Data Sheet: IT Compliance

Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI, or PCI DSS) was developed by the PCI Security Standards Council to assure cardholders that their details were secure during payment card transactions. The Council, which now governs the Standard, was founded by a group of major payment card providers (VISA, MasterCard, JCB, Discover and American Express). It provides a single consistent standard for the protection and security of sensitive cardholder data. Demonstrating PCI compliance is a continuous process, validated annually: Assess – Remediate – Report, and hence requires a sustainable compliance program.

What is the scope of Payment Card Industry Security Standard?

The PCI standard represents security best practices and is wide ranging, detailed and prescriptive. It makes a number of demands in areas including IT infrastructure, security policies and data encryption. The standard is organized into 6 categories of 12 security requirements. These are listed below:

Build and Maintain a Secure Network	• **Requirement 1**: Install and maintain a firewall configuration to protect cardholder data • **Requirement 2**: Do not use vendor supplied defaults for system passwords and other security parameters
Protect Cardholder Data	• **Requirement 3**: Protect stored cardholder data • **Requirement 4**: Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	• **Requirement 5**: Use and regularly update antivirus software • **Requirement 6**: Develop and maintain secure systems and applications
Implement Strong Access Control Measures	• **Requirement 7**: Restrict access to cardholder data by business need-to-know • **Requirement 8**: Assign a unique ID to each person with computer access • **Requirement 9**: Restrict physical access to cardholder data
Regularly Monitor and Test Networks	• **Requirement 10**: Track and monitor all access to network resources and cardholder data • **Requirement 11**: Regularly test security systems and processes
Maintain an Information Security Policy	• **Requirement 12**: Maintain a policy that addresses information security

Who is affected?

Any merchant, service provider or other organization that stores, processes or transmits cardholder (Primary Account Number) data is required to implement PCI.

Non-compliance can result in fines and other penalties, including forfeiture of the right to process card transactions, perhaps permanently. In addition, non-compliance can invite the attention of damaging negative publicity, lawsuits, loss of business and market share.

What is the current driver?

In September 2008 Visa Europe released revised guidelines for penalties that will affect merchants and service providers post data security breach. These penalties apply to all levels of merchants and service providers but are predominantly focused at driving compliance for e-commerce merchants in the level 2, 3 and 4 categories. The scale of the penalties has resulted in many smaller merchants' directly addressing PCI compliance and looking to external organizations to help them become compliant through consultancy services.

Symantec products for Payment Card Industry Data Security Standard

Often when customers contact Symantec regarding products to help with PCI compliance, they have a specific pain point in mind that relates directly to a particular requirement of the PCI standard. For example, they may have an issue with centralised log management (which relates to requirement 10 of the PCI standard), securing critical assets (which relates to requirements 2, 8, 10 & 12) or policy creation and management (which relates to requirement 12).

Symantec has a range of products to help with these issues. To make it easier for customers to identify the correct product or products, Symantec has mapped each of its products against the PCI standard. The table below shows the mapping of some customer's requirements to Symantec products and how they relate to the PCI standard.

Customer Requirement	PCI DSS Requirement	Symantec Product
Antivirus	Requirement 5	Symantec Endpoint Protection
Securing critical assets, alerting, intrusion detection/ prevention, and integrity file monitoring	Requirement 2, 8, 10, 11, and 12	Symantec Critical System Protection
Centralized log management, information security management, and alerting	Requirement 10	Symantec Security Information Manager
Policy and compliance management	Requirement 6, 8, 9, and 12	Symantec Control Compliance Suite
Identification and protection of credit card data	Requirement 3 and 4	Symantec Data Loss Prevention
Gateway and network control	Requirement 4	Symantec Gateway Security products
Network access control	Requirement 1	Symantec Network Access Control
Security information alerting/knowledge	Requirement 12	Symantec DeepSight Services
Backup and protection of credit card data	Requirement 3	Symantec Enterprise Vault
Gateway and network control	Requirement 1 and 12	Symantec Managed Security Services (IDS/firewalls, etc.)
Network configuration, application management, server management, and asset management	Requirement 1, 2, 6, and 8	Altiris product family from Symantec

How can Symantec help?

