FORTINET

WHITE PAPER

Assessment Readiness for Payment Card Industry Data Security Standard (PCI DSS v1.2) Compliance

Contents

Introduction

Retailers that fail Payment Card Industry Data Security Standard (PCI DSS) assessments can be fined up to $500,000. Additional penalties can range from increased assessment requirements to retraction of credit card processing privileges. Generally, retailers that process over 20,000 credit card transactions per year must fill out an annual self-assessment and conduct quarterly network scans by an approved vendor. Retailers that process over 6 million credit card transactions per year are also subject to annual on-site assessments. While on the surface the PCI standard seems straight forward, upon deeper inspection in preparation for an on-site assessment, compliance can become more complicated.

PCI DSS is an important challenge not only for U.S. Retailers, but also for any organization that holds, processes or passes cardholder data from any of the participating branded cards, including Visa International, MasterCard Worldwide, American Express, Discover Financial Services and JCB International. For instance in Canada, to achieve compliance with the Visa Account Information Security (AIS) Program, merchants and service providers must also adhere to PCI DSS.

A few strategic security investments at the network and application layer security can significantly simplify PCI DSS compliance, while maintaining cost-efficiency. This paper highlights top reasons for assessment failure or security breach, and outlines a better way to secure your payment card infrastructure. It will discuss leveraging a Unified Threat Management (UTM) approach with an integrated Vulnerability Management (VM) strategy within an ISO/IEC 27001/2 Information Security Management System (ISMS) framework that supports critical PCI compliance criteria.

PCI DSS Requirements

PCI DSS consists of 6 control objectives and 12 requirements. This standard encompasses a group of principles for security management, policies, procedures, network architecture, software design and other critical protective measures. Fortinet provides a unified multi-threat management system with solutions and professional services to simplify PCI assessment readiness.

PCI DSS CONTROL OBJECTIVES		
CONTROL OBJECTIVE	REQUIREMENT	FORTINET SOLUTION
1. Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data	• FortiGate integrated firewall
	2. Do not use vendor-supplied defaults for system passwords and other security parameters	• FortiDB vulnerability management • FortiScan OS vulnerability management • FortiWeb web application password checking
2. Protect Cardholder Data	3. Protect stored cardholder data	• FortiDB vulnerability management • FortiWeb web application firewall
	4. Encrypt transmission of cardholder data across open, public networks	• FortiGate IPSec VPN
3. Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by malware	• FortiGate integrated AV • FortiClient integrated AV • FortiMobile integrated AV • FortiMail integrated AV • FortiGuard automated AV updates
	6. Develop and maintain secure systems and applications	• FortiGate integrated network vulnerability scanning for remote locations • FortiDB vulnerability management • FortiWeb web application security

		• FortiScan OS vulnerability management • FortiAnalyzer network vulnerability scanning for centralized locations
4. Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know	• FortiDB vulnerability management
	8. Assign a unique ID to each person with computer access	• FortiGate integrated database or hooks to Active Directory
	9. Restrict physical access to cardholder data	• Fortinet professional services in partnership with FortiPartner VAR solutions
5. Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data	• FortiDB assessing and monitoring • FortiAnalyzer event reporting, vulnerability scanning
	11. Regularly test security systems and processes	• FortiDB vulnerability management • FortiScan OS vulnerability management
6. Maintain an Information Security Policy	12. Maintain a policy that addresses information security	• FortiManager security policy mgmt appliance • FortiScan OS vulnerability management

Figure 1: Summary of PCI DSS v1.2 Control Objectives

ISO/IEC 27001/2 for PCI DSS Compliance

When preparing for a PCI assessment, too often retailers stop after ticking through the PCI DSS checklist. While the checklist may include good detail on technical compliance and specific content to include as part of the annual submission report, ISO/IEC 27001/2 provides an overall framework that addresses important control objectives that can ultimately support consistent compliance across systems. This ISO/IEC guideline establishes a common baseline of best practices that many agree can support efforts for developing organizational security standards and effective security management practices on an ongoing basis.

The PCI DSS addresses much of the granular detail around how payment card related controls should actually be implemented, and ISO/IEC 27001/2 offers guidance on the prerequisites required for an overall security management framework. This guidance includes issues like scope definition, management commitment/sponsorship and ongoing improvement plans. Fortinet provides an established practice around ISO/IEC 27001/2 that aligns with an assessment-ready PCI DSS solution.

