QUALYS®

Mapping the Qualys Cloud Suite to the **PCI Data Security Standard** Requirements

REQUIREMENT 1:

Install and Maintain a Firewall Configuration to Protect Cardholder Data

	PCI DSS 3.2 Requirement	Qualys Coverage of Requirement	Qualys Cloud Suite
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	Qualys is able to check for the presence of firewalls and ensure appropriate configurations.	PC
1.4	Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network. Firewall configurations include: • Specific configuration settings are defined for personal firewall software. • Personal firewall software is actively running. • Personal firewall software is not alterable by users of mobile and/or employee- owned devices.	Qualys is able to check for presence of personal firewalls deployed on servers, desktops and laptops.	VM PCI
1.5	Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	Qualys can send surveys to affected parties to ensure that documentation and the location of documentation is known.	SAQ

VM = Vulnerability Management
PCI = PCI Compliance
PC = Policy Compliance
WAS = Web Application Scanning
SAQ = Security Assessment Questionnaire
WAF = Web Application Firewall

REQUIREMENT 2:

Do Not Use Vendor-Supplied Defaults for System Passwords & Other Security Parameters

	PCI DSS 3.2 Requirement	Qualys Coverage of Requirement	Qualys Cloud Suite
2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).	Qualys can verify that vendor defaults are not used by checking for default and system accounts on servers, desktops and network devices.	VM PC PCI
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST)	Qualys can effectively and automatically validate the compliance of deployed systems to configuration standards, mandated by PCI DSS.	VM PC PCI
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	Qualys can help discover systems on the network as well as detect the network exposed services that are running on systems and thus significantly reduce the effort needed to bring the environment into compliance.	VM PC PCI

	PCI DSS 3.2 Requirement	Qualys Coverage of Requirement	Qualys Cloud Suite
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.	Qualys can scan systems to determine if services or protocols that are in use are secure and if the proper settings have been implemented.	VM PC PCI
2.2.4	Configure system security parameters to prevent misuse.	Qualys policies can scan systems and ensure that best practice settings are in place to prevent misuse.	PC
2.2.5	Remove all unnecessary functionality, such as scripts, drivers, features, sub-systems, file systems, and unnecessary web servers.	Qualys can help discover some of the insecure and typically unnecessary functionality exposed to the network and thus significantly reduce the effort needed to bring the environment in compliance.	VM PC
2.3	Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non- console administrative access.	Qualys can validate that encrypted protocols are in use across the systems and that unencrypted communication is not enabled on servers and workstations (SSH, not telnet; SSL, not unencrypted HTTP, etc).	VM PC PCI

REQUIREMENT 3:

Protect Stored Cardholder Data

3.3	Mask PAN when displayed (the first gix and last four digits are the maximum number of digits to be displayed), suc that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.	Qualys can scan web applications to identify and alert when full PANs are displayed or otherwise present in web pages.	WAS

	PCI DSS 3.2 Requirement	Qualys Coverage of Requirement	Qualys Cloud Suite
3.4	Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN). • Truncation (hashing cannot be used to replace the truncated segment of PAN). • Index tokens and pads (pads must be securely stored). • Strong cryptography with associated key-management processes and procedures.	Qualys can confirm that encryption is in use across the PCI in-scope systems by checking system configuration settings relevant to encryption.	VM PC PCI
3.5	Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.	Qualys can validate security settings relevant to protection of system encryption keys. In addition, Qualys can be used to send surveys to affected parties to ensure that documentation and the location of documentation is known.	VM PC PCI SAQ

REQUIREMENT 4:

Encrypt Transmission of Cardholder Data Across Open, Public Networks

4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use.	Qualys can validate the use of strong cryptographic protocols by checking relevant system configuration settings as well as detect instances of insecure cipher use across the in-scope systems.	VM PC PCI

	PCI DSS 3.2 Requirement	Qualys Coverage of Requirement	Qualys Cloud Suite
4.1.1	Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.	Qualys can attempt to detect wireless access points from the network side and to validate the use of proper encryption across these access points.	VM PC
4.3	Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	Qualys can send surveys to affected parties to ensure that documentation and the location of documentation is known.	SAQ

REQUIREMENT 5:

Protect All Systems Against Malware & Regularly Update Anti-virus Software or Programs

5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	Qualys can validate whether antivirus software is installed on in-scope systems.	VM PC PCI
5.2	Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirement 10.7.	Qualys can validate that anti-virus mechanisms are current, perform scans and generate logs.	PC
5.3	Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	Qualys checks for running status of antivirus tools.	VM PC PCI

	PCI DSS 3.2 Requirement	Qualys Coverage of Requirement	Qualys Cloud Suite
5.4	Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	Qualys can send surveys to affected parties to ensure that documentation and the location of documentation is known.	SAQ

REQUIREMENT 6:

Develop and maintain Secure Systems and Applications

6.1	Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.	Qualys VM is the industry leading vulnerability management solution that scans systems and web applications, generates reports and prioritizes vulnerabilities identifying the most critical ones that need attention first.	VM WAS
6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor supplied security patches. Install critical security patches within one month of release.	Qualys can be used to detect missing OS and application patches and security updates. Qualys is constantly updated with new vulnerability information can be used in a process of tracking newly discovered vulnerabilities.	VM PC PCI
6.6	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes. Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2. • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	Qualys can be used to crawl and test web applications to identify vulnerabilities. In addition, Qualys is able to continually inspect web application traffic to automatically detect and block a wide range of web application attacks.	WAS WAF PCI

