Meeting Vulnerability Scanning Requirements for PCI

PCI is shorthand for the Payment Card Industry Data Security Standard (PCI-DSS) – a comprehensive set of information security requirements originally developed by MasterCard and Visa to protect personal and financial data about cardholders. PCI affects the network and IT operations of all organizations that store, process or transmit credit cardholder data, including retail stores, toll-free sales catalogs, online merchants and back-room service providers.

"More than 50% of all PCI Approved Scanning Vendors (ASVs) and Qualified Security Assessors (QSAs) use QualysGuard for vulnerability scanning."

During the last few years, an unprecedented number of exposures or losses of personal financial data by some of these organizations have triggered calls for strict regulation. The credit card industry is stepping up efforts to strengthen cardholder data security by raising member validation requirements for compliance with PCI. The current released PCI standard (version 1.1) has six categories and 12 requirements for security controls. Of those, Qualys provides the leading vulnerability scanning solution for Requirement 11, the regular testing of security systems and processes.

Testing Security Is Critical for Protecting Cardholder Data

At most, organizations with untested systems can only hope that nothing bad happens to cardholder data. Continuous, systematic vulnerability assessment is the only way to measure security, maximize protection, and achieve compliance with PCI. Regular, on-going vulnerability management provides actionable information in order to identify and fix security risks proactively. As highlighted in PCI Requirement 11: "Vulnerabilities are being discovered continually by hackers and researchers, and being introduced by new software. Systems, processes and custom software should be tested frequently to ensure security is maintained over time and with any changes in software."

PCI Standard Requires Vulnerability Scanning

Per Requirement 11.2 of the PCI Data Security Standard (DSS):

> *Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).*
>
> *Quarterly external vulnerability scans must be performed by a scan vendor qualified by the payment card industry. Scans conducted after network changes may be performed by the company's internal staff.*

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

Chief Information Officer
Tribune Broadcasting

The Need for Internal and External Scans

The PCI DSS requirements specify the need for both internal and external scans for validation. An internal scan assesses security inside the firewalled perimeter of a company's network. The purpose is to test vectors that could be susceptible to attacks originating from inside the network. An external scan assesses security of all Internet-facing hosts that could be vulnerable to attacks that originate from outside the network.

Both types of vulnerability scans are important to accurately measure network security, and to gather data that is instrumental for rapid remediation of any discovered weaknesses. For purposes of compliance with PCI DSS reporting standards, organizations must report verifiable results of vulnerability scanning once a quarter for their network perimeter audits. Those scans must be completed by a qualified scan vendor. Companies must also do internal vulnerability scans once a quarter (or more frequently as suggested), but are only required to report results of external scans at this time.

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 Q
	2	– Any merchant processing between **150,000 to 6 million transactions** per year		Required Annually Q	Required Quarterly Q
	3	– Any merchant processing **between 20,000 to 150,000 transactions** per year		Required Annually Q	Required Quarterly Q
	4	– **All other merchants** not in Levels 1, 2, or 3, regardless of acceptance channel		Required Annually Q	Required Quarterly Q
SERVICE PROVIDER	1	– **All processors and all payment gateways**	Required Annually*		Required Quarterly Q
	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 Q
	3	– Any service provider that is not in Level 1 and stores, processes or transmits **less than 1 million accounts/ transactions annually**		Required Annually Q	Required Quarterly Q

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

Q = Requirement met by QualysGuard

Qualys Solutions for PCI Compliance

- **QualysGuard PCI**
  Subset of other QualysGuard services that meets requirements for documenting external perimeter scans and submitting a self-assessment questionnaire.
- **QualysGuard Express**
  Supports full vulnerability management capabilities in addition to external and internal scans/reporting for PCI in small-to-medium sized companies.
- **QualysGuard Enterprise**
  Supports full vulnerability management capabilities in addition to external and internal scan/reporting for PCI in large companies.

Other Testing Requirements for PCI Validation

Individual payment card brands set additional requirements for PCI validation. For example, MasterCard's Site Data Protection Plan and Visa's Cardholder Information Security Program stipulate separate compliance validation requirements for merchants and service providers. These vary depending on the size of company and annual transaction volume (see chart, above). Requirements include:

Annual On-Site Security Audit – The largest companies must 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 companies must complete a yearly self-assessment questionnaire. QualysGuard automates and simplifies this requirement online.

Quarterly Network Scans – These are required of all companies and to be conducted by a certified third-party ASV or QSA. Companies may use the QualysGuard application (directly or via a Qualys partner) to meet this requirement. All 65,535 ports on external networks must be scanned, all vulnerabilities detected and any level-3 through level-5 severity vulnerabilities must be remediated. Two reports must be issued in accordance with this testing — a technical report detailing all vulnerabilities identified with solutions for remediation; also an executive summary report with a PCI-approved compliance statement suitable for submission to acquiring banks for validation.

To learn more about PCI Compliance and Qualys' solutions, visit:
http://www.qualys.com/solutions/pci_compliance/

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