QUALYS®

WHITE PAPER

WINNING THE PCI COMPLIANCE BATTLE

A Guide for Merchants and Member Service Providers

Table of Contents

ON DEMAND SECURITY

"The things that PCI is looking for are really the motherhood and apple pie issues of security making sure that firewalls are only passing traffic on accepted and approved ports, that servers are running only those services that really need to be live, that databases aren't configured with vendor-supplied defaults—it's all standard security-assessment stuff."

Diane Kelly, Vice President
and Service Director
Burton Group

I. The Payment Card Industry Locks Down Customer Data

The last several years have seen an unprecedented assault on personal and financial data that customers have knowingly or unwittingly entrusted to retailers, banks, service providers and credit card companies. Bank of America, BJ's Wholesale Club, CardSystems Solutions, Choicepoint, Citigroup, DSW Show Warehouse, Hotels.com, LexisNexis, Polo Ralph Lauren and Wachovia are just a few of the names that have been boldly exposed in the media and pummeled in the financial markets after major data security breaches were revealed. Credit card data in particular has been compromised so frequently that calls for government intervention and regulation became widespread.

Taking another approach, the payment card industry countered the criminal onslaught with a homegrown security initiative that is at once broader in scope and more granular in its requirements than any measures additional government regulation might have imposed. The Payment Card Industry Data Security Standard is a comprehensive security standard that establishes common processes and precautions for handling, processing, storing and transmitting credit card data.

PCI, as it is almost universally known, was originally developed by MasterCard and Visa through an alignment of security requirements contained in the MasterCard Site Data Protection Plan (SDP) and two Visa programs, the Cardholder Information Security Plan (CISP) and the international Account Information Security (AIS). In September of 2006, a group of five leading payment brands including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International jointly announced formation of the PCI Security Standards Council, an independent council established to manage ongoing evolution of the PCI standard. Concurrent with the announcement, the council released version 1.1 of the PCI standard.

"There's no other regulatory or industry compliance requirement that's quite this granular. PCI is kind of its own unique animal, but the data you collect in a PCI compliance scan can be useful in meeting many other kinds of audit and assessment requirements—an ISO 27001 certification or a Sarbanes-Oxley audit, for instance. You'll be looking at many of the same things. After all, most compliance comes down to things like whether your firewall is correctly configured."

Diane Kelly, Vice President
and Service Director
Burton Group

II. Compliance Requirements of the PCI Data Security Standard

The PCI Data Security Standard requirements apply to all payment card network members, merchants and service providers that store, process or transmit cardholder data. The core requirements are organized in six categories:

PCI DSS
Build and Maintain a Secure Network 1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, 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 cardholder 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

Figure 1: PCI DSS Principles and Requirements

III. Participation and Validation Requirements

While the newly-established PCI Security Standards Council will manage the underlying data security standard, compliance requirements are set independently by individual payment card brands. While requirements vary between card networks, MasterCard's Site Data Protection Plan and Visa's Cardholder Information Security Program are representative. They stipulate separate compliance validation requirements for merchants and service providers, which vary depending on the size of the company. Compliance levels are defined based on annual transaction volume and corresponding risk exposure as outlined in figure 2.

Merchant & Service Provider Levels & Validation Actions

	LEVEL	CRITERIA	ON-SITE SECURITY AUDIT	SELF-ASSESSMENT QUESTIONNAIRE	NETWORK SCAN
MERCHANT	1	– Any merchant, regardless of acceptance channel, processing **more than 6 million transactions** per year – Any merchant that suffered a security breach, resulting in an account compromise	Required Annually *		Required Quarterly
	2	– Any merchant processing between **150,000 to 6 million transactions** per year		Required Annually	Required Quarterly
	3	– Any merchant processing **between 20,000 to 150,000 transactions** per year		Required Annually	Required Quarterly
	4	– **All other merchants** not in Levels 1, 2, or 3, regardless of acceptance channel		Required Annually	Required Quarterly
SERVICE PROVIDER	1	– **All processors and all payment gateways**	Required Annually *		Required Quarterly
	2	– Any service provider that is not in Level 1 and stores, processes or transmits **more than 1 million accounts / transactions** annually	Required Annually *		Required Quarterly
	3	– Any service provider that is not in Level 1 and stores, processes or transmits **less than 1 million accounts / transactions** annually		Required Annually	Required Quarterly

** On-Site Security Audits may be conducted through Qualys PCI Consulting Partners - http://www.qualys.com/partners/pci*

Figure 2: Merchant & Service Provider Levels and Validation Actions

Validation Requirements

Annual on-site security audits – MasterCard and Visa require the largest merchants (level 1) and service providers (levels 1 and 2) to have a yearly on-site compliance assessment performed by a certified third-party auditor.

