



Healthcare Cybersecurity Guide

Healthcare cybersecurity that stops attackers in their tracks –
but won't get in the way of patient care

Cybersecurity and patient care

Think about patient care, and our first thoughts are of doctors, nurses, and other healthcare professionals who deliver medical services. But, as healthcare becomes increasingly reliant on technology – from AI to cloud computing, to connected devices – and attackers continue to evolve their techniques, cybersecurity plays a direct and significant role in enabling the delivery of patient care.

“Ineffective cybersecurity is a clear and present danger to patient safety... cyber incidents can significantly disrupt health and care systems and directly contribute to patient harm.”

Institute of Global Health Innovation, Imperial College London

The COVID-19 pandemic has accelerated the adoption of digital health technologies such as remote patient monitoring solutions, online consultations, and in-home devices, and led to an increase in mobile/remote staff. While these changes have delivered significant efficiency improvements to the healthcare sector that will continue in the long term, they have also increased the cybersecurity challenge healthcare IT teams face.

“[Cyber attackers] are seeking to exploit the fact that digitalization in the future for healthcare is going to become more and more important.”

John Noble, Chair, Information Assurance and Cyber Security Committee, NHS Digital

Healthcare cybersecurity challenges

A 2021 Sophos survey of 328 healthcare IT professionals across 30 countries revealed that cybersecurity is getting a lot tougher. 63% of respondents said the number of cyberattacks they experienced increased over the course of 2020 – likely driven, at least in part, by adversaries taking advantage of the pandemic in their attacks. As a result, it’s perhaps not surprising that 70% said their cybersecurity workload increased over the course of 2020.

It’s not just the volume of attacks that is increasing; they’re also getting more complex. 60% said that cyberattacks are now too advanced for their IT team to deal with on their own.



Complexity is the enemy of security

Healthcare organizations typically have a higher than average user-to-IT staff ratio. The more complex the security infrastructure, the harder it is for overstretched IT teams to keep it up to date, and also to take full advantage of the protection capabilities on offer.

Sophos: Securing healthcare

Sophos works with healthcare organizations globally to address their cybersecurity challenges and enable the delivery of uninterrupted patient care. In the face of the growing frequency and sophistication of attacks, we can help you keep your data and organization safe while also enabling busy IT teams to reduce their cybersecurity workload. Read on for details of how we can help address the most common cybersecurity challenges facing healthcare organizations.

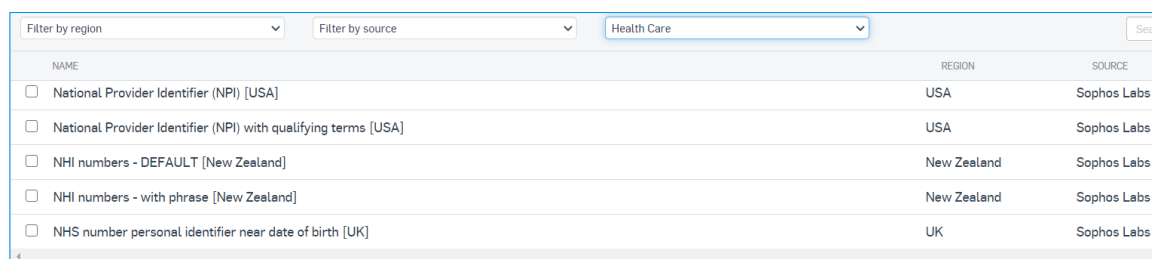
Secure sensitive data wherever it's held

Healthcare organizations hold many forms of sensitive data, from medical records to social security numbers to Personally Identifiable Information (PII). With so many different types of sensitive data within a healthcare organization – and so many places where it's stored and used – protecting it all can be difficult.

Sophos' preventative and active protection tools provide security across the entire healthcare network, right down to individual devices.

Securing the device or workload that holds the data

Sophos Intercept X endpoint and server protection deploys multiple layers of protection to secure data on your Windows, Mac, Linux, and virtual machines. Healthcare-specific data loss protection rules, using healthcare terms or data types, elevate your protection.



