Reference card for healthcare

Cybersecurity is a critical concern for the healthcare sector because cyberattacks threaten not only the availability of health information and the integrity of clinical systems, but also the safety and well-being of patients. Healthcare organizations — including large systems like the NHS — remain attractive targets for financially motivated threat actors who steal sensitive patient data and sell it on the dark web for insurance and identity fraud. These attacks disrupt care, erode patient trust, and strain already limited resources.

This document provides a reference on how Sophos solutions assist healthcare organisations to meet their cybersecurity requirements and deliver uninterrupted patient care.

The table below demonstrates how each product provides evidence of meeting each requirement of the Cyber Assessment Framework (CAF)-aligned Data Security and Protection Toolkit (DSPT). The CAF Principle Mapping column can serve as formal evidence in cyber assurance submissions (e.g., to NHS DSPT reviewers or internal auditors).

Each product entry aligns directly to one or more CAF principles — so you can compile a cross-reference quickly when demonstrating compliance.

DSPT-CAF Objective	Sophos Solution	How It Helps	CAF Principles & Sub-Principles
Objective A: Managing Risk	Sophos Cloud Optix	Asset management and visualisation across cloud/ hybrid, identifying and classifying resources and risks.	**A3 - Asset Management:** Identification, classification, and status of assets (A3.a)
	Sophos MDR, Sophos XDR, Sophos EDR	Integrates threat intelligence and risk insights to inform risk posture and decision-making.	**A1 - Governance:** Security governance, policies, and leadership (A1.a) **A2 - Third-party Risk:** Managing risks from suppliers and partners (A2.a) **A4 - Supply Chain Assurance:** Supply chain security (A4.a)
Objective B: Protecting Against Cyber Attacks and Data Breaches	Sophos Firewall	MFA, AI threat detection, segmentation to prevent attacks on healthcare systems and data.	**B2 - Identity & Access Control:** Authentication and identity management (B2.a, B2.b) **B3 - Data Security:** Data encryption, classification, protection (B3.a, B3.b) **B4 - System Security:** System integrity & patching (B4.a, B4.b) **B5 - Network Security:** Network segmentation, resilience (B5.a, B5.b)
	Sophos Device Encryption	Ensures devices and data are protected with full disk encryption and compliance reporting.	**B3 - Data Security** (as above), **A3 - Asset Management** (as above)
	Sophos Switch	Network access control, authenticates users/devices, prevents unauthorised LAN access.	**B2 - Identity & Access Control** (as above) **B5 - Network Security** (as above)
	Sophos Mobile	Device management and compliance rules keep sensitive data secure on mobile/personal devices.	**B2 - Identity & Access Control**, **B3 - Data Security**, **A3 - Asset Management**

SOPHOS

DSPT-CAF Objective	Sophos Solution	How It Helps	CAF Principles & Sub-Principles
	Sophos Wireless	Encrypted Wi-Fi sessions, endpoint health monitoring, and network segmentation.	**B3 - Data Security**, **B5 - Network Security**
	Sophos Email	Controls policies to prevent data breaches, encryption, and anti-phishing.	**B3 - Data Security**, **B1 - Service Protection Policies:** Safeguarding service operations (B1.a)
	Sophos Cloud Optix	Least privilege enforcement, cloud IAM risk identification and continuous exposure scanning.	**B3 - Data Security**, **C2 - Anomaly Detection:** Behavioural analytics for identifying anomalies (C2.a)
	Sophos ZTNA	Checks identity, device health/ compliance before granting zero-trust access.	**B2 - Identity & Access Control**, **B5 - Network Security**, **A4 - Supply Chain Assurance**
Objective C: Detecting Cybersecurity Events	Sophos MDR, Sophos XDR	24/7 monitoring, threat hunting and anomaly detection across endpoints, network, and cloud.	**C1 - Security Monitoring:** Detection of compromise (C1.a, C1.b) **C2 - Anomaly Detection** (C2.a) **D2 - Investigation and Analysis** (D2.a)
	Sophos Endpoint, Sophos Mobile	HIPS, behaviour analytics, deep learning to identify malicious activity.	**B4 - System Security (Malicious behaviour detection)**, **C2 - Anomaly Detection**
	Sophos Cloud Optix	Detects/configuration drift and alerts on anomalies.	**C2 - Anomaly Detection**, **B4 - System Security**
	SophosLabs Intelix	Inspects/blocks files before endpoint impact.	**B4 - System Security**, **C2 - Anomaly Detection**
Objective D: Minimising the Impact of Incidents	Sophos MDR	Expert-led response, containment, rapid remediation.	**D1 - Incident Response & Recovery:** Capability for responding and recovering (D1.a, D1.b)
	Synchronised Security (Sophos suite-wide)	Telemetry sharing enables coordinated isolation and malware cleanup for rapid containment.	**D1 - Incident Response & Recovery**, **B5 - Network Security**
	Sophos MDR Sophos XDR Sophos EDR Sophos Emergency Incident Response	Enables detailed forensics, post-incident investigation, root cause analysis.	**D2 - Investigation and Analysis**, **C2 - Anomaly Detection**
Objective E: Using and Sharing Information Appropriately	Sophos Email	Enforces policy, supports encryption for lawful email sharing and transfer of patient information.	**B1 - Service Protection Policies**, **B3 - Data Security**
	Sophos Phish Threat	Training modules educate staff on information sharing and phishing risks; automates awareness campaigns.	**B1 - Service Protection Policies**, **A1 – Governance**
	Sophos Cloud Optix	Monitors data usage/access in cloud environments, supports audit-ready lawful sharing evidence and access records.	**A1 - Governance**, **B3 - Data Security**

