Heimdal

Heimdal Identity Threat Detection and Response (ITDR)

Stop identity attacks before they become breaches

Solution Brief

INTRODUCTION

Identity is the new perimeter. Attackers no longer need to break in when they can simply log in with stolen credentials, abused privileges or compromised cloud accounts. Traditional tools focus on endpoints or network traffic and often miss the early signs of identity misuse.

Heimdal ITDR (Identity Threat Detection and Response) is designed to close this gap. It gives security teams continuous visibility into how users log in, what they access and how privileges are used across endpoints and cloud services such as Microsoft 365. When behaviour looks risky, Heimdal ITDR helps you investigate, block and clean up the threat from the same console.

By combining identity analytics, email threat intelligence, endpoint telemetry and built in privilege control, Heimdal ITDR helps organisations of all sizes stop account takeover, Business Email Compromise and identity driven ransomware before they escalate.

HEIMDAL ITDR AT A GLANCE*

Heimdal ITDR brings together identity, endpoint, email and network telemetry in a single platform so you can see how identities are used and misused across your estate and respond quickly.

Heimdal ITDR is delivered through:

Core ITDR capabilities

- **Threat-hunting and Action Center (TAC)**
  Unified console with User and Estate views for correlating identity, email, endpoint and DNS events and triggering response.
- **Heimdal Email Security ATP with Fraud Prevention**
  Detects phishing, spoofing, Business Email Compromise patterns, malicious forwarding and risky mailbox rules.

Recommended add-on modules

- **Heimdal PAM suite (PASM and PEDM)**
  Available as an add-on to Heimdal ITDR. Replaces standing admin rights with controlled, audited, just-in-time elevation on endpoints.
- **Heimdal Remote Access Protection (RAP, part of the Heimdal NGAV module or EDR suite)**
  Available when the Heimdal NGAV suite is deployed. Controls and monitors remote access into endpoints and can shut down unauthorised sessions that rely on stolen credentials.

Managed delivery option

- **Heimdal SOC (optional managed-ITDR service)**
  Correlates Heimdal identity, endpoint, email and DNS events with relevant alerts from perimeter firewalls, where these are integrated into the service scope.

*Features and coverage vary by Heimdal modules selected and service scope. Not all capabilities apply in every deployment.

KEY IDENTITY SECURITY CHALLENGES

Account takeover and BEC risk

Attackers increasingly target user identities and email accounts, using stolen credentials and MFA fatigue to compromise Microsoft 365 and other cloud services.

Hidden persistence and data exfiltration

Malicious forwarding rules, mailbox manipulation and silent access to files make it hard for security teams to see when an account has been compromised.

Standing admin rights on endpoints

Local admin accounts and unmanaged privilege elevation give attackers easy paths to lateral movement and ransomware once a single identity is breached.

Fragmented visibility across tools

Identity logs sit in one place, email threats in another and endpoint alerts somewhere else. Without correlation, teams waste time pivoting between consoles.

Limited capacity to monitor 24/7

Many organisations do not have an in house SOC. Alerts are missed out of hours and teams struggle to keep up with investigations and response.

IMPACT AND BENEFITS

Earlier detection of identity attacks

Correlating suspicious sign ins, mailbox activity, file access and endpoint events makes it easier to spot account compromise at the “strange behaviour” stage instead of at the breach stage.

Reduced risk from admin and privileged accounts

Local admin rights are replaced with just in time elevation. Even if credentials are stolen, attackers have far less room to move laterally or deploy ransomware.

Fewer consoles, faster investigations

The Threat-hunting and Action Center brings identity, email, endpoint and DNS data into one view. Analysts can quickly pivot from a risky user to the devices, emails and events associated with that identity.

Less dependence on SIEM and SOAR

Many SIEM projects fail due to complexity and cost. Heimdal ITDR includes correlation, alerting and response workflows out of the box, so teams can gain ITDR capability without deploying a separate SIEM or SOAR stack.

Optional 24/7 managed cover

With Heimdal MXDR SOC, organisations that lack an in house SOC can gain round the clock monitoring, triage and response using the same platform, policies and playbooks.

KEY ITDR FEATURES

Suspicious sign-in and identity activity monitoring

Detect impossible travel, unusual locations, new devices and repeated MFA failures across Microsoft 365 and other identity providers. Risk views make it easy to focus on the accounts that matter most.

Malicious email forwarding and mailbox rule detection

Identify unauthorised forwarding rules, hidden folders and mailbox behaviours that can indicate Business Email Compromise, data exfiltration or insider threats. Rules can be investigated and remediated directly from the console or by Heimdal SOC.

Anomalous access to files and cloud data

Monitor access to content in cloud services such as Microsoft 365 for unusual patterns, including sudden permission changes and bulk downloads.

Behaviour analytics for users and identities

Track user behaviour over time across email, web, endpoint and identity events to spot when actions drift from normal baselines and may indicate compromise.

Endpoint privilege and admin control (Heimdal PAM suite – add-on)

Heimdal PAM enforces least privilege on endpoints, with approved or automated elevation and a full audit trail of administrative actions.

Remote access protection (Heimdal RAP – NGAV feature)

Heimdal RAP gives visibility and control over remote access into endpoints, helping to block unauthorised sessions that rely on compromised credentials.

Built-in response via TAC

From TAC, analysts can isolate devices, adjust or revoke elevation, disable or lock accounts and close remote sessions in a few clicks to contain identity threats quickly.

MANAGED ITDR WITH SOC

For organisations that prefer a managed service, Heimdal ITDR can be delivered as part of Heimdal SOC, our 24/7 managed detection and response offering.

The SOC team:

- Monitors identity, email, endpoint and network alerts around the clock
- Reviews and validates suspicious sign ins, mailbox changes and email forwarding rules
- Investigates high risk accounts and associated devices
- Takes corrective actions such as disabling malicious rules, isolating endpoints and executing response playbooks through your agreed policies
- Provides clear reporting on identity incidents and remediation

This model lets you keep control of strategy and policy while Heimdal handles day to day monitoring and incident response.

CONCLUSION

Identity attacks will only increase as organisations move more services and data to the cloud. Heimdal ITDR gives you the visibility, context and control you need to defend your users, protect sensitive information and meet regulatory expectations without adding unnecessary complexity.

Whether you’re an internal team or a service provider, we’ll help you choose the right mix of Heimdal ITDR and managed SOC.

Capterra ★★★★★ 4.8/5 | Expert Insights ★★★★★ 4.8/5 | Gartner peerinsights ★★★★★ 4.8/5

Learn More