PCI DSS Compliance Reference Card

SOPHOS
Cybersecurity made simple.

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 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.

REQUIREMENTS	SOPHOS PRODUCT	HOW IT HELPS MEET COMPLIANCE
REQUIREMENT ONE Install and maintain a firewall configuration to protect cardholder data.	Sophos UTM/Firewall	‣ 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. ‣ Creates granular and manageable firewall rule sets that specify addresses, ports, protocols, and specific application traffic and behavioral patterns. Sophos firewalls can also perform Network Address Translation (NAT), detect and block spoofed IP addresses, and perform stateful traffic inspection.
	Sophos Intercept X Advanced Sophos Intercept X Advanced for Server	‣ Includes a powerful local firewall (endpoints) and host-based intrusion detection and traffic control and monitoring, and 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.
REQUIREMENT TWO Do not use vendor-supplied defaults for system passwords and other security parameters.	Sophos Central	‣ Sophos Central enforces use of non-default passwords sufficiently complex to withstand typical “brute force” attacks.
REQUIREMENT THREE Protect stored cardholder data.	Sophos UTM/Firewall Sophos Intercept X Advanced	‣ 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 Appliance Sophos UTM/Firewall	‣ Leverages Sophos SPX encryption to dynamically encapsulate email content and attachments into a secure encrypted PDF.
	Sophos Mobile	‣ Sophos Secure Workspace secures work documents with AES-256 encryption, allowing a secure way to manage, distribute, and edit business documents and view web content on mobile devices. Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. Emails and documents can be stored in the secure and encrypted Sophos Container and accessed with the Sophos Secure Email and Sophos Secure Workspace apps.
	Sophos SafeGuard Enterprise Sophos Central Device Encryption	‣ Encrypts data on Macs, Windows, and mobile devices. Device Encryption provides centrally-managed, full disk encryption using Windows BitLocker and Mac FileVault. Sophos application-based (synchronized) encryption is automatic and always-on, i.e. content is encrypted as soon as it is created and it stays encrypted even when shared or uploaded to a cloud-based file-sharing system or removable devices. Role-based management is available to separate authorization levels and your encryption policies, keys and self-service key recovery can be centrally managed.

PCI DSS Compliance Reference Card

SOPHOS
Cybersecurity made simple.

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

REQUIREMENTS	SOPHOS PRODUCT	HOW IT HELPS MEET COMPLIANCE
REQUIREMENT FOUR Encrypt transmission of cardholder data across open, public networks.	Sophos SafeGuard Enterprise	Encrypts data on Macs, 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 Wireless Sophos UTM/Firewall	Creates dynamic encrypted Wi-Fi sessions, protecting payment card data in transit on Sophos managed networks and hotspots.
	Sophos UTM/Firewall	Allows for policy-based encryption for VPN tunnels, protecting payment card data in transit.
	Sophos Email Appliance Sophos UTM/Firewall	SPX email encryption allows encrypting of sensitive data automatically as files and content are emailed to parties outside the organization.
REQUIREMENT FIVE Protect all systems against malware and regularly update anti-virus software or programs.	Sophos Intercept X Advanced for Server Sophos Intercept X Advanced	Integrates innovative technology like malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease.
	Sophos UTM/Firewall Secure Web Gateway	Monitors and blocks web site access for malware infections and execution, and also integrates up-to-date threat intelligence on malicious sites from Sophos.
	Sophos Email Appliance and Sophos Email on Central Sophos UTM/Firewall	Uses real-time threat intelligence to detect and block 99% of unwanted email at the gateway and our anti-spam engine catches the rest, including the latest phishing attacks, malicious attachments, and snowshoe spam.
	Sophos for Virtual Environments	Protects virtual servers and desktops from malware.
	Sophos Mobile	The Sophos Mobile Security app offers leading anti-malware and antivirus protection together with potentially unwanted app detection for Android devices.
	Sophos for Network Storage	Sophos for Network Storage scans file systems on storage platforms from EMC, NetApp and Oracle/Sun for malware.
REQUIREMENT SIX Develop and maintain secure systems and applications.	Sophos Intercept X Advanced Sophos Intercept X Advanced for Server	Blocks vulnerabilities in applications, operating systems, and devices with its exploit prevention capabilities.
	Sophos Mobile	Proactively monitors Android devices via Security Advisor and Privacy Advisor and warns users of potential vulnerabilities.

