Reference Card for Healthcare

SOPHOS

Healthcare providers are incredibly dependent on real-time patient data, which implies that healthcare data is a goldmine for cyber attackers. Any data that becomes compromised could prove legitimately life-threatening. Sophos offers advanced and comprehensive protection that secures organizations against ransomware and other critical advanced threats by working at every stage of the attack chain. Sophos solutions also help you meet the compliance requirements of stringent regulations including HIPAA, PCI DSS, and other requirements. Here's some of the key ways in which Sophos products ensure cybersecurity in healthcare.

CHALLENGE	SOPHOS PRODUCT	HOW IT HELPS
Loss of PHI	Sophos XG Firewall/ SG UTM Sophos Intercept X Advanced with EDR	Data Leakage Prevention (DLP) capabilities in Sophos products can detect sensitive data and prevent leaks of PHI details via email, uploads, and local copying.
	Sophos Email on Central	Sophos Email Content Control safeguards sensitive information leaving the organization by scanning all emails for keywords and file types. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to ensure compliance.
	Sophos Mobile	Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the contents in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location.
	Sophos SafeGuard Encryption Sophos Central Device Encryption	Encrypts data on macOS, Windows, and mobile devices. SafeGuard can manage BitLocker and FileVault full disk encryption, as well as always-on file encryption stored on hard disks, USB sticks, cloud storage, file shares, memory cards, and CDs/DVDs. All data encrypted with SafeGuard remains encrypted as files move across the network. Authenticates users for access to specific protected devices, files, and/or folders with the use of user- or group-specific keys. Supports multi-factor authentication, tokens, and smart cards for user authentication.
	Sophos Cloud Optix	Visualize cloud infrastructure instantly and detect suspicious traffic patterns, reveal high-value workloads, and uncover hidden data breach points.

Reference Card for Healthcare

SOPHOS

CHALLENGE	SOPHOS PRODUCT	HOW IT HELPS
Controlled access to PHI	Sophos XG Firewall/ SG UTM	User awareness across all areas of our firewall governs all firewall polices and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group. Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
	Sophos Mobile	Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location.
	Sophos Email on Central Sophos XG Firewall/ SG UTM	Prevents messages containing sensitive data from leaving the organizations, with data loss prevention rules providing policy driven encryption in transit and at rest. SPX encryption dynamically encapsulates email content and attachments into a secure encrypted PDF to help protect email content from unauthorized access.
	Sophos Wireless Sophos XG Firewall/ SG UTM	Provides a guest portal along with full logging of all authentication and connection activity, including unique user accounts.
	Sophos SafeGuard Encryption	Provides role-based management to separate authorization levels, as well as detailed logging of all access attempts. Access to keys and recovery keys is kept separate from OS login privileges.
	Sophos Intercept X Sophos Intercept X for Server	Configurable role-based administration provides granular control of administrator privileges.
	Sophos Cloud Optix	AI-powered monitoring instantly identifies suspicious console login events, API calls, and assumed-role API calls that suggest shared or stolen user credentials are being used by an attacker remotely to gain unauthorized access.

Reference Card for Healthcare

SOPHOS

CHALLENGE	SOPHOS PRODUCT	HOW IT HELPS
Secure sharing of PHI	Sophos Email on Central Sophos XG Firewall/ SG UTM	Sophos SPX encryption provides encryption in transit and at rest. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to ensure 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 SafeGuard Enterprise	Encrypts data on Macs, Windows, and mobile devices. SafeGuard can manage BitLocker and FileVault full disk encryption, as well as always-on file encryption stored on hard disks, USB sticks, cloud storage, file shares, memory cards, and CDs/DVDs. All data encrypted with SafeGuard remains encrypted as files move across the network.
	Sophos XG Firewall/ SG UTM	Allows for policy-based encryption for VPN tunnels, protecting data in transit.
Continuous Availability of PHI	Sophos XG Firewall/ SG UTM	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 Main Facility	Sophos Firewall/UTM	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Sophos SD-RED [SD-WAN Remote Ethernet Devices] extends a secure network to a remote location easily by establishing a secure, dedicated VPN tunnel.
	Sophos SafeGuard Encryption	Authenticates users for access to specific files/folders with the use of user- or group-specific keys for SafeGuard encryption.
	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.

Reference Card for Healthcare

CHALLENGE	SOPHOS PRODUCT	HOW IT HELPS
	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	Cloud Optix provides AI-powered monitoring that instantly identifies suspicious console login events, API calls, and assumed-role API calls that suggest shared or stolen user credentials are being used by an attacker remotely to gain unauthorized access.
Secure connected medical devices	Sophos XG 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	Delivers Unified Endpoint Management (UEM) and security management for mobile devices, helping ensure sensitive data is safe, devices are protected, and users are secure. Sophos Mobile Security for Android provides leading antivirus, ransomware, and unwanted app protection for Android devices.
	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. The Security Heartbeat also shares this information with Sophos Encryption, which revokes the encryption keys on the affected machine until the problem is fixed to prevent any data theft. After the systems have been automatically returned to their initial, clean state, the XG Firewall restores network access to the device, the encryption keys are returned, and your network is botnet-free.

Reference Card for Healthcare

SOPHOS

CHALLENGE	SOPHOS PRODUCT	HOW IT HELPS
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.
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. The Security Heartbeat also shares this information with Sophos Encryption, which revokes the encryption keys on the affected machine until the problem is fixed to prevent any data theft. After the systems have been automatically returned to their initial, clean state, the XG Firewall restores network access to the device, the encryption keys are returned, and your network is botnet-free.
Ransomware and Other Malware Attacks	Sophos Intercept X Sophos Intercept X Advanced with EDR Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary capabilities into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease.
	Sophos XG 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 Sandstorm, optional cloud sandbox technology, inspects and blocks executables and documents containing executable content before the file is delivered to the user's device.
	Sophos Email on Central Sophos XG Firewall/ SG UTM	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.

Reference Card for Healthcare

CHALLENGE	SOPHOS PRODUCT	HOW IT HELPS
	Sophos Mobile	Delivers Unified Endpoint Management (UEM) and security management for mobile devices, helping ensure sensitive data is safe, devices are protected, and users are secure. Sophos Mobile Security for Android provides leading antivirus, ransomware, and unwanted app protection for Android devices.
	Sophos Managed Threat Response	A dedicated, round-the-clock team of threat hunters and response experts constantly scan for and act on suspicious activity.
	Sophos Cloud Optix	Delivers continuous analysis and visibility needed to detect, respond, and prevent security and compliance gaps that leave organizations exposed.
	Sophos Phish Threat	Provides phishing simulation emails and online tutorials to train users on how to spot and stop phishing emails.
Phishing Protection	Sophos Email on Central Sophos XG Firewall/ SG UTM	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.
	Synchronized Security feature of Sophos Email and Sophos Phish Threat	Sophos Email 'At Risk Users' report highlights exactly which users are clicking email links re-written by time-of-click URL protection. Identifying users who have either been warned or blocked from visiting a website due to its risk profile. It's then simply one-click from the report to enroll users in Phish Threat simulations and security awareness training – increasing their threat awareness and reducing risk.
	Sophos Phish Threat	Provides simulated phishing cyberattacks and security awareness training for the organization's end users. Courses cover a wide range of topics, from phishing and cybersecurity overview lessons through to data loss prevention, password protection, and more.

SOPHOS