Sophos protection for the NHS

Solution Brief
Today’s Challenges Facing the NHS Around the Network Perimeter

NHS organisations are adopting new technologies like network-connected medical devices, telehealth, remote patient monitoring, and medical apps such as picture archiving and communication systems (PACS). At the same time, they are embracing the internet first strategy, cloud adoption, machine learning and artificial intelligence (AI), and mobility to foster better patient care and improve access to patient data. As they do so, cybercriminals deploy increasingly sophisticated attack methods to gain access to sensitive patient and healthcare data that is far more valuable on the dark web than any other type of information.

The unique IT security capabilities of Sophos offer award-winning protection for NHS organisations in order to best ensure uninterrupted patient care, secure patient data and medical operations, and achieve compliance with increasingly stringent industry regulations such as DSPT, NIS, CQC, and Cyber Essentials Plus.

It is necessary to improve visibility of local internet breakout traffic so it can be better monitored and enable better analysis of encrypted network traffic. This will improve detection of security threats and enable more preventative actions and controls to be used to protect critical systems and their associated data.
Sophos Solution Brief – Healthcare

Sophos protection for the NHS

What can Sophos do to help?

Protection at every step:
- Network perimeter
- Endpoints
- Datacentres
- Mobile devices
- Public cloud
- Email
- File and device encryption

Best visibility, protection, and response for your network
- Powerful Sandstorm sandboxing
- Deep learning with artificial intelligence
- Top performing intrusion prevention system (IPS)
- Advanced threat and botnet protection
- Web protection with dual AV, JavaScript emulation, and SSL inspection
- Anti-exploit and anti-ransomware protection
- Visibility into your network, users, and apps

End-to-end endpoint protection
- The industry’s top-rated malware detection, ransomware prevention, and exploit protection – available with easy-to-use endpoint detection and response (EDR)

Public cloud security
- Unparalleled real-time visibility of your public cloud assets along with exposure of those assets to the external world
- Simplify compliance, governance, and security monitoring in the cloud with the power of AI and automation features in Sophos Cloud Optix
- Security analytics and monitoring across multiple public clouds at the same time
- End-to-end security from development stage to the production environment

Support for compliance with regulations pertinent to the NHS:
- DSPT, NIS, CQC, and Cyber Essentials Plus

What we do better than the rest

Sophos Synchronized Security defends against coordinated attacks with cross-product data sharing and zero-touch response
- Endpoint, network, mobile, Wi-Fi, email, and encryption products all share information in real time and respond automatically to incidents
- Isolate infected endpoints, blocking lateral movement
- Restrict Wi-Fi for non-compliant mobile devices
- Block outbound mail and scan endpoints on detection of compromised mailboxes
- Revoke, shred, and re-issue encryption keys if a threat is detected
- Identify all apps on the network

Protection against the widest range of endpoint threats
- Best performing malware detection engine with deep learning-based AI and EDR
- Protects even when the host is offline

App visibility and control
- Visibility and granular control over thousands of applications allows you to build custom policies based on category, risk, technology, and more
- Synchronized App Control identifies all applications – known, unknown, unidentified, or generic – allowing you to prioritize the ones you want and block the ones you don’t

User identity
- User identity powers all firewall policies and reporting, offering next-gen controls over apps, web surfing, bandwidth quotas, and other network resources

Cloud-management platform for all Sophos products
- Sophos Central is the intuitive, fully featured, and unified console for managing your Sophos products
- Trial new products in just a couple of clicks
- Minimize overhead and maximize efficiency thanks to a common interface
Use case: **Protect NHS organisations’ network perimeters**

Sophos XG Firewall’s complete next-gen protection offers all the advanced networking, protection, user and app controls you need to keep your NHS network secure and compliant.

Powerful next-gen protection technologies like deep learning and industry-leading intrusion prevention offers the best protection against ransomware, cryptomining, bots, worms, hacks, breaches, and advanced persistent threats.

