WHITEPAPER

Taking care of the NHS with Sophos MDR: Sophos business case

SOPHOS

In the UK, ransomware remains a persistent and growing threat to healthcare. In Q2 2025 alone, 52 ransomware attacks were publicly disclosed against UK healthcare organisations, a record high and a 63% increase compared to the same period in 2024. From January to June 2025, 211 ransomware incidents were tracked in the sector, with nearly half (44%) of organisations stopping attacks before encryption, while 50% still ended up paying a ransom to recover data.[1]

63%

The year-over-year increase in publicly disclosed ransomware attacks against UK healthcare organisations in Q2 2025.

The financial and operational toll of these attacks is significant. Capita (the organisation that runs critical services for the NHS, local councils, and the military) now estimates that a March 2023 cyberattack has cost £29.3 million to date, up from the £25 million suggested at the time.[2]

The sector also continues to feel the effects of devastating incidents in recent years. The WannaCry cyberattack on the NHS in 2017, for example, cost a reported £92 million and cancelled 19,000 appointments, causing widescale disruption to patient care.[3]

Recent years have continued to produce costly and high-profile cases. A major 2024 ransomware attack on NHS pathology provider Synnovis disrupted hospital services for months and cost £32.7 million. In another case, Advanced Computer Software Group was fined £3 million following a ransomware breach in August 2022 that exposed almost 80,000 NHS patient records.[4]

Existing cybersecurity measures often fail to meet the evolving threat landscape. In 2025, exploited vulnerabilities and resourcing gaps remain leading causes of breaches, with 40% of healthcare ransomware victims unaware of the exact security flaw exploited.[5]

According to the Sophos State of Ransomware in Healthcare 2025 report, ransomware continues to significantly disrupt global private sector healthcare organisations, with a striking 85% of those hit reporting that the attacks caused them to lose business or revenue.

Healthcare remains a prime target due to the critical nature of its services, where downtime or data loss can force costly operational shutdowns and damage trust. Despite improvements in defences, ransomware payments and recovery costs are falling, but the financial and reputational damage from lost revenue remains a profound challenge.

Further insight from Sophos X-Ops reveals the following:

- 72% of healthcare IT leaders observed an increase in the complexity of attacks.
- 74% of healthcare organisations recovered all data after paying a ransom.

SOPHOS

- 26% of healthcare organisations did not completely recover their data despite paying.
- $1.85 million was the average cost to remediate following attack on a healthcare organisation.
- 40% of healthcare organisations took over a month to recover after an attack.

Existing security is great but never watertight

The UK government is intensifying its efforts to compel the NHS to safeguard itself against cyber threats. As of 2025, large NHS organisations, including Trusts, Integrated Care Boards (ICBs), CSU, and ALBs, must complete the DSPT (Data Security and Protection Toolkit) self-assessment based on the NCSC Cyber Assessment Framework (CAF), rather than the older National Data Guardian standards. This shift marks the sector's broader transition toward an outcomes-driven, evidence-focused approach, central to NHS England's long-term cybersecurity strategy, as organisations must demonstrate how products and services can be mapped to CAF objectives.

NHS England's Cyber Security Operations Centre (CSOC) also acts as the national authority for cyber incident monitoring, response, and intelligence sharing across the NHS. It provides central oversight on risks and incidents, ensuring that threats are managed holistically and that lessons learned from major cyber events like the Synnovis attack are disseminated and converted into better defences sector-wide. The system successfully blocks approximately 21 million malicious emails monthly, protecting about 1.7 million devices across the NHS network. But cybersecurity threats come in many guises as part of a constantly growing and evolving landscape.

Many NHS Trusts use a Microsoft stack, and as such rely on Microsoft Defender Antivirus. While this and the NHS CSOC improve protection in the security landscape, they cannot catch every attack. Sophos boasts AAA ratings in independent security tests like SE Labs, with top-tier performance in detecting and blocking real-world and simulated attacks, but again, there is no silver bullet service when it comes to complete cyber protection. What happens then when the outer layer of security is breached?

Managed Detection & Response (MDR)

If we accept that, at some point, the outer perimeter of any security solution will be breached, the next pressing challenge becomes identifying that breach as soon as possible and carrying out remedial action before it becomes a critical issue. However strong the security solutions are, technology alone cannot stop the most sophisticated active adversaries who use advanced techniques to evade detection and avoid triggering security tools.

