

Rapid PCI Compliance and Security for Large Retailers

*How Fortinet provides Security, Compliance and New
Services in One Cost-Effective Solution*

White
Paper



Security, Compliance, and New Services in One Solution

FORTINET[™]

Executive Summary

The Payment Card Industry Data Security Standard (PCI) provides broad requirements for securing personal nonpublic information used on digital technology in retail. PCI is a self-governing standard devised by the world's largest credit card providers including VISA, MasterCard and American Express. Retail companies that process credit card information are required to implement best practices and technologies to secure this information. Other sectors have similar requirements such as HIPAA for healthcare, Gramm-Leach-Bliley for financial services, and FISMA for federal government agencies. As with those standards, no one security product alone is adequate for full PCI compliance so retailers can usually be assured of juggling many technologies to secure and comply across hundreds or thousands of stores. By using an all-in-one security device that integrates the most important technologies, retailers can comply faster with PCI – and achieve comprehensive security. Fortinet provides the integrated means for rapid PCI compliance with an integrated multi-threat device for security that is easy to deploy, easy to manage, and automatically aware of blocking the latest threats.

Strengthening Retail Data Security with PCI

The leading credit card providers have several objectives for PCI. One is protecting consumer confidence in the credit card industry. Another is to certify that retailers have done their best to ensure the safety and privacy of customers' nonpublic personal information. By following best security practices and using appropriate technology for PCI compliance, retailers can concurrently create an environment of information security that will repel attacks and actually protect customer data.

There is enormous pressure on retailers to ensure safety and privacy of customer information. Private information about more than 90 million individuals was breached from February 2005 through July 2006, according to the Privacy Rights Clearinghouse. Almost every week the news reveals yet another breach, which attests to the continued lack of serious effort by many organizations to implement basic best practices that secure personal information in databases. Many industry sectors are subject to regulations for securing these data, such as Gramm-Leach-Bliley, HIPAA and others. These standards all aim to raise the quality of information security to create stronger protection for consumer data.

PCI is just starting to get traction among retailers. It was initiated by VISA in 2001 and merged with a similar program by MasterCard in 2004. As of summer 2006, only about 20 percent of the largest retail organizations processing credit card transactions are in full compliance with PCI, according to VISA. Anecdotal evidence suggests compliance might be closer to one in 10. Some observers say PCI is too complex for retailers, or in some cases is overly specific in technical requirements. A big challenge for retailers is effectively deploying a myriad of best practices and technologies for security in hundreds or even thousands of stores. As is typical for retail, remote stores often lack resources and employees with technological wherewithal to install and manage security solutions.

Nevertheless, the stakes for PCI compliance are high. Retailers that do not comply may receive financial penalties and could be decertified for processing credit card transactions.

The first step in achieving PCI compliance is to understand what the standard expects of retailers. By comparing PCI specifications with existing security policy and solutions, a retail organization can devise an action plan for compliance.

What PCI Specifies for Retailers

The PCI standard includes six broad themes with 12 supporting requirements for networks and applications. Some specifications are for following well-established best practices for information security. Examples include specific guidance on use of passwords or what kind of customer information may or may not be stored in a database, instructions on where to store the data, and directives to purge obsolete data. Other specifications are for use of

Benefits of PCI Compliance	
Everyone	<ul style="list-style-type: none"> • Limited risk • More confidence in the payment industry
Member	<ul style="list-style-type: none"> • Protected reputation
Merchant & Service Provider	<ul style="list-style-type: none"> • Competitive edge gained • Increased revenue and improved bottom line • Positive image maintained • Customers are protected
Industry	<ul style="list-style-type: none"> • "Good security neighbors" encouraged
Consumer	<ul style="list-style-type: none"> • Information is safeguarded • Identity theft prevention

Privacy Rights Clearinghouse reference:
<http://www.privacyrights.org/ar/ChronDataBreaches.htm>

particular security technologies that address various weaknesses in the information infrastructure, such as deploying firewalls to regulate IP packet flow through the network.

