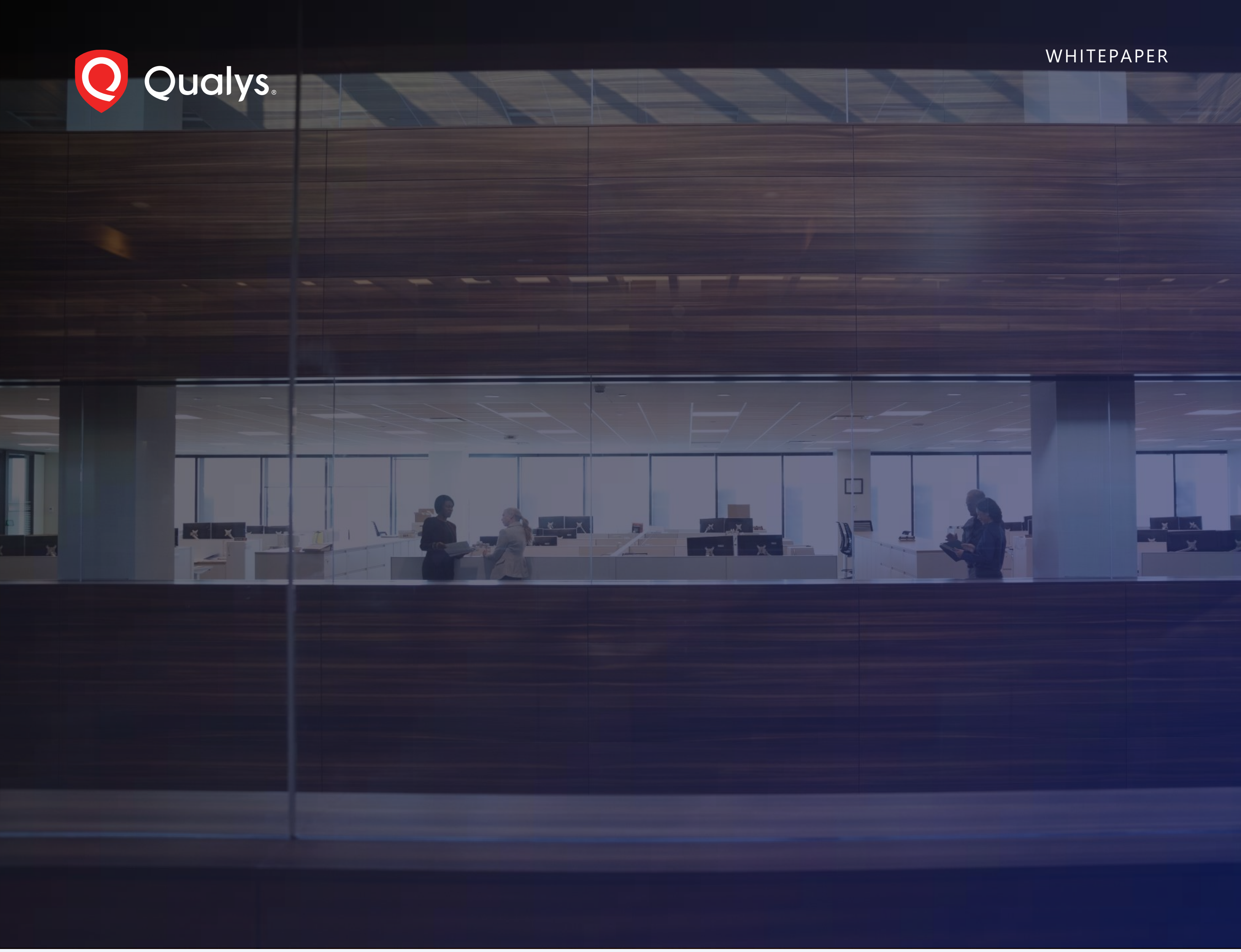
WHITEPAPER



PCI DSS 4.0: Ensuring Compliance with the New Requirements

Contents

Compliance is an ongoing requirement for organizations of all sizes. Obligations may include national and international laws, government regulations, frameworks, and operating requirements set by specific industry or government entities. Compliance for cybersecurity is a major driver and one of its most prominent requirements is the Payment Card Industry's Data Security Standard (PCI DSS).

