Heimdal®

THREAT HUNTING

Heimdal Threat-hunting and Action Center (TAC)

Leverage the Power of Unity in a Single Platform.

Solution Brief

Unified Threat-Hunting and Incident Response Across Your Entire IT Environment

The **Heimdal Threat-hunting and Action Center (TAC)** is a comprehensive, fully integrated SIEM and XDR solution that offers real-time insights across networks, endpoints, cloud environments, emails, and Microsoft 365 users.

With built-in User and Entity Behavior Analytics (UEBA) and Extended Threat Protection (XTP), Heimdal ensures robust, real-time protection against today's most sophisticated cyber threats.

TAC allows security teams to visualize, hunt, and act on threats across both **estate monitoring** (covering endpoints, networks, and cloud) and **user monitoring** (focused on user behaviors within cloud environments, like Microsoft 365).

KEY CAPABILITIES

- **Unified Visibility Across Endpoints and Users:** Monitor all network endpoints, network, and user activities in Microsoft 365 environments from a single pane of glass.
- **Centralized Threat Intel & Data Analysis:** Access real-time risk scores, MITRE ATT&CK catalogued events, and centralized data intelligence for a comprehensive view of threats.
- **Login Anomaly Detection (LAD):** Detect suspicious behavior like failed logins, logins from new geographies, anonymized IPs, or suspicious browsers. Built-in responses such as Logout, Acknowledge, and Dismiss streamline response and reduce manual review.
- **Email Security (ESEC) & Email Fraud Protection (EFP):** Track and analyze email activities for signs of spear phishing, fraud, and malicious attachments, and act on quarantined items.
- **Ransomware Encryption Protection (REP):** Identify ransomware-related activities and correlate them with user or endpoint behavior to quickly neutralize the threat.
- **Dynamic Risk Scoring:** Correlate data from LAD, ESEC, and REP to generate a comprehensive risk score for each user and device, enabling quick and efficient threat prioritization.
- **One-Click Remediation:** Take immediate action, such as isolating devices, logging out users, or revoking access with a single click.

Threat-hunting & Action Center

Dual-Faceted Threat Hunting: Estate and User Monitoring

Visualize

Gain full visibility across your infrastructure and workforce—covering endpoints, networks, cloud environments, and Microsoft 365. Monitor both device- and user-based behaviors through risk maps, login telemetry, and email activity.

Hunt

Detect and correlate anomalies using integrated threat data. Use pre-computed scores and forensic analytics to track infections, phishing, ransomware, login anomalies, and insider threats across the estate and M365 user accounts.

Action

Take immediate steps from the TAC interface: isolate endpoints, quarantine files, revoke sessions, log out users, or elevate investigations—whether the threat originates from infrastructure or identity.

Unified Action Center

The **Heimdal Threat-hunting and Action Center (TAC)** provides a unified interface for responding to security incidents across both endpoints and users. From a single pane, security teams can take real-time actions, such as:

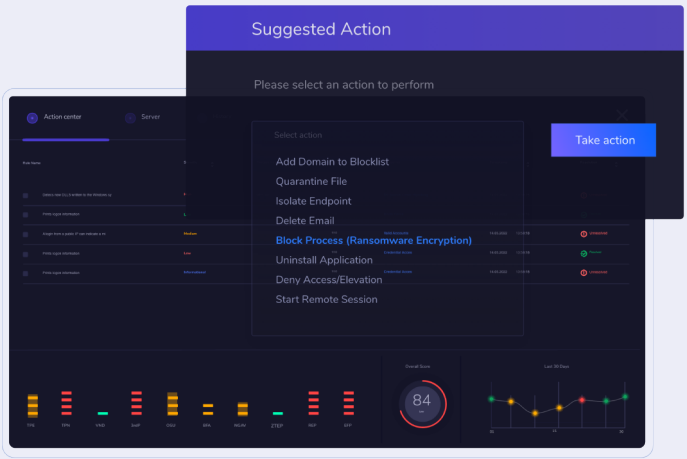
- Isolating compromised devices or users from the network.
- Revoking access or logging out users based on suspicious behavior.
- Quarantining threats or scanning devices for further investigation.

