Reference Card for the Pharmaceuticals Industry

Pharmaceuticals is a large, critical industry impacting human lives and healthcare. Pharmaceutical organizations hold huge volumes of sensitive data, including classified intellectual property (IP), R&D data on pharmaceutical advances and technologies, proprietary information on drugs and development, and patient data. Extensive reliance on third-party supply chain vendors, cloud migrations, IT/OT convergence, and COVID-19 are some of the challenges this industry faces to ensure cybersecurity and safe operations.

This document provides a general reference on how Sophos' advanced threat prevention technologies offer pharmaceutical organizations a multi-layered approach for the widest range of protection from latest threats.

Security Challenge	Sophos Solution	How it helps
Ensure authorized access to sensitive data	All Sophos products	Sophos' user-identity based policy technology allows organizations to enforce role-based user-level controls over network resources and other organization's assets.
	Sophos Firewall	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
	Sophos Cloud Optix	Adopt the principle of least privilege across public cloud environments with Sophos Cloud Optix, 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. It also includes 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 Zero Trust Network Access (ZTNA)	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	Sophos Central Device Encryption	Authenticates users for access to specific files/folders with the use of user- or group-specific keys.
	Sophos Mobile	Encrypts documents within a secure container on a mobile device managed with Sophos Mobile. Sophos Secure Workspace can dynamically encrypt content sent to cloud-based storage services and applications. It enforces device encryption and monitors compliance relative to encryption policy.
Secure sensitive data at rest	Sophos Cloud Optix	Public cloud security benchmark assessments proactively identify shared storage services (e.g. Amazon S3), hard drive snapshots, and databases without encryption enabled, or with public access enabled and ports exposed. Guided remediation then instructs the administrator on how to protect these services and data at rest.
	Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS.
Proactive protection against security breaches	Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.

SOPHOS

Security Challenge	Sophos Solution	How it helps
	Sophos Intercept X Sophos Intercept X Advanced with XDR 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. Goes beyond the endpoint, pulling in rich network, 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.
	Sophos Firewall	Allows real-time insights into network and user events, quick and easy access to historical data, and easy integration with third-party remote management and monitoring tools (RMMs).
	Sophos Managed Threat Response (MTR)	Helps to proactively hunt threats 24/7 and neutralize even the most sophisticated threats with Sophos' managed detection and response services – backed by an elite team of threat hunters and response experts who take targeted actions on your behalf.
	Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	Sophos Cloud Optix	Cloud Optix enables organizations to design public cloud environments to meet Amazon Web Services, Microsoft Azure, and Google Cloud Platform security best practice standards and maintain them. This agentless service continually monitors public cloud resources, providing the visibility to proactively identify unsanctioned activity, vulnerabilities, and misconfigurations. › Comprehensive asset inventory and network visualizations of security groups, cloud workloads, share storage, databases, IAM roles, and more › Automatic identification of security best practice and compliance gaps leaving organizations exposed, with guided remediation. › 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. › Integrate security in the DevOps CI/CD pipeline to scan container images and infrastructure-as-code templates and more to block vulnerabilities pre-deployment.
Zero Trust Network Access approach	Sophos Zero Trust Network Access (ZTNA)	Control access to applications and data based on user identity and device health. Individual users and devices become their own micro-segmented perimeter that are constantly validated and verified.
Lateral movement protection	Sophos Firewall	Limits access between untrusted devices and critical servers with segmentation of the internal network and by applying policies, adding a layer of protection and logging to disrupt the attack chain. Lateral Movement Protection, a Synchronized Security feature, prevents the threat or hacker from spreading to other systems, stealing data, or communicating back to the host.
	Sophos Zero Trust Network Access (ZTNA)	Controls access to applications and data based on user identity and device health. Individual users and devices become their own micro-segmented perimeter that are constantly validated and verified. This ensures there's no lateral movement of device or user access between resources on the network.
Perimeter protection	Sophos Firewall	Includes IPS, APT, antivirus, sandboxing with deep learning, and web protection to monitor and block malicious, anomalous, and exploitive traffic from inbound or outbound access. Sophos Sandboxing inspects and blocks executables and documents containing executable content before the file is delivered to the user's device.
	Synchronized Security feature in Sophos products	Synchronized Security is a complete portfolio of world-class Sophos security products that work together, responding automatically to incidents and delivering enhanced security insights. Zero-touch incident response slashes exposure to threats while the integrated product portfolio minimizes security gaps. Enhanced insight into network traffic lets you identify and address hidden risks. Centralized management enables you to focus on priority alerts.
	Sophos Email Sophos Firewall	Uses real-time threat intelligence to detect and block unwanted email at the gateway, and our anti-spam engine catches the rest – including the latest phishing attacks, malicious attachments, and snowshoe spam.