Gain complete control over apps, web surfing, bandwidth quotas, and other network resources with Sophos’ user identity-based firewall policies and reporting. Classify and control all unknown, unidentified, or generic applications by identifying them and then prioritizing or blocking them with our Synchronized App Control technology. Keep patient identifiable data (PID) safe with user-based monitoring and control of keyword and downloadable content with our web keyword monitoring, file download filtering, and outbound email data-loss prevention (DLP) technologies. This includes the ability to look for NHS and CHI numbers.

Then pair XG Firewall with Sophos’ leading Intercept X endpoint protection – featuring unmatched exploit prevention, CryptoGuard ransomware protection, and much more – for the ultimate defence against advanced threats and zero-touch response in the event of an attack.

Use case: **Protect NHS endpoints**

NHS endpoints like MRI scanners, infusion pumps, patient monitors, surgery robots, and other medical equipment are the most life-critical resources, and yet the most vulnerable to hackers. Data from such medical devices is shared across multiple endpoint devices, making it easily available.

**Sophos offers the strongest malware detection, ransomware prevention, and exploit protection combined with endpoint detection and response (EDR) features.**

Industry-leading deep learning combined with threat intelligence from SophosLabs takes Sophos’ threat prevention to unmatched levels.

Sophos Synchronized Security unifies defences with real-time intelligence sharing between your endpoints and firewalls, automatically isolating infected systems, instantly cleaning up malware, and giving you complete visibility of all the apps on your network.
Use case: Secure NHS mobile devices

The NHS is making more use of mobile devices as they help improve patient experience and productivity. However, most of these consumer-oriented devices were never designed to secure sensitive healthcare information such as PID. Yet more and more numbers of mobile devices are used to store, process, and transmit PID. If PID is stolen, made public, or altered, NHS organizations can face severe penalties via GDPR and lose the trust of their patients.

Sophos Mobile helps you ensure sensitive healthcare information on mobile devices stays safe and separated from personal data thanks to secure and AES-256 encrypted containers. Save time with effortless email and data-access configuration, and protect your users from malicious links in documents and content with anti-phishing technology. You can even restrict container access based on time, Wi-Fi network, or location.

Sophos Mobile Security protects against malicious apps, ransomware, spam, potentially unwanted applications (PUAs), and low-reputation apps on Android. It monitors device health continuously to ensure that you are notified if a device is compromised and can take remediating action or automatically revoke access to corporate resources.

Use case: Protect NHS data centers

NHS organisations are big consumers of modern digital technology, with X-rays and MRI machines generating a considerable amount of high-fidelity imaging and diagnostic data. Heartrate monitors, pedometers, and other wearable healthcare devices are sending real-time data to practitioners to give patients quick and accurate treatment – and, in turn, generating significant healthcare data.

As the use of technology grows, so too does the need for data storage. Data centres – essential in healthcare – require strong controls to protect data, ensure availability, and restrict access to information on the basis of need-to-know.

Sophos Intercept X for Server secures your server environment – in the cloud, on premises, or in hybrid environments. Block the latest malware threats, stop ransomware, prevent dangerous exploit techniques, and deny hackers.

Endpoint detection and response (EDR) gives you visibility across your server estate, allowing you to hunt down evasive threats, see and control exactly which applications are running, and automatically respond to incidents.

And with Intercept X for Server and Sophos XG Firewall working together, you can isolate compromised servers to stop threats from spreading laterally while such threats are automatically cleaned – all while getting 100% visibility of the apps running on your servers, stopping unknown apps from communicating outbound.
Use case: Protect the NHS’s use of public cloud workloads

NHS organizations, similar to other large organizations, are actively moving their workload to the public cloud to take advantage of better cost and agility. However, the NHS works with highly confidential customer and patient data that needs to be protected. And the NHS must adhere to stringent compliance requirements.