Internationally recognized as a de-facto security standard and crafted to apply to a wide range of industries, ISO/IEC 27001/2 describes two different set of standards: (1) ISO 27001 specifying a standard

"Selection of the Fortinet appliance was driven by a number of factors: the PCI compliance flexibility to use a single device and be able to deal with diverse requirements across a set of locations; a cost effective device that I could affordably place into locations that required minimal firewall/VPN configuration; and yet the ability to scale up with that same device to a rather sophisticated environment that had multiple network segments and required external Internet access that required a rather sophisticated design from a PCI perspective."

Tom Lindblom,
Vice President
and Chief Technology Officer,
CKE Restaurants

for an Information Security Management System (ISMS), and (2) ISO/IEC 27002 detailing over a hundred security codes of practice for information security management, from business continuity planning and system access control to asset classification and security policies.

Mapping Fortinet Solutions to an ISO Framework	
Compliance Requirement	• PCI • SOX • NERC • ML 52-109 • AGA • ML-52-111 • GLBA • HIPAA
Security Risk Assessment	• FortiGate – Vulnerability assessment/management, Asset Identification, Asset Classification, Network Vulnerability Scanning for remote locations • FortiDB – Database Vulnerability Management • FortiAnalyzer – Vulnerability assessment/management, Asset Identification, Asset Classification, Network Vulnerability Scanning for centralized locations • FortiScan - Vulnerability assessment/management, Asset Identification, Asset Classification, Asset Risk Value • FortiWiFi/FortiAP – detect unwanted rogue wireless devices
Enterprise Security Design	• VAR Professional Services • Fortinet Professional Services • Enterprise Security Architecture Design and Document.
Enterprise Security Deployment	• FortiGate – Fully integrated UTM, including vulnerability management • FortiManager – Centralized management for FortiGate devices, FortiClient agents, FortiMail messaging security, and FortiAnalyzer centralized reporting • FortiAnalyzer – Centralized logging, reporting and analysis, as well as vulnerability management • FortiClient – Multi-threat security for endpoint s • FortiMobile – Multi-threat security for mobile devices • FortiWeb – Web application firewall • FortiDB – Vulnerability management for databases • FortiMail – Comprehensive messaging security • FortiScan – Vulnerability management • FortiWiFi/FortiAP –Secure encrypted wireless network access
Security Awareness Programs	• VAR Professional Services • Fortinet Professional Services • Professionally designed, delivered, documented Security Awareness Programs.

Enterprise Security Information Event Management	• FortiManager • FortiAnalyzer • FortiScan • FortiDB	• FortiWeb • FortiMail • Augmented with Fortinet Alliance Partners Security Event Management Solutions
Assessment and Compliance Reporting	• FortiGate • FortiScan • FortiManager	• FortiAnalyzer • FortiDB • FortiWeb

Figure 2: ISO Framework Fortinet Mapping Table

There are several key themes in ISO/IEC 27001/2 relevant to PCI, including the following.

- Definition and scope, Policy Creation (PCI req. 12)
- Risk assessment, Asset Identification and Classification (PCI req. 12)
- Risk mitigation plan and control objectives (PCI req. 12)
- Statement of applicability (PCI req. 12)
- Products or solutions implementation (PCI req. 7-9)
- Logical and physical access (PCI req. 9)
- User awareness training (PCI req. 10-11) • Incident response and notification system (PCI req. 10)
- Internal/external security assessment, penetration testing, vulnerabilities assessment and patching (PCI req. 5-6)
- System maintenance, patch management (PCI req. 5-6)
- Business Continuous Planning/Disaster Recovery Testing (PCI req. 11)
- Compliance and internal assessment – Reporting and Policy Enforcement (PCI req. 10)

Fortinet Professional Services address the first four ISO framework themes described above. In PCI, the first priority of most retail organizations is to understand the assets (hosts, etc.) that will be within the scope of a PCI assessment and also the assets that they need to segment away so they are not in scope. They then will need to identify those assets, do a Threat Risk Assessment and classify each of the assets (giving a risk value to each asset). The FortiScan and FortiDB appliances from Fortinet are ideal for use as tools to establish a baseline and identify and classify these assets. Later the FortiScan and FortiDB can be used for ongoing Assessment and Compliance reporting. Next steps include selection of the products that would be deployed for the PCI solution, where the 12 PCI DSS requirements come in. Fortinet helps retailers define a PCI Enterprise Security Architecture with professional services to design and document a security architecture optimal for PCI. An example architecture may include the following elements from Fortinet.

