FORTINET

WHITE PAPER

Towards A Consolidated Approach For PCI-DSS Compliance In Healthcare

Introduction

In recent years we've witnessed the extraordinary lengths to which cybercriminals will go to breach target networks and steal valuable data for monetary or competitive gain. This phenomenon is particularly apparent in the world of electronic commerce, where account details of credit card users are sold for a premium on the black market.

Fortunately, the principal stakeholders in the card payment ecosystem have defined a standard that has proven to be highly effective (albeit not infallible) at protecting data from such breaches. Over the past five years, the Payment Card Industry Data Security Standard (PCI-DSS) framework has evolved from being mere guidelines without enforceable sanctions to a 'must-have' certification that you are required to obtain if you are involved in manipulating, storing or transmitting cardholder data.

This 'must-have' certification applies to EVERY healthcare organization involved in accepting payment via credit cards. PCI-DSS regulations are separate and distinct from HIPAA. Being HIPAA compliant does not mean your organization is PCI-DSS compliant.

Despite its seemingly narrow focus on cardholder data protection, PCI-DSS spans most IT disciplines and skills. This includes networks, databases, web applications, file systems and encryption along with core security-related processes such as vulnerability and configuration management. As a result, the cost of implementing compliance has become alarmingly high, bringing into question the applicability of the standard in terms of risks versus reward.

Earlier this year, the Ponemon Institute conducted a study on the actual costs of compliance among 160 enterprises, including 46 international ones. The results of this study showed that for mid-size organizations, the total cost of compliance with regulations such as PCI-DSS, SoX, HIPAA and others, averages $3.5 million. However, the cost of non-compliance was measured at $9.4 million, nearly triple the cost of compliance. While these figures illustrate a sizeable benefit for investment in compliance, the cost burden remains high.

If your organization is not compliant with PCI DSS, you may not be able to process credit card transactions in certain markets. Aside from suspension of one's ability to process credit card transactions, a data breach for non-compliant providers may cost hundreds of thousands of dollars in fines alone (VISA can impose fines up to $500,000 per incident). It's important to note that compliance with HIPAA does not mean your are compliant with PCI DSS.

Organizations of different sizes have different PCI-DSS compliance requirements. Below is a breakdown of Visa's PCI compliance level definitions. Details can be found at http://usa.visa.com/merchants/risk_management/cisp_merchants.html

- PCI Compliance Level 1 – Organizations processing over 6 million Visa transactions annually (all channels) or Global merchants identified as Level 1 by any Visa region
  - Annual Report on Compliance ("ROC") by Qualified Security Assessor ("QSA") or internal auditor if signed by officer of the company
  - Quarterly network scan by Approved Scan Vendor ("ASV")
  - Attestation of Compliance Form
- PCI Compliance Level 2 - Organizations processing 1 million to 6 million Visa transactions annually (all channels)
  - Annual Self-Assessment Questionnaire ("SAQ")
  - Quarterly network scan by ASV
  - Attestation of Compliance Form
- PCI Compliance Level 3 - Organizations processing 20,000 to 1 million Visa e-commerce transactions annually
  - Annual SAQ
  - Quarterly network scan by ASV
  - Attestation of Compliance Form
- PCI Compliance Level 4 - Organizations processing less than 20,000 Visa e-commerce transactions annually and all other organizations processing up to 1 million Visa transactions annually
  - Annual SAQ recommended

- Quarterly network scan by ASV if applicable
- Compliance validation requirements set by acquirer

So, what strategies can healthcare organizations employ to reduce the complexities and costs of a PCI implementation? What are the principal concerns to consider in terms of PCI implementation?

PCI-DSS is multi-disciplinary and to fully comply with the standard, it is essential to take a global consolidated approach to address all 12 requirements as a whole before focusing on solving individual elements. The core IT disciplines to be considered are: Networking – Fixed and Wireless; Data and Databases; IT Assets/End-Points; and Web Applications.

Fixed Network

The PCI core requirement covers controlled network segregation, inbound/outbound traffic flows and DMZ implementation. Specific functions include: real-time perimeter anti-virus, IPSec/VPN tunneling support, IDS/IPS, use of strong cryptography (SSL/IPSec), default 'deny-all' settings, support of digital certificates and two-factor user authentication, event monitoring, federated device management and reporting, and network vulnerability analysis support. These services cannot be provided by a legacy firewall, even a so-called next-generation firewall. The only way to cost effectively provide all these services and avoid the deployment of multiple devices is through the use of a Unified Threat Management (UTM) device. A UTM-based solution can help organizations cover the fixed network requirements of PCI while achieving greater overall PCI effectiveness and simultaneously minimize implementation and operational costs.