Effectively halting sophisticated attacks necessitates human-driven efforts in threat detection, investigation, and remediation. That's where managed detection and response (MDR) comes in.

Sophos MDR delivers a comprehensive, 24/7 service provided by specialists with expertise in identifying and addressing cyberattacks that cannot be entirely thwarted by technological solutions alone.

Even though in-house security operations can be executed using endpoint detection and response (EDR) and extended detection and response (XDR) tools, opting for an MDR service — whether in collaboration with your internal team or as a fully outsourced solution — offers substantial advantages.

As the volume, complexity, and impact of cyber threats continues to rise, organisations are increasingly turning to MDR to identify and counter advanced attacks that technology alone cannot thwart. According to Gartner, over half of all global enterprises already use MDR.

Additional expertise and time

Opting for MDR over solely in-house security operations presents a significant advantage in bolstering defence against ransomware and other sophisticated cyber threats. MDR providers encounter a significantly higher volume and diversity of attacks compared to individual organisations, providing them with experience and expertise that is challenging to replicate internally. Moreover, MDR service providers exhibit heightened proficiency in using threat hunting tools, facilitating quicker and more accurate responses.

Collaborating within a larger team also enables analysts to share their knowledge and insights, fostering a swifter response and cultivating a form of "community immunity." This concept involves applying learnings from one organisation to others with a similar profile.

Adopting MDR frees up IT resources to dedicate toward business-centric initiatives. The labour-intensive and unpredictable nature of security operations often hinders IT teams from concentrating on more strategic projects.

Takeaways

Integrate network telemetry into your detection stack to improve visibility, accelerate investigations, and flag anomalous activity — especially lateral movement and command-and-control traffic.

Broader expertise

- MDR teams see thousands of attacks daily — far beyond what any single organization encounters — giving them unmatched threat-hunting skills.

Faster response

- Shared intelligence and advanced tools enable rapid detection and remediation, reducing dwell time and minimizing impact.

IT efficiency gains

- Free your team from unpredictable, often false-positive security tasks so they can focus on strategic business initiatives.

SOPHOS

Users of Sophos MDR consistently express substantial efficiency improvements in their IT operations, empowering them to more effectively contribute to their organisation's overarching objectives.

24/7, 365 coverage

Given the global presence of malicious actors, the potential for an attack exists at any given moment. MDR services offer substantial reassurance and peace of mind by ensuring continuous, 24/7 coverage.

This translates to tangible relief for IT teams, allowing them to rest easier at night. The constant expert coverage and a consistently high level of cyber readiness provides ensures the organisation is effectively safeguarded.

Sustaining a 24/7 in-house security operations team is costly, demanding highly-skilled experts that are difficult and costly to hire, train, and retain. MDR services offer a cost-efficient solution for fortifying an organisation's security, enabling it to maximise the value of its cybersecurity budget.

Selecting an MDR provider

There are several factors to consider when selecting an MDR provider:

Options for support and engagement
Are you seeking an MDR provider to handle your threat response entirely, collaborate with your team in threat response, or simply alert your team for independent action? Organisations need to determine a preferred level of support and interaction and evaluate vendors accordingly. Sophos MDR functions as an extension of an internal IT team, adapting to its needs. Whether providing fully managed 24/7 support or assisting an in-house team, Sophos aligns with your requirements.

Breadth and depth of threat experience
Deeper experience in responding to cyber threats contributes to enhanced defence capabilities. Evaluate the scope of experience that MDR vendor analysts possess and how they apply shared insights across their clients' environments. Assess the depth of security expertise within a vendor's MDR team and the quality of contextual insights provided to assist analysts in prioritising and investigating alerts.

Sophos MDR safeguards over 35,000 organisations globally, spanning diverse sectors including healthcare, education, manufacturing, retail, technology, finance, government, services, and more. Sophos X-Ops and the Counter Threat Unit (CTU) supports Sophos MDR with over 30 years of malware expertise and world-leading AI capabilities. These teams deliver profound insights and analysis, aiding MDR agents in swiftly identifying and neutralising attacks.

Day-to-day customer experience

A proficient MDR vendor should function as an integral part of your team. It is crucial to choose a vendor with whom you'd like to collaborate throughout the contract period. Engage with current customers to gain insights into their experiences and explore independent review platforms to gather feedback from other clients.

