SOPHOS

Cybersecurity Guide for Healthcare

Sophos' expert threat analysts and world-leading threat intelligence help you to identify and respond to advanced threats faster, 24/7.

For healthcare organizations, the need to safeguard the sensitive patient data they store and to preserve business continuity at all costs makes them a prime target for cybercriminals. 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 uninterrupted patient care.

Sophos secures healthcare against a wide range of cyberattacks, including human-led threats that technology alone cannot prevent. From managed detection and response (MDR) to endpoint and network security, Sophos enables healthcare organizations to optimize their defenses and frees IT teams to focus on the business.

A Sophos Whitepaper. October 2023

Cybersecurity Challenges in Healthcare

Healthcare is at increased risk of privacy and data breaches because of the complex and vast list of compliance requirements, rapid uptake of digitalization, fewer IT resources, and inadequate security. Protected health information (ePHI) is highly valued on the dark web, and cyber criminals are keen to get their hands on it. It's perhaps not surprising that cyber threats in healthcare continue to grow.

A 2023 Sophos survey of 233 IT professionals in the healthcare sector revealed that 60% of organizations were hit by ransomware in 2022. Almost three-quarters of healthcare organizations (73%) hit by ransomware had their data encrypted, up from 61% the year prior. In addition, 37% of those who had data encrypted reported that data was also stolen.

> *"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

60%
of healthcare organizations hit with ransomware

73%
of attacks on healthcare resulted in data being encrypted

$2.2M
average cost to remediate following an attack

85%
of private-sector healthcare organizations hit by ransomware said it caused them to lose business/revenue

37%
of attacks where data was encrypted also resulted in data being stolen

73%
in healthcare used backups to restore encrypted data

42%
in healthcare paid the ransom to restore encrypted data

100%
of healthcare organizations that had data encrypted got data back

Source: Sophos' global survey on The State of Ransomware 2023

Behind these statistics are a number of changes in the threat landscape:

The professionalization of cybercrime

One of the most significant developments over the last year has been the development and professionalization of the cyber threat economy. Criminal groups increasingly specialize in a particular component of an attack, for example, initial access, ransomware, information-stealing malware, and more, and offer it as a service to other criminals. These 'as-a-service' models lower the skill threshold required to conduct an attack, increasing the volume of adversaries and threats.

These specialist services provide execution guidance and resources for their criminal customers, enhancing the effectiveness of the attacks. Illustrating this point, in March 2022, an associate of the Conti ransomware-as-a-service group published an archive that included a rich trove of documentation and guidance designed to instruct an "affiliate" attacker in the steps required to conduct a ransomware attack.

Attackers are also adopting many of the behaviors of legitimate IT service providers, including asking ransomware victims to 'rate their service' once they have decrypted the files post-payment.

The evolution of attacker tactics, techniques, and procedures

Adversaries frequently exploit weaknesses in organizations' security posture in an attempt to avoid being stopped by security solutions. These include:

- Exploiting unpatched vulnerabilities – This was the number one method adversaries used to penetrate organizations in attacks that Sophos' incident responders were brought in to remediate last year, used in 47% of incidents.
- Exploiting legitimate IT tools – Many of the top tools used by IT professionals are also abused by adversaries, including PowerShell, PsExec, and PowerShell, to exploit stolen access data and credentials. By posing as legitimate users, attackers hope to trick their way into an environment.

The cybersecurity challenges for this sector don't end here. Healthcare organizations also need to contend with insider threats (both malicious and accidental), strict regulatory compliance requirements, and third-party vendor risks, amongst other challenges.

