SOPHOS

ITHealth

Taking Care of the NHS with Sophos MDR: ITHealth & Sophos business case

Overview of rising security threats in healthcare

Cybersecurity represents a huge ongoing challenge for healthcare providers. Cyber-attackers have the potential to expose clinical networks to hacking, malware, ransomware and other activities which in turn could have dire consequences for patient safety and privacy, plus severe financial ramifications.

In the UK, 81% of healthcare organisations were hit by ransomware in 2021, and Capita, the organisation that runs services for NHS, councils and military, reported in March 2023 that a cyber-attack could cost it up to £25 million. We don't have to dig too deep to find examples in the public domain.

The WannaCry cyber-attack on the NHS in 2017 for example, not only cost a reported £92 million, but also caused the cancellation of 19,000 appointments resulting in untold chaos and harm to the lives of patients.

In May 2021, the Health Service Executive in Ireland experienced a security breach that impacted 80% of its IT infrastructure. The attack cost the Department of Health a reported €1 million and cost the HSE €53 million with long-term costs that could rise to €500 million.

Existing cybersecurity measures are not always enough to protect against attacks, the threat landscape is ever evolving. Identifying, risk-assessing and remediating vulnerabilities represents a key challenge to NHS organisations because of the implications for patient care, service availability, finance and reputation.

According to data taken from the Sophos State of Ransomware in Healthcare 2023 report, 85% of private-sector healthcare organisations hit by ransomware reported the attack caused them to lose business/revenue, this is slightly above the global cross sector average of 84%.

While further insight from Sophos X-Ops reveals the following:

- 67% of healthcare IT leaders observed an increase in the complexity of attacks
- 2% of healthcare organisations recovered all data after paying a ransom
- $1.85 million was the average cost to remediate following attack on a healthcare organisation
- 20% of healthcare organisations took over a month to recover following an attack
- 65% is the percentage of data recovered by healthcare organisations after paying a ransom

Existing security is great but never watertight

The UK government is intensifying its efforts to compel the NHS to safeguard itself against cyber threats. Service providers are required to demonstrate their security measures against various criteria. Additional information regarding the specific requirements and methods to prove their security can be accessed on the NHS Digital website.

In addition to this, NHS trusts now have a direct connection to NHS England's Cyber Security Operations Centre (CSOC), which helps to protect against suspicious activities within the NHS network. The system successfully blocks approximately 21 million malicious emails on a monthly basis. But cybersecurity threats come in many guises as part of a constantly growing and evolving landscape.

Looking elsewhere, many NHS Trusts use a Microsoft Stack, and as such rely on Microsoft Defender Antivirus and while this and the NHS CSOC are welcome additions to the security landscape, they cannot catch every attack. Sophos itself boasts a 99.98 percent success rate in blocking malicious 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.

Effectively halting sophisticated attacks necessitates human-driven efforts in threat hunting, investigation, and response. This is the role filled by MDR, or managed detection and response, services.

MDR represents a comprehensive, round-the-clock service provided by specialists with expertise in identifying and addressing cyber-attacks that cannot be entirely thwarted by technological solutions alone.

Even though in-house threat hunting can be executed using EDR (endpoint detection and response) and XDR (extended detection and response) 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 technological solutions alone cannot thwart. According to Gartner, half of all global enterprises will have adopted MDR for threat monitoring, detection, and response by 2025.

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 an 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 towards business-centric initiatives. The labour-intensive and unpredictable nature of threat hunting often hinders IT teams from concentrating on more strategic projects. 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. Security responsibility ultimately lies with the MDR provider. The constant expert coverage and a consistently high level of cyber readiness provides robust assurance data and the organisation as a whole are effectively safeguarded.

Sustaining a round-the-clock in-house threat hunting team is costly, demanding a up to five or six full-time personnel. MDR services offer a cost-efficient solution for fortifying an organisation's security, enabling it to maximise the value of its cyberecurity budget.

Furthermore, by enhancing protection, MDR services significantly diminish the likelihood of encountering a financially hard-hitting data breach, and thus avoiding the economic challenges associated with addressing a major incident.