The industry's PCI Council created PCI DSS to ensure security for the global payment system. PCI DSS globally applies to all entities that store, process, or transmit payment cardholder data (CHD) or sensitive authentication data (SAD) or could impact the security of the cardholder data environment (CDE). Specifically, this includes all entities involved in payment account processing. If your company is a merchant, processor, acquirer, issuer, or other related service provider, **even if your credit card provider uses tokenization**, you must comply with PCI DSS mandates or face potentially stiff penalties. Policies are set by the Executive Committee, which includes American Express, Discover Financial Services, JCB International, Mastercard, UnionPay, and VISA, Inc.

This whitepaper describes what PCI DSS means for payment data security, where risks reside, what's required for compliance, and how the Qualys Cloud Platform automatically fulfills vital elements for compliance while reducing risk to sensitive data.

Why PCI DSS Matters Today

Since its origin in 2004, PCI DSS is the cybersecurity model followed even outside the payment industry due to its comprehensive, systematic approach to establishing and maintaining security of payment data. Some may joke about various compliance regimes as merely checking off the boxes. But with PCI DSS, if your organization follows the standard, it will, in return, earn the highest probability of having true security for sensitive data.

In other words, compliance is not just a burden, but can be your best friend in achieving strong security. On the flip side, if you fail to comply, credit card companies may "pull your plug" and restrict or remove your ability to accept credit card payments. Tokenization helps, if used by your credit card provider, but you likely still need to comply with PCI DSS requirements. This is especially true if you collect marketing data on customers. The brand damage and revenue risk for PCI DSS compliance failures are exceedingly high. Fines of up to $100,000 per month can be levied for larger firms, and can start at $5,000 per month for smaller organizations.

Even more concerning, most U.S. States now have stringent Civil Codes, such as the California Consumer Privacy Act (CCPA), that slap firms with penalties and fines for exposing Personally Identifiable Information (PII), such as anything related to credit card data. Most states also allow for a "private cause of action" that lets attorneys sue on behalf of private citizens for such exposure. Legal discovery and court costs can easily soar into the millions of dollars, followed by brand-damaging headlines.

Experts say PCI DSS sets the gold standard for cybersecurity. The scope of the newest version, 4.0, is enormous. There are six tactical goals, twelve primary requirements, and hundreds of sub-requirements and testing procedures – 356 pages in all. Version 4.0 also introduces two approaches to compliance. One is the legacy "defined" approach, which strictly follows the technical and process requirements and testing procedures. The other is a risk-based approach allowing a customized process or a blend of defined and custom processes.

For security and compliance professionals, perhaps the most frustrating aspect of pursuing PCI DSS compliance is no single vendor provides all the tools and services required. Consequently, establishing and maintaining PCI DSS compliance processes can be complex, from smaller businesses to large enterprises. To understand why, let's consider where potential vulnerabilities reside and how PCI DSS 4.0 addresses these via its new requirements.

Where PCI DSS Vulnerability Risks Reside

PCI DSS requirements aim for vulnerabilities potentially occurring anywhere in the payment-processing ecosystem. If your company uses physical or virtual devices, systems, or services like these, you'll want to pay attention.

- Cloud-based systems
- Endpoint devices (mobile, laptop, PC)
- Paper-based storage systems
- Point-of-sale devices
- Remote access connections
- Windows and Linux servers
- Transmission of cardholder data to service providers
- Vulnerabilities in systems operated by service providers and acquirers
- Web-shopping applications
- Wireless hotspots

Vulnerabilities may appear in other resources whose potential scope extends to hardware, software, networking, applications, supply chain, partners, and service providers; no wonder achieving payment security is a big challenge. And hence the reason why the scope of PCI DSS is so broad – it must address a multitude of potential vulnerabilities across many disciplines.