The platform's dynamic risk scoring engine aggregates telemetry across multiple modules—giving security teams a comprehensive view of their organization's posture and enabling intelligent prioritization.

Supported LAD Alert Types:

TAC's Login Anomaly Detection (LAD) engine detects critical user-based anomalies in Microsoft 365 environments, including:

- **Impossible Travel** – logins from geographically distant locations within an unrealistic timeframe
- **Unusual Login** – access from new or unrecognized countries
- **Anonymized IP Address** – logins via VPNs or proxies
- **Suspicious Browser** – access from unknown or untrusted browsers



Each LAD alert includes built-in remediation options: acknowledge, dismiss, or logout user—empowering teams to act instantly or escalate intelligently.

THREAT HUNTING

Threat-hunting & Action Center

Heimdal®

Benefits for Enterprises, MSPs, and SecOps

For Enterprises

- **Comprehensive User and Endpoint Monitoring:** Track risk levels and anomalies in real time for both users and devices.
- **Faster Incident Response:** Consolidate monitoring for endpoints and users, minimizing investigation times and improving remediation speed.
- **Microsoft 365 Protection:** Protect your users' identities and data through dynamic risk scoring and targeted remediation within M365 environments.

For MSPs

- **Multi-Tenant Management:** Manage multiple clients through a single platform, ensuring both endpoint and user protection.
- **Streamlined Operations:** Automated detection and response capabilities allow MSPs to handle more clients with fewer resources.
- **Scalable Threat Hunting:** Easily onboard new clients and scale security services without added complexity.

For SecOps Teams

- **Unified Threat Detection:** Use TAC to visualize risk across both users and devices, simplifying investigations.
- **Actionable Insights:** Take quick remediation actions from the Action Center—whether isolating a device or logging out a compromised user.
- **Reduced Alert Fatigue:** Contextualized alerts and pre-computed risk scores help SecOps teams prioritize real threats and avoid false positives.

Technical Requirements

To fully activate Heimdal's Threat-hunting and Action Center (TAC), the following modules are required:

Estate Monitoring: TAC requires the NGAV+XTP & MDM module for activation, along with at least two complementary modules, such as DNS Security, Ransomware Encryption Protection (REP), or Email Security (ESEC), to deliver comprehensive estate protection.

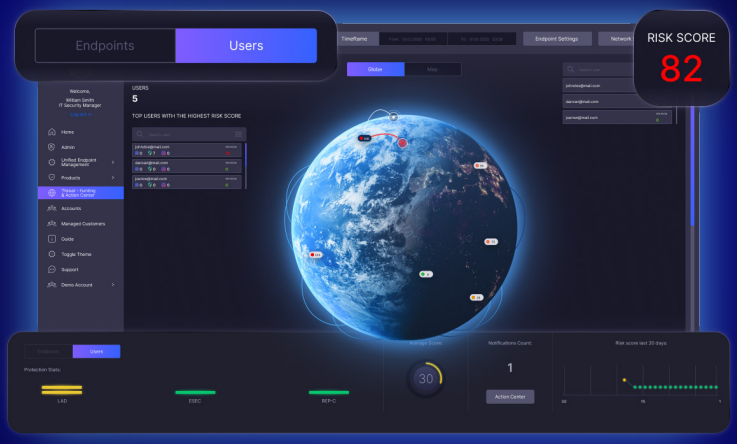
User Monitoring: Requires Login Anomaly Detection (LAD), Email Security (ESEC), and Ransomware Encryption Protection (REP) to track login anomalies, email threats, and ransomware-related user behavior.

Heimdal Threat-hunting & Action Center (TAC)

A Unified Threat-Hunting Solution for Complete Security Coverage

Revolutionize the way you manage cybersecurity with Heimdal's TAC. Get real-time visibility, automated remediation, and in-depth insights into both your endpoints and users. Stay ahead of sophisticated threats with advanced monitoring and actionable intelligence—all in a single platform.

Get a Demo →



heimdalsecurity.com

Gartner peerinsights ★★★★★ SOURCEFORGE ★★★★★ Capterra ★★★★★ Expert Insights ★★★★★