NHS North West London Enhances Cybersecurity with Heimdal's PEDM, Application Control, and DNS Security

With Heimdal's unified platform, NHS North West London ICB enforced Zero Trust principles, streamlined privilege management, and elevated threat prevention across its entire GP

Case Study - Public Sector, Healthcare

CHALLENGES

Admin Privilege Risks Across 400 GP Practices

Historically, NHS North West London ICB issued local admin rights to all GP practice devices. This created serious security risks, including unauthorized software installations, insider threats, and privilege escalation attacks.

Overcoming Cultural Resistance to Security Changes

Doctors and staff were accustomed to full admin control, making it difficult to enforce new security policies. The IT security team needed executive buy-in and a structured communications strategy to drive adoption.

Reducing IT Costs & Physical Site Visits

Prior to Heimdal, IT engineers had to physically visit GP practices to remediate security issues. This was costly, inefficient, and slow, leaving devices vulnerable for longer periods.

NHS
North West London
NHS Foundation Trust

ABOUT NHS NORTH WEST LONDON

NHS North West London Integrated Care Board (ICB) is responsible for securing one of the UK's largest healthcare regions, supporting 400 GP practices and over 10,500 devices. With a mission to modernize IT security, the ICB sought to eliminate privilege risks, prevent cyber threats, and improve operational efficiency.

SOLUTION

Why NHS North West London Chose Heimdal

To address these challenges, NHS North West London ICB deployed:

- Privileged Elevation & Delegation Management (PEDM) – Removed permanent admin rights and enabled controlled, time-limited privilege escalation.
- Application Control – Allowed only approved applications, preventing unauthorized installations and reducing malware risk.
- DNS Security – Blocked malicious domains and phishing attempts, stopping threats at the network level.
- Compliance & Auditing – Provided full visibility & 90-day logs to meet NHS security standards (DSPT Toolkit & Cyber Assurance Framework - CAF).
- Remote Security Management – Allowed IT teams to manage security centrally, eliminating unnecessary site visits.

IMPLEMENTATION & ADOPTION

From Pilot to Full Rollout

The ICB first tested Heimdal across five GP practices, ensuring compatibility with clinical systems EMIS and SystmOne. The successful trial led to full deployment across all 400 GP practices.

To ensure smooth adoption, a communications campaign was launched, educating staff on how to request privilege elevation while reinforcing the importance of Zero Trust security.

> ***"We developed a policy, secured board-level approval, and implemented a communication campaign to educate staff. In just a few weeks, Heimdal significantly enhanced our security posture."***
>
> **Abhilash Abraham**
> Head of IT Security & Cybersecurity, NHS North West London ICB

HEIMDAL'S IMPACT

Eliminating Privilege-Based Security Risks

- Permanent admin rights removed, reducing privilege escalation attacks.
- Only approved applications can be executed, preventing unauthorized software installations.

Faster Incident Response & Reduced IT Costs

- Significantly reduced IT site visits, cutting operational costs.
- Enabled real-time isolation of compromised devices, stopping threats before they spread.

Seamless Integration with NHS IT Ecosystem

- Heimdal solutions worked alongside existing security tools, without forcing vendor lock-in.
- Fully aligned with NHS Cyber Assurance Framework (CAF) and DSPT Toolkit compliance

ACKNOWLEDGING LEADERSHIP SUPPORT

The success of this transformation was driven by strong leadership support. David Thomas, Deputy Director of ICT and Kevin Jarrold, CIO NWL ICB played a critical role in securing board approval, ensuring that the policy changes and security rollout had full executive backing.

> ***"Our leadership understood the need for cultural change and actively supported the transition, facilitating the seamless enforcement of Zero Trust security across our practice."***
>
> **Abhilash Abraham**
> Head of IT Security & Cybersecurity, NHS North West London ICB

Heimdal®

NHS North West London Enhances Cybersecurity with Heimdal's PEDM, Application Control, and DNS Security

CONCLUSION

NHS North West London's deployment of Heimdal PEDM, Application Control, and DNS Security has redefined cybersecurity best practices in the NHS. By removing admin rights, preventing unauthorized applications, and blocking cyber threats at the DNS level, the ICB has achieved:

- Stronger security with Zero Trust enforcement
- Seamless compliance with NHS security regulations (CAF, DSPT)
- Significant cost savings by eliminating unnecessary IT visits
- A more resilient and secure IT infrastructure for the future

"Heimdal revolutionized our approach—not just to security, but to risk management, compliance, and operational efficiency across NHS North West London."

Abhilash Abraham
Head of IT Security & Cybersecurity, NHS North West London ICB

WHY ACCESS & APPLICATION CONTROL MATTER IN HEALTHCARE

In healthcare, security isn't just about protection — it's about precision. Over-provisioned access and unregulated applications can introduce serious risks. Heimdal's PEDM and Application Control give NHS North West London the tools to enforce least privilege, block unauthorised software, and stop threats before they impact patient care — all without disrupting clinical workflows.

WHY HEIMDAL FOR HEALTHCARE?

The healthcare sector faces increasing cyber threats, regulatory challenges, and the need for uninterrupted patient care. Heimdal provides a unified security platform tailored to the demands of healthcare organizations, ensuring compliance and proactive threat defense.

- **Comprehensive Protection** – From ransomware defense to DNS security, Heimdal safeguards healthcare institutions across all attack vectors.
- **Regulatory Compliance** – Supports CAF, GDPR, HIPAA, and other frameworks with automated tools and reporting.
- **Streamlined Security Management** – A unified console provides full visibility and control, reducing complexity for IT teams.
- **Proactive Threat Prevention** – AI-driven intelligence and 24/7 monitoring detect and stop cyber threats before they impact critical operations.
- **Cost-Effective & Scalable** – Designed to fit healthcare institutions of all sizes, ensuring long-term security resilience.

Heimdal empowers healthcare organizations to secure patient data, prevent cyber threats, and ensure operational continuity with minimal disruption.

Learn More →

Gartner peerinsights ★★★★★ SOURCEFORGE ★★★★★ Capterra ★★★★★ Expert Insights ★★★★★