- FortiGate – Network Scanning/Vulnerability Management for Retail locations, Firewall, Network Segmentation and Identity based policy, Mitigating controls with AV and IPS.
- FortiManager – Change Management, Integration with ticketing systems for full documentation of changes, Policy push and Firmware upgrades. Document controls.
- FortiAnalyzer – Operational logging or access, Firewall logging and user logging, Network Scanning/Vulnerability Management for Centralized locations, Aggregation of scan data from remote locations.
- FortiAP & FortiWiFi – Air Monitoring and Rogue AP detection to protect against unwanted network access and data leakage as mandated by PCI DSS 1.2
- FortiWeb – Web Application firewall for PCI clients who have internal or external Web applications, SSL offload.
- FortiDB – Mitigating controls – For retailers that cannot encrypt their database – a documented control for VA and Database Activity Monitoring (DAM). Even if they do encrypt their database, this is put in as a control.
- FortiScan – Internal scanning of clients for purposes of Real-time Threat Risk Assessment and mitigating controls.

Fortinet Professional Services and Training Services provide creation of process and policy ensures ongoing compliance with Training of staff specific to the operation and maintenance of the overall solution for an ongoing PCI aligned ISO framework.

Top Reasons Retailers Fail PCI Assessments

Although in most cases retailers that fail an assessment have failed multiple requirements, some of the top requirements that retailers tend to fail most often are reviewed below. These common reasons for PCI assessment failure can be avoided without an infrastructure overhaul.

Insufficient Protection of Stored Data

Retailers frequently run into trouble when they store cardholder data. Insufficient protection of stored data goes to PCI DSS requirement #3 – Protect stored cardholder data. Although as a best practice retailers are advised NOT to store unnecessary cardholder data beyond receiving the authorization code, many do. They may find it easier to store this cardholder data for recurring bills such as subscription services, for instance. Although in most cases the risks of storing cardholder data outweigh the benefits. In some cases retailers fail to effectively isolate the data from less secure parts of the network. In other cases retailers fail to properly encrypt that data. This data needs to be encrypted throughout the entire process. Inconsistent or incomplete encryption is a common issue as encryption may be protecting data in one part of the network, but not in another.

Though even with the right amount of network segmentation and encryption, there still may be potential issues once the data is stored in a database. Typically these issues are related to access control and monitoring as required by #10 – Track and monitor all access, in addition there may be underlying vulnerabilities in the database server software itself. If retailers still choose to store data beyond receiving authorization codes, solutions like FortiDB vulnerability assessment/management and monitoring and the FortiWeb web application firewall, can play important roles in keeping stored data safer. The FortiWeb SSL offload feature for instance provides an acceptable means of accelerating traffic by offloading SSL traffic to a separate device designed specifically for SSL acceleration or SSL termination, This technique is safer as web servers no longer need to touch the encrypting and/or decrypting process traffic. Offloading SSL termination also increases the number of connections that can be handled for clusters of SSL VPNs. FortiGate IPSec VPN can help with encryption as related to requirement #4 – Encrypt transmission of cardholder data across open, public networks. Innovative features in FortiGate like SSL Inspection bring an added layer of protection by checking for Trojans and other malware that may be hiding in protected SSL traffic.

Inadequate Testing of Security Systems and Processes

While many retailers do successfully implement sufficient security controls, they sometimes fail when it comes to testing. Inadequate testing goes to PCI DSS requirement #11 – Regularly test security systems and processes. This issue is related to requirement #10 - Track and monitor all access to network resources and cardholder data. Some retailers who fail their PCI assessment do so because they have no monitoring in general or no assessment trail at all. Having inadequate or no network activity logs, for instance, comes up all too often. Without good logging, it may be nearly impossible to spot hacker activity attempting to access credit card data. Lack of regular scans for software vulnerabilities and abnormal activity can also be of concern.

