SOPHOS

Cybersecurity Guide for the Pharmaceutical Sector

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

The pharmaceutical industry is home to valuable patent and IP data, patient and clinical trial data, data from R&D on pharmaceutical advances and technologies, and more. Extensive reliance on third-party supply chains, rapid digitalization, move to multi-cloud environments, and rising adoption of IoT technology are some factors leading to a broader attack surface in the sector. A data or privacy breach would mean operational disruption in the manufacturing of life-saving drugs, repeating clinical trials for the discovery of new drugs or invention of new therapies, contaminated drugs, legal challenges, lost consumer trust and business revenue, and more.

Sophos secures organizations in the pharmaceutical sector 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 organizations to optimize their defenses and frees IT teams to focus on the business.

A Sophos Whitepaper. May 2023

Cybersecurity Challenges in Pharma

Thanks to the pandemic, pharma companies are in the spotlight now more than ever before. As the pharma sector moves towards increased digitalization and storing valuable research and patient data online, cyber threats in this sector continue to grow in both volume and complexity because of the evolving 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. Pharma organizations also need to contend with insider threats (both malicious and accidental), and third-party vendor risks, amongst other challenges.

Sophos Security for the Pharma Sector

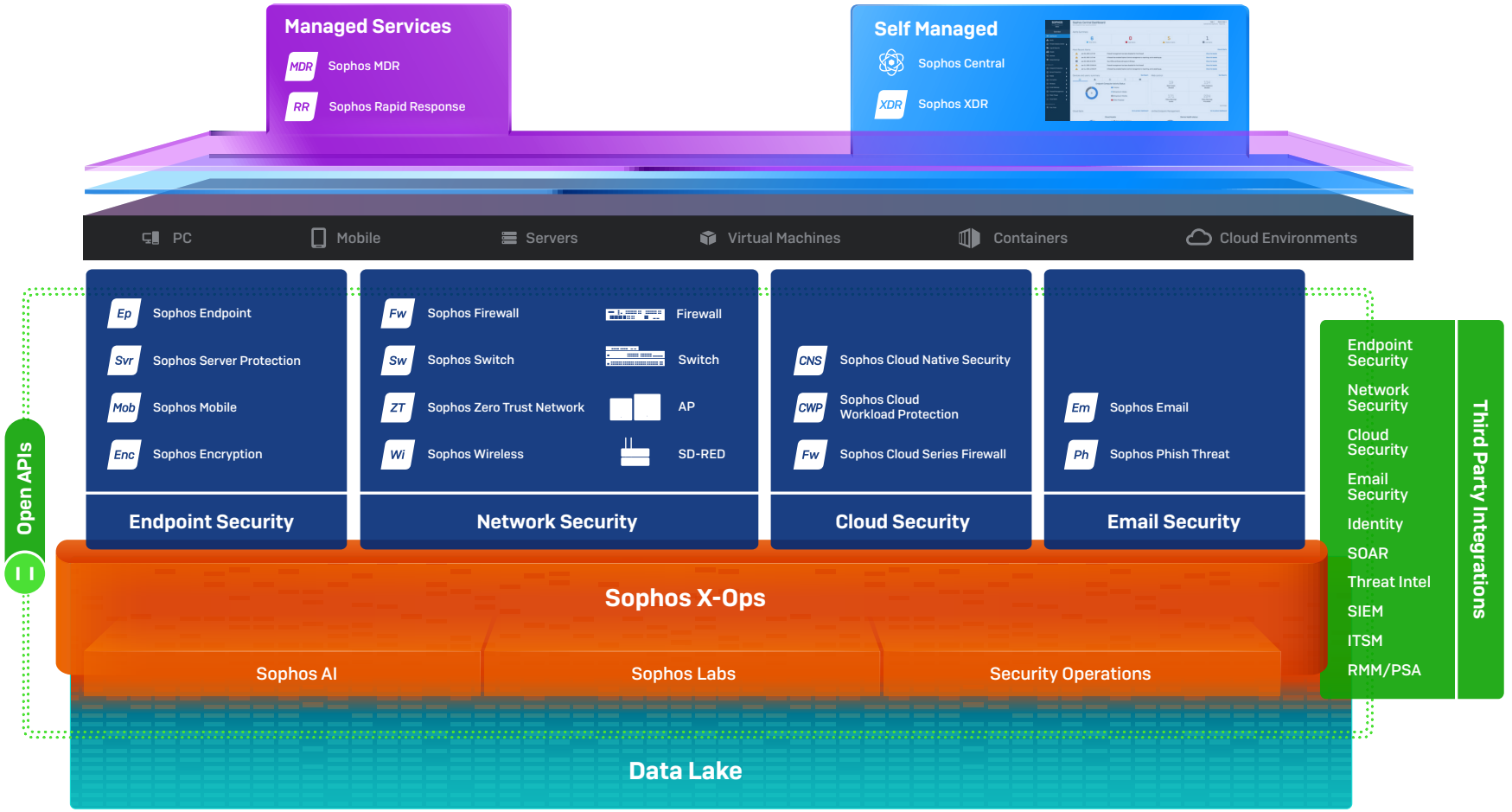
Sophos delivers advanced cybersecurity solutions that enable pharma organizations to manage and reduce cyber risk. Our adaptive cybersecurity ecosystem provides a full portfolio of market-leading services and products that elevate our customers' defenses against even the most advanced threats, all powered 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 of August 1, 2022