Wireless Network

In many ways, the wireless network is subject to the same constraints as the fixed network but it must also meet the following key functions:
1) Support for both 'thick' and 'thin' access point (AP) solutions that can work in a seamless management framework
2) Detection of rogue APs against a defined hardware inventory
3) Support and logging of wireless IDS/IPS
4) Support for WPA or WPA2 Enterprise mode with 802.1X authentication and AES encryption

In practice, the best approach in larger deployments is to minimize the deployment of thick APs, which have wireless control, IPS and other security features built into the physical devices, and favor the deployment of thin access points, which are much easier to manage and maintain. Thin APs tunnel wireless traffic to wireless controllers, allowing significant economies of scale and a simplified security management capability through a 'single pane of glass' management console for increased visibility and policy enforcement.

IT Assets / Endpoints

IT assets include servers, desktops, laptops, operating systems, mobile devices and network equipment. The objective is to ensure that all assets that constitute the PCI cardholder data environment are subject to core security management processes. Here, in order to have the most effective approach in meeting the PCI DSS requirements at minimal cost and complexity, it is important to consider the management of deployed endpoint security technologies and controls. The top 5 elements on the checklist are:
1) Support for asset vulnerability management to ensure that all operating systems are patched to the latest version and to assess configuration specific vulnerabilities
2) Configuration management capability against globally accepted best practices for operating system platform deployment (e.g. NIST, FDCC)
3) Endpoint policy control to blacklist/whitelist software, processes, devices, drivers, access lists etc.…
4) Automated remediation of configuration and audit issues for cost-effective operation
5) Deployment of client/mobile device anti-virus, preferably administered centrally

Data & Databases

It is impossible to comply with PCI DSS without implementing a database security solution to protect against data loss or fraud. Whether due to an error or a deliberate intent to harm, data loss can have serious consequences. In order to meet PCI-DSS compliance, a database security solution must include:
1) Database-specific vulnerability assessment and penetration testing
2) Configuration management for assessment against global best practices and/or the organization's own data security standards
3) Access control assessment both at the database and application levels
4) Real-time monitoring of database users and their activity on both database and critical cardholder data.

In order to simplify the creation and enforcement of data security policies that will help meet PCI-DSS compliance, it is important to look for a centrally-managed database security solution that provides all of the above features on one device. Enhanced solutions include features such as automatic database and sensitive data discovery. Other desirable functions include pre-built policies that cover standard industry and government requirements which when combined with a comprehensive set of graphical reports deliver out-of-the-box readiness and immediate value for PCI-DSS compliance.

Web Applications

Since web applications are exposed to the outside world by definition, the PCI-DSS standard addresses them in detail in requirement 6.6. There are two methods that a company can apply in order to be in compliance with PCI DSS: a) Conduct yearly code reviews or b) Deploy a Web application firewall. While code reviews/testing is important, a significant cost saving can be made through the implementation of a Web application firewall.

The key functions that should be included in such a solution include:
1) Support of OWASP Web security guidance, cross-site scripting (XSS) and cross-site request forgery (CSRF) vulnerability protection
2) Support for DoS and buffer overflow attacks at both the HTML and HTTP level
3) Access control and web application user authentication
4) Monitoring and management of error events
5) Incorporation of a web application vulnerability scanning capability for regular internal scans.

How Fortinet Can Help

Fortinet's FortiGate® consolidated security systems enable those in the healthcare industry touched by PCI compliance standards to secure multiple, geographically-dispersed sites and critical applications such as billing and patient records, while complying with PCI-DSS regulations and without overloading the IT budget or personnel. Powered by specialized FortiASIC™ processors purpose-built for content and network processing, FortiGate systems provide full, multi-layered security that scales from remote clinic appliances and mobile applications to multi-gigabit core network or data center platforms. Every FortiGate system offers complete threat protection within a single solution: firewall, intrusion prevention system (IPS), application control, VPN, traffic shaping, antivirus, antispyware, antispam, Web content filtering and vulnerability management. FortiManager™ and FortiAnalyzer™ management and reporting appliances enable centralized control of any size deployment, including vulnerability management and logging/archiving for regulatory compliance. Fortinet database security and compliance products offer centrally managed database hardening; fast, comprehensive policy compliance; and vulnerability assessment for improved data security across the organization.