FortiDB vulnerability assessment/management offers comprehensive database testing and FortiScan operating system (OS) vulnerability management reviews operating systems and network servers and assists with patch management. PCI DSS 1.2 enhanced requirement# 5.2 to include all operating system types in the sample of system components for testing procedures. In addition to database monitoring and assessing with FortiDB, FortiAnalyzer event reporting helps retailers track access to network resources. This kind of review is also important for Web applications that touch cardholder data. Web application firewalls like FortiWeb can mitigate such risk. FortiWeb supports compliance with the Open Web Application Security Project (OWASP) “Top 10” relating to sub-requirement 6.5 – Develop all Web applications based on secure coding guidelines such as the OWASP guidelines and sub-requirement 6.6 – Ensure that all Web-facing applications are protected against known attacks by either having application code reviewed by a specializing organization or “Installing an application-layer firewall in front of Web-facing applications.” By some estimates, Web application vulnerabilities account for the largest percentage of compromise cases, including applications that are vulnerable to SQL Injection and other attacks.

Insufficient Access Controls

According to one study, more than 80% of all cases related to data breach involve insider negligence, not necessarily involvement. Thus, it is important to add controls even for privileged users who access the network, databases and applications. There also tends to be a number of poor password management cases for assessment failure, for example, use of a Web-based program to remotely manage POS device systems with a common user ID and password. Moreover, poor Web application coding can result in weak password control. FortiGate integrated database or hooks to Active Directory help with requirement #8 - Assign a unique ID to each person with computer access. FortiWeb also enforces some level of password checking, ensuring that password fields have to have a mix of alpha/numeric as related to requirement #2. FortiDB vulnerability assessment/management, assessing and monitoring with features like Separation of Duties help support requirement #7 - Restrict access to cardholder data by business need-to-know.

Isolation of Wireless Networks - Guidelines

Following headlines of wireless hackers raiding retailer POS systems, the presence of wireless networks can raise compliance concerns – even when no credit card transactions go over those wireless networks. In fact many of the new enhancements between PCI DSS 1.1 and 1.2 deal with wireless issues, for example:

- PCI DSS requirement# 2.1.1 was clarified to specify that the requirement applies to wireless environments and deleted references to specific wireless technologies like WEP in order to emphasize using strong encryption technologies for wireless networks, for both authentication and transmission.
- Requirement# 4.1.1 prohibited WEP for new wireless implementations after March 31, 2009 and for current wireless implementations after June 30, 2010.
- Requirement# 11.1 was re-focused on testing for the presence of wireless access points and added an option to implement wireless IDS/IPS.
- Requirement# 12.3 was changed to include “remote access technologies, wireless technologies, removable electronic media, email usage, internet usage, laptops and personal data/digital assistants (PDAs)” in the list of critical employee-facing technologies to address.

Assessors may require some tightening and segmentation of the wireless environment to further isolate any wireless networks from the rest of the network. FortiWifi, a line of wireless security gateways from Fortinet, provide an added layer of protection for retailer hosted wireless networks. In fact they can be used to create multiple separate virtual wireless networks, each with its own level of security and requisite firewall policies.

Misconfigured Firewall/VPN

Although having a Firewall/VPN solution with antivirus may seem like an easy checkbox to fill for an assessment, a number of retailers failed to meet requirement #1 - Install and maintain a firewall configuration to protect cardholder data. This is often due to misconfiguration. Solutions like FortiGate appliances that plug-in to the network with little tuning simplify the process. Best practices recommend frequent updates.

Securing Retail Outlets – Branch in a Box

Especially with new specifications adding requirements for on-site assessments of smaller merchants, finding a streamlined solution to secure even small outlets that process credit card transactions is important. Aside from potentially failing security assessments, security breach of private financial information when card holders present their personal data at the point of sale (POS) may be the worst case scenario for retailers implementing PCI DSS compliance to avoid. Whether an established enterprise or just starting out, being a credit card merchant authorized to accept credit cards for payment of goods and services opens the door to a whole set of new security challenges.

A credit card is swiped, a dollar amount is entered and your customer’s cardholder data is transmitted electronically via an authorization request. It seems simple until you consider headlines like, "T.J. Maxx Breach Costs Hit $17 Million" with expected losses of 3 cents per share from the theft of over 45 million credit cards by wireless hackers breaching PCI systems at retail outlets. Some estimates put the average cost of a data breach at $202 per record for U.S. retailers

annually. As attackers become increasingly sophisticated in the pursuit of profit, retailers must remain vigilant in taking the proper security measures, while balancing cost efficiency. PCI standards support this effort and industry leading network and data application security solutions like those from Fortinet help Retailers stay ahead of the hacker sophistication curve to avoid the PCI security pitfalls that have lead to assessment failures and expensive security breaches that damage reputations and dampen sales. Fortinet provides an easy solution to secure retail outlets with FortiWifi.

