Achieving PCI compliance with Sophos

SOPHOS

Did you know your security solution can help with PCI compliance too?

High-profile data losses have led to increasingly complex and evolving regulations. Any organization or retailer that accepts payment card transactions, or collects, processes or stores credit card transaction information must comply with Payment Card Industry Data Security Standard (PCI DSS).

Protecting your data is enough of a headache without having to keep up with regulations and quickly prove compliance during audits. Furthermore, failure to comply with PCI risks fines, unwanted press and loss of business.

Sophos integrates all the protection you need to keep your data safe and help your business be PCI compliant. You can manage Sophos solutions simply and quickly, enabling you to focus on what's important.

The following document explains how Sophos helps organizations comply with requirements specific to the Payment Card Industry Data Security Standard (PCI DSS) v1.2.

PCI DSS

Sophos supports all 12 PCI DSS requirements. Sophos also offers professional service support that can assist in addressing the sections of PCI DSS in greater detail, including creating an information security policy and password management.

Requirement 1: Install and maintain a firewall configuration to protect cardholder data	Sophos supports this requirement by…
1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.	Blocking ports with the Sophos client firewall, in addition to blocking traffic types (TCP, IP, UDP), IP addresses, and allowing application rules to be set. The Sophos client firewall can be configured to allow only trusted connections to cardholder data.
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	Establishing policies for accessing cardholder data with the Sophos client firewall. Access reporting is available for all allowed or blocked traffic in over a specified period of time.
1.3.1 Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.	Allowing inbound traffic to a specific protocol and to specific IP addresses with the Sophos client firewall.
1.3.2 Limit inbound internet traffic to IP addresses within the DMZ.	Allowing inbound traffic to a specific protocol and to specific IP addresses with the Sophos client firewall.
1.3.3 Do not allow any direct routes inbound or outbound for traffic between the internet and the cardholder data environment.	Preventing computers with cardholder data from accessing the internet with the Sophos client firewall. Also by using application control to stop the use of internet-enabled applications.
1.3.5 Restrict outbound traffic from the cardholder data environment to the internet such that outbound traffic can only access IP addresses within the DMZ.	Creating Network Access Control (NAC) enforcement templates to prevent access to the DMZ from specific applications.
1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network).	Inspecting UDP, IP and TCP traffic types with the Sophos client firewall to prevent direct access from the internet to cardholder data on PCs.
1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the internet (for example, laptops used by employees), which are used to access the organization's network.	Continuously checking company computers — even laptops that are not connected to the network — to ensure that a company approved firewall is installed and running. If it is not, Sophos NAC blocks the computer from the network. Non-compliant guest computers receive a message directing users on how to fix the problem.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	Sophos supports this requirement by…
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	Ensuring industry accepted policies that require specific password configurations are followed. If not, passwords are not accepted and data cannot be accessed.
Requirement 3: Protect stored cardholder data	Sophos supports this requirement by…
3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy.	Ensuring hard disks containing encrypted data are securely disposed of via an encryption key-wipe capability.
3.2 Do not store sensitive authentication data after authorization (even if encrypted).	Scanning data that's saved to removable storage. If sensitive data is found, Sophos warns the end-user, blocks it, or reports it. Only allow data to be stored on specific devices or encrypted devices. Custom rules can be created to protect PINs and verification codes.
3.4 Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs) - Strong cryptography with associated key management and processes and procedures	Providing strong encryption of all data stored on laptops, desktops, servers and on portable media. Encryption keys are managed independently of the operating system access controls.
3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse.	Securely storing encryption keys with further layers of encryption and making them available to authorized end users and administrators only after strong authentication. Options include username and password authentication with multi-factor options including tokens, smartcards and biometrics.
3.6 Fully document and implement all-key management processes and procedures for cryptographic keys used for encryption of cardholder data.	Providing secure, strong, standards-based processes for key generation, storage, and distribution. Sophos encryption is FIPS 140-2 and Common Criteria EAL 3+ certified.
Requirement 4: Encrypt transmission of cardholder data across open, public networks	Sophos supports this requirement by…
4.1 Use strong cryptographic and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks	Providing the ability to secure emails that contain sensitive information using SPX encryption in the Sophos Email Appliance. Enforcing both incoming and outgoing Transport Layer Security (TLS) encryption and certificate verification for connections with email relays on the internet.
4.2 Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat).	Automatically enforcing policies block emails containing unencrypted sensitive data from leaving the organization with the Sophos Email Appliance or Sophos PureMessage for Lotus Domino or Microsoft Exchange. And with the Sophos Email Appliance you can encrypt sensitive data using SPX encryption as it leaves the organization via email. Sensitive files on network file shares can also be encrypted from end-to-end using SafeGuard LAN Crypt.