Security Challenge	Sophos Solution	How it helps
Privileged Account Management	Sophos Cloud Optix	Adopt the principle of least privilege across public cloud environments with Sophos Cloud Optix, 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. It 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.
Secure DevOps	Sophos Cloud Optix	Prevent security breaches that exploit vulnerabilities and resource misconfigurations pre-deployment. Seamlessly integrate Sophos security and compliance checks at any stage of the development pipeline. › Scan container images in ECR, ACR, Docker Hub registries, as well as GitHub and Bitbucket IaC environments to identify operating system vulnerabilities and fixes to prevent threats pre-deployment. › Automatically detect misconfigurations, embedded secrets, passwords, and keys in Terraform, AWS CloudFormation, Ansible, Kubernetes, and Azure Resource Manager (ARM) template files. › Seamlessly integrate with GitHub and Bitbucket early on to receive on-demand scan results in the Cloud Optix console, or use the REST API to scan IAC templates and container images at any stage of development. › Continuously monitor and detect drift in configuration standards, and prevent, detect, and automatically remediate accidental or malicious changes in resource configuration before they are compromised.
Mitigate advanced threats	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	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. Delivers advanced protection from the latest drive-by and targeted web malware, URL/malicious site filtering, web application filtering, and cloud-based filtering for offsite protection.
	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.
	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 Threat Response (MTR)	Incorporates vulnerability intelligence to provide customers with proactive security posture improvements.
Ransomware protection	Sophos Firewall	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 Intercept X with XDR	Introduces multiple security layers, 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.
	Sophos Managed Threat Response (MTR)	Proactively hunt threats 24/7 and neutralize even the most sophisticated threats with our managed detection and response services backed by an elite team of threat hunters and response experts who take targeted actions on your behalf.
	Sophos Rapid Response Service	Get incredibly fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.

Security Challenge	Sophos Solution	How it helps
Minimize supply chain risks	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 Threat Response (MTR)	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 Zero Trust Network Access (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 in hybrid/multi-cloud environments	Sophos Intercept X for Server with XDR	Offers cloud workload protection that secures business-critical virtual machines and virtual desktops without sacrificing performance. Protect cloud workloads from the latest threats, including ransomware, fileless attacks, and server-specific malware, with XDR included to hunt down suspicious activities and perform critical IT operations tasks. Control exactly which applications can and can't run on your virtual machines and receive notifications for any unauthorized change attempts to critical files and folders with inbuilt application control.
	Sophos Cloud Optix	Sophos cloud security posture management solution enables teams to proactively reduce organizational risk from unsanctioned activity, vulnerabilities, misconfigurations, and insecure identities in multi-cloud environments.
	Sophos Firewall	Protects environments from the latest network threats and vulnerabilities with a complete cloud edge firewall solution featuring IPS, ATP, and URL filtering. Extend your secure network with flexible SD-WAN and VPN connectivity options, while Sophos Web Application Firewall (WAF) hardens cloud workloads against hacking attempts.
	Sophos Zero Trust Network Access (ZTNA)	Constantly verifies the user – typically with multi-factor authentication and an identity provider – and validates health and compliance of the device for users to securely connect to corporate resources from any location. It elevates protection and minimizes the risk of lateral movement within the network by continually assessing identity and device health before allowing access.
	Sophos Managed Threat Response (MTR)	Helps take the weight of 24/7 threat monitoring and response. Receiving telemetry from Sophos products running on AWS, Azure and GCP this experienced team continuously monitors your cloud environments, analyzes and triages security events to prevent them from compromising your data and systems.
Support compliance	Sophos Cloud Optix	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. Automatically analyze cloud configuration settings against compliance and security best practice standards without diverting resources. Prevent compliance gaps that leave you exposed with a single view of compliance posture across AWS, Azure, and Google Cloud.
	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.
Incident response and reporting	Sophos XDR	Goes beyond the endpoint, pulling in rich network, 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.
	Sophos Managed Threat Response (MTR)	Proactively hunt threats 24/7 and neutralize sophisticated threats with our managed detection and response services – backed by an elite team of threat hunters and response experts who take targeted actions on your behalf.
	Sophos Rapid Response Service	Get fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	Sophos Cloud Optix	Scans cloud resources for security misconfigurations, profiling any alerts by risk level to help teams focus on the priority areas, and provide detailed remediation guidance to fix those issues.

Security Challenge	Sophos Solution	How it helps
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

2021-12-27 RC (PC)

SOPHOS