

Heimdal Managed Extended Detection and Response (MXDR)

24/7 managed detection and response, powered by the Heimdal Unified Security & Compliance Platform

Solution Brief

INTRODUCTION

Security teams are expected to detect, investigate and respond to threats faster than ever, often with limited people, budget and time. At the same time, attacks now move across endpoints, identities, email, DNS, remote access and network layers, making it harder to understand what is really happening from one console.

Heimdal MXDR gives organisations 24/7 managed detection and response delivered by Heimdal's Security Operations Center. It combines platform telemetry, expert investigation and agreed response actions across key security layers including endpoint, email, identity, DNS and, where configured, perimeter firewall telemetry.

Built on the Heimdal Unified Security & Compliance Platform, MXDR helps teams reduce alert fatigue, accelerate investigations and contain threats before they become business-impacting incidents.

HEIMDAL MXDR AT A GLANCE*

Heimdal MXDR is a managed SOC service that helps security teams monitor, investigate and respond to threats across their estate.

Heimdal MXDR is delivered through:

CORE MXDR SERVICE

- **24/7 Security Operations Center**
Continuous monitoring, triage and investigation by Heimdal SOC analysts.
- **MXDR ADAPT**
Defines the agreed service permissions and response model, from notify and advise through to approved action.
- **Threat investigation and analysis**
Analyst-led review of suspicious activity, including Heimdal telemetry, event logs, firewall logs where integrated, remote sessions, XTP logs, collected samples and sandbox testing where relevant.
- **Email and Microsoft 365 investigation layer**
Enriches MXDR investigations with email security, mailbox and Microsoft 365 activity, including suspicious sign-ins, forwarding rules, email fraud indicators and other account compromise signals where enabled.
- **Firewall and network-layer alert investigation**
The SOC can review perimeter firewall alerts and firewall logs where these are integrated into the MXDR service scope, helping correlate network activity with endpoint, identity, email and DNS signals.

KEY SECURITY OPERATIONS CHALLENGES

- ✓ **Too many alerts, not enough context**
Security teams often deal with large volumes of alerts across separate tools, making it difficult to identify which events need immediate action.
- ✓ **Limited 24/7 coverage**
Many organisations lack a full in-house SOC. This leaves gaps overnight, during weekends and across lean teams.
- ✓ **Threats move across multiple layers**
Modern attacks rarely stay in one place. A single incident may involve identity misuse, email compromise, endpoint activity, DNS traffic and remote access.
- ✓ **Slow manual investigations**
Without a structured workflow, analysts waste time collecting evidence, switching between consoles and deciding which response steps are safe to take.
- ✓ **Unclear response ownership**
Teams need clear rules for when the SOC should notify, advise or act, especially during high-risk incidents.

Ready to strengthen your security operations?

[Book an MXDR demo](#)



- **Response and containment**
Action through agreed policies, including endpoint isolation, antivirus scans, file quarantine, exploit removal, password reset, user logout and other approved response actions.
- **AI-assisted investigation and prioritisation**
Heimdal MXDR uses platform intelligence and analyst-led workflows to help prioritise alerts, reduce noise and accelerate investigation across endpoint, identity, email and network events.

MXDR COVERAGE AREAS

- MDR** **Managed Detection and Response (MDR)**
Endpoint, malware, exploit, ransomware and device-level threat monitoring and response.
- NDR** **Network Detection and Response (NDR)**
DNS, firewall and network-layer alert investigation where relevant data sources are integrated into the service scope.
- ITDR** **Identity Threat Detection and Response (ITDR)**
Suspicious sign-ins, login anomalies, account compromise indicators, mailbox changes, email forwarding rules, email security and fraud alerts, SharePoint / OneDrive anomalies and identity-led attack activity.

* Features, response actions and coverage vary by Heimdal modules licensed, deployed and included in the agreed MXDR ADAPT service scope. Not all capabilities apply in every deployment.

IMPACT AND BENEFITS

-  **Round-the-clock detection and response**
Continuous SOC monitoring, triage and investigation helps teams detect and respond to threats faster, even outside normal working hours.
-  **Less alert fatigue for internal teams**
The SOC filters, investigates and prioritises alerts so your team can focus on business-critical work instead of manually chasing every signal.
-  **Broader visibility across the attack chain**
MXDR correlates signals across endpoint, email, DNS, identity and network layers, helping analysts understand how an incident is unfolding.
-  **Clear response model**
MXDR ADAPT defines what the SOC can do, when it should notify you and when it can take action based on agreed permissions.
-  **Stronger resilience for lean teams**
Organisations without a full SOC can gain 24/7 monitoring, expert investigation and response support without building the function from scratch.

MANAGED RESPONSE MODEL

A managed SOC that works through your agreed scope

Heimdal MXDR is not a black box. The service is governed by MXDR ADAPT, which defines the permission category, response scope and actions available to the SOC.

Depending on the agreed service scope, Heimdal MXDR can cover:

-  **Endpoint and server alerts**
-  **Email security and email fraud alerts**
-  **Microsoft 365 user security indicators**
-  **Login anomalies and operational identity alerts**
-  **SharePoint and OneDrive anomalies, where available**
-  **DNS and web security events**
-  **Remote access activity**
-  **Perimeter firewall alerts and firewall logs, where integrated**
-  **Malware, exploit and ransomware indicators**

The SOC team can then investigate, advise or act according to your agreed policies and severity level.

KEY MXDR CAPABILITIES

24/7 SOC monitoring

Heimdal analysts monitor alerts around the clock across the security layers included in your service scope.

Alert triage and classification

Alerts are reviewed and classified by risk level, helping teams understand whether an event is informational, low, medium, high or critical.

Threat investigation

The SOC investigates suspicious events using Heimdal telemetry, endpoint data, email activity, DNS events, firewall logs where integrated and other available evidence.

Malware and exploit analysis

When needed, the MXDR team performs malware investigation, static and dynamic analysis, sample review and sandbox testing to validate impact and guide response.

Identity and email compromise monitoring

The SOC reviews Microsoft 365 and email security signals, including suspicious sign-ins, login anomalies, mailbox changes, email forwarding rules, email security alerts, email fraud alerts and operational identity alerts such as MFA issues, password rotation and password complexity. Analysts also review SharePoint and OneDrive anomalies where these signals are available in scope.

Response actions through agreed policies

Depending on MXDR ADAPT permissions, Heimdal can perform actions such as endpoint isolation, file quarantine, antivirus scans, exploit removal, disabling malicious rules, password reset or user logout.

Reporting and incident follow-up

MXDR provides analysis results, advisory reporting and post-incident reporting where relevant, helping teams understand what happened and what to improve next.

CONCLUSION

Heimdal MXDR gives organisations a practical way to strengthen security operations without building a full SOC from scratch. By combining the Heimdal Unified Security & Compliance Platform with 24/7 analyst-led monitoring and response, MXDR helps you detect threats earlier, investigate faster and contain incidents before they escalate.

Whether you need MDR, NDR, ITDR or a wider managed response model, Heimdal MXDR provides a flexible SOC service built around your environment, permissions and risk profile.



2026 Heimdal® All rights reserved. Registered trademarks and service marks are the property of their respective owners.

HOW HEIMDAL MXDR WORKS

The Heimdal MXDR workflow follows a structured path from alert classification to investigation, response and remediation. MXDR ADAPT defines whether Heimdal should notify, advise or take action based on agreed permissions and severity.

