

StillSecure PCI Complete[™]

Fully Managed PCI Compliance Solution

PCI Requirements Coverage Summary Table

June 2011

Table of Contents

Introduction.....	2
Coverage assumptions for PCI Complete deployments	2
Solution Overview: People, Process, and Technology	2
About StillSecure.....	3
Summary Table of PCI Requirements Met by StillSecure PCI Complete.....	4

Introduction

StillSecure's PCI Complete™ managed security solution, in conjunction with StillSecure partners, helps merchants and service providers comply with all portions of PCI. This summary table (page 4) describes how StillSecure's PCI Complete security solution meets specific PCI compliance requirements and minimizes the risk and liability from network attacks.

Coverage assumptions for PCI Complete deployments

There are 176 total PCI requirements. The StillSecure PCI Complete solution, when deployed in a PCI-compliant datacenter or Section 9 compliant facility, when utilized according to StillSecure's QSA certified process, will provide compliance coverage for up to 165 of these, or 94% of the total. We provide this level of coverage based on the assumption that the customer will not deviate from the QSA certified process and will take responsibility for ensuring the following basic requirements, which constitute the remaining 6%:

- Standard policies are in place for passwords, messaging, and hiring.
- Anti-virus and personal firewall software are deployed.
- WPA or WPA2 wireless security is implemented for all wireless access points.
- The customer adheres to PCI coding standards for their custom code.
- Any hosting providers used by the customer are PCI compliant.
- All point of sales systems are PA-DSS compliant and store and display credit card information masked or encrypted.
- The customer uses a unified authentication system like Active Directory or LDAP.

If the customer meets those assumptions, 100% of the PCI Requirements are covered.

Solution Overview: People, Process, and Technology

PCI Complete helps organizations comply with all 12 PCI provisions. The solution is affordable, highly automated, and fully managed by StillSecure's staff of security experts. The solution is a combination of technology, process, and expert personnel. It is designed specifically to protect organizations from malicious attacks and reduce the risk and liability of electronic fraud while assuring compliance with all PCI DSS requirements.

Systems

The PCI Complete solution meets the technological

requirements of the PCI DSS by bundling the following managed services:

- Firewall
- Intrusion Detection and Prevention System
- SSL and IPsec VPN
- Multi-Factor Authentication
- Internal PCI Vulnerability Scanning
- Internal Penetration Testing
- External ASV Vulnerability Scanning
- External ASV Penetration Testing
- Web Application Firewall
- File Integrity Monitoring
- Log Management and Monitoring

Process

The PCI Complete solution combines the following policies, procedures, and facilities to meet the process requirements of the PCI DSS:

- Network segmentation
- Change control management
- Daily event review of all security event log files
- 6 month firewall and Web app firewall rule configuration reviews
- Alert escalation procedures
- Incidence response procedures
- 24x7x365 QSA Approved and SAS 70 type II audited security operations center (SOC)

Personnel

The PCI Complete solution is fully managed and monitored by StillSecure security analysts on a 24x7x365 basis. These security experts are located in our redundant security operations centers in Florida and Colorado. Our analysts are dedicated security experts whose only responsibility is to monitor and manage network security for our customers. They are:

- Customer service focused, and responding rapidly to security events and customer inquiries (adhering to our "3rd -ring service" policy for handling incoming calls).
- A highly trained team that understands security and the costs and challenges associated with PCI compliance
- PCI experts, capable of helping you implement all facets of your PCI compliance program.

Real-time transparency into these services, processes, and policies is available to authorized customer personnel and auditors through our secure RADAR™ customer portal.

QSA Approved

The StillSecure PCI Complete service has achieved a PCI

Report on Compliance. All security controls implemented with PCI Complete, including all systems, processes, and personnel, have been scrutinized, tested, and approved for conformance with PCI requirements 1 through 12 by a Qualified Security Assessor (QSA). Therefore, a customer's cardholder data environment will inherit these controls when their systems are protected by PCI Complete. Clear evidence that the security controls are effective 24x7x365 is available through our RADAR customer portal, making the customer's PCI audit or self-assessment much more efficient and cost effective. You can rest assured that our service will allow you to pass the PCI DSS.