What PCI DSS 4.0 Requires for Compliance

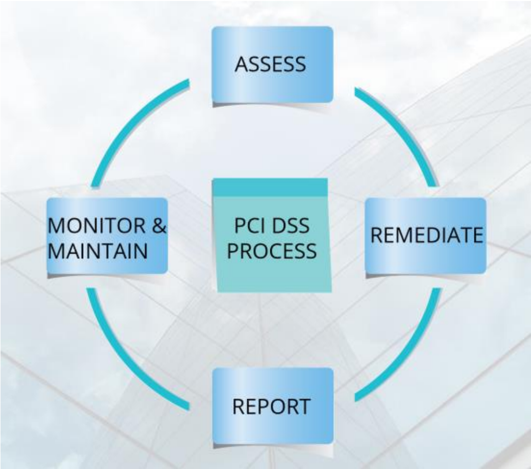
PCI DSS version 4.0 was announced in March 2022 and has 64 requirements that organizations must meet. The requirements are divided into two phases, with 13 requirements becoming mandatory on March 31, 2024, and the remaining 51 becoming mandatory on March 31, 2025. The PCI Council set four strategic goals for version 4.0:

1. Continue to meet the security needs of the payment industry. This includes stronger requirements for multi-factor authentication, passwords, and e-commerce/phishing.
2. Promote security as a continuous process. This clarifies guidance on implementing and maintaining security (see below).
3. Add flexibility for different methodologies. An acknowledgement that one size does not fit all, and some organizations need flexibility in their approach to compliance.
4. Enhance validation methods. Entails closer alignment of the Report on Compliance or Self-Assessment Questionnaire (SAQ) and Attestation of Compliance.

Four-Step Process for Compliance

With PCI DSS 4.0, the PCI Council provides four ongoing steps that organizations should use to protect payment account data. As described by its *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 4.0* (p. 4), these steps are:

1. Assess – identifying all locations of payment account data, taking an inventory of all IT assets and business processes associated with payment processing, analyzing them for vulnerabilities that could expose payment account data, implementing or updating necessary controls, and undergoing a formal PCI DSS assessment.
2. Remediate – identifying and addressing any gaps in security controls, fixing identified vulnerabilities, securely removing any unnecessary payment data storage, and implementing secure business processes.
3. Report – documenting assessment and remediation details, and submitting compliance reports to the compliance-accepting entity (typically, an acquiring bank or payment brands)
4. Monitor and Maintain – confirming that security controls put in place to secure the payment account data and environment continue to function effectively and properly throughout the year. These “business as usual” processes should be implemented as part of an entity’s overall security strategy to help ensure protection on an ongoing basis.



Note that process methodologies for using Qualys Vulnerability Management, Detection and Response (VMDR) and other applications for the Qualys Cloud Platform are completely aligned with the PCI Council's four-step process. We'll address specific synergies below.