Use Cases

Sophos can help address the most common cybersecurity challenges facing pharma 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.

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 pharma sector. Leveraging this extensive telemetry, we can generate 'community immunity,' applying learnings from defending one pharma customer to all other customers in the industry, elevating everyone's defenses.

MOST TRUSTED	TOP RATED	BEST PROTECTION
#1 Provider	**4.8/5** Gartner Peer Insights	**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 August 1, 2022	Our analysts are over 5X faster than the fastest in-house SOC teams

As of September 2022

Protecting Patent and Intellectual Property Data

The pharma industry needs to adopt a zero-trust approach of "trust nothing, verify everything" to secure access to their critical infrastructure and proprietary information. Sophos Zero Trust Network Access (ZTNA) solution continuously validates user identity, device health, and compliance before granting access to your applications and data. Establish granular controls to block lateral movement and make sure that only authorized parties can access sensitive data.

You can safeguard critical data by training your employees to look out for potential threats and creating a positive security awareness culture in the organization with automated attack simulations and security awareness training with Sophos Phish Threat.

With the huge number of laptops lost, stolen, or misplaced every day, a crucial first line of defense against the loss or theft of devices and the data therein is full-disk encryption. Sophos Encryption can secure classified pharmaceutical data at rest with full disk encryption for Windows and macOS.

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 IP data secure and separate from other network zones.

Mitigate known vulnerabilities and stop the latest cybersecurity threats such as ransomware, file-less attacks, exploits, and malware across your endpoint devices with Sophos Intercept X endpoint protection. Our data loss prevention (DLP) capabilities identify your sensitive data and prevent leaks via email, uploads, and local copying.

You can prevent data breaches with Sophos Email, which allows the creation of multi-rule DLP policies for users to ensure the protection of sensitive information with the discovery of confidential contents in all emails and attachments. It also seamlessly encrypts sensitive data to stop breaches.

Securing Against Phishing Attacks

Phishing attacks are one of the easiest ways for threat actors to gain access to your system and valuable 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. You can further prevent data loss by creating multi-rule DLP policies for groups and individual users to ensure the protection of sensitive information with the discovery of financials, confidential contents, and patient data in all emails and attachments.

Most phishing attacks infect the access points to your network by luring recipients to click on a malicious link that leads to downloading malware on the device or giving access to sensitive data to hackers. To strengthen your network against phishing attacks you must strengthen your endpoint security. Get complete protection for all your endpoints – Windows, Mac, Linux, and virtual machines – with Sophos Intercept X Endpoint, our market-leading EDR solution.

To optimize your defenses, you need layered protection: multiple sophisticated security capabilities with each playing its part in defending against advanced attacks. 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 endpoint protection report.

Protecting Against Cyber Espionage

The intellectual property of pharma organizations is a result of years of research and millions in investment in developing new drug formulations and therapies. Cyber espionage of pharmaceutical data is a major motivation for cybercriminals to gain technological or commercial advantage without the waiting period. Weak cyber defenses, unpatched and out-of-date systems and apps, and inadequate visibility into IT security incidents are a few reasons why pharma organizations become soft targets of cyber espionage.