NAME	REGION	SOURCE
<input type="checkbox"/> National Provider Identifier (NPI) [USA]	USA	Sophos Labs
<input type="checkbox"/> National Provider Identifier (NPI) with qualifying terms [USA]	USA	Sophos Labs
<input type="checkbox"/> NHI numbers - DEFAULT [New Zealand]	New Zealand	Sophos Labs
<input type="checkbox"/> NHI numbers - with phrase [New Zealand]	New Zealand	Sophos Labs
<input type="checkbox"/> NHS number personal identifier near date of birth [UK]	UK	Sophos Labs

Sophos Device Encryption provides a quick, easy way to ensure Windows and macOS devices are safely encrypted, protecting your data (and proving compliance) if they're lost or stolen.

Securing the network that the data flows through

Sophos Firewall uses AI-powered threat detection technology to prevent attacks reaching your sensitive healthcare data, critical medical systems, and other parts of your ecosystem.

Stopping loss by email – deliberate or accidental

Sophos Email encrypts personally identifiable information, patient records, medical images, and other sensitive data, stopping both accidental and malicious data breaches.

Controlling access to your data

Sophos Zero Trust Network Access (ZTNA) gives you absolute control over who can access data on your network. Very granular controls block lateral movement while ensuring only authorized people can access sensitive data.

Face healthcare's ransomware threat head-on

Ransomware is getting smarter and more disruptive – and healthcare is a lucrative target. In healthcare, the cost of ransomware isn't just about paying the ransom. The cost of losing patient data and delaying or canceling medical procedures can be huge and devastating. Sophos' proactive threat hunting and prevention tools are constantly evolving to stay ahead of ransomware – and defend your data and network from these attacks.

Stopping ransomware from holding you hostage

At Sophos, we're proud to be world leaders in protecting organizations from ransomware.

Sophos Intercept X is the world's best ransomware protection for endpoints and servers. It introduces multiple security layers in order to recognize and stop ransomware at every stage, including:

- CryptoGuard, which automatically rolls files back to a safe state if they're encrypted by an unauthorized actor
- AI-powered deep learning which blocks known and unknown ransomware
- Exploit protection that stops the techniques attackers use to download and install ransomware
- Foundational, signature-based protection from SophosLabs

Sophos Managed Threat Response (MTR) provides our highest level of ransomware protection, providing proactive threat hunting, detection, and response capabilities, all delivered as a 24/7 managed service by an expert team. We're keeping watch, even while you sleep.

Sophos Rapid Response provides emergency support during live ransomware attacks – even if you're not a Sophos customer. Our team will help you get an attack under control quickly to protect your networks, applications, and data, as well as mitigate damage and disruption.

Give users secure access from anywhere

Healthcare workers, whether frontline workers in hospitals, out in the community, or working from home, need anytime access to sensitive patient data and healthcare systems. Sophos tools enable your users to connect securely from any location – without impacting vital healthcare work.

Enabling users to connect securely from any location

Sophos Firewall provides secure connections for Windows and macOS via the free Sophos Connect VPN. It's easy to deploy and configure, and gives your remote users secure access to resources on the network, or public cloud from Windows and macOS devices. With over 1.4 Million active clients, you know you're in good company.