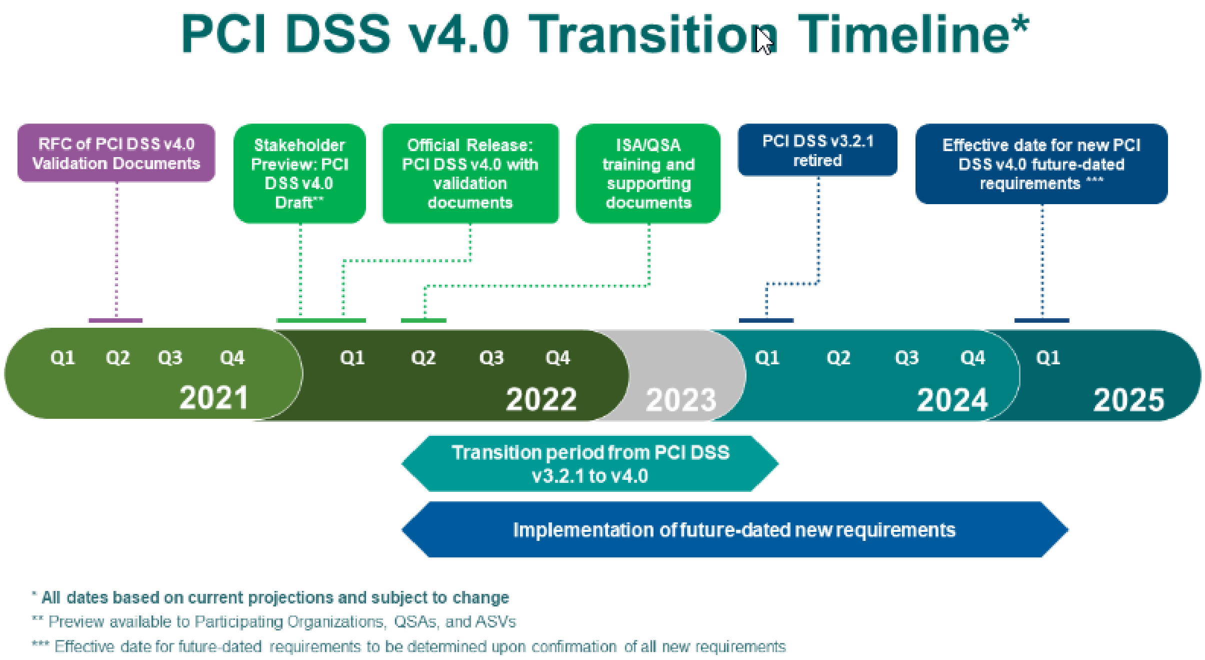
Goals and Requirements for PCI DSS 4.0

The bulk of PCI DSS 4.0 is articulation of its six tactical goals and 12 requirements. In the version 4.0 table below, a few items were tweaked but virtually all are identical to the previous version 3.2.1. Security and compliance professionals will be familiar with this table as it underpins all related compliance activity. While the third goal is about vulnerability management, all the goals and requirements are fundamental to every security program – akin to a "12-Step Program for Cybersecurity." The PCI Council also notes this similarity (see the *Quick Reference Guide*, p. 8), so everything your organization does for PCI DSS 4.0 compliance will also help protect against threats and secure elements of the entire IT ecosystem. It's another reason why the Qualys Cloud Platform is integral for compliance, as well as general cybersecurity.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	Install and maintain network security controls Apply secure configurations to all system components
Protect Account Data	Protect stored account data Protect cardholder data with strong cryptography during transmission over open, public networks
Maintain a Vulnerability Management Program	Protect all systems and networks from malicious software Develop and maintain secure systems and software
Implement Strong Access Control Measures	Restrict access to system components cardholder data by business need to know Identify users and authenticate access to system components Restrict physical access to cardholder data
Regularly Monitor and Test Networks	Log and monitor all access to system components and cardholder data Test security systems and networks regularly
Maintain an Information Security Policy	Support information security with policies and programs

Applying controls and processes to comply with PCI DSS 4.0 seems like a massive exercise, but the standard eases this by allowing the use of segmentation to reduce scope of compliance. Segmentation entails separating the cardholder data environment (CDE) – everything that's subject to compliance – from everything else in an organization's IT infrastructure. For example, segmentation may include physical servers, data storage, or networking devices; it also may include virtual instances of the same within the organization's cloud. Special segmentation rules exist for the use of third-party service providers (see Requirement 12.8 and Appendix A1). The use of segmentation can dramatically reduce the scope of what must be protected and simplifies the PCI DSS validation audit process of remaining in-scope assets.

"PCI compliance" loosely applies to fulfilling requirements of PCI DSS 4.0. But it's not the only standard for payment security. The PCI Council currently manages fifteen different PCI Security Standards.


