

PCI compliance and Sophos NAC Advanced

This document is a guide to how your company can safely and easily meet PCI standards with the help of Sophos NAC Advanced.

The need for PCI

Retailer TJ Maxx had 45.6 million credit and debit cards compromised. Bank of America, Morgan Stanley, Citibank, and many other well-known organizations have also suffered breaches in data security. In 2007 banks lost \$46 billion due to credit card fraud, and consumers lost \$5 billion. Companies large and small are at risk.

In response to the increasing credit and debit card security threats the Payment Card Industry Data Security Standards (PCI DDS) were created through collaboration with major credit card companies including MasterCard and Visa. These standards require your organization to create and maintain a full range of processes and security measures for employees and guests as part of a comprehensive information security policy. You must develop and implement measures to ensure secure management of your credit card data and controlled access to your network over which customers' card information is sent.

Failing to comply with PCI standards can result in fines and loss of credit card processing privileges, seriously impacting your ability to do business.

Sophos NAC Advanced

Sophos NAC Advanced can be critical part of your security measures – ensuring that employee and guest computers are compliant with company security policy, managing network access, and delivering the peace of mind that comes from knowing your data is safe and your company is PCI compliant.

A comprehensive and easy-to-deploy endpoint assessment and network access control (NAC) solution, Sophos NAC Advanced controls access to the network for guest, unmanaged and unauthorized computers. Non-compliant computers are identified and isolated, based on a centrally defined, policy-driven assessment. Company computers missing critical security applications and patches are fixed, while unauthorized computers seeking access to your network are blocked.

Disruption can be minimized by phasing in the enforcement of policy. The software solution is vendor-neutral and works with existing network infrastructure and security applications.

The PCI Data Security Standard

- 1 Install and maintain a firewall configuration to protect cardholder data
- 2 Do not use vendor-supplied defaults for system passwords and other security parameters
- 3 Protect stored cardholder data
- 4 Encrypt transmission of cardholder data across open, public networks
- 5 Use and regularly update anti-virus software
- 6 Develop and maintain secure systems and applications
- 7 Restrict access to cardholder data by business need-to-know
- 8 Assign a unique ID to each person with computer access
- 9 Restrict physical access to cardholder data
- 10 Track and monitor all access to network resources and cardholder data
- 11 Regularly test security systems and processes
- 12 Maintain a policy that addresses information security

For more information about Sophos NAC Advanced or to take the Sophos Endpoint Assessment Test, visit www.sophos.com today.

How Sophos NAC Advanced helps

Install and maintain a firewall

A firewall controlling access to your network is a critical tool for keeping cardholder data safe. PCI requires that firewalls are configured to stop inbound and outbound traffic not specifically required for your business.

Sophos NAC Advanced lets you do this easily and without impacting productivity. Even checking computers when they are outside the office, Sophos NAC Advanced keeps your data and your network safe at all times.

PCI Requirement 1: Install and maintain a firewall configuration to protect cardholder data	Sophos NAC Advanced can help by...
1.3.9 Installing personal firewall software on any mobile and 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 Advanced fixes or blocks the computer from the network. Non-compliant guest computers receive a message directing users on how to fix the problem.
1.4.2 Restrict outbound traffic from payment card applications to IP addresses within the DMZ	Creating NAC Advanced enforcement templates to prevent access to the DMZ from specific applications.

Use and regularly update anti-virus software

Sophos NAC Advanced supports the PCI requirement for up-to-date anti-virus software by ensuring that computers can access your network only if they have company-approved anti-virus software installed, up to date, and running. Sophos NAC Advanced can fix company-owned computers to provide immediate access to the network, and can block guest computers until they are made compliant with your security policy.

Sophos NAC Advanced includes a real-time data feed, providing the live updates that are critical to keeping your network safe from the latest threats, malware, and unwanted applications by blocking them before they can execute.