*The reality of
ransomware
in healthcare*

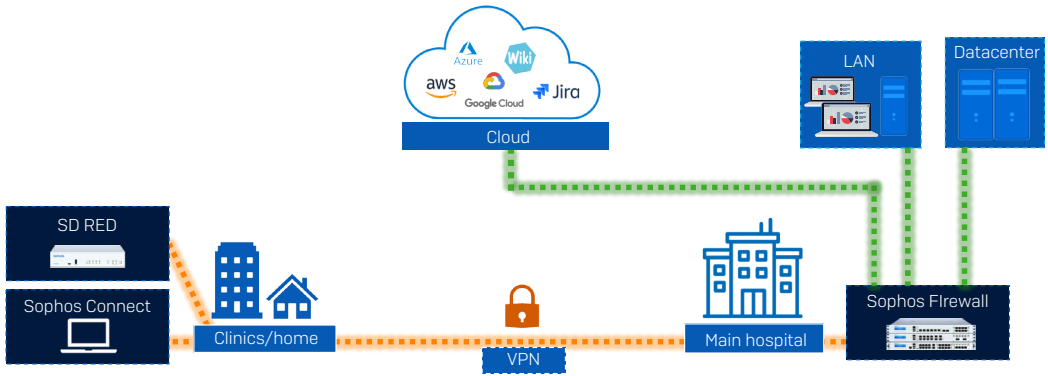
*34% hit by
ransomware
last year*

*65% of attacks
encrypted data*

*34% paid the
ransom*

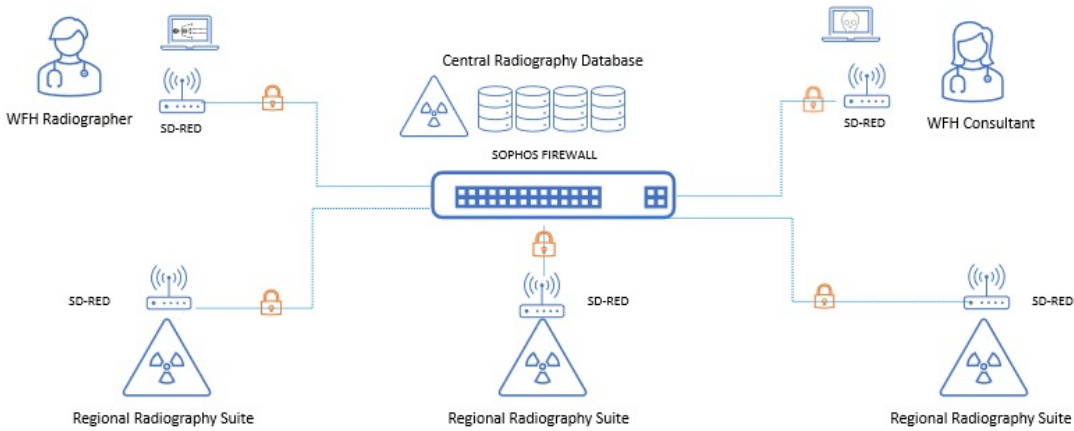
*US\$1.27M
average
recovery cost*

The State of Ransomware
2021, Sophos



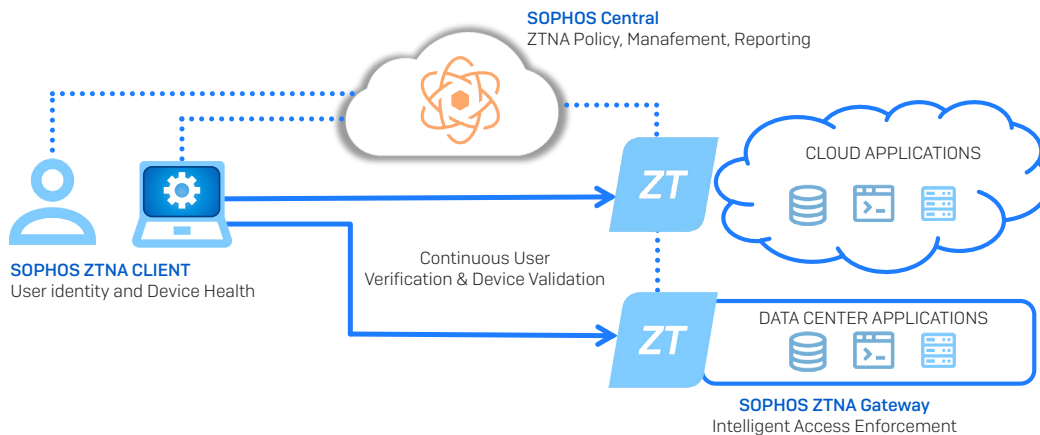
Sophos Firewall delivers secure remote access via the Sophos Connect client and SD-RED devices

For the ultimate in secure remote connectivity, **SD-RED** (remote ethernet device) is a small plug-and-play device that works with **Sophos Firewall** to connect remote sites and individuals to your main network. It's ideal for local clinics and medical suites, as well as people with highly sensitive data.