VM = Vulnerability Management
PCI = PCI Compliance
PC = Policy Compliance
WAS = Web Application Scanning
SAQ = Security Assessment Questionnaire
WAF = Web Application Firewall

	PCI DSS 3.2 Requirement	Qualys Coverage of Requirement	Qualys Cloud Suite
6.7	Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	Qualys can send surveys to affected parties to ensure that documentation and the location of documentation is known.	SAQ

REQUIREMENT 7:

Restrict Access to Cardholder Data By Business Need-to-Know

7.1	Limit access to system components and card- holder data to only those individuals whose job requires such access.	Qualys can analyze database user right and permissions, looking for broad and insecure permissions.	PC
7.3	Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	Qualys can send surveys to affected parties to ensure that documentation and the location of documentation is known.	SAQ

REQUIREMENT 8:

Assign a Unique ID to Each Person with Computer Access

8.1	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components.	Qualys can identify active default, generic accounts (root, system, etc) and indicate if they are active and have appropriate privileges.	PC
8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts.	Qualys can evaluate system configuration settings and determine if the proper lockout threshold is set.	PC
8.1.7	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	Qualys can evaluate system configuration settings and determine if the proper lockout duration is set.	PC

	PCI DSS 3.2 Requirement	Qualys Coverage of Requirement	Qualys Cloud Suite
8.1.8	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	Qualys can evaluate system configuration settings to determine that settings for idle timeout value is set properly.	PC
8.2	In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase. • Something you have, such as a token device or smart card. • Something you are, such as a biometric.	Qualys can identify user accounts with improper authentication settings, such as accounts with no passwords or with blank passwords.	VM PC PCI
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/ phrases) unreadable during transmission and storage on all system components.	Qualys can evaluate system configuration settings to determine if credentials are properly encrypted.	VM PC PCI
8.2.3	Passwords/passphrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above.	Qualys can evaluate system configuration settings to determine if password length and complexity are enforced by the system.	PC
8.2.4	Change user passwords/passphrases at least once every 90 days.	Qualys can evaluate system configuration settings to determine if the password expiration settings are enforced by the system.	PC

	PCI DSS 3.2 Requirement	Qualys Coverage of Requirement	Qualys Cloud Suite
8.2.5	Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/ passphrases he or she has used.	Qualys can evaluate system configuration settings to determine if the password history settings are enforced by the system.	PC
8.7	All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).	Qualys can validate user account security settings and password security parameters across systems.	PC

REQUIREMENT 9:

Restrict Physical Access to Cardholder Data

9.9	Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.	Qualys scans POS terminals to ensure proper configuration and detect and report on vulnerabilities and out of date or unpatched systems.	PC

REQUIREMENT 10:

Track & Monitor all Access to Network Resources and Cardholder Data

10.1	Implement audit trails to link all access to system components to each individual user.	Qualys logs and creates audit trails that links individual access to systems components.	PC

	PCI DSS 3.2 Requirement	Qualys Coverage of Requirement	Qualys Cloud Suite
10.2	Implement automated audit trails for all system components to log and reconstruct events related to access of cardholder data, identification mechanisms, invalid logical access attempts, changes to system logs and creation and deletion of system-level objects etc.	Qualys automatically creates logs and audit trails which can later be read to reconstruct events.	PC
10.4	Using time- synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	Qualys logs / audit trails are time stamped and synchronized to ensure appropriate logging of events.	PC
10.5	Secure audit trails so they cannot be altered.	Qualys can secure audits by limiting change access to administrators only.	PC
10.9	Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.	Qualys can send surveys to affected parties to ensure that documentation and the location of documentation is known.	SAQ

REQUIREMENT 11:

Regularly Test Security Systems and Processes

11.1	Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.	Qualys is used to scan for vulnerabilities both from inside and from outside the network. Qualys is an Approved Scanning Vendor (ASV) by the PCI Council and can be used for both external scanning or ongoing internal scanning.	VM PC

	PCI DSS 3.2 Requirement	Qualys Coverage of Requirement	Qualys Cloud Suite
11.2	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).	Qualys is used to scan for vulnerabilities both from inside and from outside the network. Qualys is an Approved Scanning Vendor (ASV) by the PCI Council and can be used for both external scanning or ongoing internal scanning.	VM PCI
11.3	Implement a methodology for penetration testing that includes the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800- 115). • Includes coverage for the entire CDE perimeter and critical systems. • Includes testing from both inside and outside the network. • Includes testing to validate any segmentation and scope-reduction controls. • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. • Defines network-layer penetration tests to include components that support network functions as well as operating systems. • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months. • Specifies retention of penetration testing results and remediation activities results.	Qualys includes active penetration testing that can be automated to run at specific intervals and reports on the status of all tests so that you can understand the risks to your network.	VM PCI WAS WAF

The Qualys Cloud Platform and its integrated suite of security and compliance applications provides organizations of all sizes with a global view of their security and compliance solutions, while drastically reducing their total cost of ownership. Qualys solutions include: continuous monitoring, vulnerability management, policy compliance, pci compliance, questionnaire service, log management, web application scanning, web application firewall, malware detection and SECURE Seal for security testing of web sites..

Qualys, Inc. (NASDAQ: QLYS)
Headquarters
1600 Bridge Parkway Redwood City,
CA 94065 USA
T: 1 (800) 745 4355, info@qualys.com

Qualys is a global company with offices around the world. To find an office near you, visit **http://www.qualys.com**