Breadth and depth of telemetry

Cyber criminals don't stick to a singular technology path, and your MDR vendor's strategies shouldn't either. Enhanced analyst visibility across your environment is crucial for detecting and responding to malicious activities effectively. Enquire about a vendor's technology integrations and the extent to which they can incorporate and leverage signals from various components of your IT environment.

Sophos MDR offers extensive integrations spanning the entire IT stack, including native and third-party integrations with endpoint, firewall, network, cloud, email, identity, and Microsoft 365 technologies. Sophos' vendor-agnostic approach ensures analysts have comprehensive visibility throughout the entire customer environment, thereby enhancing threat detection, investigation, and response capabilities.

If your NHS Trust already has some security cover, you need to be sure that an MDR provider can integrate successfully with the existing technology stack.

"Sophos has allowed us to reduce risks associated with cyber incidents for a fraction of the cost of standing up an in-house service. The 24/7 monitoring from Sophos gives us assurance that systems are monitored no matter the time or day and, where necessary, remedial actions are taken closing the threats before they become a major incident."

Chris Wallace, Head of Infrastructure, N3i Limited

Questions to ask yourself when evaluating an MDR provider

- Do you want full 24/7 management, collaborative threat response, or alert-only notifications?
- How deep is the vendor's experience?
- What kind of integrations do you need for MDR to fit into your existing tech stack?
- Will this vendor feel like it fits in as part of my team?

SOPHOS

Sophos MDR for Microsoft environments

Sophos MDR for Microsoft environments is now a Microsoft Verified Small and Medium Business (SMB) Solution Status through the Microsoft Intelligent Security Association (MISA).

This certification validates the depth of integration between Sophos MDR and Microsoft Defender for Business and Defender for Endpoint, demonstrating that Sophos delivers proven, enterprise-grade managed detection and response optimized for Microsoft environments.

For managed service providers (MSPs) and SMB customers, it confirms that Sophos MDR reduces cyber risk, maximizes technology investments, and fortifies your defenses against adversaries.

Sophos Intelix for Microsoft Security Copilot now also brings Sophos X-Ops' global threat intelligence directly into Microsoft's generative AI assistant for security teams.

This agent enables users to enrich alerts, analyze suspicious files, and access real-time threat context directly within Security Copilot, turning intelligence into faster, more confident decision-making. Available at no cost, the Intelix agent gives every Security Copilot user access to the same intelligence that powers Sophos' global MDR operations.

Security and IT professionals can now query Sophos Intelix in natural language from within Microsoft 365 apps, including Teams and Outlook, to investigate threats, analyze URLs or files, and receive instant, explainable verdicts. The result is actionable security intelligence seamlessly embedded into the tools organizations use every day.

MDR is a proven solution

Sophos MDR dramatically helps reduce the threat of a data breach or cyber incident. Using data from existing customers Sophos returns industry leading average response times:

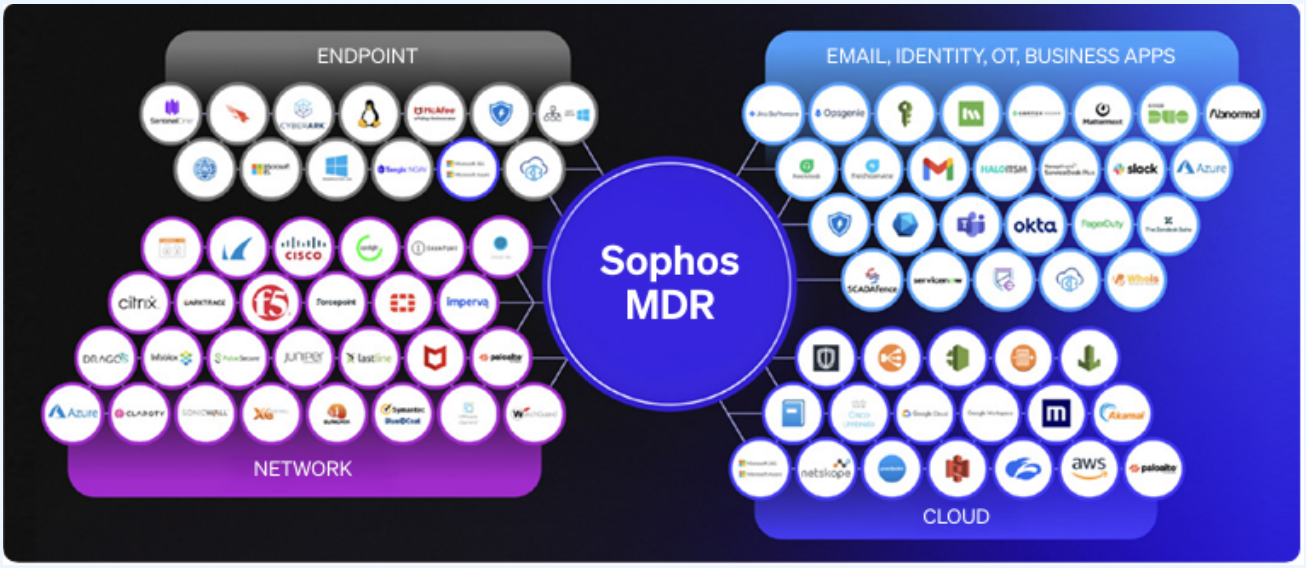
- Average Sophos MDR Threat Response Time Detect: 1 minute
- Investigate: 25 minutes
- Remediate: 12 minutes
- Total: 38 mins