How Sophos solutions work with CAF & DSPT

Together, CAF and DSPT create a complementary framework that helps organisations not only protect their systems and assets but also demonstrate accountability, compliance, and continual improvement in how sensitive data and services are safeguarded.

Sophos supports this effort by providing advanced endpoint protection, network security, cloud security, and threat detection capabilities that align directly with CAF's protective and monitoring objectives while also reinforcing DSPT standards. Through centralised visibility, automated threat response, and managed detection and response (MDR) services, Sophos helps organisations close security gaps, streamline compliance, and strengthen resilience against evolving cyber threats.

This table shows where and how each Sophos solution provides essential support.

Legend:
- High coverage = Supports 5+ CAF principles and multiple DSPT standards
- Medium coverage = Supports 3–4 CAF principles and some DSPT standards
- Focused coverage = Supports 1–2 CAF principles or niche DSPT standards

Sophos Solution	CAF Principles Supported	DSPT Standards Supported	Coverage
Sophos MDR	C1, C2, D1, D2, B5	Monitoring, incident response, audit & alerting	High
Sophos Cloud Optix	A2, A3, B4, B5, C1	Asset management, cloud security assurance, IG (NHSDSPT 9 & 10)	High
Sophos ZTNA	A2, B2, B4	Access control, secure remote access	Medium
Sophos Firewall	B1, B3, B4, B5	Network security, availability, continuity planning	Medium
Sophos XDR	C1, C2, D1, D2	Threat detection, monitoring, audit logging	High
Sophos Wireless	B1, B3, B4, B5	Secure wireless access, system security controls	Medium
Sophos Mobile	A3, B2, B3	Mobile device security, IG compliance, access & confidentiality	Medium
Sophos Mobile	B2, B3	Endpoint/mobile security, confidentiality & GDPR	Focused
Sophos Device Encryption	A3, B3	Data confidentiality, encryption (DSPT mandatory requirement)	Focused
Sophos Switch (NAC)	A3, B2, B5	Network access control, asset validation	Focused
Sophos Email	B1, B3	Confidentiality of data in transit, phishing protection	Focused
Sophos Intelix	B3, B4	Malware prevention, system hardening	Focused
Sophos Endpoint	B3, B4	Endpoint security, data protection, DSPT breach minimisation	Medium
Sophos Endpoint	B3, B4	Server hardening, resilience of systems	Medium
Sophos SD-RED	B1, B5, D1	Secure remote access, continuity & resilience	Medium
Synchronised Security	B2, B4, C1	Automated threat detection & response, IG monitoring	Medium
Sophos Endpoint	A3, B3, C1	Cloud workload security, data protection	Focused
Sophos Phish Threat	A1 (Governance – staff training), B1	Staff training & awareness (DSPT mandatory requirement)	Focused

2026-02-04 RC-EN (NP) CRE-4215