Requirement 5: Use and regularly update anti-virus software or programs	Sophos supports this requirement by…
5.1 Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers).	Protecting your computers, servers, email and web with Sophos Anti-Virus. PCI requires deployment of anti-virus where “applicable anti-virus technology exists.” Sophos Anti-Virus defends a broad range of platforms including Windows, Mac, SharePoint, UNIX and Linux. It also continuously checks company desktops and laptops to ensure that approved AV software is installed and runs with Sophos NAC. If not, blocks them from the network.
5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	Simplifying anti-virus administration – enabling easy deployment, management and compliance reporting through the Management Console. With Sophos NAC ensure your anti-virus is up-to-date and running on all computers accessing your network. And, receive automated updates every few minutes with the Sophos Appliances and Sophos PureMessage for Lotus Domino or Microsoft Exchange to ensure your email and web traffic is checked with up-to-date AV.
Requirement 6: Develop and maintain secure systems and applications	Sophos supports this requirement by…
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	Checking all desktops and laptops against your security policy – on access and on schedule – to ensure patches are installed and up-to-date with Sophos NAC Advanced. Any non-compliant computers are fixed or blocked from the network. Sophos web and email appliances automatically alert the administrator when updates are available, and can optionally auto-install.
6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the internet). Update standards to address new vulnerability issues.	Delivering small, frequent, security updates to Sophos Security and Data Protection to ensure you have the latest and best protection. You can also get an RSS feed on newly-discovered vulnerabilities at www.sophos.com.
Requirement 7: Develop and maintain secure systems and applications	Sophos supports this requirement by…
7.1.2 Assignment of privileges is based on individual personnel’s job classification and function.	Sophos SafeGuard Enterprise allows for granular assignment of roles and separation of duties between network administrators and security administrators. For example, several levels of security administrators can be defined, each with only specific access to the system and permissions to perform only the allowed, pre-defined tasks.
7.1.4 Implementation of an automated access control system.	Sophos SafeGuard Enterprise has granular role based access control and authorization for tasks that are fully automated and applied automatically when a user logs in.
7.2.2 Assignment of privileges to individuals based on job classification and function.	Sophos SafeGuard Enterprise has both pre-defined and customer security office roles that can be applied. For example, roles could include helpdesk officer, audit officer, master security officer.

Requirement 8: Assign a unique ID to each person with computer access	Sophos supports this requirement by…
Req 8.1 Assign all users a unique ID before allowing them to access system components or cardholder data	Sophos disk encryption pre-boot environment is multiuser capable, allowing each user to use their unique Windows user ID. Each user's actions are logged separately in the central audit trail.
Req 8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: • Password or passphrase • Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)	Sophos disk encryption and the admin console supports two-factor authentication with smartcards or tokens. Sophos disk encryption and the admin console support both user id/password and two-factor authentication with smartcards or tokens.
Req 8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography	By default Sophos does not store full disk encryption passwords. However, if it is configured to store the password for recovery options, the password is encrypted and protected by strong cryptography.
8.5.2 Users cannot change their password or PIN without entering the current password or PIN. 8.5.4 Users can be centrally removed from machines, revoking all access after the next policy refresh (configurable). 8.5.9 Require password change every 90 day 8.5.10 Require a minimum password length of at least seven characters. 8.5.11 Use passwords containing both numeric and alphabetic characters. 8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used. 8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts	Sophos disk encryption enforces password rules for minimum length and complexity, and also forces password changes at configurable intervals. A configurable password history function ensures users don't reuse passwords too soon. Sophos disk encryption can also lock out users after a predefined number of wrong password attempts.
Requirement 9: Restrict physical access to cardholder data	**Sophos supports this requirement by…**
9.10.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	When data needs to be disposed of, Sophos Safeguard Enterprise supports secure authorized deletion of encryption keys to ensure that encrypted data is rendered unrecoverable.