Example radiography use of Sophos Firewall and SD-RED

For next-gen secure access, **Sophos Zero Trust Network Access** puts identity at the center of defense, constantly validating the user, the device, and policy compliance. It provides a transparent 'just works' experience for users while enabling IT teams to get new users up and running quickly.



Strengthen your IT team

Our 2020 survey of 5,000 IT managers across a range of industries including healthcare revealed that 81% of respondents said their ability to find and retain skilled IT security professionals is a major challenge to their organization's ability to deliver IT security.

Whether you're looking for added expertise or capacity to supplement your resources, the security pros at Sophos can be an extension of your team, keeping your healthcare systems and patient data safe, 24/7.

Dedicated cybersecurity experts to strengthen your IT team

Sophos Managed Threat Response (MTR) is a team of threat hunting and response experts who act like an extension of your own team. They give stretched healthcare IT teams the added capacity and expertise they need to handle every threat.

The Sophos MTR team monitors your environment 24/7, proactively hunting for and validating potential threats and incidents. If they see something suspicious, they can call on the malware experts in SophosLabs to investigate and unpick suspicious indicators.

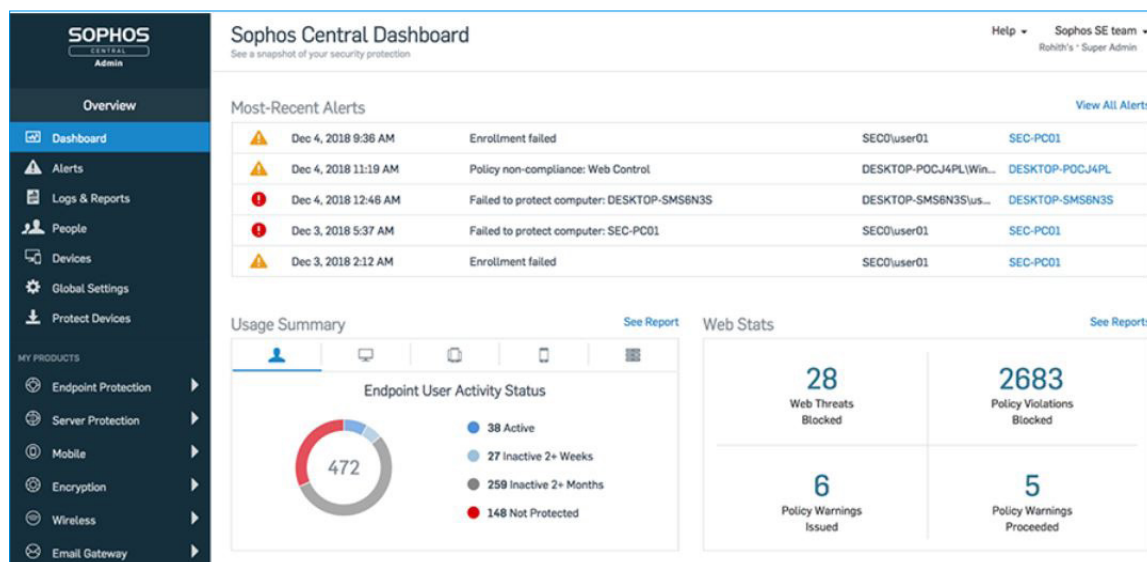
Plus, if you choose, the Sophos MTR teams can also take action on your behalf. Unlike other managed detection and response services, our team doesn't just notify you of issues; they can also neutralize the threat for you. Ultimately, you decide what level of action you want us to take and how we work with you team.

Spend less time on cybersecurity admin

When IT resources are limited, it becomes difficult to sift through the deluge of security alerts to decide which ones to attend to first. Sophos helps you cut through the noise with a single-console view of your security, and automation that solves problems before you have to worry about them – so you can focus your time on making a strategic difference.