About StillSecure

At StillSecure, we believe IT executives should be able to focus on driving the success of their company versus being distracted by security and compliance demands.

For IT executives facing escalating security threats and evolving compliance requirements, and data centers looking to cement long-term customer relationships, StillSecure designs and delivers managed network security and certified compliance solutions so you can focus on growing your core business.

For IT executives facing escalating security threats and evolving compliance requirements, and data centers looking to cement long-term customer relationships, StillSecure designs and delivers managed network security and certified compliance solutions so you can focus on growing your core business.

Headquartered in Superior, Colorado, StillSecure protects some of the most sensitive and important computer networks in the world.

For more information please call (303) 381-3830, visit <http://www.stillsecure.com>, or check out more on the StillSecure blog at <http://www.thesecuritysamurai.com>.

Summary Table of PCI Requirements Met by StillSecure PCI Complete

The PCI requirements that StillSecure's PCI Complete addresses is summarized below. The table also presents the responsibilities of the customer and the PCI-compliant datacenter or facility for meeting the level of PCI requirements coverage discussed above.

PCI requirement	StillSecure PCI Complete coverage	Partner / hosting provider responsibility	Customer responsibility
Requirement 1 <i>Install and maintain a firewall configuration to protect cardholder data</i>	<p>Firewall Service: Provides implementation of ingress/egress stateful firewall, NAT, and DMZ to prevent access from public, untrusted, and wireless networks.</p> <p>File Integrity Monitoring Service: Checks that the current, running and backup configurations for all routers and switches are in synch.</p> <p>Documentation Process: Maintains a detailed diagram of the network architecture showing all connections, wireless devices, ingress, and egress points within the cardholder environment (CDE). Also, maintains a list of all connections to the CDE that is reviewed quarterly for differences from the results of the vulnerability scan.</p> <p>Configuration Change Control Process: Handles changes, control, and testing of firewall configuration modifications as well as documentation of business justification for all allowed traffic. The system maintains administrator roles and responsibilities for network components. Includes a quarterly review of firewall rules and network documentation.</p>		<p>Requirement 1.4 Customer must install and maintain personal firewall software for all mobile devices connecting to the CDE.</p> <p>Note: PCI Complete will check that the firewall software is installed and enabled.</p>
Requirement 2 <i>Do not use vendor-supplied defaults for system passwords and other security parameters</i>	<p>Internal PCI Vulnerability Scanning Service: Checks for the use of default vendor passwords, community strings, and unnecessary user accounts. Checks that each server has only one primary function and unnecessary services are disabled. Ensures all non-console access uses secure, patched, and encrypted protocols.</p> <p>VPN Service: All non-console administrator access is encrypted using an SSL tunnel. For devices that StillSecure manages, the tunnel is established with the StillSecure SOC ensuring that all management activities are encrypted. For other devices within the CDE, the VPN service is used to connect and encrypt all management traffic to and from the CDE.</p> <p>Documentation Process: Provides the ProtectPoint Standard Configuration</p>		<p>Requirement 2.1.1 Ensure that the wireless security settings are configured according to the requirements.</p> <p>Requirements 2.2.3 and 2.2.4 Devices managed by the customer must conform to the Standard Configuration Hardening process.</p> <p>Requirement 2.4 Ensure that all other shared hosting</p>