Sophos: Securing healthcare

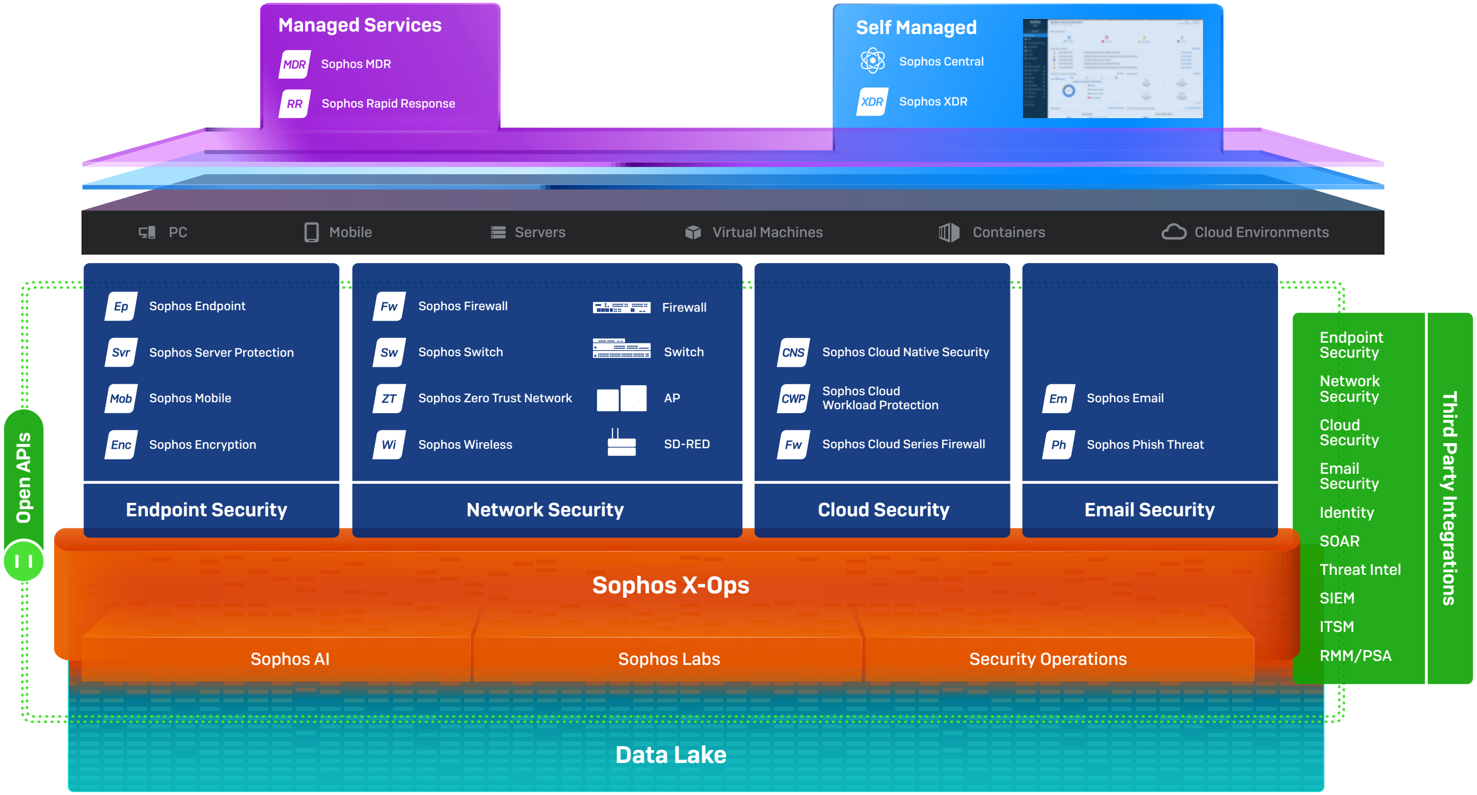
Sophos delivers advanced cybersecurity solutions that enable healthcare organizations to manage and reduce cyber risk. Our adaptive cybersecurity ecosystem provides a full portfolio of market-leading services and products that elevate our customers' defenses against even the most advanced threats, all powered by the unparalleled threat, AI, and security operations expertise of Sophos X-Ops.

Sophos delivers leading cybersecurity outcomes for over **530,000 customers** globally

No vendor has been **named a Gartner Leader** in endpoint security more times than Sophos

The **highest rated** and **most reviewed** MDR Service, Endpoint and Firewall on Gartner Peer Insights.

As on August 1, 2022



Use Cases

Sophos can help address the most common cybersecurity challenges facing healthcare organizations.

Stopping Advanced Human-Led Attacks, Including Ransomware

Sophos MDR is a fully-managed, 24/7 service delivered by experts specializing in detecting and responding to cyberattacks that technology solutions alone cannot prevent. Our expert team stops advanced human-led attacks on your behalf, neutralizing threats before they can disrupt business operations or compromise sensitive customer data.

> *"Sophos' MDR has saved us at least once in the past year from a nasty malware incident that could have turned into a full-blown ransomware attack very quickly."*
>
> Hammondcare

> *"We have a highly specialized team at our disposal that helps us to face the increasingly complex and evolving IT challenges."*
>
> DentalPro S.p.A.

With Sophos MDR, our expert analysts detect and respond to threats in minutes – using your preferred technology – whether you need a full-scale incident response or assistance making more accurate decisions.