PCI DSS Compliance Reference Card

SOPHOS
Cybersecurity made simple.

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

REQUIREMENTS	SOPHOS PRODUCT	HOW IT HELPS MEET COMPLIANCE
REQUIREMENT SEVEN Restrict access to cardholder data by business need to know.	Sophos UTM/Firewall	‣ 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.
	Sophos Wireless Sophos UTM/Firewall	‣ Provides a guest portal along with full logging of all authentication and connection activity, including unique user accounts.
	Sophos Intercept X Advanced Sophos Intercept X Advanced for Server	‣ Configurable role-based administration provides granular control of administrator privileges.
	Sophos Mobile	‣ Role-based administration assures user privacy and appropriate credentials for altering compliance.
	Sophos SafeGuard Enterprise Sophos Central Device 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.
REQUIREMENT EIGHT Identify and authenticate access to system components.	Sophos UTM/Firewall	‣ File-integrity monitoring to alert on unauthorized modifications to critical system files, configuration files, or content files. ‣ Sophos' user awareness across all areas of the firewall enables user-based policy controls regardless of IP-address, location, network, or device and user-based logs and reports. ‣ Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
	Sophos SafeGuard Enterprise	‣ Authenticates users for access to specific files/folders with the use of user- or group-specific keys for SafeGuard Enterprise.
	Sophos Central	‣ Protects privileged and administrator accounts with advanced two-factor authentication. ‣ Keeps access lists and user privileges information up to date. Procedures are in place to ensure 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 Mobile	‣ Sophos Secure Email and Sophos Secure Workspace store content securely with AES-256 encryption. Access to the container can be restricted based on device compliance rules, time, Wi-Fi, or geo-location.
REQUIREMENT TEN Track and monitor all access to network resources and cardholder data	Sophos Intercept X Advanced for Server	‣ Provides file-integrity monitoring to continuously track and alert on unplanned and unexpected changes to critical system files and applications, as well as optional files, folders, registry keys and registry values.
	Sophos Intercept X Advanced Sophos Intercept X Advanced 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 UTM/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).

PCI DSS Compliance Reference Card

SOPHOS
Cybersecurity made simple.

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

REQUIREMENTS	SOPHOS PRODUCT	HOW IT HELPS MEET COMPLIANCE
REQUIREMENT TEN Track and monitor all access to network resources and cardholder data	Sophos iView Reporting	‣ Provides intelligent centralized reporting and analytics across multiple firewalls or sites; easy monitoring and analysis of security risks across entire network; convenient backup and long-term storage for security information.
	All Sophos Products	‣ Generates security event logs that can be integrated into a centralized monitoring program for incident detection and response.
REQUIREMENT ELEVEN Regularly test security systems and processes.	Sophos Intercept X Advanced for Server	‣ File-integrity monitoring to alert on unauthorized modifications to critical system files, configuration files, or content files
	Sophos Wireless Sophos UTM/Firewall	‣ Centrally manageable in the UTM interface, it can be co-related with other scanning and discovery efforts for wireless access points and signal in the environment. Offers plug and play deployment with support for strongest encryption and wireless authentication standards.
	Sophos UTM/Firewall	‣ Includes robust intrusion detection and intrusion prevention policies that can be applied to all traffic coming into the platform.
	Secure Web Gateway Sophos UTM/Firewall	‣ Monitors and blocks malware infections and execution, and also integrates up-to-date threat intelligence on malicious sites from SophosLabs, acting as a web application intrusion detection and prevention system.
	Sophos Mobile	‣ Proactively monitors Android devices via Security Advisor and Privacy advisory and warns users of potential vulnerabilities.
	Sophos Email Appliance	‣ Dedicated hardware and virtual appliances proactively monitored by Sophos experts 24/7/365 with automated updates provided to ensure everything is running as it should.
	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 subject to change without notice. Sophos disclaims in full all warranties and guarantees. This document and the information in it 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

2018-11-12 RC-NA (NP)

SOPHOS