Selecting an MDR provider

There are a number of factors to consider when selecting an MDR provider including the following:

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. Additionally, 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 11,000 organisations globally, spanning diverse sectors including healthcare, education, manufacturing, retail, technology, finance, government, services, and more. Supporting Sophos MDR is the Sophos X-Ops team, with over 30 years of malware expertise and world-leading AI capabilities. The Sophos X-Ops team delivers 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 threat hunting 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 security integrations and the extent to which they can incorporate signals from various components of your IT environment.

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

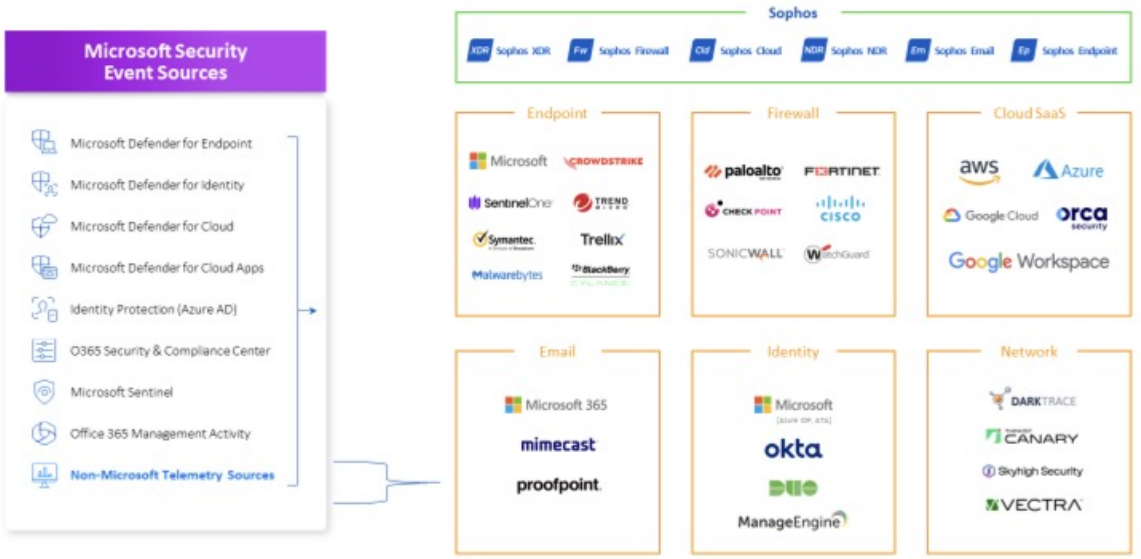
Assuming that your NHS Trust already has some security cover, you need to be sure that an MDR provider can integrate successfully with the existing technology stack. See all Sophos integrations here.

"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

Sophos MDR for Microsoft

Sophos offers seamless integration with a broad, open ecosystem of technology partners to deliver superior cybersecurity outcomes. Sophos Managed Detection and Response (MDR) also provides 24×7 security monitoring, threat investigation, and response support for Microsoft security alerts.



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 response times:

Average Sophos MDR Threat Response Time
Detect: 1 minute
Investigate: 25 minutes
Remediate: 12 minutes

Total: 38 mins

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 24x7 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 ten times over, if not more."

Hammondcare, Australia

In fact, Sophos MDR is the most reviewed and highest rated MDR provider on Gartner Peer Insights as of August 1, 2022, with an average rating of 4.8/5. Read independent customer testimonies here.

"Sophos provides us with the peace of mind that our systems are being monitored 24x7 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 24x7 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.

For more information contact ITHealth and Sophos today

About ITHealth

ITHealth provides NHS organisations with proven and trusted cybersecurity and access management solutions. Our aim is threefold: to protect the availability, confidentiality and integrity of vital NHS systems and data, to protect staff, and to protect an NHS organisation's reputation. By doing so, we ultimately protect patient care. Established for 30+ years, with the NHS as our sole focus, gives us an unrivalled and genuine understanding of NHS IT issues helping to address the most complex of NHS cyber challenges.

Visit www.ithealth.co.uk to find out more.

About Sophos MDR

Sophos MDR is the world's most trusted MDR service, securing over 17,000 organisations against the most advanced threats, including ransomware. With the highest rating on Gartner Peer Insights™ and the Top Vendor recognition in the 2022 G2 Grid® for MDR services serving the midmarket, 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.

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

2024-01-18 (WP-PC)

SOPHOS