SOPHOS
Cybersecurity evolved.

Strengthening Cybersecurity in the Pharmaceutical Industry

The pharmaceutical industry is one of the largest and the most critical, with a predicted compound annual growth rate of 13.7% through 2027[1]. Billions of people rely on this sector, for their daily medications. An interruption to manufacturing lifesaving drugs and inventing new therapies can have deadly consequences. Yet, this industry is among the most threatened by cyber crime globally. The average cost of a pharma breach in 2021 is $5.04 million, according to Ponemon Institute's Cost of a Data Breach Report[2].

Pharmaceutical organizations hold data worth billions of dollars. This includes classified intellectual property (IP), R&D data on pharmaceutical advances and technologies, proprietary information on drugs and development, and patient and clinical trials data. Factors such as growing reliance on third-party supply chains, increasing cloud migrations including hybrid and multi-vendor environments, rising adoption of Internet of Things (IoT), and accelerated push on COVID-19 vaccine development make this industry an attractive target for cyber criminals.

A Sophos Solution Brief. January 2022

Sophos Highlights

- **Sophos Cloud Edge Firewall**
  - IPS, ATP, URL filtering, Sandboxing, WAF, SD-WAN and VPN protect from latest network threats and vulnerabilities
- **Sophos Intercept X Endpoint Protection**
  - HIPS, deep learning, anti-exploit, anti-adversary, and malicious traffic detection proactively detect malicious behaviors on host
- **Sophos Intercept X Server Protection**
  - Detects cloud workloads and critical cloud services including S3 buckets, databases, and serverless functions
  - Detailed multi-cloud inventory
  - AI-powered anomaly detection
  - Automated assessment ensuring peak performance of cloud infrastructure
- **Sophos Cloud Optix**
  - Cloud security posture management
  - Complete picture of cloud resources across multi-cloud environments
  - Detection of insecure configurations and deployments, access anomalies, over-privileged IAM roles, and compliance failures from development to ongoing security of live services
- **Sophos XDR**
  - Detection and investigation across endpoints, server, firewall, and other data sources
- **Sophos ZTNA**
  - Access control to apps and data based on user identity and device health
- **Sophos Synchronized Security**
  - Enables endpoints and firewall to share real-time intelligence
  - Automatic isolation of infected computers
  - Instant cleaning up of malware
  - 100% visibility of all apps on the network
- **Sophos Managed Threat Response (MTR)**
  - Advanced 24/7 threat hunting, detection, and response capabilities delivered as a fully-managed service
  - Elite team of threat hunters and response experts take actions to remotely contain and neutralize threats

Impact of cyberattacks on pharmaceutical organizations:

- Lack of availability of critical systems and business disruptions that may halt R&D and drug production
- Loss of data, including intellectual property (IP), clinical trial data, and patient data
- Loss of market position
- Huge financial losses due to lost revenue and lawsuits
- Regulatory non-compliance and potentially hefty fines
- Loss of consumer trust
- Reduced shareholder value

The Cybersecurity Challenge in Pharma

There are many situations and attack vectors leading to the increase in cybersecurity challenges in the pharmaceutical industry.

Innovation

Pharmaceuticals is an industry built on innovation with extensive investments in R&D, intellectual property (IP) on medicines and new compounds, clinical patient data and trade secrets. When this information is stolen, it can have a devastating impact on the company.

Ransomware

Ransomware continues to be the most devastating type of cyberattack in healthcare. In 2020, 92 ransomware attacks cost the U.S. healthcare and pharmaceutical industry $20.8 billion[3]. One of the most prominent ransomware attacks in recent history was the NonPetya attack in 2017 on the pharmaceutical giant, Merck. The malware, allegedly developed by a Russian military group, racked up over USD $1 billion in damages for the company. The attack crippled more than 30,000 laptop and desktop computers at the global drug maker, as well as 7,500 servers. Many departments, including sales, manufacturing, and research units, were hit. The most devastating part was disruption of Merck's production facilities for the leading vaccine against human papillomavirus. Not only did Merck have to borrow the US government's entire emergency supply, but it also lost potential sales of $410 million. Besides the costs of ransom payments, such attacks also lead to productivity losses, halting business operations, forensic costs, business losses, legal costs, as well as eroded patient trust.