Figure 3: Example of Retail Store Infrastructure

Retailers can ease their PCI security work when it comes to finding a single device for a retail location able to support over 10 different store level applications, including broadband / routing, point-of-sale, video surveillance, guest WiFi, digital signage, traffic counters, manager/training workstations, kiosks, district manager laptop and inventory management systems. The Fortinet FortiWifi solution, a.k.a., "Branch in a Box," is the driving force behind the powerful return on investment (ROI) model that makes the Fortinet PCI compliancy solution so compelling.

FortiWifi easily ties into the overall network security structure as shown in the following network diagram. While many mid-sized retailers may not have small branch office locations, almost all have distribution centers.

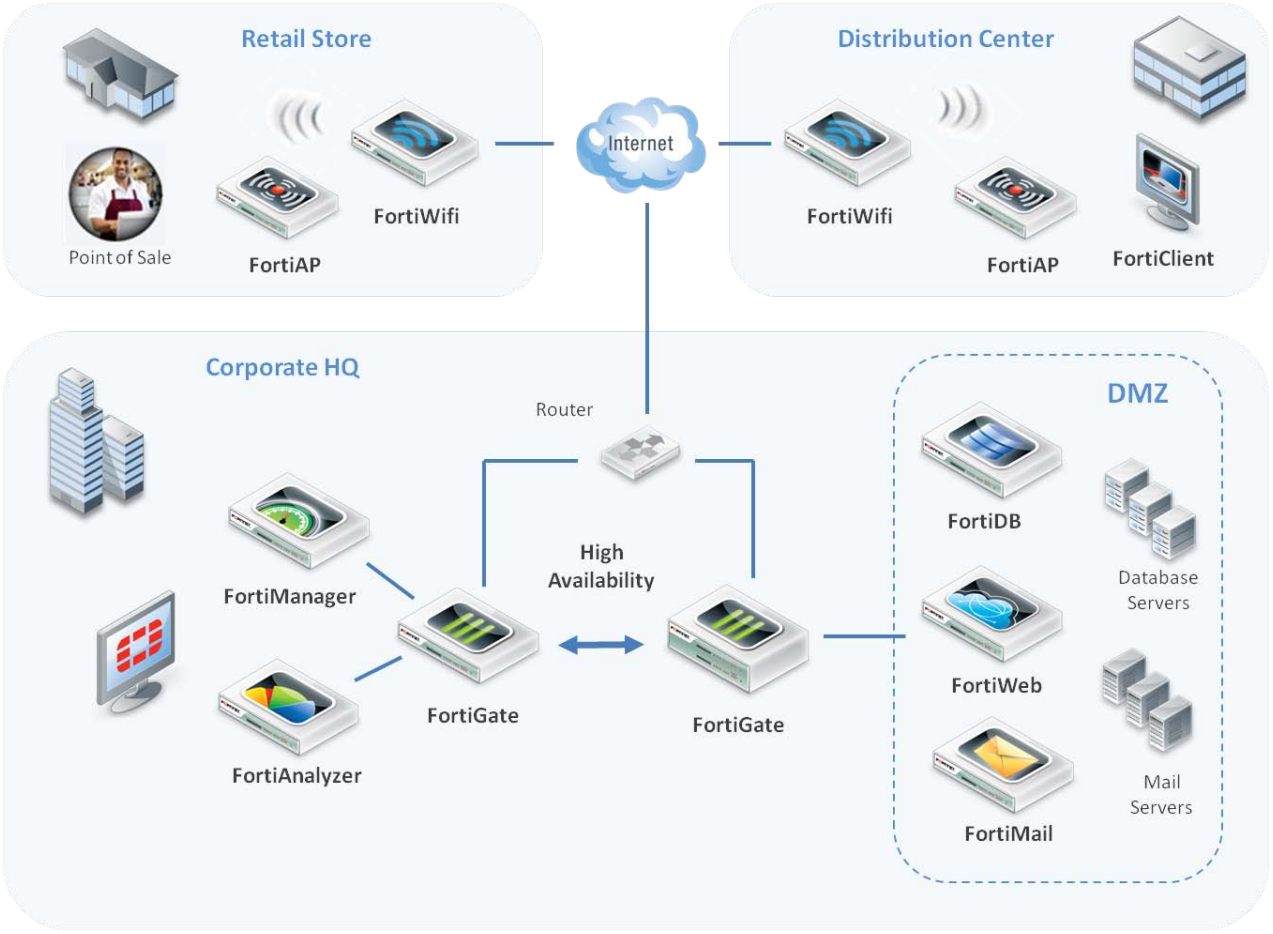

Figure 4: Overall Network Diagram of FortiWifi

Securing the Retail Enterprise

The following deployment example illustrates network segmentation and multi-layered security from the network to the application and database to the client, with logging, reporting, analysis and vulnerability management. The challenge for enterprise and smaller retailers alike is to meet or exceed security compliance standards to thwart potential attacks, while balancing performance and total cost of ownership (TCO) interests.

