Heimdal

# Security & Compliance at Scale: MFT Unifies Patching & Access for Cyber Assurance

Case Study - Public Sector, Healthcare (UK National Health Service)

## CHALLENGES

- **Patching Gap on Servers & Endpoints:** MFT lacked an automated, unified solution for patching third-party software across its extensive server and endpoint estate, directly impacting its national MDE Cyber Posture score.
- **Uncontrolled External Access:** The Trust engaged hundreds of external suppliers who required privileged access via RDP, often without complete visibility, full audit trails, or standardized MFA controls.
- **Complexity and Visibility:** The reliance on disparate systems (WSUS, SCCM, previous patching tools) complicated reporting, resource management, and providing cyber assurance that patching was occurring consistently across the entire infrastructure.
- **CAF and DSPT Compliance:** The Trust needed demonstrable, auditable evidence of control over privileged access and third-party risk mitigation to satisfy key requirements under the DSPT (e.g., B2C, B2D) and CAF.

## SOLUTION

MFT strategically adopted multiple components of the Heimdal platform, specifically selected to address its biggest security and operational gaps related to patching automation and privileged access management.

**Key Components Deployed:**

- **Patch & Asset Management with Infinity Management:** Deployed for automated operating system and third-party software patching across all **30,000+ endpoints and servers.** This unified approach provided a "set and forget" capability that was instrumental for both server and endpoint security.
- **Privileged Account Management & Session Management (PASM):** Implemented to control, audit, and secure external supplier access (Guest Accounts via Entra ID) and, subsequently, for internal IT teams, ensuring all privileged connections are monitored, justified, and time-bound (Just-in-Time access).
- **Remote Desktop:** Utilized as a secure, unified tool for IT support teams and service desk agents to offer enhanced remote assistance, supporting the redevelopment of MFT's remote support processes.

## INTRODUCTION

Manchester University NHS Foundation Trust (MFT) is one of the largest and most complex healthcare organizations in the UK. Facing continuous pressure to meet national cybersecurity standards, MFT required a scalable solution to address critical security gaps: automating third-party software patching across its massive estate, and gaining granular visibility and control over privileged access for both internal teams and a large network of external suppliers. The Trust chose Heimdal to deliver a focused, unified platform to meet these objectives and support compliance efforts like the Cyber Assessment Framework (CAF) and Data Security and Protection Toolkit (DSPT).

NHS
Manchester University
NHS Foundation Trust

## ABOUT MANCHESTER UNIVERSITY NHS FOUNDATION TRUST

MFT operates across multiple sites, managing a vast infrastructure of **over 30,000 endpoints** and over **1,300 servers** to provide comprehensive patient care services. The Trust is instrumental within the Greater Manchester Integrated Care System (ICS) and is a leader in regional healthcare collaboration. Its cybersecurity function is tasked with maintaining a continuously improving security posture, optimizing its Microsoft Defender Endpoint (MDE) score, and ensuring stringent adherence to national compliance mandates required across the NHS.

## IMPACT AND BENEFITS

- **Rapid Deployment at Scale:** Despite the massive scale of the environment, MFT achieved **100% deployment and went live in less than 3 months** from the license start date, demonstrating the platform's ease of implementation in complex enterprise environments.
- **Improved National Security Score:** The implementation of automated third-party patching was instrumental for **both servers and endpoints**, resulting in a significant and marked reduction (improvement) in MFT's national **Microsoft Defender Endpoint (MDE) Cyber Posture score.**
- **Zero-Trust for External Suppliers:** PASM enabled MFT to mandate its own MFA and Conditional Access policies, replacing unsecured RDP with controlled, audited access. Suppliers now use Guest Accounts (Entra ID) and must justify and time-limit their connections (e.g., 24-hour maximum sessions).
- **Proactive Threat Hunting and Auditability:** MFT gained complete visibility and accountability over privileged connections, enabling quick termination of sessions during a compromise and providing granular audit logs essential for CAF and DSPT reporting.
- **Strategic Partnership:** MFT leveraged a collaborative, region-wide procurement through the Greater Manchester Integrated Care System (ICS) to access strategic benefits and reduced costs, setting a blueprint for future NHS regional security projects.

## WHY HEIMDAL FOR NHS & PUBLIC SECTOR (UK)

NHS Trusts and government bodies require solutions that deliver enterprise-grade security while integrating seamlessly into existing infrastructure and adhering strictly to national compliance frameworks.

- **MDE and Compliance Optimization:** Heimdal directly assists Trusts in improving their MDE scores and providing the necessary log data and control mechanisms to satisfy key requirements of the Cyber Assessment Framework (CAF) and the Data Security and Protection Toolkit (DSPT).
- **Vendor Control and Auditability:** PASM provides the essential, centralized control required to manage and audit access for a vast network of external suppliers, enforcing zero-trust principles and securing critical patient data systems.
- **Scale and Automation:** The platform is proven to operate successfully at the scale of the largest UK Trusts, automating high-volume tasks like third-party patching across servers and desktops to free up highly specialized IT resources.
- **Strategic Partnership:** Heimdal actively engages with regional Integrated Care Systems (ICS) and national teams, offering a strategic approach to procurement and product development that aligns with the evolving needs of the NHS.

## CONCLUSION

Heimdal's unified platform provided MFT with a robust foundation for modern cyber assurance, delivering measurable improvements in patching compliance and unparalleled control over privileged access across thousands of endpoints and hundreds of external parties. By acting as a core technology provider for the Greater Manchester ICS, Heimdal is positioned as a strategic partner supporting the NHS's long-term digital security goals.

> *"The patching solution is performing as expected, resulting in a marked improvement in our MDE score. Furthermore, the PASM implementation is going exceptionally well, positioning us strongly for DSPT compliance by ensuring full visibility and auditability of all privileged access connections."*

**- Scott Willis,**
Head of Cybersecurity Architecture

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



Learn More