We use:

- Sophos' award-winning solutions, including our endpoint, firewall, cloud, and email protection
- Products from other vendors such as Microsoft, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Rapid7, Amazon Web Services (AWS), Google, Okta, Darktrace, and many others
- Any combination of our technology and other vendors' technology

Sophos MDR protects your organization from advanced attacks that technology solutions alone cannot prevent while increasing the return on your existing investments. As the world's most trusted MDR provider, we have unparalleled depth and breadth of expertise in threats facing the healthcare sector. Leveraging this extensive telemetry, we can generate 'community immunity,' applying learnings from defending one healthcare customer to all other customers in the industry, elevating everyone's defenses.

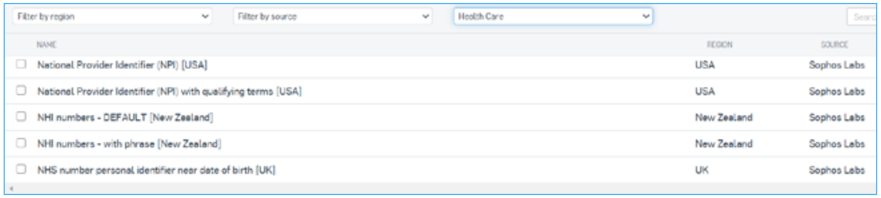
MOST TRUSTED **#1 Provider**	TOP RATED **4.8/5** Gartner Peer Insights	BEST PROTECTION **38 mins** to detect, investigate, respond
More organizations trust Sophos for MDR than any other vendor.	Highest-rated and most reviewed MDR solution as of May 31, 2023	Our analysts are over 5X faster than the fastest in-house SOC teams

As of September 2022

Securing 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). Unauthorized disclosure of sensitive data could mean violation of the privacy rights of patients and non-compliance with specific industry regulations, leading to hefty penalties. 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.

Securing the device or workload that holds the data: Get complete protection for all your endpoints – Windows, Mac, Linux, and virtual machines – with Sophos Intercept X Endpoint, our market-leading EDR solution. Healthcare-specific data loss protection rules, using healthcare terms or data types, elevate your protection.



Health Care

	NAME	REGION	SOURCE
☐	National Provider Identifier (NPI) [USA]	USA	Sophos Labs
☐	National Provider Identifier (NPI) with qualifying terms [USA]	USA	Sophos Labs
☐	NHI numbers - DEFAULT [New Zealand]	New Zealand	Sophos Labs
☐	NHI numbers - with phrase [New Zealand]	New Zealand	Sophos Labs
☐	NHS number personal identifier near date of birth [UK]	UK	Sophos Labs

With cybersecurity, there is no silver bullet, no single protection capability that will stop every threat. Each attack combines a different set of tactics, techniques, and procedures (TTPs), and as a result, to optimize your defenses, you need layered protection. Sophos Endpoint is packed with these layers of protection, including:

- Credential theft protection that prevents unauthorized system access.
- Exploit protection to stop the techniques adversaries use.
- Anti-ransomware protection which identifies and blocks malicious encryption attempts.
- Tamper protection that prevents adversaries from turning off defenses so they can deploy their payloads.

Combining multiple layers of protection technologies enables us to optimize our customers' defenses. Testament to the quality of our defenses – and the power of layered protection – we stop 99.98% of threats up-front (AV-TEST average score), and recently earned perfect scores in SE Labs

Further bolstering your defenses is Sophos Device Encryption, which 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 through which the data flows: Sophos Firewall uses AI-powered threat detection technology to prevent attacks from reaching your sensitive healthcare data, critical medical systems, and other parts of your ecosystem. Recognized as a Gartner Customers' Choice for Network Firewalls 2023, Sophos Firewall tightly integrates a full suite of modern threat protection technologies that are easy to set up and maintain.

Sophos Firewall's flexible and powerful segmentation options via zones and VLANs help you separate levels of trust on the network to reduce cyber-risk exposure to your data stores. For example, databases and servers can be segmented into a DMZ with stricter security measures than other parts of the network to keep the server hosting confidential data secure and separate from other network zones.