Third-party supply chain

The recent SolarWinds third-party supply chain breach proved to be a wakeup call for all businesses to take control of their risks from a supply-chain attack where attackers exploit a trusted third party to gain access to an organization's systems. In this case, hackers inserted malicious code into an update of SolarWind's network management software, Orion. Around 18,000 customers, including the tech giants like Microsoft, a host of US government organizations, hospitals, and power companies, installed the malicious update on to their systems, giving the hackers freeway into their compromised systems.

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.

Digitization and IIoT

Internal and external factors, expedited by the Covid-19 pandemic, have prompted pharma companies to adopt digital transformation. Digitization has enabled analytics-led data management, facilitating seamless data exchange across pharmaceutical supply chains. Industrial IoT (IIoT) technologies are delivering automation and optimization of pharma production environments, alongside continuously monitoring connected factory equipment and personnel. All of this has compelled legacy operational technology (OT) devices and systems in pharmaceutical manufacturing to converge with IT networks, suddenly leaving them exposed to the wide threat surface resulting out of the IT/OT convergence. Digitization and IIoT have also opened up a pandora's box of vulnerabilities in this sector due to the expanding attack surface, opening up new cybersecurity concerns.

Hybrid and 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. However, multi-cloud environments are leading to issues of data integrity and managing identities and permissions within the cloud. With the explosion of human and non-human entities requiring access to cloud operations, inadequate visibility and controls in cloud environments can be a significant blind spot for organizations and also the reason behind many security breaches.

Sophos Solutions That Address Cybersecurity Challenges in the Pharma Industry

SECURITY CHALLENGE	SOPHOS SOLUTION
Access Control	All Sophos products allow role-based user-level controls over network and other resources.
	Sophos Firewall facilitates two-factor authentication for VPN connections.
	Sophos Cloud Optix adopts the principle of least privilege across public cloud environments.
	Sophos ZTNA controls access to applications and data based on user identity and device health.
	Sophos Central Device Encryption authenticates users for access to specific files/folders.
	Sophos Mobile enforces device encryption and monitors compliance relative to encryption policy.
Securing sensitive data at rest	Sophos Cloud Optix proactively identifies 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 protects devices and data with full disk encryption for Windows and macOS.
Proactive security	Synchronized Security in Sophos products enables coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.
	Sophos Intercept X, Sophos Intercept X Advanced with XDR, and Sophos Intercept X for Server integrate deep learning, anti-exploit, and anti-adversary with real-time threat intelligence to prevent, detect, and remediate threats across all devices and platforms.
	Sophos Firewall delivers real-time insights into network and user events.
	Sophos Managed Threat Response (MTR) proactively hunts threats 24x7 and neutralizes even the most sophisticated threats.
	Sophos Rapid Response Service offers identifies and neutralized active threats against your organization.
	Sophos Cloud Optix continually monitors public cloud resources, providing the visibility to proactively identify unsanctioned activity, vulnerabilities, and misconfigurations.
Zero Trust Network Access approach	Sophos ZTNA controls access to applications and data based on user identity and device health.
Lateral movement protection	Sophos Firewall allows internal network segmentation. By applying policies, and with a layer of protection and logging, it helps to disrupt the attack chain.
	With Sophos ZTNA, 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.

