
Payment Card Industry Data Security Standard (PCI DSS) requirements and StillSecure® solutions matrix

1. Introduction

In an effort to combat the growing problem of electronic fraud and identity theft, payment card leaders American Express®, Mastercard® and Visa® implemented the Payment Card Industry (PCI) Data Security Standard (DSS). This standard specifies security requirements for safeguarding card members' personal data. PCI requires all service providers (also referred to as transaction processors) and merchants who store, process, or transmit cardholder information to comply with this program. The PCI Standard went into effect in December 2004 and was most recently updated in October 2008. An addendum was released in July 2009 to clarify the wireless component of the standard.

StillSecure's suite of network security solutions – both products and managed services – helps merchants and service providers comply with critical portions of PCI. This document describes how StillSecure's network security solutions directly meet specific PCI requirements and enable you to minimize the risk and liability from network attacks.

2. Background

To combat electronic fraud and identity theft, the PCI Security Standards Council has instituted the PCI Data Security Standard. Merchants and service providers who store, process, or transmit cardholder information must comply with the PCI DSS standard in order to be authorized to process credit card transactions. Designed to protect cardholders, merchants, service providers, and the payment card industry from fraud, PCI is a **mandatory** compliance program that is applied based on size and transaction volume. For example, service providers are held to a much higher standard than are merchants who do not have any e-commerce capabilities. Those with low transaction volumes may only need to validate compliance using a less rigorous method. Non-compliance may result in severe fines or penalties.

PCI compliance is based on 12 high-level security procedures and requirements. The standard defines each requirement in detail and specifies minimum acceptable standards as well as best practices. More information on PCI is available at:

- https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

StillSecure network security products and managed services (described in more detail in section 4 of this paper) help organizations comply with 8 of the 12 PCI provisions. StillSecure solutions are effective, affordable, highly automated, and easy to use / manage. They are designed to protect organizations from malicious attacks and reduce the risk and liability of electronic fraud.

The StillSecure solution suite includes:

- ProtectPoint®— Managed security services (MSS)
- Safe Access®— Network access control / endpoint compliance solution
- Strata Guard®— Intrusion detection/prevention system
- VAM®— Vulnerability management platform

StillSecure solutions support PCI by enabling users to:

- Create an on-going proactive program of PCI compliance

- Provide in-depth reporting on security status and trending
- Protect key personal card member information systems from attack or breach
- Validate security processes
- Provide audit history to support security efforts
- Automate portions of compliance to reduce costs
- Manage key portions of security and the PCI requirements
- Adequately prepare for PCI audits.

Note that PCI compliance of any technology solutions will be implementation specific. Please contact your StillSecure representative to ensure that the implementation will meet PCI DSS standards.

3. PCI compliance requirements met by StillSecure

The PCI requirements that StillSecure solutions address are detailed in Table 1. Requirements specifically pertaining to wireless are highlighted in blue.

Table 1. PCI requirements met by StillSecure solutions.

	PCI DSS 1.2 requirement	StillSecure solution	How StillSecure solves the requirement
Requirement 1: Install and maintain a firewall configuration to protect cardholder data.			
1.1.1	A formal process for approving and testing all network connections and changes to firewall and router configurations.	ProtectPoint	As part of the StillSecure ProtectPoint managed service, a formal change process for approving and testing all network connections is implemented and adhered to by our SAS 70 Type-II approved Security Operations Center (SOC). This formal process adheres to and even exceeds the requirements of the PCI Council. Customers can participate in the process in a PCI compliant manner by interacting with our security staff through the RADAR managed services portal.
1.1.2	Current network diagram with all connections to cardholder data, including any wireless networks	ProtectPoint	StillSecure's RADAR portal is set up to store both existing current and historical diagrams. If no diagrams exist, StillSecure's security consultants can help generate network diagrams showing all connections to cardholder data including wireless networks.
1.1.3	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.	ProtectPoint	StillSecure's experienced professional security consultants will work with your unique network configuration to ensure that the ProtectPoint managed firewalls are configured to provide protection at each internet connection point and DMZ ensuring that firewalls meet PCI compliance.
1.1.5	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	ProtectPoint	The ProtectPoint managed firewall service details all ports and protocols that are allowed and disallowed with business justification. If help is required to determine which ports and protocols are needed, StillSecure security consultants can assist.
1.1.6	Requirement to review firewall and router rule sets at least every six months.	ProtectPoint	As a StillSecure PCI customer a regularly scheduled PCI review will be conducted via phone or optionally in person at least every 6 months to review firewall and router rule sets, as well as other PCI and security related issues and regulations. Additionally, firewall/router rule sets are available 24x7 via RADAR.