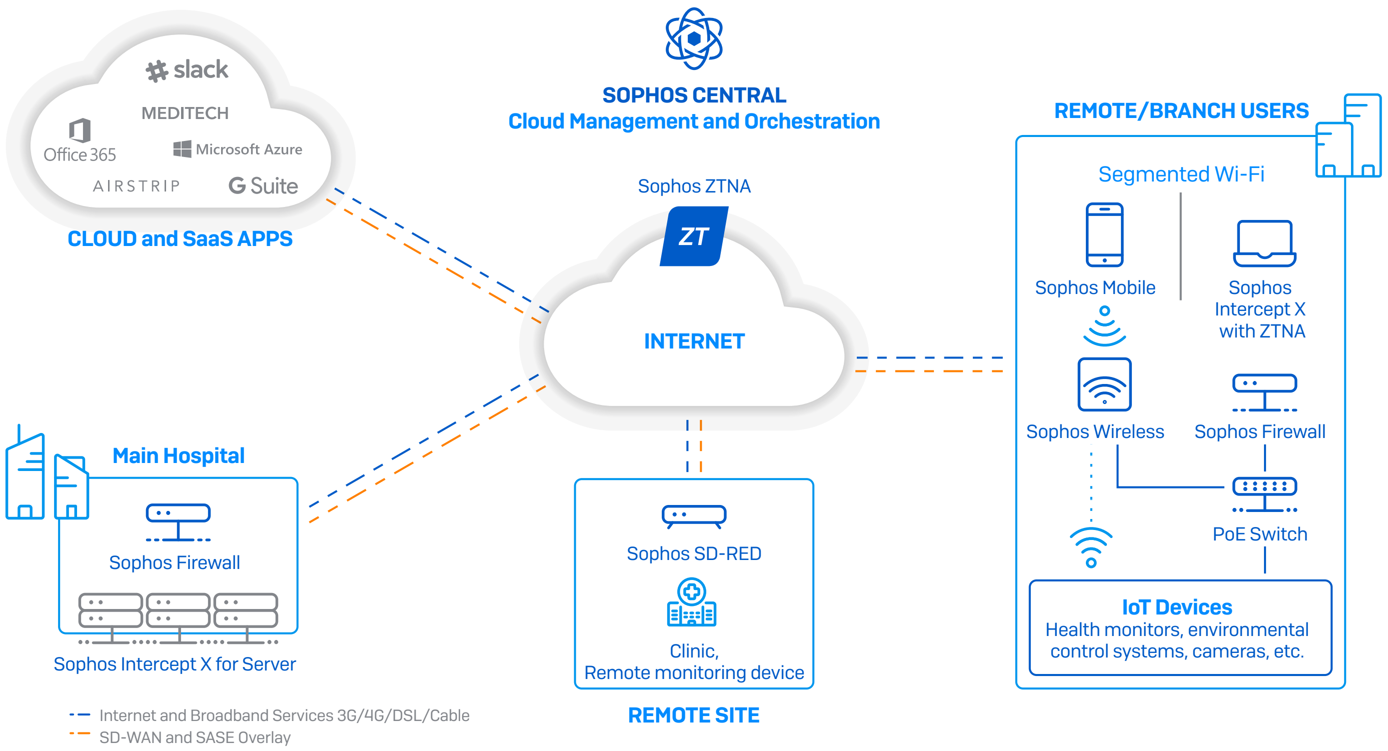
Stopping loss by email – deliberate or accidental: Sophos Email encrypts personally identifiable information, patient records, medical images, and other sensitive data, stopping both accidental and malicious data breaches. It allows you to create multi-rule DLP policies for users to ensure the protection of sensitive information with the discovery of confidential contents in all emails and attachments.

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

Enabling users to connect securely from any location

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. 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 has 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.

The Sophos Secure Access portfolio connects remote healthcare sites, safely delivers critical cloud and SaaS applications, and facilitates the secure sharing of data and information. It consists of Sophos ZTNA to secure access to applications and data, Sophos SD-RED remote Ethernet devices to extend secure healthcare networks to remote clinics or branch sites, Sophos Wireless access points for easy and safe wireless networking, and Sophos Switch network access layer switches for secure access on the LAN. Everything is managed through Sophos Central, our all-in-one cloud-based security platform.



Protection Against Insider Attacks

The risk of insiders accidentally or deliberately misusing their privileges can be a critical threat to healthcare organizations. Insider attacks may lead to fraud, theft of PHI/PII, sabotaging critical healthcare and life-supporting systems, and more.

Get insights into your riskiest users and applications to ensure that your policies are enforced before your security is compromised with actionable intelligence from Sophos User Threat Quotient (UTQ). Take your protection a step further with Sophos Firewall, which protects your sensitive data from accidental or malicious disclosure with complete policy control over web categories, applications, removable media, and mobile devices used in your network. It offers user awareness across all areas of the firewall with user-based access policies for traffic shaping (QoS), and other network resources, regardless of the IP address, location, network, or device.