Enterprise PCI Security with Fortinet Solutions

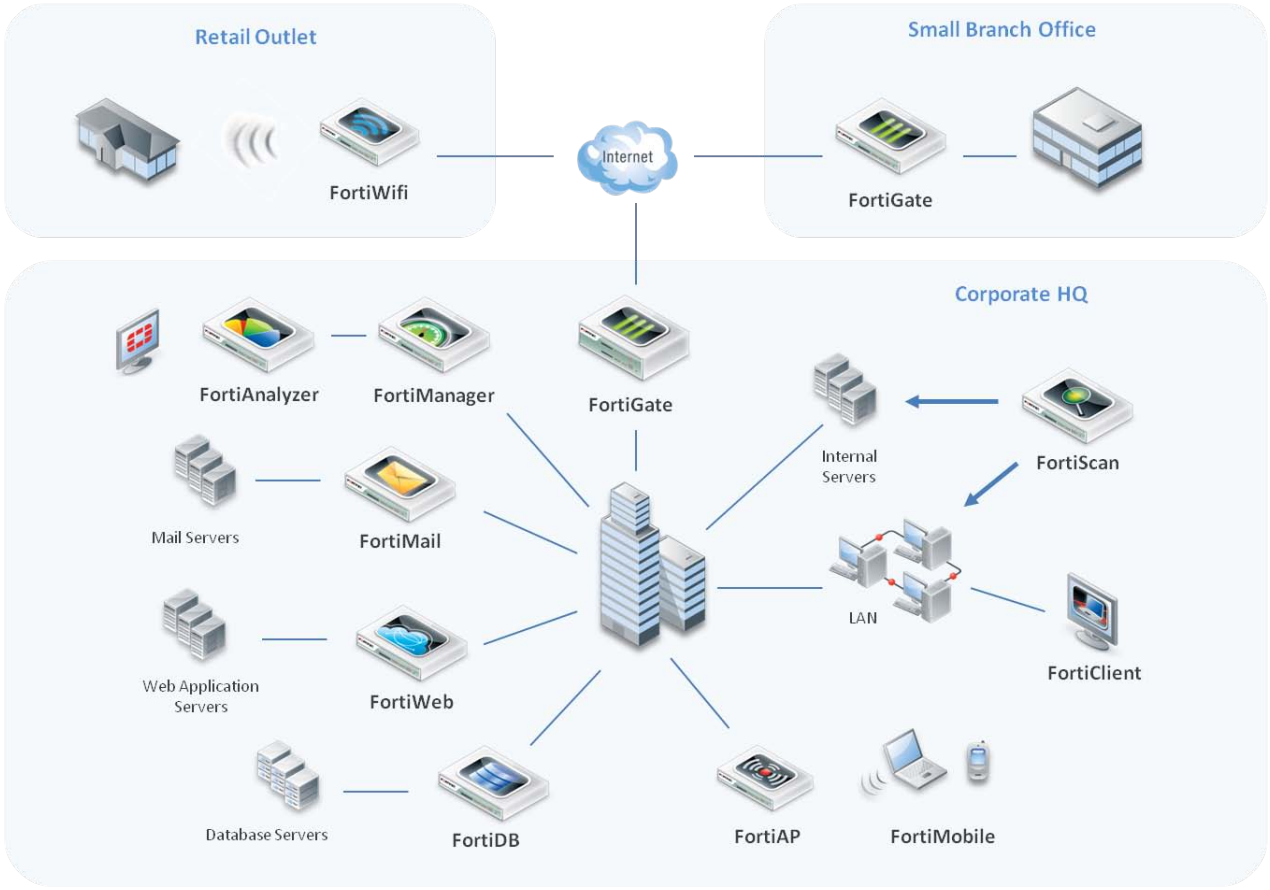

Figure 5: Fortinet PCI DSS Deployment Scenario

A Unified Threat Management Approach

A key tactic for PCI security is to put in mitigating controls by applying segmentation of inside perimeters with isolation technologies. Additionally, since some facilities may be in remote locations with little or no permanent staff, out-of-band access is required with firewall/VPN solutions to resolve problems when in-band access has failed. Key preventative strategies include firewall/VPN to establish security perimeters, network segmentation and group-based authentication, as well as implementation of antivirus controls and intrusion prevention systems (IPS). The deployment of these types of technologies in single point products may amount to six or more separate security devices, which may prove cost prohibitive to the electrical producer. Point product solutions can be difficult to manage, requiring multiple management interfaces, with no integration between vendors and no single vendor for issue resolution. Point products are expensive to deploy and maintain with multiple vendor contracts and renewal schedules, costly support licensing, data resource allocation (power, rack space, cooling) and multiple inspection steps that may tax network performance. Furthermore, lack of integration may lead to reduced security. Since retail POS and related control systems need to be readily available at all times, availability of these systems is one of the most critical aspects of any secure network architecture. Therefore, the deployed solutions in most circumstances would be configured in a high-availability scenario, further increasing complexity and costs.

While it is difficult (and expensive) to manage six or more different point product security devices with limited integration in a network that has to be highly available, a streamlined Unified Threat Management (UTM) platform that integrates firewall/VPN, intrusion prevention and antivirus features running in high availability mode protects control systems more efficiently. A UTM approach reduces the number of vendors and appliances, provides comprehensive security, minimizes

down-time from individual threats, simplifies security management, improves detection capabilities and coordinates alerting, logging and reporting. Integration of advanced features like Application Control from the network down to the client level with centralized management and reporting gives retailers granular visibility and control to enforce security policy.