Some of the benefits of the Fortinet solution include:

- FortiGate systems provide scalable, comprehensive protection against network-level and content-level threats without degrading performance of critical applications, network availability or uptime.
- Easily-managed platforms with integrated, multi-threat protection reduce management burden and capital expenditures for lower TCO.
- FortiClient™ end-point security agents provide comprehensive, centrally-managed security for remote personal computers and mobile laptops, with support for 3G for remote locations without wireline broadband.
- FortiWiFi™ appliances with built-in wireless access points and PC Card slots for broadband wireless support rapid deployment for access in clinics and remote sites.
- FortiAP™ wireless access points support high speed 802.11n wireless, with FortiGate platforms acting as a wireless controller, driving down the cost of wireless networks.
- FortiManager and FortiAnalyzer appliances ease management of multiple sites and help maintain PCI compliance with extensive logging and archiving capabilities to help safeguard credit card usage by customers and guests.
- FortiDB™ database security and compliance products protect critical database resources with hundreds of pre-installed policies covering standard industry and government requirements and security best practices, including compliance reporting for important regulations such as PCI-DSS.
- Extensive virtual domain and security zone capabilities deliver fine-grained control of network and application access across multiple, widely-dispersed sites. This allows employees and patients or visitors shared access to the network without compromising security.
- Multiple security functions available on every FortiGate system for easy addition to existing solutions and incremental deployment without incremental investment in hardware or software.

Fortinet's broad product portfolio touches many aspects of PCI compliance. Below is a graph explaining what products meet the needs of which PCI standard.

PCI DSS	Description	Fortinet Solution
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data. 1. Do not use vendor-supplied defaults for system passwords and other security parameters.	**FortiGate** integrated firewall functionality **FortiDB** vulnerability assessment and auditing **FortiWeb** Web application password checking **FortiScan** OS vulnerability management
Protect Cardholder Data	3. Protect stored data. 4. Encrypt transmission of cardholder data and sensitive information across public networks.	**FortiDB** vulnerability assessment and monitoring **FortiWeb** Web application firewall **FortiGate** IPSec VPN
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software. 5. Develop and maintain secure systems and applications.	**FortiGate** integrated AV **FortiClient** and **FortiMobile** integrated AV **FortiMail** integrated AV **FortiGuard** automated AV updates **FortiGate** vulnerability management **FortiDB** vulnerability assessment, auditing and monitoring **FortiWeb** Web application security **FortiScan** OS vulnerability management **FortiAnalyzer** network vulnerability scanning
Implement Strong Access Control Measures	7. Restrict access to data by business need-to-know. 7. Assign a unique ID to each person with computer access. 7. Restrict physical access to cardholder data.	**FortiDB** vulnerability assessment, auditing and monitoring **FortiGate** integrated database or hooks to Active Directory. Fortinet professional services in partnership with FortiPartner VAR solutions
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. 10. Regularly test security systems and processes.	**FortiDB** auditing and monitoring **FortiAnalyzer** event reporting, vulnerability scanning **FortiDB** vulnerability assessment **FortiScan** OS vulnerability management **FortiGate** vulnerability management
Maintain an Information Security Policy	12. Maintain a policy that addresses information security.	**FortiManager** security policy management appliance **FortiScan** OS vulnerability management

Conclusion

The multi-disciplinary nature of PCI-DSS requires healthcare organizations to deploy a variety of different security technologies. Consequently, organizations often deploy a combination of security technologies from different vendors in order to fully address the requirements of the standard. Unfortunately, using a large number of solutions from a variety of vendors often results in a wide array of disparate products and services introduced into the PCI solution. The result is spiraling complexity (in terms of support, maintenance, resource training, etc.) and increased total cost of ownership. Minimizing the number of vendors to work with, to a single one if possible, is the only way to dramatically reduce both operating and capital expenses while removing complexity from implementation and management. A common platform provided by a single vendor will also enable you to enhance your security posture, coverage and visibility for a lower overall risk of PCI project failure. In summary, a consolidated approach allows you to increase performance, improve security and reduce cost

About Fortinet

Fortinet delivers unified threat management and specialized security solutions that block today's sophisticated threats. Our consolidated architecture enables our customers to deploy fully integrated security technologies in a single device, delivering increased performance, improved protection, and reduced costs. Purpose-built hardware and software provide the high performance and complete content protection our customers need to stay abreast of a constantly evolving threat landscape. Our customers rely on Fortinet to protect their constantly evolving networks in every industry and region in the world. They deploy a robust defense-in-depth strategy that improves their security posture, simplifies their security infrastructure, and reduces their overall cost of ownership.

FortiGuard® Security Subscription Services deliver dynamic, automated updates for Fortinet products. The Fortinet Global Security Research Team creates these updates to ensure up-to-date protection against sophisticated threats. Subscriptions include antivirus, intrusion prevention, web filtering, antispam, vulnerability management, application control, and database security services.

FortiCare™ Support Services provide global support for all Fortinet products and services. FortiCare support enables your Fortinet products to perform optimally. Support plans start with 8x5 Enhanced Support with return and replace hardware support or 24x7 Comprehensive Support with advanced hardware replacement. Options include Premium Support, Premium RMA, and Professional Services. All hardware products include a 1-year limited hardware warranty and a 90-day limited software warranty.

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
300 Beach Road #20-01
The Concourse, Singapore 199555
Tel: +65-6513-3734
Fax: +65-6295-0015

WP-PCI-DSS-201111