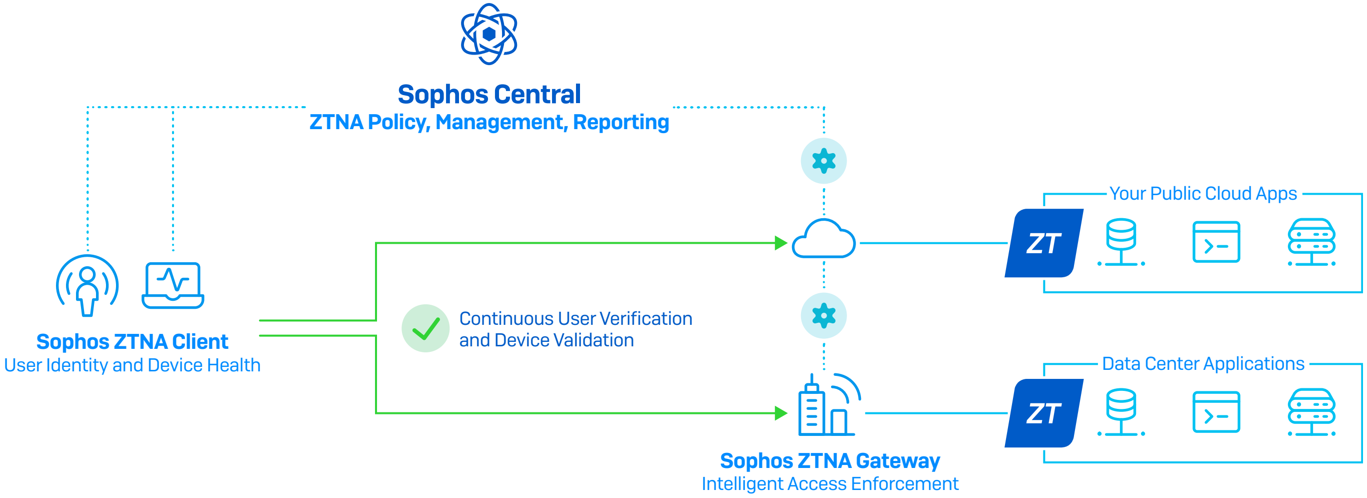
Reducing Supply Chain Risks

Healthcare has a vast and complex third-party vendor network. A vulnerability in any of a supplier's networks can rapidly propagate to infect the healthcare organization.

The use of AI, exploit prevention, behavioral protection, and other advanced technologies in Sophos Intercept X can help healthcare organizations defend against threats that infiltrate via third-party suppliers. Plus, our powerful XDR functionality enables you to automatically identify suspicious activity, prioritize threat indicators, and quickly search for potential threats across your endpoint and servers.

Get 24/7 expert support with over 500 specialists working around the clock to proactively hunt for, validate, and remediate potential supply chain threats and incidents on your behalf with Sophos MDR.

Protect against supply chain attacks that rely on supplier access to your systems via very granular access controls with Sophos ZTNA, which authenticates requests from trusted partners, irrespective of their location. The unique integration of Sophos Endpoint and Sophos ZTNA automatically prevents compromised hosts from connecting to networked resources, preventing threats from moving laterally and getting a foothold on your network.


Sophos Central
ZTNA Policy, Management, Reporting
Your Public Cloud Apps
ZT
Sophos ZTNA Client
User Identity and Device Health
Continuous User Verification and Device Validation
Data Center Applications
ZT
Sophos ZTNA Gateway
Intelligent Access Enforcement

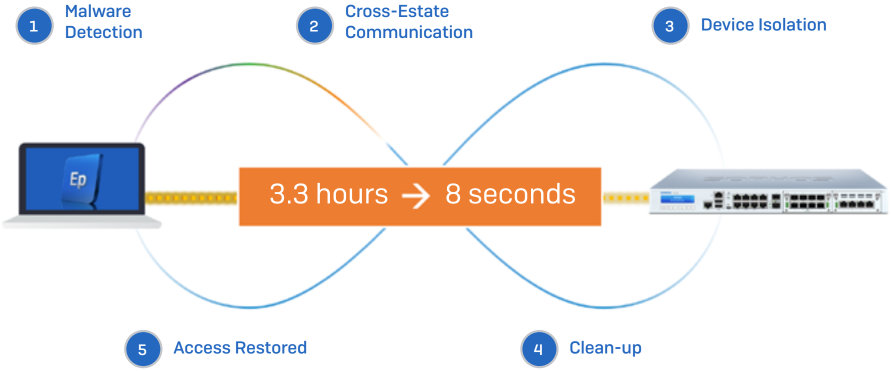
Automating Your Protection

The Sophos Adaptive Cybersecurity Ecosystem (ACE) enables Sophos products to share threat, health, and security information in real-time and work together to respond automatically to threats. It brings together the power of Sophos' threat intelligence, next-gen technologies, data lake, APIs, and Sophos Central management platform, creating an adaptive cybersecurity ecosystem that constantly learns and improves.