PCI Requirement 5: Use and regularly update anti-virus software or programs	Sophos NAC Advanced can help by...
5.1 Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers)	Continuously checking company desktops and laptops, to ensure that company approved anti-virus software is installed and running. If it is not, Sophos NAC Advanced fixes or blocks the computer from the network.
5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware.	Ensuring that all computers, on or off the network, have company-approved and current anti-malware software actively running. If not, then fixing or blocking it from the network.
5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	Delivery of real-time feeds to keep Sophos NAC Advanced up to date on critical checks.

Update and install the latest security patches

Sophos NAC Advanced gives you robust, centrally managed, assessments of security patches on all company-owned computers, on or off your network. There are over 1000 predefined security application and operating system patch checks, and you can also create your own custom checks. Contextual assessments that check only for patches relevant to a given computer keep your network efficient and productive.

PCI Requirement 6: Develop and maintain secure systems and applications	Sophos NAC Advanced can help 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 – on access and on schedule – to ensure patches are installed and up to date. If they are not, it blocks access to the network until the patch(es) is installed.
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.	Delivery of real-time data feeds to keep Sophos NAC Advanced up to date on critical patches.

Implement strong data access control measures

Sophos NAC Advanced supports your company's data access management needs and PCI requirements with a solution that is flexible and secure. With Sophos NAC Advanced you control which users and groups can access cardholder information ensuring limited access and complete data security.

PCI Requirement 7: Restrict access to cardholder data by business need-to-know	Sophos NAC Advanced can help by...
7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access.	Requiring user authentication to access the network and by giving users access only to required servers and applications.

Protect against unauthorized access

Sophos NAC Advanced can help prevent unauthorized access to cardholder data by requiring authentication credentials and checking on additional security, such as encryption. It uses enforcement mechanisms such as DHCP, 802.1x, and VPN and can restrict wireless access for guests or business partners, quarantining non-compliant computers.

PCI Requirement 8: Assign a unique ID to each person with computer access	Sophos NAC Advanced can help by...
8.1 Identify all users with a unique user name before allowing them to access system components or cardholder data	Denying access to cardholder systems for unauthenticated users, and by integrating with most common authentication systems
8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: 1) password, 2) token devices (e.g., SecurID, certificates, or public key), 3) biometrics	Supporting user authentication via password and token devices. (Biometric authentication is not currently supported.)
8.3 Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS [Remote Authentication and Dial-In User Service]) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.	Supporting two-factor authentication for remote access. Sophos NAC Advanced supports RADIUS, VPN, DHCP and 802.1x.

Monitor networks

Sophos NAC Advanced supports the PCI requirement to monitor all network access by a specific user. Sophos NAC Advanced keeps records of access attempts for at least three months, enabling you to monitor and track suspicious behavior.

PCI Requirement 10: Track and monitor all access to network resources and cardholder data	Sophos NAC Advanced can help 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.

Test security systems

PCI requires network vulnerability scans at least quarterly, as well as the use of host-based intrusion and prevention systems (HIPS) to monitor and alert your company to suspected network threats.

Sophos recommends quarterly vulnerability scans by Qualified Data Security scanning firms certified by the PCI Security Standards Council. Sophos NAC Advanced augments these scans by continuously scanning computers attempting to access your network, then quarantining or fixing computers that do not meet your security policy.

Sophos NAC Advanced integrates with Sophos Behavioral Genotype™ HIPS, and third-party IPS, technology to ensure it is properly installed, working, and up to date with the latest protection. This makes HIPS monitoring and testing a routine maintenance activity, rather than the beginning of a long fixing process.

PCI Requirement 11: Regularly test security systems and processes	Sophos NAC Advanced can help 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 attempting to access your network, then quarantining or fixing any that do not meet your security policy.
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.	Checking Sophos Anti-Virus (part of Sophos Endpoint Security and Control) with Behavioral Genotype to ensure it is installed, working, and up to date with the latest protection.

For more information about Sophos NAC Advanced or to take the Sophos Endpoint Assessment Test, visit www.sophos.com today.