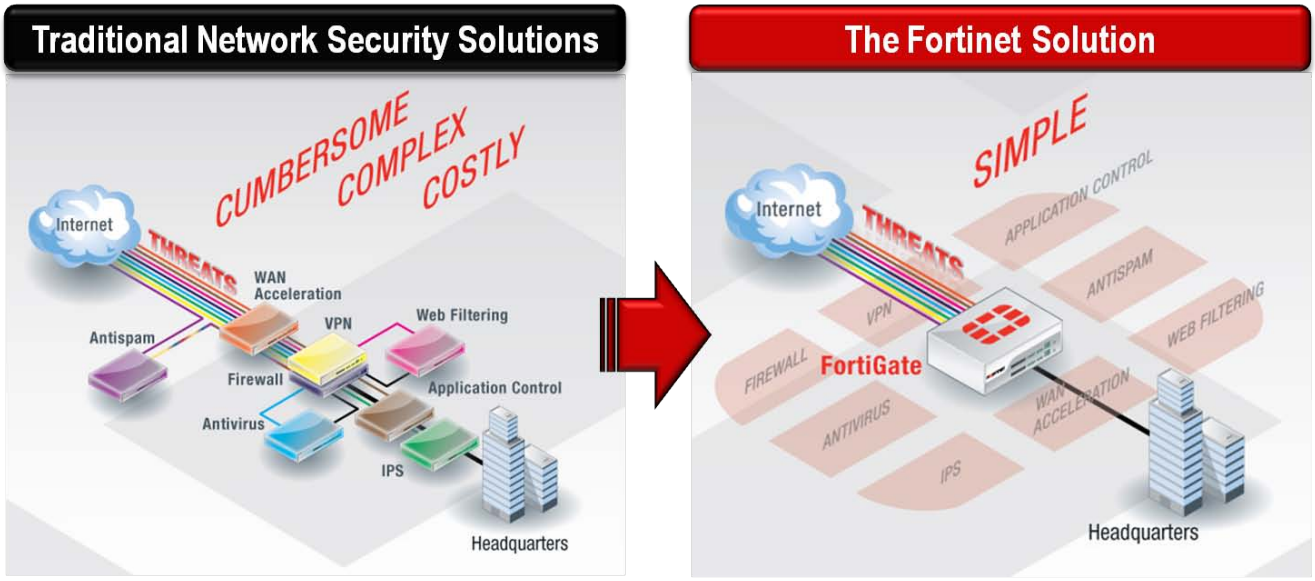

Figure 6: Point solutions vs. Unified threat management

High-Performance ASICs

Fortinet provides a UTM platform delivering high-performance and best-of-breed network security through intelligent integration in FortiGate™ appliances with custom ASIC (Application Specific Integrated Circuits) based silicon processing hardware for high-speed networks. Fortinet contributes to the effective security and scalable performance provided by a UTM solution with specialized hardware, software and evolving security content. Fortinet's strong commitment to independent certification helps to ensure validated security functionality. The unified approach allows for comprehensive security reporting with output log/report information in a common format – a core component for any large organization.

This new generation of network processor can be programmed with current firewall and IPS policy to filter traffic, detect protocol anomalies and expedite traffic delivery at the interface level— without burdening the rest of the system. When traffic bypasses other portions of the system, state information and not the actual packets can be communicated to alleviate general purpose processor congestion to further improve performance. These levels of performance are critical as networks are upgraded to take advantage of increasingly faster LAN and WAN standards, such as 10-Gigabit Ethernet and beyond.

FortiASIC content processors are specifically engineered to perform high-speed comparisons of objects to known threat patterns and only contain scanning logic in hardware. The threat pattern data and signatures, which are constantly updated by the FortiGuard Distribution Network are stored in memory and not in the hardened ASIC.

Summary

FortiGate™ UTM solutions employing custom ASIC-based processing hardware are able to accommodate high-speed networks, such as internal network segments, and are able to secure and process traffic as close to line rate as possible. In order to achieve the most benefit and offer the highest levels of security effectiveness and efficiency, complete integration of specialized hardware with software and security content is essential. Fortinet Enterprise Security including FortiGate, FortiManager, FortiAnalyzer, FortiClient, FortiMobile, FortiWeb, FortiDB, FortiMail and FortiScan and Professional Services provides a complete solution. Fortinet simplifies network security assessment-ready PCI compliance without sacrificing