Example 1: Automated incident response

- If Sophos Intercept X identifies a threat, 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.

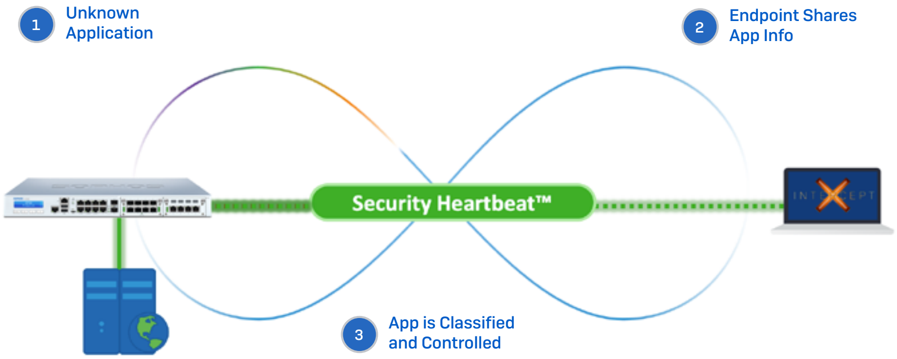
This whole process, which manually takes about three and a half hours, happens in just eight seconds.



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.

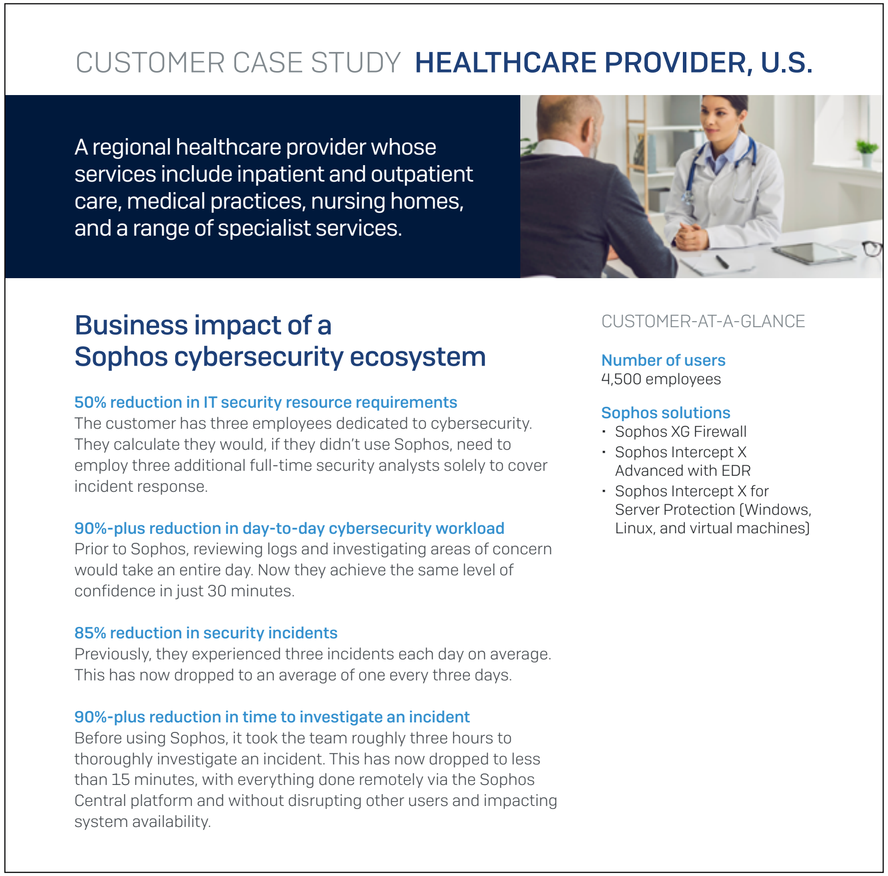
- If Sophos Firewall sees an application that doesn't match a known signature, instead of assigning it to a bucket of generic traffic such as 'HTTPS', Sophos Firewall contacts Sophos Intercept X.
- Intercept X passes back the application name, patch, and category to Sophos Firewall for classification. 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.