PCI Requirements	Solutions	Products
Build and Maintain a Secure Network	Endpoint protection	Symantec Network Access Control, Symantec Endpoint Protection, Critical System Protection
Protect Cardholder Data	Entitlements	Control Compliance Suite, Critical System Protection
	Data loss prevention	
	Access controls	Symantec Data Loss Prevention
	Data identification/classification	
Maintain a Vulnerability Management Program	Configuration management	Altiris suites and solutions
	Vulnerability management	Control Compliance Suite
Implement Strong Access Control Measures	Endpoint protection	Control Compliance Suite, Critical System Protection
	Configuration management	Symantec Endpoint Protection
Regularly Monitor and Test Networks	Vulnerability scanning	Symantec Security Information Manager
	Logging and incident response	Control Compliance Suite, Critical System Protection
Maintain an Information Security Policy	Disseminating policies	Control Compliance Suite
	Ensuring compliance with policies	

Symantec Product Definitions

Symantec™ Endpoint Protection

Symantec Endpoint Protection combines Symantec AntiVirus™ with advanced threat prevention to deliver unmatched defense against malicious attacks for laptops, desktops and servers.

Symantec™ Critical System Protection

Symantec Critical System Protection provides proactive Host Intrusion Protection through exploit prevention, endpoint controls, along with Host Intrusion Detection based security monitoring and auditing to help ensure server integrity and compliance across heterogeneous platforms.

Symantec™ Security Information Manager

Symantec Security Information Manager enables organizations to apply a documented, repeatable process for responding to security threats and addressing IT policy compliance via a comprehensive incident management program.

Symantec™ Control Compliance Suite

Symantec Control Compliance Suite provides end-to-end coverage for the IT compliance lifecycle, including policy management, technical and procedural controls assessment, reporting and remediation.

Symantec Brightmail Gateway

The Symantec Brightmail Gateway delivers inbound and outbound messaging security for email and IM, with effective and accurate antispam and antivirus protection, advanced content filtering, and data loss prevention technology.

Symantec™ Network Access Control

Symantec Network Access Control is a complete end-to-end network access control solution which securely controls access to corporate networks, enforces endpoint security policy and easily integrates with all existing network infrastructures.

Symantec™ Data Loss Prevention

Symante Data Loss Prevention enables customers to discover and mange data whether it is stored on the network or on a disconnected endpoint, as well as prevent data from exiting any network gateway or endpoint.

Symantec DeepSight™ Services

Symantec Global Intelligence Services provide insight into the latest global, industry and local threats and attacks so organizations can respond proactively to emerging threats.

Symantec Enterprise Vault™

Symantec Enterprise Vault is the industry's leading platform for archiving from email, file system, and collaborative environments.

Symantec™ Managed Security Services (IDS/firewalls etc.)

Symantec Managed Security Services delivers real-time security protection, helping organizations establish compliance, minimize business impact, and reduce overall security risk at acceptable cost in the face of today's emerging threats.

Altiris Product Family from Symantec

The Altiris product family addresses four fundamental components of lifecycle management: Client management, server management, service desk and IT asset management.

Summary

- PCI is critical to many customers today – PCI compliance cannot be ignored
- Symantec products help customers to achieve a sustainable and cost-effective response to PCI compliance requirements
- Symantec products are backed by Symantec's considerable breadth and depth in security consultancy, managed security services, industry-leading security research, security assessments, and best-in-class IT products

Visit our website

www.symantec.com/pci

To speak with a Product Specialist in the U.S.

Phone: +44 (0) 118 943 6363

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

Symantec World Headquarters

20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

02/09 20011544

Confidence in a connected world.