	PCI DSS 1.2 requirement	StillSecure solution	How StillSecure solves the requirement
1.2	Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.	ProtectPoint	StillSecure's experienced security professionals will configure and implement the firewall to restrict connections between untrusted networks and any systems in the cardholder data environment and document them as part of our PCI implementation service.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	ProtectPoint	StillSecure will implement a "PCI best practices" firewall rule set that will comply with this DSS. StillSecure will then manage the firewall and on going rule changes.
1.2.3	Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	ProtectPoint	A StillSecure security consultant will configure your firewall or, if necessary, install additional firewalls (optional) to deny or control any wireless traffic to a CDE.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	ProtectPoint	The ProtectPoint managed firewall service provides this function.
1.3.1	Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.	ProtectPoint	StillSecure security consulting will design a DMZ for connectivity to the CDE. The standard ProtectPoint managed security appliance has multiple ports that can be configured as required to comply with this requirement.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	ProtectPoint	StillSecure security consultants will design a compliant DMZ and set up firewall rules which are specifically configured to provide the required limiting function to specific IP addresses in the DMZ. By default, all other in-bound traffic is dropped.
1.3.3	Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment.	ProtectPoint	StillSecure security consultants will design network access to prevent direct routes to the CDE directly from the internet. MSS firewall rules will control this and are available to view via the RADAR portal at anytime.

	PCI DSS 1.2 requirement	StillSecure solution	How StillSecure solves the requirement
1.3.4	Do not allow internal addresses to pass from the Internet into the DMZ.	ProtectPoint	The MSS firewall appliance can be specifically configured to provide the required limiting function for all internal IP addresses. The rules can be confirmed anytime via the RADAR portal.
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.	ProtectPoint	StillSecure security consulting will configure your firewall rules to provide this limiting function of the outbound traffic from the restricted area to access only IP addresses within the DMZ. Confirmation of these rules can be made via the RADAR portal at anytime.
1.3.6	Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)	ProtectPoint	The MSS firewall and IDS/IPS service uses a stateful inspection engine.
1.3.8	Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space. Use network address translation (NAT) technologies – for example, port address translation (PAT).	ProtectPoint	StillSecure's managed firewall service supports this functionality. StillSecure security consultants can assist in implementation.
1.4	Install personal firewall software on mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organizations network.	ProtectPoint Safe Access VAM	StillSecure scanning solutions can test, audit and report on which devices are compliant with this requirement.

	PCI DSS 1.2 requirement	StillSecure solution	How StillSecure solves the requirement
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.			
2.1	Always change the vendor-supplied defaults before installing a system on the network – for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	ProtectPoint VAM	The ProtectPoint vulnerability scanning service and VAM both test, audit, and report on the use of default passwords. StillSecure security consultants can help change the default passwords if needed.
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.	ProtectPoint VAM	The ProtectPoint vulnerability scanning service and VAM both test, audit, and report on the use of default passwords. StillSecure security consultants can help change the default passwords if needed.
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.	ProtectPoint Safe Access VAM	The ProtectPoint vulnerability scanning service, Safe Access, and VAM enable you to audit, test and report on those configurations on an on-going basis. These configuration standards can address security vulnerabilities and industry-accepted system hardening standards. StillSecure security consultants can develop appropriate configuration standards if needed.
2.2.1	Implement only one primary function per server.	ProtectPoint VAM	Both the MSS and VAM can test, audit and report devices for more than one primary function. If any issues are found, the solutions log the issue, assign mitigation to appropriate personnel, and confirm the successful remediation. StillSecure security consultants can help you design server functionality and design if needed.

	PCI DSS 1.2 requirement	StillSecure solution	How StillSecure solves the requirement
2.2.2	Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function).	ProtectPoint VAM	Both the vulnerability scanning MSS and VAM can test, audit, and report on devices for unnecessary and insecure services and protocols that are enabled. If any issues are found, the solutions log the issue, assign mitigation to appropriate personnel, and confirm the successful remediation. StillSecure security consultants can help identify unnecessary and insecure services and protocols if needed.
2.2.3	Configure system security parameters to prevent misuse.	ProtectPoint Safe Access VAM	Security settings and parameters can be tested, audited and reported by the three solutions outlined to ensure compliance with this requirement. Once a posture has been chosen, StillSecure solutions can automatically (on a scheduled basis) test devices to ensure they comply with the policy. StillSecure security consultant will help configure security parameters to prevent misuse if needed.
Requirement 4: Encrypt transmission of cardholder data across open, public networks.			
4.1	Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.	ProtectPoint	StillSecure offers both SSL and IPSEC VPN services. By utilizing StillSecure ProtectPoint managed VPN services, cardholder data can be securely transmitted over open, public networks. Strong encryption capabilities with StillSecure's managed VPN services are especially important when transmitting cardholder data over a wireless segment.
4.2	Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat).	ProtectPoint Strata Guard	The ProtectPoint managed intrusion detection / prevention services and Strata Guard have rules and the ability to create customized rules to ensure that PAN data not encrypted is blocked and the transmitting device is prevented from doing so. StillSecure security consultants can design PAN transmission to ensure they are never sent in the clear if needed.
Requirement 5: Use and regularly update anti-virus software or programs.			
5.1	Deploy anti-virus mechanisms on all systems commonly affected by malicious software (particularly personal computers and servers).	ProtectPoint Safe Access VAM	StillSecure scanning and testing services can ensure on an on-going basis that all systems contain anti-virus solutions and that they are up-to-date and running. If desired, any systems without anti-virus can be denied access to the network. StillSecure's managed services, ProtectPoint, provide gateway anti-virus for email protection.