PCI DSS v4.0 Transition Timeline*

RFC of PCI DSS v4.0 Validation Documents
Stakeholder Preview: PCI DSS v4.0 Draft**
Official Release: PCI DSS v4.0 with validation documents
ISA/QSA training and supporting documents
PCI DSS v3.2.1 retired
Effective date for new PCI DSS v4.0 future-dated requirements ***
Q1
Q2
Q3
Q4
2021
Q1
Q2
Q3
Q4
2022
2023
Q1
Q2
Q3
Q4
2024
Q1
2025
Transition period from PCI DSS v3.2.1 to v4.0
Implementation of future-dated new requirements

* All dates based on current projections and subject to change

** Preview available to Participating Organizations, QSAs, and ASVs

*** Effective date for future-dated requirements to be determined upon confirmation of all new requirements

Data courtesy of PCI Security Standards Council

How Qualys Drives PCI DSS 4.0 Compliance

The Qualys Enterprise TruRisk Platform includes over twenty apps, and many of these can help organizations ensure PCI DSS 4.0 compliance in two ways: One is by enabling automatic documentation of compliance – this is a status check of whether many of the controls for PCI DSS 4.0 requirements are in place, and whether they are doing their respective jobs. Two, with various integrated Qualys security applications such as Vulnerability Management, Detection & Response, Web Application Scanning, Policy Compliance, File Integrity Monitoring, and several others, the platform provides specific controls for a robust subset of PCI DSS 4.0 requirements.

Compliance rules like PCI DSS 4.0 force security stakeholders to do two types of checks: ensure required controls are in place, and verify the controls are working as needed. Qualys helps automate this process with two applications for the Qualys Cloud Platform.

Some mid-sized and most large enterprises must use a Qualified Security Assessor (QSA) to conduct a PCI DSS audit, verify compliance, and submit results in a formal Report on Compliance. Performing this process can be an onerous, time-consuming task depending upon the size and complexity of the in-scope cardholder data environment. Organizations using this approach also place their cardholder and sensitive authentication data in potential jeopardy as the required annual assessment is just that – a point in time measurement that within hours, could fall out of compliance if one or more controls fail. The PCI Council advises stakeholders that "compliance is not always equivalent to security" – a point driven home by the 24x7 barrage of attacks against all internet-facing environments. Hence the provision of a 4-step continuous process for compliance described above.

Outlined below are several Qualys solutions with descriptions showing how each of these can help ensure compliance for various PCI DSS 4.0 requirements.

Qualys Policy Compliance (PC) enables continuous assessment of the cardholder data environment. Qualys PC provides a ready-to-use mandate-based template for PCI DSS 4.0 consisting of security checks that automate the assessment of in-scope PCI assets. These checks automatically scan technical secure configuration assessment requirements.

Qualys PC provides support for different in-scope operating systems, databases, web servers, devices, and so forth. It also simplifies and accelerates the formal annual PCI DSS assessment via collaboration with the Qualified Security Assessor – including automatic generation of the Report on Compliance. The ability to create custom dashboards and reports ensures an always audit ready status should an auditor require something non-standard.

Numerous requirements in almost every section refer to Policy Compliance capabilities, such as ensuring that "all changes to network connections and changes to configurations of network security controls are approved and tested in accordance with Requirement 6.5.1." Qualys PC enables you to automate security configuration evaluations and rapidly identify compliance with the PCI DSS v4.0 technical security requirements. Qualys PC also provides out-of-the-box reports that customers can run to quickly document their preparation for PCI DSS v4.0 Standard. Qualys has released a ready-to-use mandate-based template for PCI DSS v4.0 consisting of security checks that automate the assessment of 'in-scope' PCI assets. This template simplifies the process merchants must undertake to validate PCI compliance for a key set of technical controls that need to be validated across different technologies. Qualys PC can now automatically scan for all these PCI controls and provide a detailed report to validate ongoing compliance.

Qualys Security Assessment Questionnaire (SAQ) helps mid-sized and smaller enterprises use an instrument prescribed by PCI DSS 4.0 called a Self-Assessment Questionnaire (SAQ). As the link explains, there are nine different SAQs, which correspond to your type of organization and environment. Eligible organizations can use the SAQ to self-evaluate their compliance with PCI DSS. Validation results are submitted to the organization's acquiring bank or payment brand(s) with an Attestation of Compliance.

