Reference Card for Pharmaceutical Industry

The pharma sector holds valuable patent and IP data, patient and clinical trial data, data from R&D on pharmaceutical advances and technologies, and more. However, the sector's extensive reliance on third-party supply chains, rapid digitalization, the move to multi-cloud environments, and the rising adoption of IoT technology are some factors leading to a broader attack surface in the sector.

Sophos dramatically reduces the threat response time of pharma organizations with its next-gen services and products, allowing organizations to consolidate their security management with a single vendor. This document provides a general reference on how Sophos solutions help pharma organizations meet their cybersecurity requirements for uninterrupted operations.

Security Challenge	Sophos solution	How it helps
Protecting patent and IP data	Sophos Firewall	Supports flexible multi-factor authentication options including directory services for access to key system areas. 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.
	Sophos Intercept X Sophos Intercept X for Server	Mitigate known vulnerabilities and stop the latest cybersecurity threats such as ransomware, file-less attacks, exploits, and malware across your endpoint devices. Our data loss prevention (DLP) capabilities identify your sensitive data and prevent leaks via email, uploads, and local copying.
	Sophos Cloud Optix	Adopt the principle of least privilege across public cloud environments with Sophos Cloud Optix, the Cloud Security Posture Management solution. The SaaS based service connects disparate actions with Sophos AI to pinpoint unusual access patterns and locations to cloud provider consoles in near real time to identify credential misuse or theft. And includes an IAM visualization tool that provides a complete map of IAM relationships and allows teams to quickly and easily identify over-privileged access and create right-sized IAM policies before they are exploited in cyberattacks.
	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	Sophos Central Device Encryption	Secures classified pharmaceutical data at rest with full disk encryption for Windows and macOS.
	Sophos Managed Detection and Response (MDR)	24/7 monitoring of the environment plus investigation and neutralization of malicious activities secures against data loss through adversarial activities.
	Sophos Email	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 your sensitive data to stop breaches.

Security Challenge	Sophos solution	How it helps
Protection against phishing attacks	Sophos Email	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 Phish Threat	Educates and tests end users against phishing, credential harvesting, or attachment attacks, through automated attack simulations, quality security awareness training, and actionable reporting metrics.
	Sophos Intercept X Sophos Intercept X for Server	Get complete protection for all your endpoints – Windows, Mac, Linux, and virtual machines – multiple layers of protection technologies including credential theft protection, exploit protection, anti-ransomware protection, and tamper protection, that optimize your defenses.
Protection against cyber espionage	Sophos Firewall	Includes next-gen IPS that offers advanced protection from hacks and attacks using a uniform signature format backed by SophosLabs. Offers 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	Helps 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)	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 citizens' data and classified information wherever it resides.
Proactive security for uninterrupted operations	Sophos Firewall	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.
	Sophos Intercept X Sophos Intercept X for Server	The exploit prevention capabilities 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 XDR	Pulls in rich network, endpoint, email, cloud, and mobile data sources to give you an even broader picture of your cybersecurity posture with the ability to drill down into granular detail when needed. With data from each product flowing into the Sophos Data Lake you can quickly answer business critical questions, correlate events from different data sources and take even more informed action.
	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.
	Sophos Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
	Sophos Managed Detection and Response (MDR)	Stop the exploitation of vulnerabilities by adversaries with 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.

Security Challenge	Sophos solution	How it helps
Protection against advanced malware attacks	Sophos Intercept X Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease across all devices and platforms. Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers. Endpoint Protection application control policies restrict the use of unauthorized applications.
	Sophos Firewall	Includes next-gen IPS that offers advanced protection from hacks and attacks using a uniform signature format backed by SophosLabs. Besides traditional servers and network resources, it also identifies and protects users and applications on the network. Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network.
	Sophos Sandboxing	Complements Sophos web and email security products and Sophos Firewall by inspecting and blocking executables and documents containing executable content before the file is delivered to the user's device.
	Sophos Intercept X for Mobile	Detects malicious and potentially unwanted applications installed on Android devices using Intercept X deep learning technology alongside intelligence from SophosLabs global research team. Integration with Microsoft Intune allows administrators to build conditional access policies, restricting access to applications and data when a threat is detected.
	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
	Sophos Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
	Sophos Managed Detection and Response (MDR)	Sophos MDR continuously monitors signals from across the security environment, including network, email, mobile, identity, endpoint and more, enabling us to quickly and accurately detect potential cybersecurity events. Anomalous behaviors and code use are detected, investigated, and correlated to identify malicious activities and enable us to quickly neutralize the event.
Minimizing the risk of supply chain attacks	Sophos Intercept X with XDR	Provides comprehensive defense in depth against threats that get in via third party suppliers using AI, exploit prevention, behavioral protection, anti-ransomware and more. Plus, powerful XDR functionality enables you to automatically identify suspicious activity, prioritize threat indicators, and quickly search for potential threats across your endpoint and servers.
	Sophos Managed Detection and Response (MDR)	Delivers expert threat hunting and remediation as a fully-managed service. Sophos specialists work around the clock to proactively hunt for, validate, and remediate potential supply chain threats and incidents on your behalf.
	Sophos ZTNA	Safeguards against supply chain attacks that rely on supplier access to your systems via very granular access controls. This cloud-delivered solution validates user identity, and device health and compliance before granting access to resources. It authenticates requests from trusted partners, irrespective of the location.

Security Challenge	Sophos solution	How it helps
Protection against insider threats	Sophos Firewall	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. Offers 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). Offers the most extensive set of user authentication options available on any firewall, including Active Directory integration, and even our unique and easy-to-use Synchronized User ID solution that facilitates seamless user authentication across the firewall and endpoints to offer tighter, granular user access, blocking an external attacker as well as a malicious insider from gaining access to sensitive systems or data.
	Sophos Cloud Optix	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.
Securing resources in the cloud	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.
Securing remote access environments	Sophos Secure Access portfolio	Includes Sophos ZTNA to support secure access to applications, Sophos SD-RED remote Ethernet devices to safely extend your network to branch offices and remote devices, Sophos Wireless access points for easy and secure wireless networking, and Sophos Switch for secure access on the LAN. Everything is managed through a single cloud-based security platform – Sophos Central.
Supporting regulatory compliance	Sophos Cloud Optix	Eliminates compliance gaps with a single view of your compliance posture across AWS, Azure, and Google Cloud environments. Continuously monitors compliance with custom or out-of-the-box templates and audit-ready reports for standards such as FFIEC, GDPR, HIPAA, PCI DSS, and SOC2.
	Sophos Central	Provides flexible reporting tools that allow visualization of network activity and security over time. It offers several built-in compliance reports as well as easy tools to create custom reports.
	Sophos Central Device Encryption	Makes it easy to verify encryption status and demonstrate compliance which is especially useful in cases of lost or stolen devices where pharma companies must prove that these missing devices are encrypted.
Ensuring user awareness and training	Sophos Phish Threat	Educates and tests end users against phishing, credential harvesting, or attachment attacks, through automated attack simulations, quality security awareness training, and actionable reporting metrics.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2023-05-16 CC (PS)

SOPHOS