Annual self-assessment questionnaire – In lieu of an on-site audit, smaller merchants (levels 2, 3 and 4) and service providers (level 3) are required to complete a self-assessment questionnaire to document their security status.

Quarterly external network scans – All merchants and service providers are required to have external network security scans performed quarterly by a certified third-party vendor. Scan requirements are rigorous: all 65,535 ports must be scanned, all vulnerabilities detected of level 3-5 severity must be remediated, and two reports must be issued—a technical report that details all vulnerabilities detected with solutions for remediation, and an executive summary report with a PCI approved compliance statement suitable for submission to acquiring banks for validation.

"First of all, you have to use an approved PCI vendor, so that's pretty much a binary decision. Beyond that, customers really need to consider their comfort level with the service provider's methodology—the way that reports are presented and the level of transparency into the data collection process. Intrusiveness is also an important consideration: some scanning tools are more invasive than others, and customers need to be sure that these are low-touch processes that won't cause disruption on their networks. Reusability of the scan data in other security management processes and with other SIM tools is another thing to look for. This is good data they're getting, and it's applicable beyond PCI."

Diane Kelly, Vice President
and Service Director
Burton Group

Validation Enforcement

While non-compliance penalties also vary among major credit card networks, they can be substantial. Participating companies can be barred from processing credit card transactions, higher processing fees can be applied; and in the event of a serious security breach, fines of up to $500,000 can be levied for each instance of non-compliance.

Since compliance validation requirements and enforcement measures are subject to change, merchants and service providers should closely monitor the requirements of all card networks in which they participate.

IV. Selecting a PCI Network Security Testing Service

At first exposure, PCI compliance and validation requirements can appear daunting, particularly the external scan requirement. Merchants can simplify the selection process by establishing a few key selection criteria.

Three important things to look for in a PCI network scanning service are:

- ***Accuracy*** – It's extremely important that a testing service be able to accurately identify real vulnerabilities and not generate a large inventory of false positives, each of which must be manually evaluated for remediation. False positives (and false negatives) can significantly and unnecessarily inflate the workloads and labor costs of maintaining PCI compliance.

- ***Efficient vulnerability remediation process*** – The service provider must offer tested and documented remediation processes for all identified vulnerabilities, and provide expert technical support assistance.

- ***Automated report preparation and on-line filing*** – Automatic report preparation and electronic filing greatly simplify compliance administration and reduces the attendant workload.

"For us, the major advantage of an online service like QualysGuard PCI is that it's accessible from everywhere in the world. That lets us perform the external network scan as part of our onsite work with a customer. Another advantage is the fact that it is tailored specifically for PCI compliance evaluation, including the reports. That saves us time and saves the customer money."

Stephan Engelke, Security Consultant and PCI Auditor
Excelsis Business Technology

"PCI compliance is extremely intimidating for organizations relying on the payment card industry for the majority of their transactions. The QualysGuard PCI On Demand platform reduces the cost and complexity of security and compliance for organizations through the software-as-a-service model."

Dr. Michael G. Mathews, CTO
CynergisTek

Rose Ryan, J.D., a research analyst in IDC's Security Products and Services group, urges merchants to also consider the service provider's background and core expertise. "The most successful vendors in this space have a history in security assessment and management as well as compliance services. I also think it's important to evaluate a provider's ability to adapt as requirements change, and look for good partnerships in the consultant community for remediation referrals. Smaller companies should also search out specialized PCI offerings from established security management providers that help make PCI compliance affordable."

V. Introducing On Demand PCI: QualysGuard PCI

One such specialized solution is QualysGuard PCI, a network scanning, security assessment and reporting platform delivered on QualysGuard, the industry-leading on demand solution for vulnerability management and policy compliance. QualysGuard PCI is provided on demand as a Web application with no hardware or software to be installed and maintained on the customer network. It allows merchants and service providers to complete all validation requirements. Using QualysGuard PCI users can easily complete and submit the PCI self-assessment questionnaire online, and perform pre-defined PCI scans on all external systems to identify and resolve network and system vulnerabilities as required by the PCI standard.