SOPHOS

But don't just take our word for it:

"Sophos MDR is our comfort blanket. The team are our trusted advisors; on hand to quickly respond to any queries. The added security of proactive 24/7 protection provides piece of mind knowing the team are searching and resolving any active threats."

South East Coast Ambulance Service NHS Foundation Trust, UK



"Sophos provides the equivalent coverage and workload of six full-time staff for the cost of less than one."

Detmold Group, Australia

"Bringing all of our security products under one roof has allowed us to save money and drive efficiency as well."

Independent Parliamentary Standards Authority, UK

"Sophos MDR pays for itself in spades. If it stops one major incident a year, it's paid for itself 10 times over, if not more."

Hammondcare, Australia

"Sophos provides us with the peace of mind that our systems are being monitored 24/7 by expert threat hunters. I certainly sleep better knowing Sophos are able to respond on our behalf outside of office hours."

Mark Thornton, ICT Operations Manager, Birmingham and Solihull Mental Health NHS Foundation Trust

The only way to reliably detect and neutralise determined attackers is with 24/7 coverage, operating on signals from a diverse range of event sources and employing actionable threat intelligence into real-time attacker behaviours.

Organisations that are struggling to keep pace with well-funded adversaries who are continuously innovating and industrialising their ability to evade defensive technologies need all the help they can get. Sophos MDR can discover and intercept these steps before they result in a data breach, ransomware or other type of costly compromise.

About Sophos MDR

Sophos offers industry-leading MDR alongside a comprehensive portfolio of cybersecurity technologies — including endpoint, network, email, and cloud security, extended detection and response (XDR), identity threat detection and response (ITDR), and next-gen SIEM. Together with expert advisory services, these capabilities help organisations proactively reduce risk and respond faster, with the visibility and scalability needed to stay ahead of evolving threats.

Sophos MDR is the world's most trusted MDR service, securing over 35,000 organisations against the most advanced threats, including ransomware. With the highest rating on Gartner Peer Insights[TM] and ranked No. 1 overall in Managed Detection and Response (MDR) in the G2 Winter 2025 Reports, with Sophos MDR, your cyber defences are in good hands.

For more information and to discuss how it can help you, speak with one of our advisors or visit www.sophos.com/mdr today.

A Leader in the Gartner 2025 Magic Quadrant for Endpoint Protection Platforms for the 16th consecutive time

The only vendor to be named a Gartner Peer Insights "Customers' Choice" for Endpoint Protection Platforms, Extended Detection and Response, Managed Detection and Response, and Network Firewalls. Read independent customer testimonies here.

1 https://news.sophos.com/en-us/2025/06/24/the-state-of-ransomware-2025/
2 https://www.londonstockexchange.com/news-article/CPI/half-year-results/16588926
3 https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/
4 https://www.hsj.co.uk/technology-and-innovation/synnovis-cyber-attack-cost-trusts-33m/7036796.article
5 https://ico.org.uk/action-weve-taken/enforcement/ico-fines-software-company-for-nhs-data-breach/

SOPHOS

Ready to assess your cybersecurity program?

Speak to a Sophos expert today.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2026-01-15 WP-EN (NP) CRE-4233