Without adding another agent to manager, organizations can use the app included with Qualys Compliance helps automate the process of collecting and validating required information and completing the SAQ. Business process control automation includes all stakeholders inside and outside your organization. Simplified questionnaires are automatically sent to appropriate respondents who enter results into a browser. Pre-formatted SAQ templates may be customized as needed. Respondents may electronically delegate questions to peers who are better able to answer them, especially if collecting the information requires human action. The final SAQ is automatically prepared for submission and can then be submitted to the acquirer or payment brand(s). Qualys SAQ makes the process easy, accurate, comprehensive, centralized, scalable, and uniform across your entire organization.

Qualys Vulnerability Management, Detection, and Response (VMDR) – VMDR is a foundational solution for managing CDE cyber risks (Req. 2, 5, 6, 11). It addresses the third goal for a CDE vulnerability management program, and Requirement 11's need for regularly testing security of CDE systems and networks. VMDR excels at detecting internal and external risks, and efficiently responding to vulnerabilities. Authenticated scanning is a new PCI DSS 4.0 requirement. Unlike other scanners, VMDR performs authenticated scans, such as for certificate inventory. VMDR also includes Qualys PCI ASV Compliance to ensure compliance for external scans, which require ASV. As an Approved Scanning Vendor (ASV), Qualys has been authorized by the PCI Security Standards Council to conduct the quarterly scans required to show compliance with PCI DSS. This helps ensure accurate and effective PCI ASV compliance testing, reporting, and submission.

Qualys Web Application Scanning (WAS) – WAS continuously detects vulnerabilities and misconfigurations of CDE internal and external-facing web applications (Req. 6, 11). This app finds malware in web apps and informs DevOps teams on exposed payment data and other PII.

Qualys File Integrity Monitoring (FIM) – FIM provides "low-noise" CDE integrity monitoring efforts and compliance (Req. 1, 10, 11, 12), including unauthorized modification and change detection that accurately separates false alerts from positive hits and allows for whitelisting. Qualys FIM also includes File Access Monitoring (FAM) to alert on unauthorized file access and agentless network device support. Both are now needed to comply with new PCI DSS 4.0 requirements.

Qualys CyberSecurity Asset Management (CSAM) with External Attack Surface Management (EASM) – CSAM provides an accurate, context-rich inventory of all CDE cyber assets to identify security gaps (Req. 2) and CSAM provides full visibility and control of the CDE's external attack surface (Req. 2, 12).

Qualys Patch Management – Patch Management enables automating the entire patching process for operating systems, mobile devices and third-party applications – even for remote devices within the cardholder data environment (Req. 1, 6, 10, 11).

Custom Assessment & Remediation – PCI DSS 4.0 requires organizations to maintain an up-to-date inventory of all bespoke and custom software, including APIs. CAR creates reusable custom detections and remediations while allowing for deployment of custom configurations.

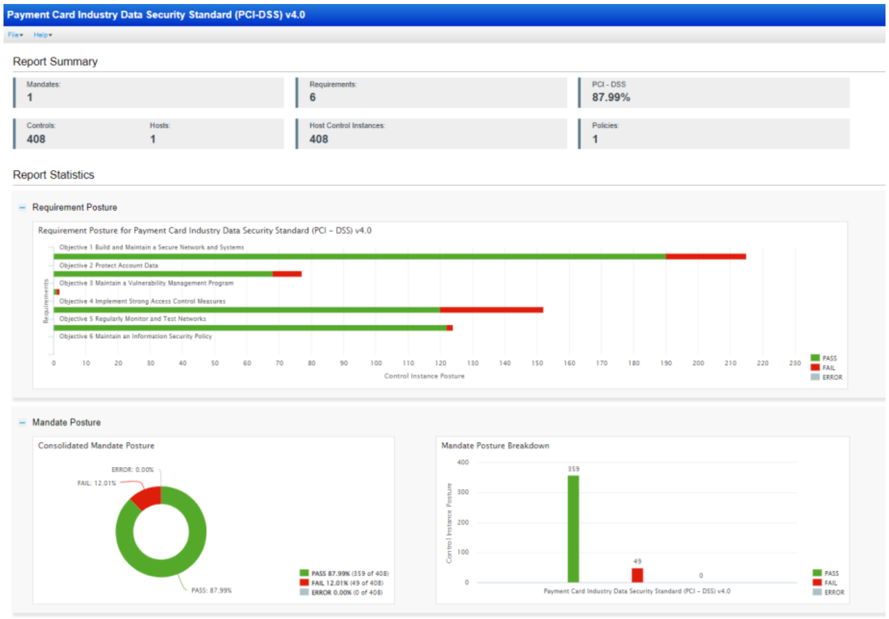
Qualys TotalCloud – PCI DSS 4.0 includes several requirements that refer to cloud controls such as access controls, monitoring and logging, incident response, patching and updates, scans, and more. Qualys TotalCloud can measure risk with 360-degree scanning to detect vulnerabilities and detect malware with up to 99 percent accuracy.