Simplifying cybersecurity management

Sophos Central is our unified web-based platform where you can manage all your Sophos security products. No more jumping from console to console to secure your organization; with Sophos Central, you can easily deploy and manage your protection and conduct cross-product investigations that correlate data from multiple services all in one place.



Manage all your cybersecurity through the Sophos Central platform

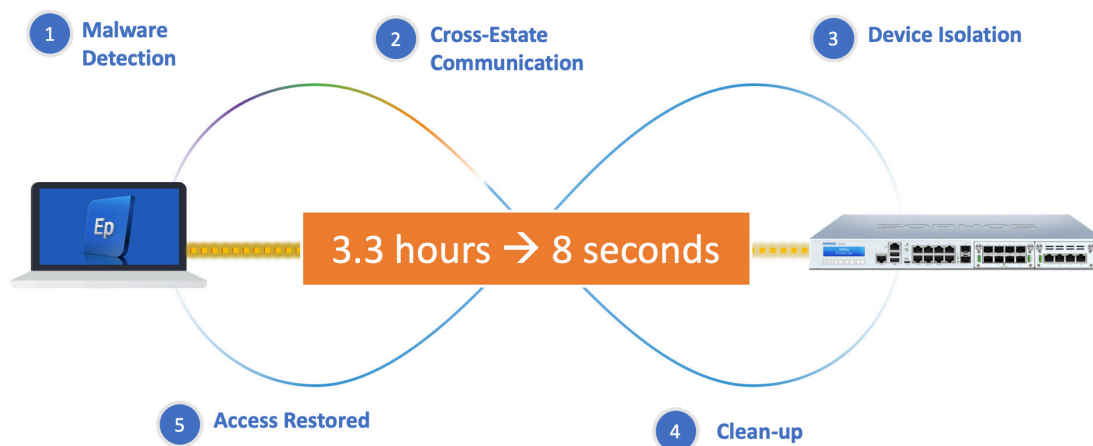
Automating your protection

Sophos Central enables Sophos products to actively share information and work together in real time to respond automatically to incidents. This integration and automation elevates your protection while reducing the workload burden on IT teams.

Example 1: Automated incident response

- If Sophos Intercept X identifies a threat on the endpoint, it notifies Sophos Firewall instantly.
- Sophos Firewall automatically isolates the infected endpoint from the network, including from other devices on the same LAN.
- Intercept X cleans up the threat, and notifies Sophos Firewall when it's done.
- Sophos Firewall immediately restores network access.

This whole process, which manually takes about three and a half hours, happens in less than eight seconds.

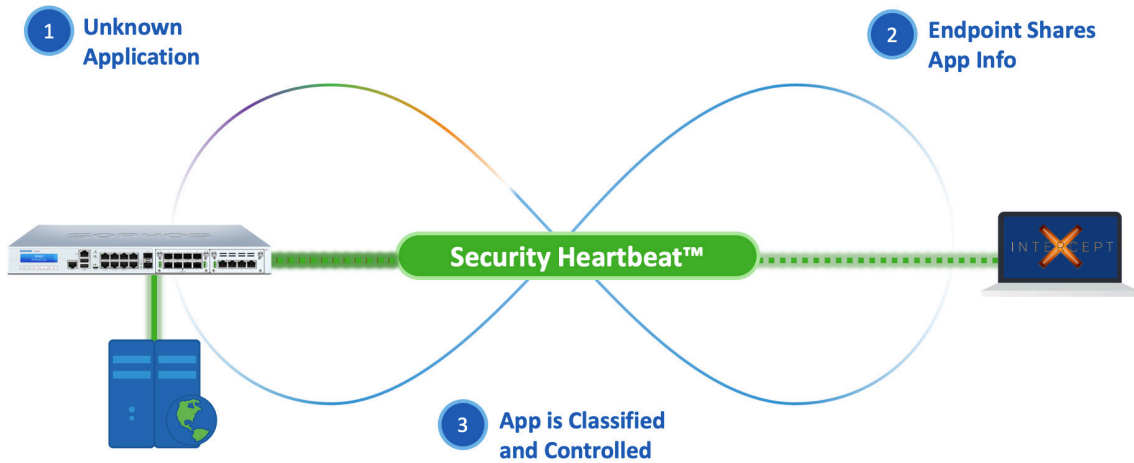


Automating incident response

Example 2: Identify all unwanted apps on the network

On average, 43% of network traffic goes unidentified. Some are custom applications that don't have a standard signature. Other times it's because the app wants to hide its identity from the firewall because it's up to no good.