	PCI DSS 1.2 requirement	StillSecure solution	How StillSecure solves the requirement
5.2	Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	ProtectPoint Safe Access VAM	StillSecure scanning and testing services can ensure that all systems have current anti-virus DAT files and that the process is actively running. If desired with Safe Access, any systems without current or actively running anti-virus can be denied access to the network. Up-to-date gateway anti-virus services are provided by StillSecure's managed services platform.
Requirement 6: Develop and maintain secure systems and applications			
6.1	Ensure that all system components and software have the latest vendor-supplied security patches. Install critical security patches within one month of release.	ProtectPoint Safe Access VAM	A core functionality of StillSecure scanning solutions is to ensure that all systems are patched. The solutions provide tests to ensure that devices have the latest vendor patches installed. If desired, through the use of Safe Access, end users could be denied access to the network unless their devices were completely patched. Note that VAM can provide full logging and historical data confirming the remediation of any issues. Both Safe Access and VAM can provide an automated process to ensure that all relevant security patches have been installed within one month of their release. ProtectPoint managed vulnerability scanning can provide this solution as an outsourced service.
6.2	Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.	VAM	VAM and Safe Access provide a built-in vulnerability feed. This feed, created by StillSecure's Security Alert Team (SAT), provides 24x7x365 access to the latest vulnerabilities, checks for the issues, and remediation information. This feed is offered at no charge with VAM. This feed may be combined with other publicly available information to create a "super" feed of vulnerability information. This combined with a regular schedule of auditing and testing will result in compliance with this requirement.

	PCI DSS 1.2 requirement	StillSecure solution	How StillSecure solves the requirement
6.5	Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the OWASP Guide. Cover prevention of common coding vulnerabilities in software development processes, to include the following: (see list under 6.5 in the PCI DSS document)	ProtectPoint VAM (coming later in 2009)	StillSecure scanning solutions will have web application scanning capabilities later in 2009. These capabilities will include testing for cross-site scripting, SQL injection, and other web application tests.
6.6	For public facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: <ul style="list-style-type: none"> ▪ Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes ▪ Installing a web-application firewall in front of public facing web applications 	ProtectPoint VAM (coming later in 2009)	Both the ProtectPoint vulnerability scanning service and VAM will incorporate web application scanning tests later this year.

	PCI DSS 1.2 requirement	StillSecure solution	How StillSecure solves the requirement
Requirement 8: Assign a unique ID to each person with computer access.			
8.3	Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.	ProtectPoint	StillSecure's ProtectPoint managed VPN service provides two-factor secure remote access for traffic originating from outside of the network by employees, administrators, and trusted third parties.
Requirement 11: Regularly test security systems and processes.			
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).	ProtectPoint VAM	ProtectPoint managed vulnerability scanning and VAM provide vulnerability scans and then track the remediation efforts for any issues. Both StillSecure solutions can be utilized internally or externally. Most customers have used StillSecure solutions to prepare and manage remediation and then utilize a third-party service for their audit. The reports delivered by the MVS and VAM show regular scanning as well as differentials, changes, etc.
11.4	Use network intrusion detection systems, and/or intrusion prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up to date.	ProtectPoint Strata Guard	ProtectPoint managed intrusion detection/prevention services and Strata Guard, an award winning intrusion detection / prevention product, both meet the needs of this requirement. These StillSecure solutions can also be utilized to protect wireless segments as well. StillSecure security consultants can assist in placing sensors in the proper locations for compliance with this requirement.