1 Unknown Application
2 Endpoint Shares App Info
Security Heartbeat™
3 App is Classified and Controlled

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). These advantages add up, delivering huge efficiency and productivity benefits for IT teams.

> *"Customers running Intercept X endpoint and Sophos Firewall managed through Sophos Central consistently report a reduction in admin workload of at least 50%, and reductions 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.

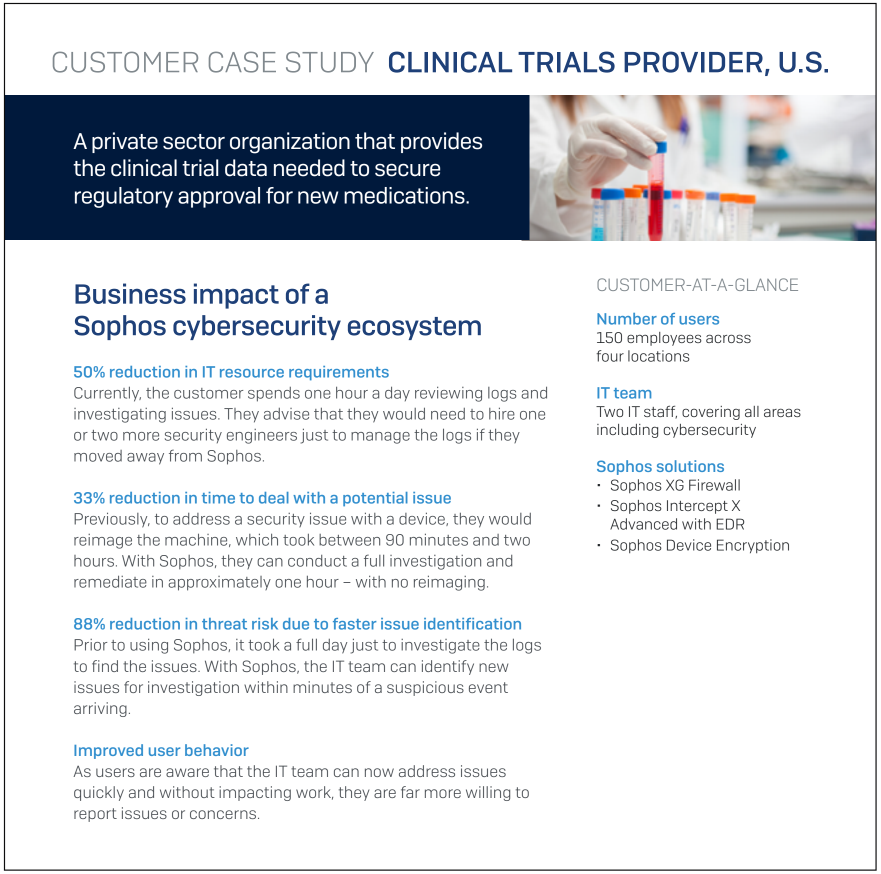
85% reduction in security incidents
Previously, they experienced three incidents each day on average. This has now dropped to an average of one every three days.

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

Ensuring Operational Efficiency

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.

Sophos Intercept X gives you oversight of which apps are installed on your users' devices. Any unsanctioned apps in use can be addressed directly – and even remotely uninstalled where necessary.

Sophos Firewall can 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.

Simplifying Cybersecurity Management

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 must worry about them – so you can focus your time on making a strategic difference.

Sophos Central is our unified web-based platform where you can manage all your Sophos security products. You can easily deploy and manage your protection and conduct cross-product investigations that correlate data from multiple services all in one place.

Meeting Regulatory Requirements

Healthcare faces strict data security requirements by regulations and standards such as HIPAA, PCI DSS, and GDPR due to the vast amount of private and sensitive data they hold.

Ensuring encryption of critical corporate and customer records and transactions, ePHI, and other sensitive data can mean the difference between a safe harbor and the need for public breach notification. Sophos Device Encryption protects your devices and data with full disk encryption for Windows and macOS that helps you verify device encryption status and demonstrate compliance.

Sophos Cloud Optix helps you eliminate compliance gaps with a single view of your compliance posture across AWS, Azure, and Google Cloud environments. Continuously monitor compliance with custom or out-of-the-box templates and audit-ready reports for standards such as FFIEC, GDPR, HIPAA, PCI DSS, and SOC2.

