Heimdal®

Heimdal for Compliance: NHS Cyber Assessment Framework (CAF)

Empowering Healthcare with Resilient Cybersecurity

Data Sheet

Introduction

The Cyber Assessment Framework (CAF), developed by the UK's National Cyber Security Centre (NCSC), is a comprehensive guideline introduced in 2018 to enhance the cybersecurity posture of organizations managing essential services, including those in the healthcare sector. The framework is designed to help organizations achieve and demonstrate an appropriate level of cyber resilience

Latest Developments

In 2024, the NHS began transitioning its cybersecurity framework to align with the **National Cyber Security Centre's (NCSC) Cyber Assessment Framework (CAF)**. This change is part of the Department of Health and Social Care's (DHSC) Cyber Security Strategy for Health and Social Care 2023–2030, aiming to enhance cyber resilience across the sector. The CAF provides a comprehensive, outcome-focused approach to safeguarding essential healthcare services, making it a critical step for organizations responsible for patient data and operational continuity.

For NHS organizations and suppliers designated as operators of essential services (OES), adopting the CAF-aligned Data Security and Protection Toolkit (DSPT) will become a **mandatory requirement soon.** NHS England has already started notifying organizations about their scheduled transition, ensuring they are supported throughout the process. This shift is not just a recommendation—it is a structured mandate that ensures organizations meet the evolving cybersecurity challenges while aligning with national priorities.

For healthcare providers, this means compliance with the CAF is not just about meeting regulatory obligations; **it's about protecting patient trust**, ensuring uninterrupted care, and minimizing the risks posed by sophisticated cyber threats. Implementing CAF-aligned measures now prepares your organization for the future and helps strengthen the entire healthcare ecosystem against cyber risks.

Main Components of CAF

CAF is structured into four key objectives:

1. **Managing Security Risk:** Establishing governance, risk management, and asset management practices.
2. **Protecting Against Cyber Attacks:** Implementing policies, identity management, and system security measures.
3. **Detecting Cyber Security Events:** Establishing monitoring and proactive attack discovery mechanisms.
4. **Minimizing Impact of Cyber Incidents:** Developing response plans and learning from incidents to improve security posture.

WHY IS CAF IMPORTANT?

For healthcare providers, especially within the NHS, adhering to CAF is crucial for:

- ✓ **Regulatory Compliance:** Ensuring alignment with national cybersecurity standards and legal requirements.
- ✓ **Patient Data Protection:** Safeguarding sensitive patient information against breaches.
- ✓ **Operational Continuity:** Maintaining uninterrupted healthcare services by mitigating cyber threats.

WHO IS CAF FOR?

CAF is applicable to:

- ✓ **Healthcare Organizations:** NHS trusts and other entities delivering essential healthcare services.
- ✓ **IT and Security Professionals:** Individuals responsible for implementing and managing cybersecurity measures within healthcare settings.

WHY DOES IT MATTER?

For decision-makers in the healthcare sector, CAF compliance is not just a regulatory obligation but a proactive measure to:

- ✓ **Enhance Trust:** Reassure patients and stakeholders about the security of their data.
- ✓ **Prevent Cyber Incidents:** Reduce the risk of ransomware attacks, data breaches, and other cyber threats.
- ✓ **Ensure Service Delivery:** Protect critical healthcare operations from disruptions caused by cyber incidents.

Heimdal for Compliance: NHS Cyber Assessment Framework (CAF)

Heimdal Coverage of CAF

A1: Governance

- **Board Direction**: Heimdal helps enforce effective board-level cybersecurity policies through its Threat Hunting and Action Center (TAC), a centralized platform offering visibility and control over security operations.
- **Roles and Responsibilities:** Heimdal's Privilege Elevation and Delegation Management (PEDM) ensures secure delegation of user roles and permissions, supporting a clear governance structure by temporarily elevating privileges when necessary while enforcing Zero Trust principles.
- **Decision-Making:** Heimdal provides senior leaders with real-time insights and forensic capabilities using solutions like DNS Security and Ransomware Encryption Protection, enabling data-driven risk management decisions.

A2: Risk Management

- **Risk Management Process:** Heimdal's Patch and Asset Management (PAM) automates risk identification and mitigation. It provides real-time insights into vulnerabilities, ensuring risks are addressed promptly while maintaining compliance.
- **Assurance:** Heimdal's Extended Detection and Response (XDR) platform enhances confidence by delivering continuous monitoring, advanced analytics, and compliance-focused reporting.

A3: Asset Management

- **Asset Inventory:** Heimdal's Patch and Asset Management (PAM) maintains detailed asset inventories and lifecycle tracking, allowing organizations to identify and prioritize essential assets effectively.

