

**Using Network Access Control (NAC)  
to Support Compliance with the  
Payment Card Industry Data  
Security Standard (PCI DSS)**



As consumers' awareness of the threats to cardholder information increases, businesses recognize that they need to protect the sensitive data involved in everyday commerce. More and more high-profile cases of large-scale credit card data theft bring many data security issues to light. Criminals seeking to profit from cardholder data theft have understood the inadequacies in many organization's attempts to protect cardholder data for quite some time.

### Protecting Cardholder Data: PCI DSS Compliance

To help organizations protect cardholder and other sensitive data, the major card brands developed the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS includes 12 major requirements and a number of associated sub-requirements that aim to achieve six main goals:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

Any organization that is at all involved in the processing, storage or transmission of cardholder data is required to comply with the PCI DSS. To enforce the standard, the major card brands issue fines for non-compliant organizations that fall victim to a breach. In addition, many acquiring banks have set deadlines for their merchants to comply and issue fines for organizations that fail to meet them.

The standard is based on data security best practices and the requirements do not exceed measures called for in any reasonable data security program. What makes the PCI DSS effective is its prescription for a holistic, layered approach to protecting sensitive data. Compliance with a single requirement will not make an organization secure. No single security solution can protect against a breach of IT security. An organization must implement multiple, layered security controls to truly defend against today's threats. Nevertheless, many organizations fail to comply with the entirety of the PCI DSS of which Trustwave's unceasing caseload of cardholder data breach investigations is evidence. Every breached organization that Trustwave investigates fails to comply with at least one (and often numerous) PCI DSS requirements.

### Network Access Control (NAC) and Compliance

PCI DSS compliance requires a layered set of security controls (many of which Trustwave's solution suite can satisfy). A robust Network Access Control (NAC) solution is just one of many technologies that support compliance with the PCI DSS and protect an organization's network and sensitive data.

Trustwave's patented NAC solution delivers the following PCI DSS-related benefits:

- Monitors health and status of anti-virus programs
- Checks endpoints' security patch status
- Restricts endpoints' access based on business need-to-know
- Tracks and analyzes endpoint behavior
- Reports on network behavior and trends
- Restricts service ports on endpoints
- Supports definition and documentation of policies

Trustwave's agent-less NAC solution provides a scalable means to assess the compliance status of network endpoints. In addition, its profiles of endpoint behavior monitor and manage the risks associated with all endpoints throughout the network. Trustwave NAC also allows an organization to easily and efficiently distribute security policy throughout an enterprise via a flexible, centrally managed policy console.



Trustwave NAC supports PCI DSS compliance and the protection of cardholder data via the following:

- Providing scalable mechanisms to address endpoint health
- Integrating patch monitoring into existing tools
- Gathering and tracking identity information for users of all endpoints entering the network
- Providing segment-level, and in some cases endpoint-specific, network policies that can be distributed throughout the enterprise
- Enforcing policies based on real-time analysis of packets emitted by endpoints
- Enabling remediation, so that non-compliant endpoints can gain network access as quickly as possible without tying up help desk resources
- Providing analysis and real-time data on compliance status throughout the enterprise
- Providing relevant historical reporting features to demonstrate compliance and highlight areas that need attention
- Allowing for consistent, centrally managed security policy throughout a network environment

While no single security solution can satisfy all of the PCI DSS requirements, Trustwave NAC supports the fulfillment of six of the 12 requirements. The table below outlines the ways in which the Trustwave NAC solution can fulfill or support fulfillment of specific requirements from the PCI DSS version 1.2.