The general themes and requirements of PCI are listed below. Requirements specifically met by various features of Fortinet are in italics. See www.visa.com/CISP for more background and downloads about the general PCI standard.

Build and Maintain a Secure Network

1. *Install and maintain a firewall configuration to protect data*
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored data
4. *Encrypt transmission of cardholder data and sensitive information across public networks*

Maintain a Vulnerability Management Program

5. *Use and regularly update anti-virus software*
6. *Develop and maintain secure systems and applications*

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. *Track and monitor all access to network resources and cardholder data*
11. *Regularly test security systems and processes*

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

All merchants and service providers processing credit card transactions must comply with PCI. Requirements vary slightly depending upon which of four levels a merchant falls under based on total number of credit card transactions processed each year. Validation actions for compliance include:

- On-Site Security Audit (usually an annual requirement for larger organizations)
- Self-Assessment Questionnaire (usually an annual requirement for smaller organizations)
- Network Vulnerability Scan (usually a quarterly requirement)

Credit card issuers and acquirers must also identify and review the list of all third-party service providers that they use or are used by their merchants and ensure they are PCI compliant.

“We selected Fortinet’s integrated network security systems because they not only provided the best functional range—including antivirus, firewall, VPN, IPS, content filtering and traffic shaping—they also offered the best price-performance.”

*– Antonia Ebner, Head of IT Dept.
Pierre Lang Jewelers*

The PCI Security Audit

PCI self-audit procedures are explained in the *Payment Card Industry Security Audit Procedures* manual on the MasterCard International Site Data Protection web site:

https://sdp.mastercardintl.com/doc/pci_audit_procedures.doc

Requirements for Securing Large Retail Operations

Fulfilling requirements for PCI compliance can simultaneously create stronger information security for retailers who follow best practices and implement appropriate security solutions. There is nothing particularly unusual about technical security requirements for retail stores. While computing there is on a smaller scale compared to the corporate headquarters, the basic needs for protection from hazards transmitted over the Internet are similar. Typical security applications and functionality necessary for retail stores include:

Antivirus Gateway. Detects and eliminates viruses, worms and spyware in real time. Scans incoming and outgoing email attachments, FTP, and HTTP traffic.

Firewall. Inspects content in network packets to ensure no unauthorized traffic passes into or out of the intranet. With adequate performance, a firewall can be deployed in-line for real-time protection.

Intrusion Detection and Prevention. Stops attacks at network perimeter by analyzing traffic for worms, viruses and other hazards. Analysis techniques include behavior-based learning and heuristics in addition to signatures defining known hazards.

VPN. Enables secure communications tunnels across the public Internet between computing devices. With adequate performance, a VPN can authenticate users, encrypt data and manage sessions.

Antispam. Eliminates entry to the intranet of junk email, file attachments and web access of blacklisted websites, domains and key words.

Web-based Content Filtering. Processes all Web content to block inappropriate material and malicious scripts from Java Applet, Cookies and ActiveX scripts entering the intranet. Assures improved productivity by minimizing time wasted on non-business use of the network.

Vulnerability Scanning. This automated process checks network devices and applications to identify and rank the severity level of known vulnerabilities caused by unpatched software, misconfigurations and other causes. Scan reports provide a blueprint to remove vulnerabilities for stronger security.

All these security applications can and should be installed at every retail network endpoint. The biggest challenge is operational – how to deploy them and manage their use in a cost-effective manner.

Fortinet Secures Large Retail Operations

The most difficult security challenge for retailers is to cost effectively implement applications across multiple stores. Staff and resources are usually stretched too thin. Ease of centrally administrating security is crucial given the limited technical experience of a typical store clerk. As a specialist to the retail sector, Fortinet has globally helped secure tens of thousands of stores in large retail organizations with its family of integrated multi-threat security solutions.

Fortinet's integrated security gateway appliance merges all security applications into one high-performance box and is the leading solution in the multi-threat security market. It provides the benefits of an appliance but easily scales to hundreds or even thousands of stores. The Fortinet architecture fully integrates all security functions, including data synthesis and centralized management of all devices. Appliances from Fortinet uniquely use ASIC acceleration technology to power all security applications in one convenient device. Fortinet's integrated multi-threat solutions cost less to operate and manage than point appliances and servers. Fortinet includes optional fault-tolerant configurations to eliminate any point of failure.