Get powerful protection from the latest advanced cyber threats while accelerating your important SaaS, SD-WAN, and cloud application traffic with Sophos Firewall. Recognized as a Gartner Customers' Choice for Network Firewalls 2022, Sophos Firewall tightly integrates a full suite of modern threat protection technologies that are easy to set up and maintain. It offers flexible and powerful segmentation options via zones and VLANs. This provides ways to separate levels of trust on your network while enabling added protection against lateral movement between different parts of your network.

Sophos XDR can help you keep the systems and apps updated with regular patch management by offering the most complete view of your cybersecurity posture. By pulling in rich data from your network, email, cloud, and mobile data sources, it helps you locate systems and devices that are unpatched or have out-of-date software.

Sophos Managed Detection and Response (MDR) service reduces the threat response time dramatically for pharma organizations with a fully managed 24/7/365 service delivered by experts that are armed with critical visibility and context for seeing the entire attack path, enabling a faster, more comprehensive response to security threats that technology solutions alone cannot prevent. Our threat-hunting experts monitor and investigate alerts from across the network, leveraging network, firewall, cloud, email, and endpoint security tools to identify and investigate suspicious activities and protect patient data and classified IP information wherever it resides.

Protection Against Insider Attacks

Insider threats, whether accidental, intentional, or socially engineered, can cause massive damage to pharma organizations. More specifically, the risk of insiders with authorized access to classified data misusing their privileges can be a critical threat and can lead to leaked intellectual property and sabotage of drug discovery or launch.

Get insights into your riskiest users and applications with actionable intelligence from Sophos User Threat Quotient (UTQ) that ensures your policies are enforced before your security is compromised. 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.

An alternative safeguard is the principle of least privilege where users have access only to the network resources they need. Sophos Cloud Optix, our Cloud Security Posture Management solution, connects disparate actions with Sophos AI to pinpoint unusual access patterns and locations to cloud provider consoles in near real-time that can help you identify credential misuse or theft. An IAM visualization tool that provides a complete map of IAM relationships allows your IT teams to identify over-privileged access and create right-sized IAM policies before they are exploited in cyberattacks quickly and easily.

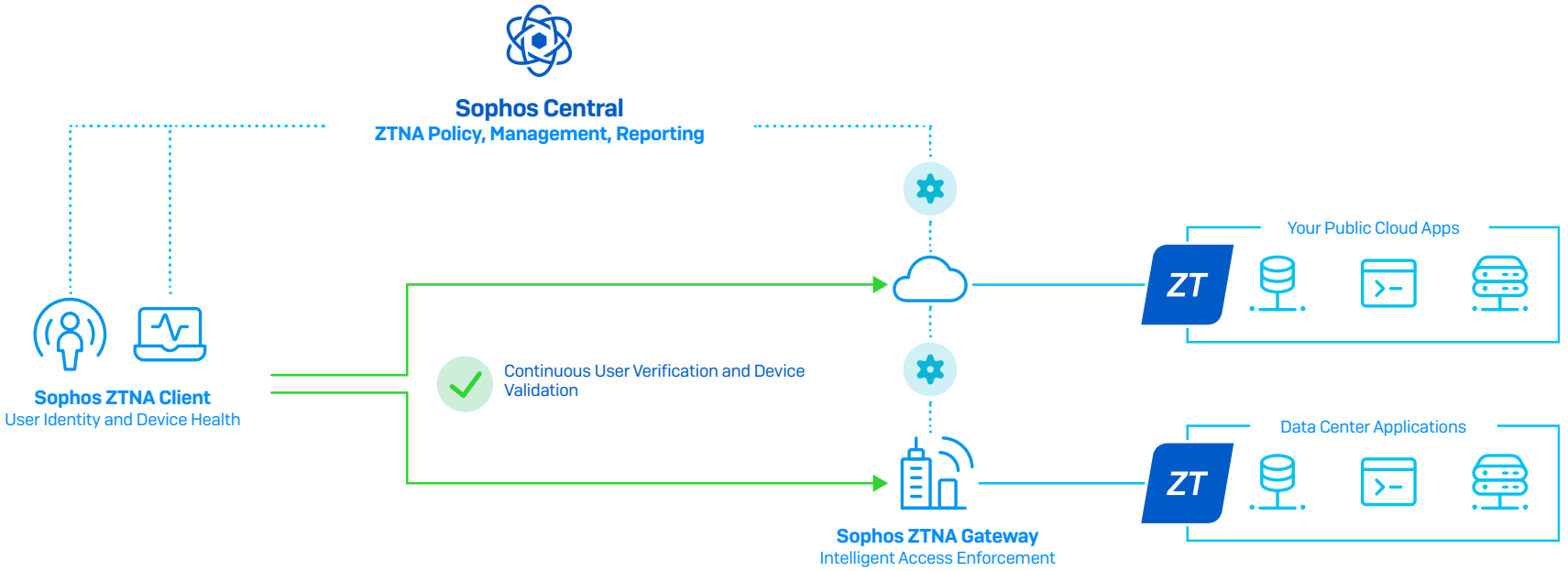
Reducing the Risk of Third-Party Supply Chain Attacks