	PCI DSS 1.2 requirement	StillSecure solution	How StillSecure solves the requirement
Requirement 12: Maintain a policy that addresses information security for employees and contractors.			
12.2	Develop daily operational security procedures that are consistent with requirements in this specification (for example user account maintenance procedures, log review procedures)	ProtectPoint Safe Access VAM	A number of best practice daily operational security procedures can be driven from StillSecure scanning and testing solutions. Safe Access provides for device compliance on a per-login basis, thus ensuring that on a continuous basis that endpoints are compliant with internal security policies. VAM and ProtectPoint scanning services provide for scheduled vulnerability scanning and remediation efforts. By utilizing StillSecure solutions, organizations can create a daily operational procedure for compliance. StillSecure security consultants can assist in developing daily operational security policy and procedures, including the use of StillSecure products and services to comply with this regulation.
12.5.1	Establish, document, and distribute security policies and procedures	ProtectPoint Safe Access VAM	Existing security policies and procedures can be audited, validated, and enforced by StillSecure solutions. All three solutions will conduct regularly scheduled, automated testing of endpoint or server security policies. Any deviations can be escalated to the appropriate personnel and remediated accordingly. In addition, if security policies and procedures do not exist, StillSecure security consultants have the expertise and experience to establish, document and distribute the applicable security policies and procedures.
12.5.2	Monitor and analyze security alerts and information, and distribute to appropriate personnel	ProtectPoint Safe Access Strata Guard VAM	StillSecure's SAS 70 Type-II SOC personnel monitor and analyze security alerts 24x7x365 for ProtectPoint managed services. In addition, all StillSecure solutions assist in monitoring for security alerts and disseminating the information to the appropriate personnel. All solutions allow for role-based access to their data and also provide for alerts via email, pagers, or phone.
12.9.1	Create the incident response plan to be implemented in the event of system breach.	ProtectPoint	StillSecure's Security Operations Center (SOC) has a detailed incident response plan for customer system breaches. This plan is based on best practices.
12.9.3	Designate specific personnel to be available on a 24/7 basis to respond to alerts.	ProtectPoint	StillSecure managed security services utilize a 24x7 staffed Security Operations Center (SOC). The SOC staff reviews alerts in real time and responds and escalates for each event based on the client's security handling policy. Customers indicate in their handling policy how the SOC is to escalate and notify. The customer may elect to be notified by email notification and/or by phone 24x7.

	PCI DSS 1.2 requirement	StillSecure solution	How StillSecure solves the requirement
12.9.4	Provide appropriate training to staff with security breach response responsibilities.	ProtectPoint	StillSecure managed security staff members are constantly trained in diagnosing and responding to security events. The central tool that the analysts use to review alerts includes features that enforce actions based on the severity of the event and the customer's security handling policy. StillSecure security consultants can train your staff on what to do in the event of a breach as well.
12.9.5	Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.	ProtectPoint Strata Guard	Data from both the ProtectPoint managed intrusion detection and prevention service and Strata Guard are maintained and can be correlated to any incident response reports.
12.9.6	Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	ProtectPoint	StillSecure's managed security services are available 24x7x365 to assist customers with incidents. StillSecure personnel often are the first line of defense during an incident and work closely with the customer through handling of the problem. StillSecure utilizes lessons learned and best practices to ensure that its procedures evolve to maintain a best in class functionality.

4. The StillSecure suite of solutions

StillSecure solutions are available as hardware appliances, managed services, or software. All solutions directly address many critical requirements within the PCI Data Security Standard. The StillSecure suite of security solutions cost-effectively mitigates the risks of network breaches and dramatically reduces costs through proactive process and automation.

Solutions include:

- **ProtectPoint**[®] —Best-in-class managed security services that protect you from Internet attack, stopping unauthorized access and preventing worms, trojans, and viruses from taking down your network. Subscription-based ProtectPoint services deliver both the technology and the round-the-clock expertise needed to protect your network and bring you into compliance with data security policies. Services include managed intrusion detection/prevention, gateway anti-virus, VPN, content filtering, anti-spam, and many others.
- **Safe Access**[®] —Awarded the Best Endpoint Security Solution 2006 and 2008 by SC Magazine (and named an SC Magazine 'Best Buy'), Safe Access protects the network by ensuring endpoint devices are free from threats and in compliance with security policies before they are allowed on the network.
- **VAM**[®] —Our award-winning vulnerability management platform identifies, tracks, and manages the repair of network vulnerabilities across the enterprise. VAM manages the vulnerability management lifecycle from end to end, mitigating the risk of network exploitation and compromise.
- **Strata Guard**[®] —Strata Guard is an award-winning family of network-based intrusion detection/prevention systems (IPS/IDS) that provide real-time, zero-day protection from network attacks and malicious traffic. Strata Guard also can be utilized in a "post-connect" NAC scenario to quarantine devices generating malicious traffic.

Visit www.stillsecure.com to learn more about StillSecure products.

5. About StillSecure

StillSecure delivers comprehensive network security that protects organizations from the perimeter to the endpoint. Offering both products and managed security services, StillSecure enables customers to affordably deploy the optimal blend of technologies for locking down their assets and complying with security policies and regulations. StillSecure customers range from mid-market companies to the world's largest enterprises and agencies in government, financial services, healthcare, education, and technology. For more information please call (303) 381-3830, or visit <http://www.stillsecure.com>.