"Simple, centralized management and automatic updates using Fortinet's FortiProtect service make this a great hands-off experience for us."

— Jeff Nelson, IT Director
Jenny Craig

Fortinet Provides Key Integrated Technologies Required for PCI Compliance

Fortinet's family of integrated multi-threat appliances provide large retailers with a convenient, cost-effective way to rapidly comply with PCI while deploying effective information and network security. The appliances include a wide array of security services built into an all-in-one box. Several specifically contribute to specifications for PCI compliance; associated PCI requirements are noted in parentheses:

- Antivirus Gateway (Requirement 5)
- Firewall (Requirement 1)
- Intrusion Detection and Prevention (Requirement 11)
- VPN (Requirements 2 and 4)
- Antispam (Requirement 5)
- Web-based Content Filtering (Requirements 5 and 6)
- Vulnerability Scanning (Requirement 11)
- Timely Patching (Requirement 6)

Ensuring the security of network-attached systems in large-scale retail is essential for PCI compliance, and the safety of ongoing operations and private customer information. There is a high overhead cost associated with using best-of-breed server-based applications or with numerous point solution appliances for information security. By contrast, an integrated multi-threat security architecture is simple and easier to deploy and manage – especially for businesses with hundreds of retail establishments and limited technical resources at each site. Multi-threat is the only architecture that enables automated reporting of enterprise security performance and provides for the fastest response to new vulnerabilities. Total cost

of operations is also much lower with multi-threat appliances. The total cost of ownership for Fortinet’s solution in a network of 250 retail stores is about one-fourth the costs of server-based or point appliance solutions.

Fortinet Meets Key Criteria for Multi-Threat Appliances

- ✓ **Data Protection & Access Control** – Integrates all major security applications in one device.
- ✓ **Maximum Up-Time** – Fail-safe configurations ensure non-stop security of network operations.
- ✓ **Deployment** – Rapid implementation and easy, centralized management.
- ✓ **Compliance** – Comprehensive features bring compliance for key requirements of PCI.
- ✓ **Hot Spot Wireless** – Integrated wireless access with security gateway.

Rapid implementation of security with Fortinet’s solution also allows large retail organizations to quickly go after new retail business opportunities that rely on a secure networking infrastructure. Examples include wireless hot spots for customer internet access from retail sites; wireless point-of-sale for more efficient transactions and inventory tracking; internet telephony services; and other emerging applications such as Radio Frequency Identification (RFID) tracking, in-store rich media, wireless barcode and kiosks, and remote store operations monitoring. All these benefits are available with Fortinet’s solution in addition to compliance with PCI.

Summary

We invite your organization to investigate the benefits of using Fortinet’s solution for securing retail operations, and for compliance with the PCI security standard. For more information on Fortinet’s all-in-one retail security solutions, please contact your trusted security solution provider or call us directly at 866.868.3678 / +1 408.235.7700.



About Fortinet

Fortinet is the pioneer and leading provider of ASIC-accelerated multi-threat security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection--including firewall, antivirus, intrusion prevention, Web content filtering, VPN, spyware prevention and antispam--providing customers a way to protect multiple threats as well as blended threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified eight times over by the ICSA (firewall, antivirus, IPSec, SSL, IDS, client antivirus detection, cleaning and antispayware). Fortinet is privately held and based in Sunnyvale, California.

FORTINET

1090 Kifer Road, Sunnyvale, CA 94086 USA
 Tel +1-408-235-7700 Fax +1-408-235-7737
 www.fortinet.com

©2006 Fortinet, Inc. All rights reserved. Fortinet, FortiGate, FortiOS, FortiAnalyzer, FortiASIC, FortiLog, FortiCare, FortiManager, FortiWiFi, FortiGuard, FortiClient, and FortiReporter are registered trademarks of the Fortinet Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. Licensed under U.S. Patent No. 5,623,600

WPR126-0806-R1