- If Sophos Firewall sees an application that doesn't match a known signature, instead of assigning it to a bucket of generic traffic such as 'HTTPS', Sophos Firewall contacts Sophos Intercept X.
- Intercept X passes back the application name, patch, and category to Sophos Firewall for classification. The application is then automatically assigned to the appropriate group.
- If that group has control measures applied (e.g. block) then the same rules are applied. If necessary, for example with custom apps, the admin can manually set a category and policy to apply.



Identifying all apps and processes on the network

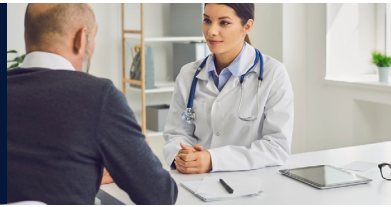
Reducing TCO in real world environments

The benefits of a Sophos cybersecurity system add up. Combining next-gen technologies, automated incident response, real-time sharing of information, and a unifying management platform has a huge impact – on both protection and overall total cost of ownership (TCO).

*Customers running Sophos Intercept X endpoint and Sophos Firewall say they would need to **double their security headcount to maintain the same level of protection** if they didn't have a Sophos system, and report a reduction in security incidents of up to 85%.*

CUSTOMER CASE STUDY HEALTHCARE PROVIDER, U.S.

A regional healthcare provider whose services include inpatient and outpatient care, medical practices, nursing homes, and a range of specialist services.



Business impact of a Sophos cybersecurity ecosystem

50% reduction in IT security resource requirements

The customer has three employees dedicated to cybersecurity. They calculate they would, if they didn't use Sophos, need to employ three additional full-time security analysts solely to cover incident response.

90%-plus reduction in day-to-day cybersecurity workload

Prior to Sophos, reviewing logs and investigating areas of concern would take an entire day. Now they achieve the same level of confidence in just 30 minutes.

85% reduction in security incidents

Previously, they experienced three incidents each day on average. This has now dropped to an average of one every three days.

90%-plus reduction in time to investigate an incident

Before using Sophos, it took the team roughly three hours to thoroughly investigate an incident. This has now dropped to less than 15 minutes, with everything done remotely via the Sophos Central platform and without disrupting other users and impacting system availability.

CUSTOMER-AT-A-GLANCE

Number of users

4,500 employees

Sophos solutions

- Sophos XG Firewall
- Sophos Intercept X Advanced with EDR
- Sophos Intercept X for Server Protection (Windows, Linux, and virtual machines)

CUSTOMER CASE STUDY CLINICAL TRIALS PROVIDER, U.S.

A private sector organization that provides the clinical trial data needed to secure regulatory approval for new medications.



Business impact of a Sophos cybersecurity ecosystem

50% reduction in IT resource requirements

Currently, the customer spends one hour a day reviewing logs and investigating issues. They advise that they would need to hire one or two more security engineers just to manage the logs if they moved away from Sophos.

33% reduction in time to deal with a potential issue

Previously, to address a security issue with a device, they would reimage the machine, which took between 90 minutes and two hours. With Sophos, they can conduct a full investigation and remediate in approximately one hour – with no reimaging.

88% reduction in threat risk due to faster issue identification

Prior to using Sophos, it took a full day just to investigate the logs to find the issues. With Sophos, the IT team can identify new issues for investigation within minutes of a suspicious event arriving.

Improved user behavior

As users are aware that the IT team can now address issues quickly and without impacting work, they are far more willing to report issues or concerns.