SECURITY CHALLENGE	SOPHOS SOLUTION
Perimeter protection	Sophos Firewall includes IPS, APT, antivirus, sandboxing with deep learning, and web protection.
	Synchronized Security feature in Sophos products brings together Sophos security products that work together, respond automatically to incidents, and deliver enhanced security insights.
	Sophos Email detects and block unwanted email at the gateway with real-time threat intelligence, and our anti-spam engine catches the rest.
Privileged Account Management	Sophos Cloud Optix includes an IAM visualization tool offering a complete map of IAM relationships, allowing teams to quickly and easily identify over-privileged access and create right-sized IAM policies before they are exploited in cyberattacks.
Secure DevOps	Cloud Optix integrates Sophos security and compliance checks at any stage of the development pipeline to prevent breaches and resource misconfigurations pre-deployment.
Mitigate advanced threats	Sophos Intercept X and Sophos Intercept X for Server integrate deep learning, anti-exploit, and anti-adversary along with real-time threat intelligence to prevent, detect, and remediate threats across all devices and platforms.
	Sophos Firewall leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to identify the latest ransomware and unknown threats.
	Sophos Sandboxing inspects and blocks 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.
	Sophos Cloud Optix detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
	Sophos Managed Threat Response 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 identify the latest ransomware and unknown threats.
	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 proactively hunts threats 24/7 and neutralizes even the most sophisticated threats backed by an elite team of threat hunters and response experts.
	Sophos Rapid Response Service identifies and neutralizes active threats against your organization.
Minimize supply chain risks	Sophos Intercept X with XDR provides defense in depth against threats getting in via third party suppliers using AI, exploit prevention, behavioral protection, anti-ransomware and more.
	Sophos Managed Threat Response (MTR) delivers expert threat hunters that proactively hunt for, validate, and remediate potential supply chain threats and incidents on your behalf.
	Sophos ZTNA safeguards against supply chain attacks by validating user identity, and device health and compliance before granting access to resources.
Security in hybrid/multi-cloud environments	Sophos Intercept X for Server with XDR protects 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.
	Sophos Cloud Optix's 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' cloud edge firewall includes IPS, ATP, and URL filtering and allows secure network extension with flexible SD-WAN and VPN connectivity options, while Sophos Web Application Firewall (WAF) hardens cloud workloads against hacking attempts.
	Sophos ZTNA constantly verifies the user and validates health and compliance of the device for users to securely connect to corporate resources from any location.

SECURITY CHALLENGE	SOPHOS SOLUTION
	Sophos Managed Threat Response (MTR) delivers expert threat hunters who continuously monitor your cloud environments, as well as analyze and triage security events to prevent them from compromising your data and systems.
Support compliance	Sophos Cloud Optix 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. Allows a single view of compliance posture across AWS, Azure, and Google Cloud.
	Sophos Central 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.
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.
	Sophos Managed Threat Response proactively hunts threats 24/7 and neutralizes sophisticated threats, backed by an elite team of threat hunters and response experts.
	Sophos Rapid Response Service identifies and neutralizes active threats by an expert team of incident responders.
	Sophos Cloud Optix scans cloud resources for security misconfigurations, profiling alerts by risk level to help focus on the priority areas, and provides detailed remediation guidance to fix those issues.
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.

Use Cases

Here are few ways by which Sophos products strengthen cybersecurity in the pharmaceuticals industry.

Secure the network perimeter

Sophos cloud-edge firewall uniquely delivers all-in-one protection by integrating the best of breed technologies: high-performance IPS and ATP stop the latest hacks and attacks, sandboxing and machine learning block the latest zero-day file-based threats, an integrated web application firewall to harden your cloud servers against hacking attempts, and the advantage of SophosLabs Threat Intelligence. Get unmatched visibility and insight into all your network traffic, whether it's encrypted, evasive, or elusive with Sophos' Xstream TLS inspection, and an extensive built-in reporting. Manage all your Sophos firewalls effortlessly with Sophos Central, our cloud management platform.

Protect sensitive data at rest and in transit

All Sophos products work on user-identity based policy technology, which allows pharma organizations to enforce role-based user-level controls over network resources. Sophos' data protection works to secure stored data as well as data transmitted over email, both on premises and in the cloud. Sophos Central Device Encryption authenticates users for access to specific files/folders with the use of user- or group-specific keys. Sophos ZTNA ensures data access to only authorized people within and outside your organization by continuously validating user identity, device health, and compliance before granting access to applications and data. Delivering data protection over email, Sophos Email offers granular control of data breach prevention policies, including multi-rule policies for groups and individual users, with seamless integration of encryption. For users working on personal devices as well as remote workers, Sophos Mobile delivers a rich set of device management capabilities, containers, and market-leading encryption to keep sensitive business email and documents protected on mobile devices. Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device.

Secure your hybrid/multi-cloud environment

Secure resources and sensitive data in the public cloud with Sophos Intercept X for Server with XDR cloud workload protection. It secures business-critical virtual machines and virtual desktops 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. Sophos Cloud Optix delivers asset and network traffic visibility for Amazon Web Services (AWS), Microsoft Azure (Azure), and Google Cloud Platform (GCP). View accurate inventories and generate on-demand topology visualizations for multi-cloud environments in a single console, continually analyzed for security risks, over-privileged access, and spend anomalies. Sophos cloud edge firewall protects environments from the latest network threats and vulnerabilities with a complete cloud edge firewall solution featuring IPS, ATP, and URL filtering. Sophos Managed Threat Response team receives telemetry from Sophos products running on AWS, Azure, and GCP and the expert threat hunters continuously monitor your cloud environments, analyze and triage security events to prevent them from compromising your data and systems.