PCI DSS Requirement		Trustwave NAC Solution
<b>Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters</b>		
2.2	Develop configuration standards for all system components that address all known security vulnerabilities and are consistent with industry-accepted definitions.	Enables an organization to define configuration standards and policies that can be inherited from a root 'domain' structure in the Trustwave NAC policy engine.
2.2.1	Implement only one primary function per server.	Verifies that devices run only one server application and restricts non-compliant endpoints' network access until remediation is performed.
2.2.2	Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function).	Tests all endpoints for active services and protocols that are unnecessary and insecure and restrict those endpoints' network access until remediation is performed.
2.2.3	Configure system security parameters to prevent misuse.	Tests security settings on a regular basis to ensure compliance with security policy.
2.2.4	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	Provides automated tests for finding unnecessary functionality and restrict non-compliant endpoints' network access until remediation is performed.
<b>Requirement 5: Use and regularly update anti-virus software or programs</b>		
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	Ensures that all required systems have an anti-virus application installed and restricts non-compliant endpoints' network access until remediation is performed.



PCI DSS Requirement Cont.		Trustwave NAC Solution Cont.
5.2	Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	Ensures that all required systems have an anti-virus application installed and running and that the signature file is up to date and restricts non-compliant endpoints' network access until remediation is performed.
<b>Requirement 6: Develop and maintain secure systems and applications</b>		
6.1	Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.	Ensures that all required endpoints have current operating system patches, anti-virus updates, anti-spyware updates and firewall updates (version) and restricts non-compliant endpoints' network access until remediation is performed.
<b>Requirement 7: Restrict access to cardholder data by business need-to-know</b>		
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access...	Provides authorization capabilities that restrict access based on user login to allow an administrator to define what users should have network access to specific devices.
<b>Requirement 11: Regularly test security systems and processes</b>		
11.1	Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.	Continuously ensures that endpoints are correctly configured to identify and stop unauthorized access attempts through system scans, behavioral monitoring and user authentication and then restricts non-compliant endpoints' network access until remediation is performed.
11.4	Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data	Continuously monitors all network traffic and identifies zero day threats while providing the unique capability to isolate endpoints that show anomalous behavior, and alert based on various protocols (SNMP, SMTP, etc.).
<b>Requirement 12: Maintain a policy that addresses information security for employees and contractors</b>		
12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.	Allows administrators to enforce policy by requiring pre-admission authentication and system scans and customize user-facing screens to allow the display of policy information.
12.5.2	Monitor and analyze security alerts and information, and distribute to appropriate personnel.	Provides role-based access to ensure that the appropriate information is displayed to each administrator, allows administrators to generate reports for security event analysis and provides multiple protocols for alerting personnel.
12.9.5	Include alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems.	Provides multiple standard protocols for alerting personnel when defined events occur.



## Conclusion

Again, Trustwave's NAC solution is merely one element in a holistic, layered security program. However, Trustwave NAC does aid in the fulfillment of a number of PCI DSS requirements and most important, it provides a centralized mechanism by which an organization can manage the compliance of network endpoints. Trustwave NAC enables an organization to control admission to the network, ensuring that uninvited, infected, out-of-policy and non-compliant endpoints do not access and harm the network. Before granting network access, Trustwave NAC gathers the following information about an endpoint:

- Device type
- Whether it is known or unknown
- Past policy compliance and threat history
- Whether it is entering via a wired or wireless connection
- What services are currently running on the endpoint (such as instant messaging, file transfer protocol services, or peer-to-peer networking)

Trustwave NAC then creates a risk profile to evaluate whether to admit the endpoint to the network based on its compliance and other factors. The endpoint may then be required to register on the network, connect to a designated quarantine server for remediation or undergo a combination of additional security checks. These features of Trustwave NAC not only help fulfill a number of PCI DSS requirements, but provide a solution to continually monitor endpoints and remediate non-compliant endpoints before they're granted access to the network.

## About Trustwave

Trustwave is the leading provider of on-demand and subscription-based information security and payment card industry compliance management solutions to businesses and government entities throughout the world. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its flagship TrustKeeper® compliance management software and other proprietary security solutions. Trustwave has helped more than 30,000 organizations—ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers—manage compliance and secure their network infrastructure, data communications and critical information assets. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, Africa, China and Australia. For more information, visit <https://www.trustwave.com/>.