CUSTOMER-AT-A-GLANCE

Number of users

150 employees across four locations

IT team

Two IT staff, covering all areas including cybersecurity

Sophos solutions

- Sophos XG Firewall
- Sophos Intercept X Advanced with EDR
- Sophos Device Encryption

Give busy healthcare workers a security safety

In a high-pressure healthcare setting, risks arising from human error will always be difficult to eliminate and control. Sophos provides a vital safety net so people can work quickly, without worry.

Stop threats from reaching your users

We can help take the pressure of your users – and by extension your IT team – by both stopping the threats reaching your users in the first place:

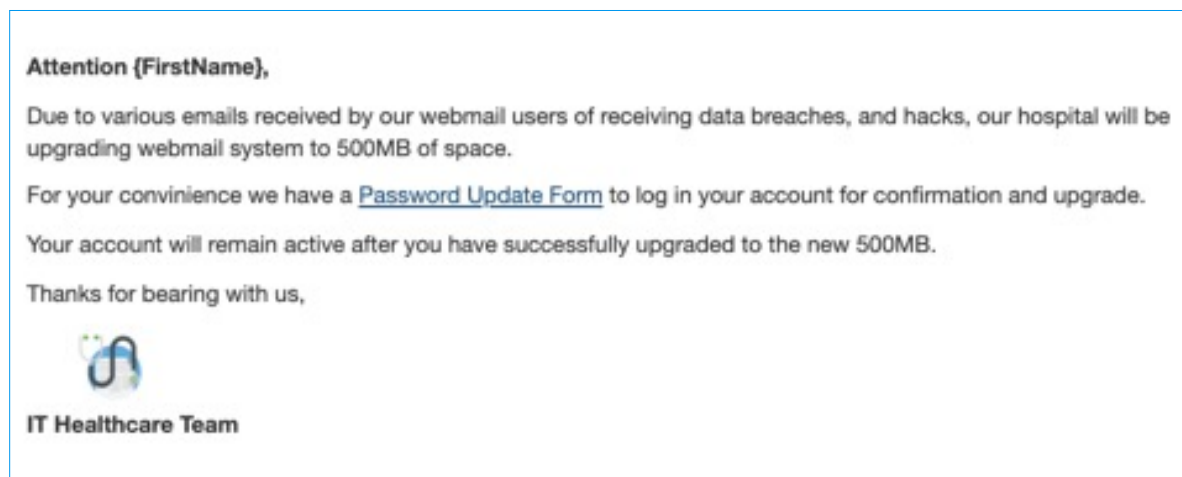
Intercept X with EDR combines anti-ransomware, exploit prevention, and AI-powered detection to stop threats at multiple points in the attack chain. Users can relax knowing the world's best endpoint protection has got their backs.

Sophos Email places predictive, AI-powered security directly in your users' inbox. It identifies malicious emails and removes them automatically, before users even have a chance to click a suspicious link.

The Sophos cybersecurity ecosystem enables Sophos products to work together to respond automatically to threats, stopping and cleaning up threats in just seconds.

Train your users on how to spot threats

Sophos Phish Threat helps users identify malicious emails through simulated phishing emails and online training. You can target training at those who most need it, either due to the nature of their role or their performance in the simulation testing.



Sample phishing simulation email in Sophos Phish Threat

Implement security that doesn't slow down healthcare

Keeping everything working and moving is more important in healthcare than most other industries. And for this, many healthcare users deploy unapproved apps to make their jobs easier. This leaves your network and data at high risk. Sophos helps you tackle shadow IT without getting in the way of your day-to-day operations.

Advanced protection that keeps everything moving

Intercept X with EDR secures your endpoints and servers – stopping threats from disrupting your users. The EDR capabilities enable you to remotely query your users' devices and, if necessary, remediate the machine.