Requirement 10: Track and monitor all access to network resources and cardholder data.	Sophos supports this requirement by…
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	Tracking and reporting all network access attempts – successful and unsuccessful - with Sophos NAC. The Sophos Email and Web appliances logs all access and actions taken by any user of the email system, administrator or otherwise.
10.2.1 Verify all individual accesses to cardholder data is logged.	Logging whenever cardholder data is emailed, moved or copied from a PC to removable storage. Sophos SafeGuard Enterprise provides over 250 types of logs including who has logged on to PCs that contain sensitive information
10.3 Record at least the following audit trail entries for all system components for each event: • User identification • Type of event • Date and time • Success or failure identification • Origination of event • Identity or name of affected data, system component, or resource	Providing an audit log of all accesses and actions taken by any user of the systems, administrator or otherwise with Sophos Email and Web appliances.
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter	Providing an FTP backup mechanism for all logs, -including the audit log - using Sophos Email and Web appliances.
Requirement 11: Regularly test security systems and processes	**Sophos supports this requirement by…**
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).	Continuously scanning computers that attempt to access your network, then quarantining or fixing any that do not comply with your security policy. Sophos regularly runs Qualys PCI DSS vulnerability scans on the Email appliance to ensure system compliance.
11.4 Use network intrusion detection systems, host based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up to date.	Providing host-based intrusion protection systems in Sophos Anti-Virus with Behavioral Genotype. Sophos NAC Advanced checks to ensure your anti-virus is installed, working and up to date with the latest protection.
11.5 Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	Alerting the administrator and Sophos Support in the case of any unauthorized file modification of the Sophos Email and Web appliances.
Requirement 12: Maintain a policy that addresses information security for employees and contractors	**Sophos supports this requirement by…**
12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.	Using data leakage prevention functionality to warn and educate end-users - using alerts - that sensitive data is about to be moved, copied, or emailed. And, by providing Sophos for free to your users for use on their home computers to build awareness on the importance of protecting personal and cardholder data.

Sophos Protection

Get complete threat and data protection with Sophos Security and Data Protection. Endpoint, email and web are covered, with protection against known and unknown malware threats, data loss, device control and application control. The Sophos Security and Data Protection license includes the following, which you can choose to license separately if you wish:

- Sophos Endpoint Security and Data Protection — A single integrated solution for both anti-malware and data protection in a single agent and across all your platforms. It also combines integrated NAC and full disk encryption to secure your data and ensure policy compliance.
- Sophos Email Security and Data Protection — All your email security and data protection needs covered in one license — giving you access to all our Groupware protection and Email appliance software.
- Sophos Web Security and Control — The first managed appliance to proactively ensure safe web browsing, blocking suspicious URLs, hijacked or infected websites, and download of spyware, viruses, malware and unwanted content.

Got very specific needs? Then consider Sophos Endpoint Security and Control for anti-malware and data protection, Sophos SafeGuard Enterprise for advanced, centrally managed encryption of PCs & removable media, and Sophos NAC Advanced for network access control.

Sophos can support your compliance needs and our team of specialists can help you create security policies that are right for your environment. To find out more visit www.sophos.com.

Boston, USA | Oxford, UK

SOPHOS
WWW.SOPHOS.COM