Pharmaceutical organizations rely heavily on third-party vendors for critical activities like R&D, clinical research, supply of APIs and other key ingredients for generic drugs, and more. Warehouse, logistics, and freight forwarding partners are invaluable in pharma supply chains. As a result, the supply chain of pharma companies is a goldmine consisting of data on intellectual property, PHI, R&D, and a lot more. Because most of these third-party vendors have direct access to pharma manufacturing systems and data, any breach in the third-party ecosystem is a direct threat to the pharma organization.

Defend against threats that may infiltrate your organization via third-party suppliers by using AI, exploit prevention, behavioral protection, and other advanced technologies in Sophos Intercept X. 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.

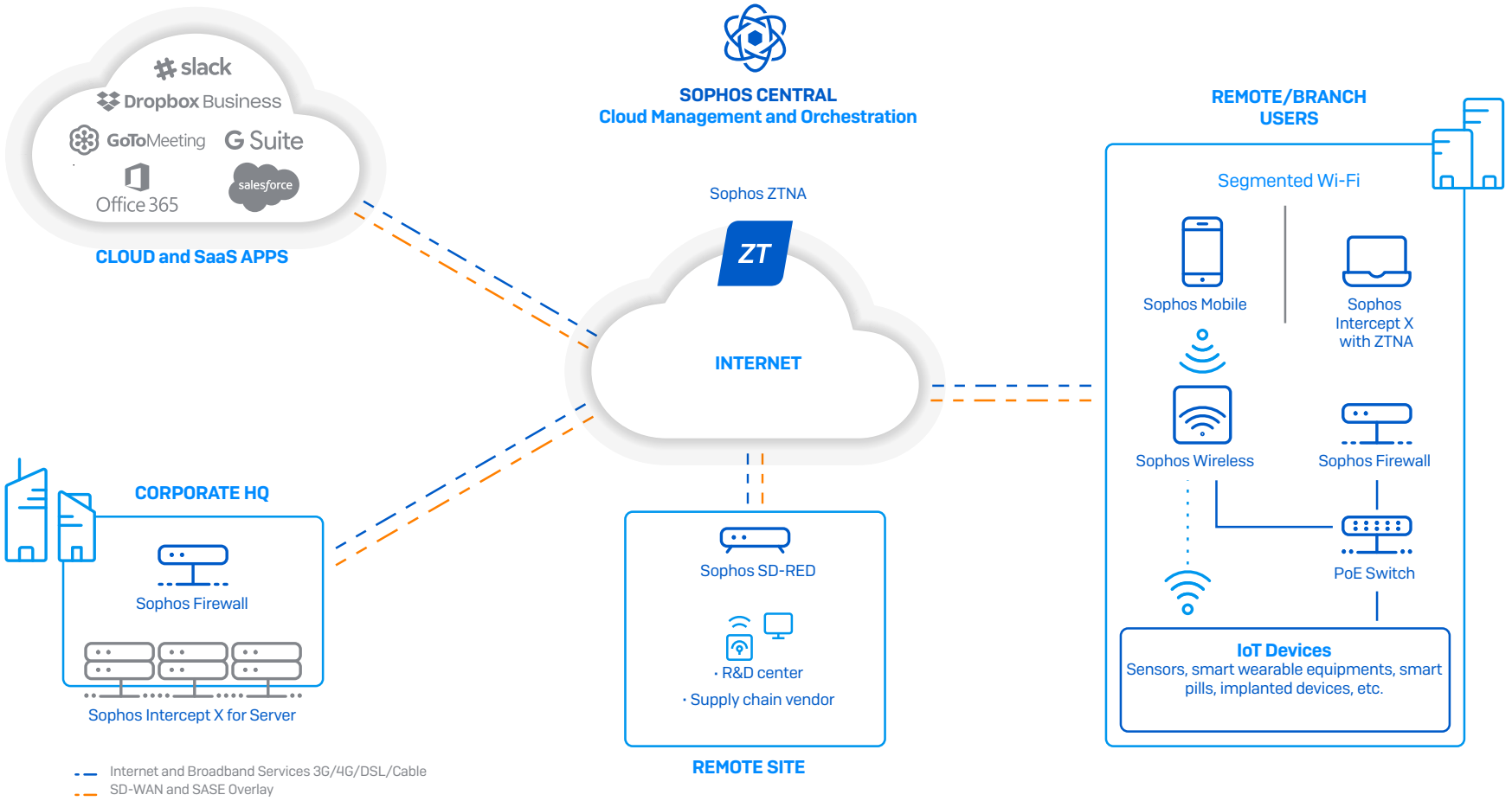
Protect against supply chain attacks that rely on supplier access to your systems via very granular access controls with Sophos ZTNA, which authenticates requests from trusted partners, irrespective of their location. The unique integration of Sophos Endpoint and Sophos ZTNA automatically prevents compromised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