The use of mobile devices has become commonplace in healthcare, enabling healthcare providers to access and maintain patient records and prescriptions and to communicate and consult, resulting in better clinical decision-making and improved patient outcomes. However, easy access to critical business data on mobile devices threatens the security of sensitive corporate and customer data held by healthcare organizations. Sophos Mobile ensures the integrity of your sensitive data on mobile devices by enforcing device encryption and denying access to email, network, and other resources if a device is not compliant with the company policy.

Securing Resources in the Cloud

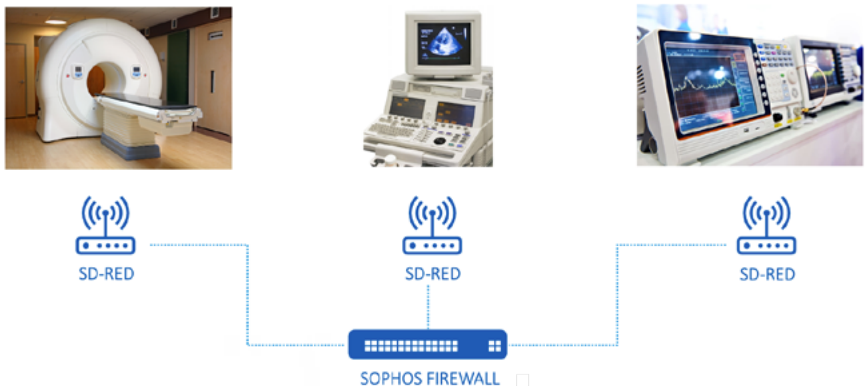
The cloud is integral to the successful day-to-day operations of healthcare organizations. It offers greater speed and flexibility than traditional on-premises resources, as well as the opportunity to move from one-off capital expenses to distributed operating costs. However, the cloud is also a major target for cybercriminals looking to exploit less established cybersecurity practices than in traditional on-premises environments.

Sophos Cloud Native Security provides complete multi-cloud security coverage across environments, workloads, and identities. It protects your cloud infrastructure and data with flexible host and container workload security for Windows and Linux. Multi-layered technologies protect against ransomware and other advanced attacks including cloud-native behavioral and exploit runtime detections that identify threats such as container escapes, kernel exploits, and privilege-escalation attempts. Plus, it also makes it easy to keep on top of your cloud spend. You can quickly identify if your account is being abused and eject the adversaries before they rack up a big bill.

Securing Legacy Technology

One of the challenges of 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/upgraded 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, as well as with secure remote access. By putting an 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.



Protection Against Phishing Attacks

Phishing attacks are one of the easiest ways for scamsters to gain access to your system and sensitive data.

One of the best ways to stop phishing attacks is to train your employees on how to recognize a phishing scam. Create a positive security awareness culture in your organization with Sophos Phish Threat which offers a collection of more than 30 security awareness training modules to educate and test your end users through automated attack simulations, quality security awareness training, and actionable reporting metrics.

Allow only trusted senders into your employees' inboxes with Sophos Email that scans all inbound messages for key phishing indicators such as brand spoofing and impersonation attempts in real-time using SPF, DKIM, and DMARC authentication techniques and email header anomaly analysis. This helps to spot and block phishing emails before they reach your users.

Sophos Email uses advanced Natural Language Processing (NLP) machine learning to block targeted impersonation and Business Email Compromise (BEC) attacks. It includes a setup assistant that integrates with AD Sync to automatically identify the individuals within an organization who are most likely to be impersonated. It scans all inbound mail for display name variations associated with those users, further extending protection against phishing imposters.

Conclusion:

Cyberattacks like ransomware, exploits, and phishing can have severe business and reputational consequences for healthcare organizations. Protecting your IT environments and sensitive data requires an integrated security approach.

Sophos protects your systems and data wherever they exist with our next-gen services and technologies while enabling you to consolidate your security management with a single vendor. All Sophos solutions are controlled through a unified cloud-based management console, Sophos Central, which allows real-time information sharing between products, centralized management, automated incident response, and deeper insights – all of which, working together, further elevates your protection while enhancing the efficiency of your IT team.

To learn more about how Sophos secures healthcare organizations and to discuss your requirements, contact your Sophos representative or request a call-back from our security specialists.

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.

© Copyright 2023. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2023-10-05 (WP-NP)

SOPHOS