

Heimdal Email Security

Stop phishing, malware and email fraud before they reach the inbox

Solution Brief

INTRODUCTION

Email remains one of the easiest ways into a business. A familiar invoice, a trusted display name or one well-timed request can lead to stolen credentials, malware or Business Email Compromise (BEC).

Email Security scans inbound and outbound mail in Microsoft 365 & Google Workspace environments. Anti-spam and anti-malware engines, sender authentication, attachment and content inspection, quarantine and investigation tools work together in one cloud platform.

For higher-risk environments, Advanced Threat Protection (ATP) & Fraud Prevention adds sandboxing, AI-powered outlier detection, post-delivery alerts and forensic logging. Admins can see why a message was flagged and respond from the Heimdal Dashboard.

HEIMDAL MXDR AT A GLANCE*

Choose between two protection levels. Microsoft 365 customers can deploy through Heimdal's MX gateway or the M365 Exchange Connector.

Heimdal MXDR is delivered through:

CORE EMAIL PROTECTION

- **Email Security 365**
Scans inbound & outbound mail for spam, viruses, botnet activity, phishing and unsafe attachments. It also provides sender authentication, TLS controls, greylisting, allowlists and blocklists, quarantine reports and configurable archiving.

FLEXIBLE DEPLOYMENT

- **MX-record gateway**
Routes inbound emails through Heimdal's regional gateways. Outbound emails can also be relayed via Heimdal for inspection.
- **Email Security 365 – Integrated Cloud Email Security (ICES)**
For Microsoft 365, protect email through Exchange Connectors without changing MX records. Connector-based mail flow scans inbound Microsoft 365 email through configured routing, while a health check validates readiness before routing changes are applied.

ADVANCED PROTECTION

- **Email Security Advanced Threat Protection (ATP) & Fraud Prevention**
Adds advanced sandboxing, deep attachment inspection, AI-powered outlier detection, post-delivery alerts and forensic logging. More than 125 analysis vectors help expose targeted phishing, impersonation and BEC.

KEY EMAIL SECURITY CHALLENGES

- ✓ **Phishing and malicious content**
Links and attachments can steal credentials, deliver malware or set a ransomware incident in motion. Evasive content is built to get past basic filters.
- ✓ **BEC and impersonation**
Fraudulent messages can mimic executives, suppliers or colleagues without using malware. Sender checks and behavioral context matter.
- ✓ **Threats already delivered**
Sometimes a message is recognized as malicious only after delivery. Teams need to find and remove it from affected Microsoft 365 mailboxes.
- ✓ **Outbound abuse**
A compromised mailbox can send spam, malware or fraud, damaging domain reputation. Outbound scanning helps contain the fallout.
- ✓ **Disconnected tools**
Separate consoles for email, users and remediation slow investigations and leave teams piecing together context.

UNIFIED VISIBILITY AND RESPONSE

- **Heimdal Dashboard and Threat-hunting and Action Center (TAC)**

Shows inbound and outbound activity, user anomalies, domain status, message details and audit history. With ICES, quarantined, rejected and security-relevant email events can also be reviewed in TAC.

**Features and available actions vary by license, protection level, deployment method, email platform, configured modules, tenant consent and permissions.*

IMPACT AND BENEFITS



Stop threats before they reach users

Layered checks cover reputation, authentication, TLS, malware, spam, attachments and advanced threats. Suspicious mail can be tagged, quarantined or rejected.



Find attacks ordinary filters miss

Advanced Threat Protection & Fraud Prevention combine deep content analysis, sandboxing and behavioral signals to detect BEC, impersonation and targeted fraud that conventional malware filters miss.



Fit deployment around your environment

Use the MX gateway with Microsoft 365 or Google Workspace. Exchange Online customers can instead use the M365 connector without changing their MX records.



Investigate and clean up faster

Real-time views, granular filters, message details and audit logs keep the evidence together. With the required Microsoft 365 permissions, admins can move delivered messages to Deleted Items or remove them from the mailbox.



Give users control without losing oversight

Quarantine reports and the end-user console let users review messages and manage personal lists. Admins decide what users can preview or release, and whether they can allow the sender.

KEY EMAIL SECURITY FEATURES



Anti-spam, malware and phishing protection

Inspects inbound and outbound mail through Heimdal's regional cloud infrastructure, combining IP reputation, configurable spam scoring, virus and malware scanning, phishing protection and attachment rules.



Sender and transport checks

Supports SPF and DMARC validation, outbound DKIM signing and TLS controls. DNSSEC and DANE/TLSA are supported for inbound SMTP.



Quarantine, investigation and retention

Set actions by score or threat type, let users manage personal lists, search mail-flow activity, track remediation in audit logs and archive email for up to one year.



Advanced Threat Protection & Fraud Prevention

Machine learning, deep content inspection, sandboxing and neural-network analysis spot suspicious links, clickbait and anomalies in language, HTML, attachments and sending times.

MICROSOFT 365-READY DEPLOYMENT AND RESPONSE

Microsoft 365 customers can protect email through Exchange Connectors without changing MX records. Connector-based mail flow scans inbound Microsoft 365 email through configured routing, reducing setup friction where MX changes are slow or sensitive.

The Microsoft 365 integration provides:



Connector deployment without MX changes



Connector-based inbound mail flow



Faster Microsoft 365 rollout



A health check that validates connector readiness



M365 email visibility in TAC



Inbox investigation with email, endpoint and identity context

Available visibility and response actions depend on the configured modules, tenant consent and Microsoft 365 permissions.

CONCLUSION

Email attacks are more than a spam problem. They exploit trust, timing and everyday business conversations. Email Security protects the full mail flow with layered controls, advanced analysis and practical investigation and clean-up tools.

Start with Email Security 365 for core protection. Add Advanced Threat Protection (ATP) & Fraud Prevention when BEC, impersonation and evasive content demand behavioral analysis and stronger forensics. Microsoft 365 customers can choose the MX or connector route that best fits their environment.

