PCI DSS Compliance Reference Card

SOPHOS

Payment Card Industry Data Security Standard (PCI DSS) v3.2

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes, including Visa, MasterCard, American Express, Discover, and JCB. The standard covers all major areas of a security program across 12 sections in an effort to optimize the security of debit, credit, and cash card transactions and to protect the misuse of personal information given by cardholders.

NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
	BUILD AND MAINTAIN A SECURE NETWORK AND SYSTEMS		
1	Install and maintain a firewall configuration to protect cardholder data	Sophos XG Firewall/ SG UTM	Allows stateful and deep-packet inspection for all network traffic with top-performing IPS and dual-engine antivirus performance and effectiveness. Perimeter defenses stops attacks on your network, including reconnaissance detection, spoofing, DoS, DDoS protection, and packet-based attacks (ICMP).
		Sophos Intercept X Sophos Intercept X for Server	Includes powerful local firewall (endpoints) and host-based intrusion detection and traffic control and monitoring. Creates detailed log events of all malicious activity on endpoint and servers, helping to identify suspicious activity on systems that may be in scope for PCI DSS.
2	Do not use vendor-supplied defaults for system passwords and other security parameters	Sophos Central	Enforces use of non-default passwords sufficiently complex to withstand typical "brute force" attacks.
	PROTECT CARDHOLDER DATA		
3	Protect stored cardholder data	Sophos XG Firewall/ SG UTM Sophos Intercept X Advanced with EDR	Data Leakage Prevention (DLP) capabilities in Sophos products can detect credit or debit card numbers and can prevent leaks of credit and debit card details via email, uploads, and local copying.
		Sophos Email on Central Sophos XG Firewall/ SG UTM	Sophos Email Content Control safeguards sensitive information leaving the organization by scanning all emails for keywords and file types. Leverage Sophos SPX encryption that dynamically encapsulates sensitive emails and attachments into a secure encrypted PDF.
		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 SafeGuard Encryption Sophos Central Device Encryption	Encrypts data on Mac OS, 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.
4	Encrypt transmission of cardholder data across open, public networks	Sophos XG Firewall/SG UTM	Allows for policy-based encryption for VPN tunnels, protecting payment card data in transit.
		Sophos Wireless Sophos XG Firewall/ SG UTM	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos-managed networks and hotspots.
		Sophos SafeGuard Encryption	Encrypts data on Mac OS, Windows, and mobile devices. SafeGuard can manage BitLocker and FileVault encryption, as well as encryption for 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 Email on Central Sophos XG Firewall/SG UTM	SPX email encryption allows encrypting of sensitive data automatically as files and content are emailed to parties outside the organization.

NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
		MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM	
5	Protect all systems against malware and regularly update antivirus software or programs	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 Intercept X Sophos Intercept X Advanced with EDR 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.
		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.
		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 for virtual environments	Protects virtual servers and desktops from malware.
		Sophos for network storage	Scans file systems on storage platforms from EMC, NetApp, and Oracle/Sun for malware.
6	Develop and maintain secure systems and applications	Sophos Intercept X 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. Endpoint Protection application control policies restrict the use of unauthorized applications.
		Sophos XG Firewall	Visibility and control over thousands of applications via customizable policy templates with granular controls based on category, risk, technology, or other undesirable characteristics (P2P apps, IMs, games, and other harmful software); fully automated application security with pre-defined policy templates for commonly used enterprise applications/software packages; Synchronized Application Control in XG Firewall identifies all networked applications in the environment running on Sophos-managed endpoints. View a full list of controlled software/applications.
		Sophos Mobile	Monitor mobile devices for jailbreaking and side-loading of applications. Deny access to email, network, and other resources if device is not in compliance with policy.
		Sophos Intercept X for Server	Server Lockdown allows only trusted whitelisted applications and associated files to run.
		Sophos Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.

NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
	IMPLEMENT STRONG ACCESS CONTROL MEASURES		
7	Restrict access to cardholder data by business need to know	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 Central on Email 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	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.
8	Identify and authenticate access to system components	Sophos XG Firewall/ SG 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 Email on Central Sophos XG Firewall/ SG UTM	Sophos SPX encryption provides encryption in transit and at rest. SPX encryption dynamically encapsulates email content and attachments into a secure encrypted PDF to ensure compliance.
		Sophos SafeGuard Enterprise	Encrypts data on Mac OS, 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 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 Sophos XG Firewall/ SG UTM	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos managed networks and hotspots.
		Sophos Cloud Optix	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.

NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
	REGULARLY MONITOR AND TEST NETWORKS		
10	Track and monitor all access to network resources and cardholder data	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos Intercept X Advanced with EDR	Detects, investigates, and responds to suspicious endpoint activity.
		Sophos XG Firewall	Controls remote access authentication and user monitoring for remote access and logs all access attempts.
		Sophos SafeGuard Enterprise	Provides detailed logging of all access attempts.
		Sophos Mobile	Creates detailed log events of all malicious activity on mobile devices, helping to identify suspicious activity that may try to access sensitive data.
11	Regularly test security systems and processes	Sophos Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
		Security Consulting	Sophos offers penetration testing and vulnerability assessment of security infrastructure and software deployments; and recommendations for architecture and design changes needed to better use the available infrastructure.

Specifications and descriptions are subject to change without notice. Sophos disclaims all warranties and guarantees regarding this information. Use of Sophos products alone does not guarantee legal compliance. The information in this document does not constitute legal advice. Customers are solely responsible for compliance with all laws and regulations, and should consult their own legal counsel for advice regarding such compliance.

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

SOPHOS