Sophos Cloud Optix combines the power of AI and automation to simplify compliance, governance, and security monitoring in the public cloud. Automatically discover your organization’s assets across Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) environments.

Get the power to respond to and remediate security risks in minutes, with complete network topology visualization and continuous asset monitoring.

Powerful AI detects suspicious network behaviour and risky login activity fast, with smart alerts and optional automatic remediation of risks. The platform also provides intelligent compliance capabilities that allows companies to ensure they are adhering to compliance requirements. Once the customer has enhanced visibility of the potential security attack surfaces, the platform can then be further protected using Sophos Intercept X for Server and Sophos XG Firewall, working together and sharing security intelligence.

Use case: Secure remote clinics and sites

The NHS is breaking down geographic boundaries, with telemedicine and remote healthcare becoming a much-needed norm today. Remote healthcare allows medical practitioners to offer uninterrupted care to their patients wherever they are. But to do this, medical practitioners need to collaborate and communicate with staff and colleagues at remote locations and clinics. Under such circumstances, NHS IT must ensure reliable IT support for medical technology and also provide continuous privacy, security, and availability of patient healthcare data.

Sophos makes extending your secure network to other locations effective and affordable without requiring any technical skills at the remote location thanks to Sophos RED (Remote Ethernet Device). Simply enter the RED device ID into your XG Firewall and ship it. As soon as it’s plugged in and connected to the internet, our provisioning service automatically connects it to your firewall and establishes a secure, dedicated VPN tunnel.

Furthermore, Sophos XG Firewall facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Sophos SafeGuard Encryption helps you ensure secure access to patient healthcare information by authenticating users for access to specific devices, files, and folders with user- and group-specific keys. All data encrypted with SafeGuard remains encrypted as files move across the network. SPX Encryption, available with Sophos Email and XG Firewall, dynamically encapsulates email content and attachments into a secure, encrypted PDF to ensure compliance. Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi network, or location.
Sophos protection for the NHS

Use case:
Keeping management simple and automating your response

The management of security technology is a prime example of where costs can start to accumulate. When the security technology is piecemeal or bundled with additional software as part of a larger deal, it takes several individuals to manage it from various consoles or through multiple systems. That means the IT team are focusing on managing the security technology and not on helping clinicians and healthcare practitioners understand how technology can help them drive the best patient outcomes.

Complexity in security technology, especially from a management perspective, not only takes up valuable (and costly) time, but introduces additional costs in the form of headcount. The more complexity involved in managing the technology, the more people are required to manage it. When budgets are already stretched, having more doctors, nurses, and medical staff should take preference over additional IT staff to manage overly complex security technology.

That’s not to say the technology itself should be simple. Quite the contrary. Given that hackers are more sophisticated than ever, malware is more prevalent, and the threat landscape is changing on a daily basis, the level of complexity in solving those issues is always going to be high. This is where automation comes into play to remove the management headache.

Technology is becoming smarter, and elements such as artificial intelligence (AI) and machine learning make it possible for machines to heal themselves, to isolate problems, and to fix them automatically without human intervention. Automation today can stop malware in its tracks, mitigating risks and reducing the threat of an entire network infection. This not only leaves the IT team at the healthcare trust free to help clinicians or focus on other, patient-related tasks – it further helps to reduce management and resource costs.

Sophos helps keep management overhead costs to a minimum, and automates your response through Sophos Central and our award-winning Synchronized Security platform. Advanced attacks are more coordinated than ever before and Sophos Central and Synchronized Security makes sure that your defences are too. Our revolutionary Security Heartbeat™ ensures your endpoint protection and firewall are talking to each other. It’s a simple yet effective idea that means you get better protection against advanced threats and spend less time responding to incidents. It’s so simple, it makes you wonder why nobody did it before.

Your next steps:
Discover more about Sophos and its NHS solutions by visiting the Sophos NHS webpage.
Or, you can get in touch with us. Our experts will help to build the solution that best meets your business needs and strategies.