A4: Supply Chain

- **Supply Chain Security:** Heimdal ensures secure third-party integrations by sanitizing and validating all updates through its Patch and Asset Management (PAM) module, minimizing risks from external dependencies.

B1: Policies, Processes, and Procedures

- **Policy Development & Implementation:** Heimdal's Threat Hunting and Action Center (TAC) integrates seamlessly with organizational policies, offering audit trails and compliance-focused insights. Tools like Privilege Account and Session Management (PASM) further enforce access policies.

B2: Identity and Access Control

- **Identity Verification and Access Control:** Heimdal's Privileged Account and Session Management (PASM) ensures secure access by managing privileged sessions and enforcing role-based access controls.
- **Privileged User Management:** Heimdal's Privilege Elevation and Delegation Management (PEDM) offers granular control over privileged user actions, with real-time monitoring and audit capabilities.

B3: Data Security

- **Data Understanding and Protection:** Heimdal's BitLocker Management provides end-to-end encryption management, ensuring the protection of data at rest and during transfer through its DNS Security Network module.

B4: System Security

- **Secure Configuration and Vulnerability Management:** Heimdal automates patching and system hardening with its Patch and Asset Management (PAM), ensuring vulnerabilities are addressed proactively.
- **System Resilience:** Heimdal's DNS Security and Ransomware Encryption Protection (REP) minimize risks to critical systems and ensure operational continuity.

B5: Resilient Networks and Systems

- **Design for Resilience:** Heimdal combines solutions like DNS Security Network and Ransomware Encryption Protection (REP) to ensure systems remain operational during cyber incidents.

B6: Awareness and Training

- **Cybersecurity Training:** Heimdal supports training through its Knowledge Base, which provides detailed user guides and security insights.

Heimdal for Compliance: NHS Cyber Assessment Framework (CAF)

Heimdal

Heimdal Coverage of CAF

C1: Monitoring Coverage

- **Monitoring and Alerts:** Heimdal's Extended Detection and Response (XDR) offers a unified monitoring platform, combining DNS, endpoint, and email security data to detect anomalies.

C2: Proactive Security Event Discovery

- **Proactive Monitoring:** Heimdal identifies advanced threats using AI-powered anomaly detection through its DNS Security Endpoint module.

D1: Incident Response

- **Response and Recovery:** Heimdal automates responses with tools like Automatic Device Isolation and Zero Trust Execution, supported by Ransomware Encryption Protection (REP).

D2: Lessons Learned

- **Root Cause Analysis:** Heimdal's forensic tools within the Threat Hunting and Action Center (TAC) and Extended Detection and Response (XDR) provide actionable insights for continuous improvement.

Glossary of Acronyms

1. **PASM** – Privileged Account and Session Management: Manages privileged sessions with real-time monitoring and audit trails.
2. **PEDM** – Privilege Elevation and Delegation Management: Temporarily elevates user privileges securely, enforcing Zero Trust.
3. **PAM** – Patch and Asset Management: Automates patching, vulnerability management, and asset tracking.
4. **TAC** – Threat Hunting and Action Center: Offers centralized threat detection, visualization, and mitigation capabilities.
5. **XDR** – Extended Detection and Response: Unified platform for detecting, analyzing, and responding to threats across all endpoints.
6. **REP** – Ransomware Encryption Protection: Prevents and mitigates ransomware attacks in real time.
7. **EDR** – Endpoint Detection and Response: Detects, investigates, and responds to threats at the endpoint level.

How Heimdal Can Help Maintain CAF Compliance

By integrating Heimdal's solutions, healthcare organizations can:

- **Automate Risk Mitigation:** Streamline processes to reduce vulnerabilities and ensure continuous protection.
- **Enhance Threat Detection:** Utilize advanced monitoring to identify and respond to threats promptly.
- **Support Compliance Efforts:** Maintain alignment with CAF requirements through comprehensive reporting and policy enforcement.

Why Heimdal

Heimdal delivers unified, scalable cybersecurity tailored to healthcare. Our award-winning Extended Detection and Response (XDR) platform integrates endpoint protection, privileged access, vulnerability management, and ransomware prevention—safeguarding patient data and ensuring operational continuity. Designed for proactive compliance with frameworks like CAF, Heimdal empowers healthcare organizations to reduce risks, enhance efficiency, and stay ahead of evolving threats.

For more information on how Heimdal can support your organization's compliance with the NHS Cyber Assessment Framework, visit our Healthcare Cybersecurity Solutions page.

Visit our Healthcare Cybersecurity page →

> "A perfect solution for our use case, with high expansion potential."
>
> - Head of IT Infrastructure, NHS
>
> NHS
> Mid Cheshire Hospitals
> NHS Foundation Trust

heimdalsecurity.com

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