tool toggling, management and false-positive reporting
- Reduced MTTD with risks that are pre-scored by priority indicators
- Faster MTTR with instant action and resolution center for lean teams

#### Managed Security and Service Providers

Supercharge security operations, portfolio, and customer protection

- Multi-tenant architecture enables speedy customer onboarding and management.
- Easily monitor multiple client environments through a single pane of glass.
- Resolve incidents for vulnerable customers at the point of risk with pre-scored indicators.
- Easily skill-up teams & scale operations alongside expansion of the customer base.

"Our new Threat-hunting and Action Center will supercharge SecOps and leapfrog the effectiveness of any cybersecurity operations. 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 enterprise, as well as MSP and MSSPs."

**Morten Kjaersgaard**
**CEO Heimdal®**

Gartner peerinsights ★★★★★

SOURCEFORGE ★★★★★

G2 CROWD ★★★★½

Trustpilot ★★★★½

Capterra ★★★★½

Expert Insights ★★★★½

HEIMDALSECURITY.COM