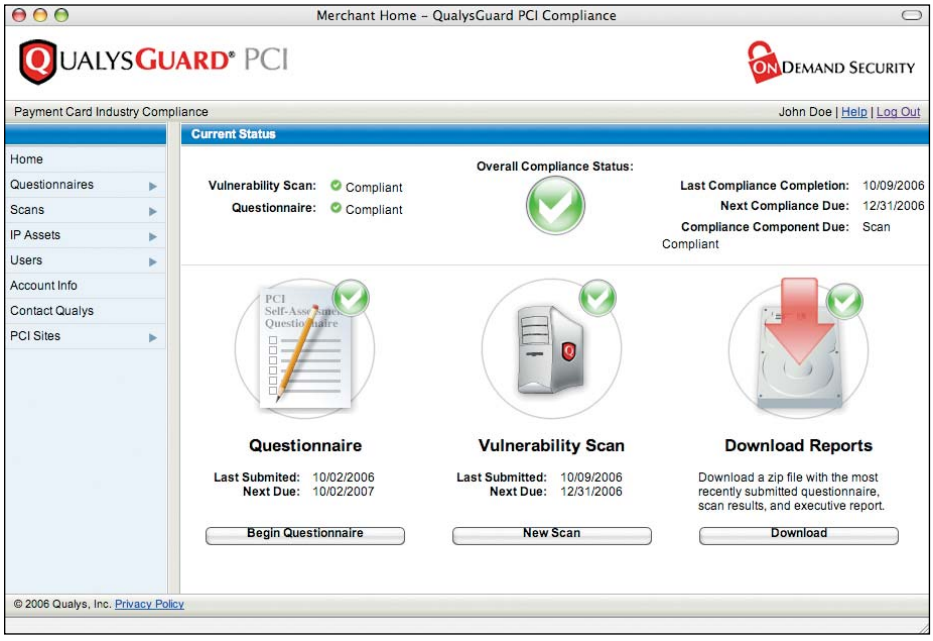

Figure 3: QualysGuard PCI Dashboard

QualysGuard PCI is certified by the PCI Council for network scanning and PCI compliance validation, and is used worldwide by merchants, security consultants and network-certified PCI auditors. Consultants and security auditors can use QualysGuard PCI in their practice to help clients achieve compliance in an efficient manner.

"With Tribune's distributed organizational structure and heterogeneous environment, we needed a rapid and economical way to scan for and eliminate server vulnerabilities. The QualysGuard PCI On Demand platform and the services of CynergisTek are helping us to verify the PCI compliance of our IT infrastructure."

Dr. Joshua Seeger, CIO
Tribune Broadcasting

"Since our business is PCI compliant, I was familiar with and had used other PCI compliance services. I was very surprised at the thoroughness of the scan from Qualys. It discovered issues that had not been brought to my attention from other compliance scans."

Sam Lehrfeld, CIO
KneeDraggers.com Inc.

Key features of QualysGuard PCI include:

- An online self-assessment questionnaire that lets the user revisit the questionnaire as often as necessary, and enables collaboration with other members within the organization.
- Unlimited PCI scanning for all systems within the user account. An organization can scan all external systems on a quarterly basis or on as needed basis in order to reach compliance.
- PCI reporting that delivers executive level and technical reports as defined by the PCI standard.
- Online filing that automatically notifies the acquiring bank when a merchant achieves PCI compliance.
- A friendly and fast process to address and eliminate false positives detected during scans.

But the most important feature of QualysGuard PCI is the Six Sigma level of accuracy made possible by the industry's most complete vulnerability knowledgebase, an encyclopedic inventory of thousands of known vulnerabilities that covers all major operating systems, services and applications. The result is a current error rate of less than 3.4 defects per million production scans.

VI. Automating the PCI Validation Process

Achieving PCI compliance may seem at first like an insurmountable task, but in fact the PCI Data Security Standard requirements represent fundamental security best practices that should be observed by any organization with IT systems and data to protect. Because networks are always connected, new devices are constantly being added, and new vulnerabilities are discovered daily, the possibility of exploitation is ever-present. PCI delivers best practice approaches that help keep companies on top of this ever-evolving situation, ensure compliance, and secure cardholder information stored within their networks.

For additional information and a 14-day free trial on how Qualys On Demand PCI can help make PCI compliance an automated, effective process for continuous security improvement, visit Qualys on the Web at **http://www.qualys.com/products/qgpci/.**

QUALYS®
www.qualys.com

USA – Qualys, Inc.
1600 Bridge Parkway
Redwood Shores
CA 94065
T: 1 (650) 801 6100
sales@qualys.com

UK – Qualys, Ltd.
224 Berwick Avenue
Slough, Berkshire
SL1 4QT
T: +44 (0) 1753 872101

Germany – Qualys GmbH
München Airport
Terminalstrasse Mitte 18
85356 München
T: +49 (0) 89 97007 146

France – Qualys Technologies
Maison de la Défense
7 Place de la Défense
92400 Courbevoie
T: +33 (0) 1 41 97 35 70

ON DEMAND SECURITY