PCI DSS Compliance Reference Card

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 in 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. This document describes how Sophos products can be effective tools to help address some of the requirements as part of a customer's efforts to comply with PCI DSS.

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.

Requirement	Sophos Product	How it helps
Requirement One: Install and maintain a firewall configuration to protect cardholder data.	Sophos Firewall	User awareness across all areas of our firewall governs all firewall polices and reporting, giving user-level controls over applications, bandwidth and other network resources. Allows for granular rule-based traffic control to specific ports and services at perimeter ingress and egress points, and can control remote access authentication and user monitoring at the perimeter.
	Synchronized Security feature in Sophos products	Synchronized Security allows Sophos Firewall and Intercept X endpoint protection to work together to identify, isolate and cleanup devices that have been compromised, preventing them from leaking confidential data. When the threat is neutralized and there is no risk of lateral movement, network connectivity is restored.
	Sophos Email Sophos Firewall	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.
Requirement Two: Do not use vendor-supplied defaults for system passwords and other security parameters.	Sophos Central	Disables or removes default passwords. Passwords are sufficiently complex to withstand targeted "brute force" attacks and must be rotated periodically.
Requirement Three: Protect stored cardholder data.	Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
	Sophos Zero Trust Network Access	Validates user identity, device health, and compliance before granting access to resources.
	Synchronized Security feature in Sophos products	Sophos Firewall with Security Heartbeat™ allows next-generation endpoint and network security to continuously share meaningful information about suspicious events across extended IT ecosystem; detects compromised / unauthorized endpoint device; allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data.

SOPHOS

Requirement	Sophos Product	How it helps
	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 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 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.
Requirement Four: Encrypt transmission of cardholder data across open, public networks.	Sophos Firewall	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Sophos RED (remote ethernet device) extends a secure network to a remote location easily by establishing a secure, dedicated VPN tunnel.
	Sophos Email	Automatically scans message bodies and attachments for sensitive data, allowing you to easily establish policies to block or encrypt messages with just a few clicks. Sophos Email Offers TLS encryption and support for SMTP/S along with push-based encryption to send encrypted emails and attachments as password protected documents direct to the user's inbox, full portal-based pull encryption to manage encrypted messages entirely from a secure portal, and S/MIME to encrypt email messages and add a digital signature to safeguard against email spoofing.
	Sophos Mobile	Sophos Secure Workspace in Sophos Mobile dynamically encrypts content sent to cloud-based storage services and applications. It enforces device encryption and monitors compliance relative to encryption policy.
	Sophos Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos managed networks and hotspots.
Requirement Five: Protect all systems against malware and regularly update anti-virus software or programs	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 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 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 Managed Threat Response	Incorporates vulnerability intelligence to provide customers with proactive security posture improvements.

Requirement	Sophos Product	How it helps
Requirement Six: **Develop and maintain secure systems and applications.**	Sophos Intercept X Sophos Intercept X for Server	Blocks vulnerabilities in applications, operating systems, and devices with its exploit prevention capabilities.
	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 PCI DSS. ‣ Integrate security in the DevOps CI/CD pipeline to scan container images and infrastructure-as-code templates and more to block vulnerabilities pre-deployment.
Requirement Seven: **Restrict access to cardholder data by business need to know.**	Sophos Zero Trust Network Access	Validates user identity, device health, and compliance before granting access to resources.
	Synchronized Security feature in Sophos products	Sophos Firewall with Security Heartbeat™ allows next-generation endpoint and network security to continuously share meaningful information about suspicious events across extended IT ecosystem; detects compromised / unauthorized endpoint device; allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data.
	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.
	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	Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device.
	Sophos Wireless	Offers visibility into wireless networks health and clients connecting to the network. With visibility into potential threats, such as rogue APs, insight into clients with compliance or connectivity issues and advanced diagnostics, identifying and troubleshooting issues is quick and easy. Enhanced Rogue AP Detection classifies neighboring Wi-Fi networks to identify threats and prevent attempts to infiltrate an organization via Wi-Fi.
Requirement Eight: **Identify and authenticate access to system components.**	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 Central	Protects privileged and administrator accounts with advanced two-factor authentication. Keeps access lists and user privileges information up to date. Provides procedures to make sure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).
	Sophos Zero Trust Network Access	Validates user identity, device health, and compliance before granting access to resources.
	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.

Requirement	Sophos Product	How it helps
	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.
Requirement Ten: 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 Sophos Intercept X for Server	Creates detailed log events of all malicious activity on endpoint systems, helping to identify suspicious activity on systems that may store or process cardholder data.
	Sophos Firewall	Provides real-time insights into network and user events, quick and easy access to historical data, easy integration with third-party remote management and monitoring tools (RMMs).
	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 Cloud Optix	Continuously monitors public cloud environments to detect and connect disparate actions with SophosAI to pinpoint unusual access patterns and locations in near real time to identify credential misuse or theft.
Requirement Eleven: Regularly test security systems and processes.	Sophos Intercept X Sophos Intercept X for Server	Consistently looks at reported false positives and false negatives to ensure the product is being continuously improved. It integrates a deep learning malware detection model that can scale to hundreds of millions of training samples and can 'memorize' the entire observable threat landscape as part of its training process. It is regularly trained by our SophosLabs team to stay up to date over time.
	SophosLabs	Delivers the global threat intelligence advantage with Sophos' state-of-the-art big data analytics system that efficiently processes millions of emails, URLs, files, and other data points analyzed each day. This data, along with our extensive experience, enables us to develop new definitions, detect entire classes of threats, and even new variants. And, Live Protection and Live Anti-spam offer the data and expert analysis from SophosLabs in real time.

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

2022-02-24 RC (PC)

SOPHOS