Securing Remote Access Environments

A typical pharmaceutical organization has an ecosystem comprising of procurement, production, and distribution functions running in sync. There is a critical need to secure remote access between the head office and the R&D center, manufacturing facilities, supply chain vendors, distribution partners, and remote workers using personal networks and devices.

The Sophos Secure Access portfolio connects remote pharmaceutical 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 organizational networks to remote and 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.



Securing Legacy Systems

Pharma manufacturing organizations struggle to secure their legacy systems that today work alongside the new-generation IoT devices and sensors. Legacy systems traditionally depended on air gaps to provide an effective defense. Today, most of these devices run out-of-date operating systems or browsers that cannot be updated because they are no longer supported – yet they need to be connected to the network.

Sophos Firewall and Sophos SD-RED can help. Put Sophos SD-RED in front of an exposed device, and it will tunnel traffic to a protective Sophos Firewall for scanning. If your network is flat, you will likely need to make changes to IP address schemes and possible switch topology – and our technical specialists can discuss your situation and show you how to do this.

In addition to this, the threat-hunting experts from Sophos MDR monitor and investigate alerts from across the network, leveraging network, firewall, cloud, email, and endpoint security tools to identify and investigate suspicious activities, remediate the incident, and provide guidance on how to harden the environment against future exploitation.

Proactive Security for Uninterrupted Operations

Continuity of network availability and manufacturing operations in pharmaceutical organizations can mean the difference between life and death. Proactive cybersecurity must be a priority for pharma organizations: whether it is about the security of drug formulations and clinical trial data from sabotage or leakage, or the security of industrial control systems, like SCADA used in the manufacturing of drugs, from disruption.

Sophos Firewall, with industry-leading machine learning technology and powered by SophosLabs Intelix, delivers advanced protection from the latest drive-by and targeted web malware, URL/malicious site filtering, and cloud-based filtering for offsite protection. Combined with our enterprise-class web application firewall, it protects your critical business applications from hacks and attacks while enabling authorized access.

The exploit prevention capabilities in Sophos Intercept X stop vulnerabilities in applications and operating systems from being exploited by attackers. Besides, the endpoint protection application control policies restrict the use of unauthorized applications in the systems.

Sophos Cloud Optix continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.

You can stop the exploitation of vulnerabilities by adversaries with our Managed Detection and Response (MDR) service that provides 24/7 detection, investigation, and neutralization of suspicious activities by human threat experts who are kept up to date on the latest threat and vulnerability developments by Sophos X-Ops. Sophos MDR continuously monitors signals from across the security environment, enabling us to quickly and accurately detect and respond to potential cybersecurity events.

Securing Data Across Multi-Cloud Environments

Reliance on the cloud, including hybrid cloud and multi-vendor environments, has picked up among pharmaceutical companies helping them streamline complex processes and reduce costs. But 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.

Conclusion:

Cyberattacks like ransomware, cyber espionage, exploits, and phishing can have severe business and reputational consequences for pharmaceutical organizations. Protecting your IT environments and intellectual property 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 pharmaceutical organizations and to discuss your requirements, contact your Sophos representative or request a call-back from our security specialists.

2023-02-05 EN-WP (PS)

SOPHOS