Reference card for Healthcare

SOPHOS
Cybersecurity evolved.

Cybersecurity is of serious concern to the healthcare sector because cyberattacks threaten not just the security of healthcare systems and availability of health information, but also the health and safety of patients. Healthcare organizations are an inviting target for financially motivated threat actors who put patient information on sale on the dark net for insurance frauds. Ransomware attacks are also widely used to earn lucrative ransom payments by making patient and back-office data unavailable.

This document provides a general reference on how Sophos products assist organizations in the healthcare sector to meet their cybersecurity requirements and deliver uninterrupted patient care.

Challenge	Sophos Product	How It Helps
Protecting the Confidentiality of PHI	**Sophos Firewall**	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
	Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
	Sophos Email	Granular control of data breach prevention policies, including multi-rule policies for groups and individual users with seamless integration of encryption. Create custom CCLs using Sophos Content Control Lists or customize out of the box templates for specific CCLs. Choose from a variety of policy outcomes including block, drop attachment, quarantine as well as log and continue mode.
	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.
	Sophos Zero-trust Network Access	Validates user identity, device health, and compliance before granting access to resources.
	Sophos Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos managed networks and hotspots.
	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.

Reference card for Healthcare

SOPHOS
Cybersecurity evolved.

Challenge	Sophos Product	How It Helps
Protecting the Integrity of PHI	**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, 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 Intercept X **Sophos Intercept X for Server**	Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers. Application Control policies restrict the use of unauthorized applications.
	Sophos Intercept X for Server	Prevents unauthorized applications from running with Server Protection, automatically scanning your system for known good applications, and whitelisting only those applications.
	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	Incorporates vulnerability intelligence to provide customers with proactive security posture improvements.

Reference card for Healthcare

SOPHOS
Cybersecurity evolved.

Challenge	Sophos Product	How It Helps
Protecting the Availability of PHI	**Sophos Firewall**	High availability with active-active load balancing or active-passive fail-over and WAN link balancing lets you easily double your performance when you need it.
Security Beyond the Main Facility	**Sophos Firewall**	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Sophos SD-RED extends a secure network to a remote location easily by establishing a secure, dedicated VPN tunnel.
	Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
	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.
	Sophos Wireless	Monitors and acts upon the health status of the device connecting to the wireless network. It automatically restricts Wi-Fi network access for unhealthy and non-compliant endpoints and mobile devices, thereby preventing lateral spread of infection.
	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.

Reference card for Healthcare

SOPHOS
Cybersecurity evolved.

Challenge	Sophos Product	How It Helps
Securing Connected Medical Devices	**Sophos Firewall**	Prevents attackers from moving through your healthcare servers and applications by compromising mission critical medical devices on the network. It also segments your network so you can strengthen your network security, creating separate levels of trust on your network, making lateral movement difficult.
	Sophos Mobile	A rich set of device management capabilities, containers, and market-leading encryption enables protection of sensitive business email and documents on mobile devices – even for users working with personal devices. Leading antivirus and ransomware protection helps to safeguard your users and devices from malicious content and apps.
	Sophos Wireless	Monitors and acts upon the health status of the device connecting to the wireless network. It automatically restricts Wi-Fi network access for unhealthy and non-compliant endpoints and mobile devices, thereby preventing lateral spread of infection.
	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.
Wireless Security	**Sophos Wireless**	Secures the growing number of mobile devices in healthcare environment with granular visibility into the health of your wireless networks. Automatically restrict Wi-Fi network access for unhealthy and non-compliant endpoints and mobile devices, thereby preventing lateral spread of infection. Separate guest Wi-Fi access from access for your healthcare staff with a daily password or time-limited voucher. All Sophos APX models have a certification for use in healthcare environments that confirms that they do not cause disruption to other medical equipment.

Reference card for Healthcare

SOPHOS
Cybersecurity evolved.

Challenge	Sophos Product	How It Helps
Proactive Security	**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 Managed Threat Response	Proactively hunt threats 24x7 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 XDR	Goes beyond the endpoint, pulling in rich network, email, and other 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 Cloud Optix	Sophos's cloud security posture management solution, Sophos Cloud Optix, enables teams to proactively improve security posture, detecting insecure configurations and vulnerabilities. By automatically mapping security and compliance standards to your environments, Cloud Optix provides the visibility needed to monitor and maintain security posture 24/7.
Ransomware and Other Malware Attacks	**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 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 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.

Reference card for Healthcare

SOPHOS
Cybersecurity evolved.

Challenge	Sophos Product	How It Helps
	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	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 Intercept X **Sophos Intercept X for Server**	HIPS, deep learning, anti-exploit, anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host. 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. Server Lockdown allows only trusted whitelisted applications and associated files to run.
	Sophos Managed Threat Response	Proactively hunt threats 24x7 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.

Reference card for Healthcare

Challenge	Sophos Product	How It Helps
Phishing Protection	**Sophos Email**	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.
	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

2021-11-17 RC-NA (PS)