Qualys Multi-Vector Endpoint Detection and Response (EDR) – EDR is recommended to integrate vulnerability management of the CDE with endpoint threat detection and response (Req. 5, 12).

Qualys Context XDR – Extended Detection and Response should be added to accelerate remediation of complex, advanced threats to the CDE using MITRE ATT&CK-driven threat hunting and analytics (Req. 10).

The mandate template for PCI DSS v4.0 provides:

- Effective controls for an organization and the ability to quickly report on implicit PCI DSS v4.0 requirements.
- Coverage of all technical secure configuration assessment requirements
- Support for different 'in-scope' operating systems, databases, web servers, network devices, etc.


Payment Card Industry Data Security Standard (PCI-DSS) v4.0
File▾
Help▾

Report Summary

Mandates: 1
Requirements: 6
PCI - DSS 87.99%
Controls: 408
Hosts: 1
Host Control Instances: 408
Policies: 1

Report Statistics

Requirement Posture
Requirement Posture for Payment Card Industry Data Security Standard (PCI – DSS) v4.0
Objective 1 Build and Maintain a Secure Network and Systems
Objective 2 Protect Account Data
Objective 3 Maintain a Vulnerability Management Program
Objective 4 Implement Strong Access Control Measures
Objective 5 Regularly Monitor and Test Networks
Objective 6 Maintain an Information Security Policy
Requirements
0
10
20
30
40
50
60
70
80
90
100
110
120
130
140
150
160
170
180
190
200
210
220
230
Control Instance Posture
PASS
FAIL
ERROR
Mandate Posture
Consolidated Mandate Posture
ERROR: 0.00%
FAIL: 12.01%
PASS: 87.99%
PASS 87.99% (359 of 408)
FAIL 12.01% (49 of 408)
ERROR 0.00% (0 of 408)
Mandate Posture Breakdown
400
300
200
100
0
Control Instance Posture
359
49
0
Payment Card Industry Data Security Standard (PCI – DSS) v4.0
PASS
FAIL
ERROR

PCI DSS 4.0 Solution Matrix

Below is a matrix showing many of the PCI DSS 4.0 requirements mapped to various Qualys solutions, along with descriptions of how each solution can help ensure compliance with each requirement.

PCI DSS 4.0 Requirement	Qualys App	Capabilities
1.2: Network security controls (NSCs) are configured and maintained.	Qualys PC, FIM, TotalCloud (TC)	FIM provides support for agentless network devices. TC offers visibility into workloads and misconfigs across multi-cloud env.
2.2: System components are configured and managed securely.	Qualys VMDR, PC, CSAM	VMDR discovers vulnerabilities, PC finds misconfigurations. CSAM does external/internal asset classification.
2.3: Wireless environments are configured and managed securely.	Quays PC	PC discovers misconfigurations for all environments.
3.3: Sensitive authentication data is not stored after authorization.	Qualys PC	PC helps cover this requirement by providing visibility into sensitive authentication data.
3.4: Access to displays of full PAN, ability to copy account data is restricted.	Qualys PC	PC helps cover this requirement by providing visibility into this data.

