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 user login behavior, such as failed logins, logins from unrecognized IP addresses, or geolocation anomalies.
- **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

Heimdal®

Dual-Faceted Threat Hunting: Estate and User Monitoring

ESTATE MONITORING

Visualize

Gain enhanced visibility into your entire digital infrastructure in real time. With TAC's Estate Monitoring, you can monitor endpoints, networks, and cloud environments from a single pane of glass. View risk scores and critical anomalies across your organization's digital assets and take proactive steps to secure your IT estate.

Hunt

Identify and track threats across devices using Heimdal's integrated threat-hunting tools. Estate Monitoring within TAC enables security teams to investigate anomalies like malware infections, suspicious connections, and device vulnerabilities. Leverage pre-computed risk scores and forensic analytics to detect and neutralize threats before they compromise your infrastructure.

Action

Respond instantly to endpoint-level threats through the Estate Action Center. With one click, security teams can isolate infected devices, quarantine malicious files, or scan for vulnerabilities across your IT environment. The platform offers actionable insights that empower you to take decisive steps against any cyber threats.

USER MONITORING (M365 SECURITY)

Visualize

Monitor user behaviors and interactions within cloud environments, such as Microsoft 365. With TAC's User Monitoring, security teams can track login attempts, user activities, and email threats across the organization. The platform offers real-time, global visibility into user risk scores, enabling you to detect anomalies and take proactive action.

Hunt

Track anomalies in user behavior through advanced monitoring capabilities. With insights from Login Anomaly Detection (LAD), Email Security (ESEC), and Ransomware Encryption Protection (REP), you can identify potential insider threats, phishing attempts, and compromised credentials. Security teams can use the User Hunt functionality to proactively neutralize risks before they escalate.

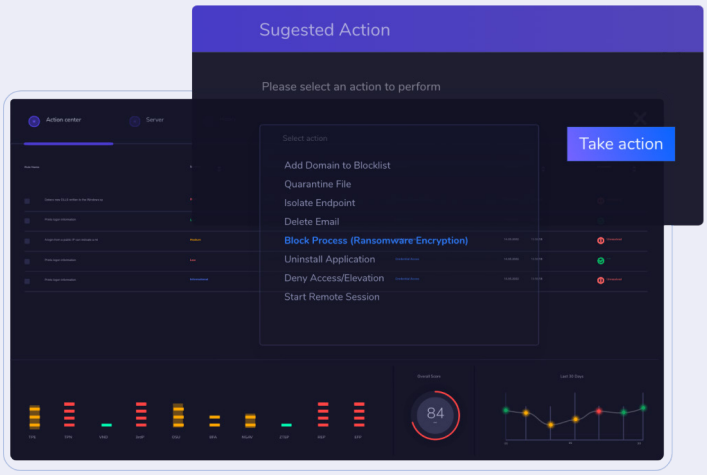
Action

Take swift, targeted action against user-related threats. The User Action Center allows security teams to log out compromised users, revoke session access, and investigate suspicious behavior with detailed forensics. Mitigate the risk of insider threats or credential compromises before they impact your organization.

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 risk scoring mechanism dynamically aggregates data from various modules, offering a comprehensive view of your organization's security posture.



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.

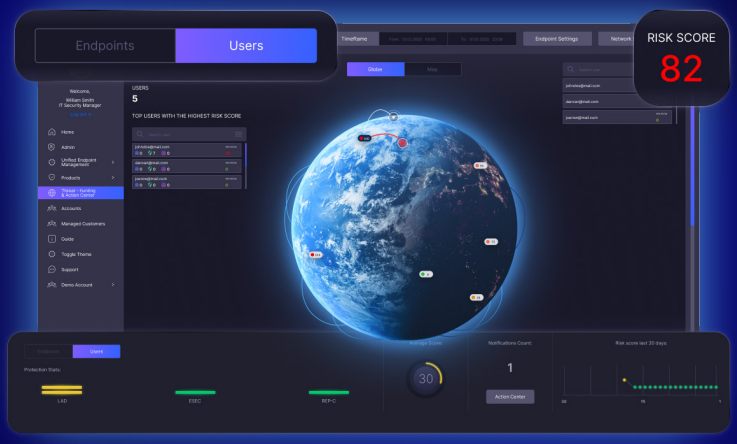
User Monitoring: Requires Login Anomaly Detection (LAD), Email Security (ESEC), and Ransomware Encryption Protection (REP) to track login anomalies, email threats, and ransomware-related user behavior.

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 ★★★★★