Minimize your risk against third-party supply chain attacks

Sophos Intercept X with XDR delivers comprehensive protection against threats that get in via third-party suppliers using AI, exploit prevention, behavioral protection, anti-ransomware, and more. The XDR functionality enables you to automatically identify suspicious activity, prioritize threat indicators, and quickly search for potential threats across your endpoint and servers. Ensure safe third-party supplier access to your systems with Sophos ZTNA that validates user identity, and device health and compliance before granting access to resources. This cloud-delivered solution takes full advantage of its unique integration with the full Sophos ecosystem, especially Sophos Intercept X endpoints, and utilizes device health to automatically limit compromised devices from accessing business resources. Access of such compromised devices is automatically limited to isolate and contain threats, preventing lateral movement. Get expert threat hunting and remediation as a fully-managed service with Sophos Managed Threat Response (MTR) where Sophos specialists work around the clock to proactively hunt for, validate, and remediate potential supply chain threats and incidents on your behalf.

Privilege access management

Adopt the principle of least privilege across public cloud environments with Sophos Cloud Optix, our cloud security posture management solution. The 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 Identity and Access Management (IAM) visualization tool that analyzes complex, interwoven IAM roles to visualize 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.

Zero Trust Network Access approach

Sophos ZTNA works on the principle of zero trust: trust nothing, verify everything. It controls access to apps 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 additionally ensures there's no lateral movement of device or user access between resources on the network.

With zero trust, users are no longer "on the network" with all the implied trust and access that usually comes with it. Instead, individual tunnels are established between the user and the specific gateway for the application they are authorized to access, and nothing more - providing a much more secure level of micro-segmentation. This has a number of benefits for security, control, visibility, efficiency and performance.

Sophos ZTNA overcomes the challenges and limitations of remote access VPN, offering a better and more secure solution for users anywhere, especially remote workers in the pharma sector affected by the pandemic.

Protection from Insider Threats

In the context of pharma, insiders include not only the organization's employees but also the suppliers, logistics partners, and contractors who require constant access to the organization's systems and resources.

Sophos Firewall with Security Heartbeat™ allows next-generation endpoint and network security to continuously share telemetry and health status; detect compromised / unauthorized endpoint device; and provide an automatic response with dynamic firewall rules and lateral movement protection to isolate a compromised host to prevent spread, hacker communication, and data loss.

Sophos Intercept X and Sophos Intercept X for Server proactively detect malicious behaviors occurring on the host with anti-exploit, anti-adversary, and deep learning technology. Powerful XDR functionality in Sophos Intercept X with XDR enables automatic identification of suspicious activity, prioritizes threat indicators, and quickly searches for potential threats across endpoint and servers.

Sophos ZTNA controls access to apps and data based on user identity and device health. Users are no longer "on the network" with all the implied trust and access that usually comes with it. Instead, individual tunnels are established between the user and the specific gateway for the application they are authorized to access, and nothing more - providing a much more secure level of micro-segmentation.

Security awareness training

Sophos Phish Threat educates and tests your users against phishing, credential harvesting, or attachment attacks, through automated attack simulations, quality security awareness training, and actionable reporting metrics. It helps you to identify your at-risk users and seamlessly enroll them into targeted phishing simulations and training to improve awareness and cut your risk of attack.

Conclusion

Cyber threats to pharmaceutical organizations are real and on the rise. The pharma sector is in the spotlight now more than ever before because of the tremendous pressure to invent and supply COVID-19 vaccines to the world. Sophos' advanced threat prevention technologies offer pharmaceutical organizations a multi-layered approach for the widest range of protection from latest threats. Our preventative and active protection tools help preempt and discover attacks on pharmaceutical systems and resources, ensuring confidentiality and availability for the pharmaceutical industry.

[1] Report finds 10% of pharma manufacturers at high risk for ransomware

[2] IBM Report: Cost of a Data Breach Hits Record High During Pandemic

[3] Ransomware attacks on US healthcare organizations cost $20.8bn in 2020

2021-12-24 (SB-PC)

SOPHOS