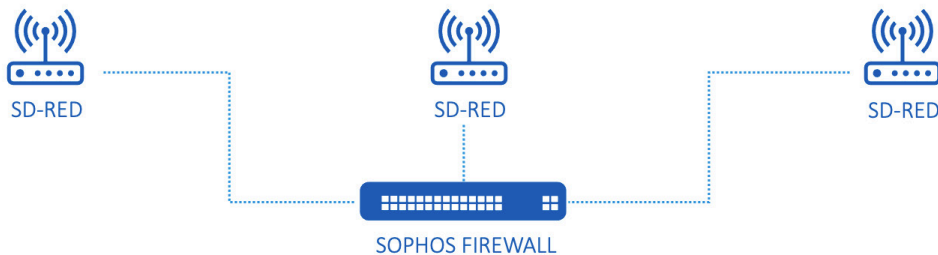
Sophos Firewall keeps your network safe from threats and makes it easy to give priority to trusted network traffic, ensuring critical processes can continue without disruption. Plus, it gives you visibility and control of shadow IT, enabling you to identify and stop activity that may put your organization at risk.

Sophos products are great on their own - and even better together. As we've seen, Sophos Intercept X and Sophos Firewall work together to respond automatically to threats and enhance your visibility.

Securing legacy technology

A challenge we hear from many healthcare organizations is the need to secure legacy equipment. These devices often run out-of-date operating systems that can't be updated due to regulatory issues, but need to be connected to the network. If a device cannot be patched/updated and doesn't have a supported antivirus or anti-malware solution, you need to look at a physical solution.

Sophos Firewall and **SD-RED** (remote ethernet device) can help here. By putting a SD-RED in front of the exposed device, it can tunnel all traffic to a protective Sophos Firewall for scanning. If your network is very flat, you will likely need to make a few small changes to IP address schemes and possible switch topology – and our technical specialists can discuss your particular situation and advise how to do this.

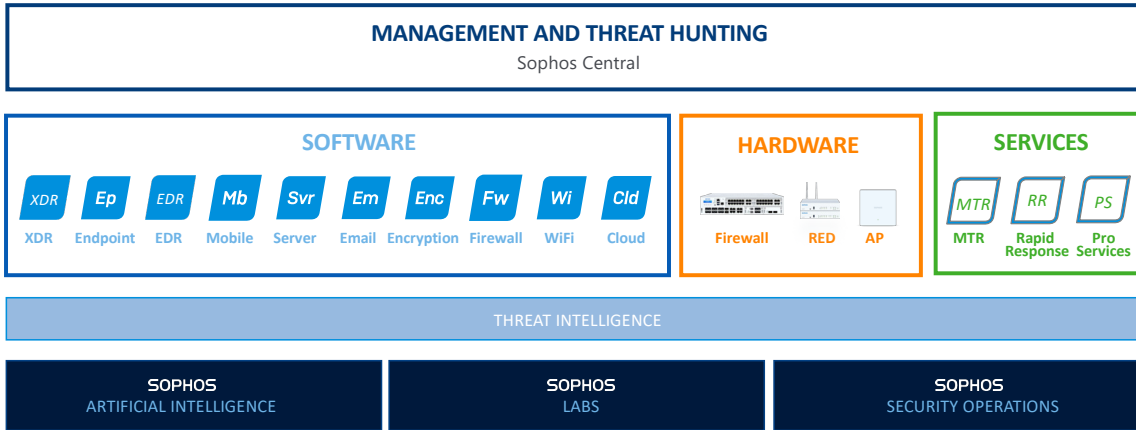


Securing legacy equipment

Conclusion

Protecting healthcare IT environments and the sensitive data they carry takes layered security. By implementing intelligent security at every vulnerable point, from networks to data, you can protect your systems, staff, and patients from internal and external risks.

All Sophos solutions are part of our adaptive cybersecurity ecosystem. They're great on their own – many organizations start with just one product – and they work even better together. As your Sophos protection grows, so do the added benefits of an integrated ecosystem: the sharing of information, the centralized management in a single console, the automated response, the deeper insights – all of which working together further elevates your protection while enhancing the efficiency of your IT team.



Securing healthcare: Sophos cybersecurity ecosystem

To learn more about how Sophos secures healthcare organizations and to discuss your requirements, contact your Sophos representative or [request a callback](#) from our security specialists.

Request a call back from our security specialists 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.