PCI requirement	StillSecure PCI Complete coverage	Partner / hosting provider responsibility	Customer responsibility
	Hardening process for all devices deployed into the CDE. HTML and PDF reports of vulnerabilities are maintained on the RADAR portal.		providers conform to PCI requirements if they store, process, or transmit cardholder data.
Requirement 3 <i>Protect stored cardholder data</i>	PCI Network Analysis Consultation: Checks that PCI card holder information is encrypted or masked where required and that the database contains only permissible data.		Requirement 3 The customer must ensure that their credit card storage and point of sales systems encrypt data and manage encryption keys in a compliant manner. Requirement 3.1 Check card holder data retention policy.
Requirement 4 <i>Encrypt transmission of cardholder data across open, public networks</i>	VPN Service: Provides strong encryption via IPSEC or SSL VPN connections across open or public networks. Site-to-site or personal VPN connections can be established depending on the customer's network architecture. Firewall Service and Change Control Process: Ensures that messaging protocols are not transmitted in and out of the CDE. Documentation Process: Provides a template for messaging policies. Web Application Firewall and Intrusion Detection and Prevention Service: Detects if credit cards are transmitted unencrypted. Escalation Process: If a detected credit card leak indicates a possible security breach, the escalation procedures are initiated.		Requirement 4.1 If a customer uses a communication mechanism that is not natively encrypted, they must ensure the payload of the transmission is encrypted. Requirement 4.1.1 Ensure their wireless network uses secure practices.
Requirement 5 <i>Use and regularly update anti-virus software or programs</i>	Internal PCI Vulnerability Scanning Service: Checks that all antivirus software is installed, DAT files are up-to-date, and a full system scan has been completed recently. File Integrity Monitoring Service and Email Security Gateway Service: For		Requirement 5.1 Deploy antivirus software on all systems within the CDE for which normal antivirus technologies apply.

PCI requirement	StillSecure PCI Complete coverage	Partner / hosting provider responsibility	Customer responsibility
	<p>systems that do not support normal antivirus technologies, the File Integrity Monitoring service and agent and Email Security Gateway Service can supplement this requirement.</p> <p>Log Management Service: Monitors the antivirus software logs to detect and alert on any antivirus system operational failures or viruses found.</p> <p>Standard Configuration Hardening Process: This process ensures that all systems deployed within the CDE have antivirus software installed or a file integrity monitoring agent if the system does not support standard antivirus technologies.</p>		
<p>Requirement 6 <i>Develop and maintain secure systems and applications</i></p>	<p>Internal and External PCI Vulnerability Scanning Service: Provides scanning for up-to-date vendor-supplied security patches, web application vulnerability scanning, penetration testing, and a process for remediation of found vulnerabilities. Scan can be performed before and after a web application is deployed. The StillSecure Security Alert Team (SAT) monitors many source sites for new vulnerabilities and creates and deploys new scans within 24 to 48 hours depending on the severity of the vulnerability.</p> <p>Web Application Firewall Service: Provides ongoing protection against web application threats for public-facing applications. The rules for protection include coverage of all vulnerabilities listed in the OWASP Top Ten and PCI DSS v1.2 requirements 6.5.1-6.5.10.</p> <p>Configuration Change Control Process: The ProtectPoint configuration change control process is used to document all changes to web applications and promotion of code into the production environment.</p>	<p>Secure Coding Training: StillSecure partner provides training on best security practices for developing web applications as well as in-depth code security audits prior to application deployment.</p>	<p>Requirements 6.3 and 6.4 Ensure software developers understand policy and best practices for secure software application development.</p>
<p>Requirement 7 <i>Restrict access to cardholder data by business need to know</i></p>	<p>VPN and Firewall Service: These services are used in conjunction to authenticate access into the CDE and limit the resources for which each user has access.</p> <p>ProtectPoint SOC Change Request Process: The change request process is a structured procedure to ensure that only authorized administrators can grant, change, or terminate user access to the CDE and users are limited to least privilege access according to job function.</p>		<p>Requirement 7.1 If a customer does not use a single unified authentication and authorization process, the customer is responsible for ensuring users have access to the CDE on a need-to-know and least-privilege basis.</p>