performance. Retailers can ease the process of PCI DSS assessment-readiness with an ISO security framework and unified threat management approach.

References

Sharon Gaudin, InformationWeek (May 2007). "T.J. Maxx Breach Costs Hit $17 Million." Retrieved on May 20, 2009, from http://www.informationweek.com/news/security/showArticle.jhtml?articleID=199601551

PCI Security Standards Council (October 2008). "Payment Card Industry (PCI) Data Security Standard: Summary of Changes from PCI DSS Version 1.1 to 1.2." Retrieved on May 20, 2009, from http://www.pcisecuritystandards.org/

PCI Security Standards Council (October 2008). "Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures, Version 1.2." Retrieved on May 20, 2009, from http://www.pcisecuritystandards.org/

Visa Cardholder Information Security Program (CISP). Retrieved on May 20, 2009, from http://usa.visa.com/merchants/risk_management/cisp.html

MasterCard Site Data Protection (SDP) program. Retrieved on May 20, 2009, from http://www.mastercard.com/us/sdp/

MasterCard Merchant Levels Defined. Retrieved on June 22, 2009, from http://www.mastercard.com/us/sdp/merchants/merchant_levels.html

Visa Account Information Security (AIS) Program. Retrieved on May 20, 2009, http://www.visa.ca/en/merchant/fraud-prevention/account-information-security/

ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management, Retrieved on May 20, 2009, http://www.iso.org/

Ponemon Institute (Feb 2009). "Fourth Annual Cost of a Data Breach, February 2009." Retrieved on May 20, 2009, http://www.ponemon.org/data-security

Open Web Application Security Project (OWASP) (2009) "OWASP Project." Retrieved on May 20, 2009, http://www.owasp.org/

FORTINET

GLOBAL HEADQUARTERS
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE
Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE
Fortinet Incorporated
61 Robinson Road, #09-04 Robinson Centre
Singapore 068893
Tel +65-6513-3730
Fax +65-6223-6784