Managed Extended Detection and Response

Heimdal offers an end-to-end, proactive, unified cybersecurity suite built to defend against next-gen threats. Its unique, multi-layered approach provides comprehensive protection through a fully integrated network and endpoint protection suite.

Key features

- Immediate enterprise protection with environment-agnostic deployment via a unified platform

- 24/7 proactive monitoring and threat remediation from accredited Heimdal SOC analysts

- Faster detection and response with automated actions across multiple environments

- Streamlined threat management to eliminate alert fatigue for security teams

- Advanced investigations and forensics handled by Heimdal free up MSP resources

- Extensive customisation with a variety of pre-configuration rules

Heimdal is the only vendor in the market with an offering that combines next-generation antivirus, DNS-level traffic filtering on the endpoint, silent, automated third-party patch management, privileged access management, email security, and a managed service in one platform.

Why Heimdal MXDR?

Heimdal Managed Extended Detection and Response (MXDR) offers total protection. Its proactive detection and response services address the growing complexity of today's security landscape. Powered by the Heimdal XDR Unified Security Platform, MXDR enables real-time threat detection, providing extensive coverage. AI-driven detection and behavioural pattern analysis ensure genuine threats are swiftly identified and mitigated, and the lightweight, easy-to-deploy design delivers rapid protection with minimal configuration.

Challenges Heimdal MXDR solves

Heimdal MXDR addresses the complexities of managing a vast and evolving attack surface. It offers 24/7 managed detection and response, ensuring critical threats are escalated and neutralised quickly. The platform's unified threat intelligence provides comprehensive visibility and expertise from dedicated Security Operations Centre (SOC) analysts. Heimdal MXDR enhances incident investigation, minimises downtime, and adapts security strategies to evolving threats. Highly customisable for MSPs, it offers tailored detection rules and outsourced 24x7x365 monitoring, making it attractive for those who wish to avoid in-house round-the-clock teams now required by an always-on cybersecurity landscape.