PCI requirement	StillSecure PCI Complete coverage	Partner / hosting provider responsibility	Customer responsibility
			Requirement 7.1.2 Conform to PCI when choosing employees who can access cardholder data.
Requirement 8 <i>Assign a unique ID to each person with computer access</i>	<p>Multi-Factor Authentication Service: Provides multi-factor authentication using hardware and software tokens, certificates, and user name and password mechanisms for all remote or internal access to PCI environment. Integration with common services such as VPN, database, and web applications.</p> <p>VPN and Firewall Service: These services are used in conjunction to authenticate access into the CDE and limit the resources for which each user has access. For remote access the VPN service is used in conjunction with the Multi-Factor Authentication Service using secure tokens, username/password, and SSL certificates for unique identification.</p> <p>ProtectPoint SOC Change Request Process: The change request process is a structured procedure to ensure that only authorized administrators can grant, change, or terminate user access to the CDE and users are limited to least privilege access according to job function.</p>		Requirement 8.5 For customer managed devices, applications, and databases, the customer must ensure these systems conform to least-privilege user authorization and authentication.
Requirement 9 <i>Restrict physical access to cardholder data</i>		PCI Certified Data Centers and Hosting Provider: Provided in conjunction with our Data Center and Provider partners, StillSecure offers PCI requirement 9 certified rack and virtualized environments.	Requirement 9 Ensure that all customer managed physical environments conform.
Requirement 10 <i>Track and monitor all access to network</i>	Log Management Service: Provides daily event reviews for all ProtectPoint and 3 rd party security logs. Also provides log retention to track user access and actions within individual systems components and retains the required audit trail entries.		

PCI requirement	StillSecure PCI Complete coverage	Partner / hosting provider responsibility	Customer responsibility
<i>resources and cardholder data</i>	<p>Provides internal centralized log storage, secured audit trails, and forensic information. Retains audit trail history for a minimum of 1 year, with 3 months available for immediate analysis.</p> <p>NTP Service: Provides synchronized time for all systems and log entries to enable accurate audit and forensics.</p> <p>File Integrity Monitoring Service: Provides file integrity checks on critical audit trail log files.</p>		
<p>Requirement 11 <i>Regularly test security systems and processes</i></p>	<p>Internal and External PCI Vulnerability Scanning Services: Provides internal and external network vulnerability scans, penetration testing, and web application vulnerability testing performed by a qualified ASV at least quarterly and when there are significant changes to the network.</p> <p>IDPS Service: Provides monitoring of traffic and 24x7x365 response to attacks.</p> <p>File Integrity Monitoring Service: Provides file integrity checks for all critical systems at least weekly for critical system files, registries, configuration files, and content files.</p>		<p>Requirement 11.1 Perform tests for rogue wireless devices on your network.</p>
<p>Requirement 12 <i>Maintain a policy that addresses information security for employees and contractors</i></p>	<p>24X7X365 Incidence Response SOC: Our SOC provides an incidence response plan and action for any issue detected from security tools we are monitoring.</p> <p>Documentation Process: Provides usage and operational security policy templates and an incident response plan. Provides a checklist for all policies that must be implemented by the customer and disseminated to employees.</p> <p>Risk Assessment Consultation: Provides an annual network analysis to identify threats and vulnerabilities resulting in a formal risk assessment.</p>		<p>Requirement 12.5 Assign a team to security responsibilities.</p> <p>Requirement 12.6 Tailor policy templates to organization requirements and disseminate policies to employees.</p> <p>Requirement 12.7 Screen potential employees.</p> <p>Requirement 12.8 Check PCI compliance of other service</p>

PCI requirement	StillSecure PCI Complete coverage	Partner / hosting provider responsibility	Customer responsibility
Additional Services	PCI Network Analysis Consultation: Provides network analysis to identify PCI resources, determines what technologies need to be deployed where, and provides a plan for network segmentation using firewall, VPN, and access control services to reduce the scope of PCI on your network. This service puts your network in a place that it can reach PCI compliance and reduces the cost of an audit significantly.		providers.