3.6: Cryptographic keys used to protect stored account data are secured.	Qualys PC	PC helps cover this requirement by providing visibility into this data.
4.2: PAN is protected with strong cryptography during transmission.	Qualys PC	PC helps cover this requirement by providing visibility into this data.
5.2: New: Malicious malware is prevented, or detected and addressed.	Qualys PC, EDR	EDR detects and protects against malicious malware, PC auto remediates misconfigurations found in EDR.
5.3: New: Anti-malware mechanisms and processes are active, maintained...	Qualys PC, EDR, VMDR	VMDR performs periodic scans, EDR and PC provide continuous behavioral analysis of systems or processes
6.2: Bespoke and custom software is developed securely.	Qualys VMDR, PC	VMDR and PC help meet this requirement by providing visibility into this data.
6.4: Public-facing web applications are protected against attacks.	Qualys WAS	WAS helps protect public-facing web applications.
6.3: Security vulnerabilities are identified and promptly addressed.	Quays CSAM, PM, VMDR, TC, PC	PM ensures patches are installed. TC remediates cloud vuln, VMDR identifies vulnerabilities, CSAM inventories assets.
6.3.1: Risk based assessment approach for vulnerability management.	Qualys VMDR	Elevate VM to risk-based VM program with business context Vulnerabilities for bespoke and custom software are covered
6.5: Changes to all system components are managed securely.	Qualys PC	PC helps detect misconfiguration changes to components.
7.2: Access to displays of full PAN, ability to copy account data is restricted.	Qualys PC, FIM	PC helps cover this requirements. FIM supports role-based access control.
8.2/3/4/5/6: User identification and related accounts for users...	Qualys PC	PC helps cover this requirement by providing visibility into this data.
10.2/3/5: Audit logs are implemented to	Qualys PC, FIM	PC helps cover this requirements. FIM maintains audit logs on any File Access Management (FAM) and file integrity, and captures user access to card holder data.

support the detection of anomalies…		
10.4: New requirement for automated mechanisms for audit log reviews.	Qualys FIM	File Access Monitoring (FAM) covers all user access even if integrity is not modified. FIM has SIEM integration for insights.
10.7: Failures of critical security control systems are detected, reported…	Qualys TC, FIM, PC, EDR, CAR	Several apps help cover this: TotalCloud, EDR, PC. FIM provides automated alerts and reports for failure of FIM solution.
11.3: External and internal vulnerabilities are regularly identified, prioritized…	Qualys VMDR, PC, PCI ASV	Qualys VMDR PCI ASV included with VMDR covers external scanning.
11.3.1.2: New requirement: authenticated internal vulnerability scans.	Qualys VMDR	VMDR covers requirements for internal scanning authentication.
11.4: External and internal penetration testing, exploitable vulnerabilities and security weaknesses are corrected.	Quays VMDR, PC, TC	PM ensures patches are installed. PC discovers misconfigs, VMDR identifies vulnerabilities, CSAM inventories assets.
11.5: Network intrusions and unexpected file changes are detected…	Quays FIM, EDR, PC	PM ensures patches are installed. PC discovers misconfigs, VMDR identifies vulnerabilities, CSAM inventories assets. FIM on PCI-scoped assets offers comprehensive coverage.
6.3.1: Risk based assessment approach for vulnerability management.	Qualys VMDR	Elevate VM to risk-based VM program with business context Vulnerabilities for bespoke and custom software are covered
6.5: Changes to all system components are managed securely.	Qualys PC	PC helps cover this requirement by providing visibility into system components.
12.1/3/4/5/8: A comprehensive information security policy…for protection of the entity's information assets…	Qualys CSAM, FIM, CAR	CSAM provides an inventory of system components that are in scope for PCI DSS. FIM provides daily logs related to file changes for review & offers an Incident Management Workflow that allows manual and automated incident creation.

Conclusions

Compliance with PCI DSS 4.0 is an important topic applicable to millions of organizations around the world. Following the requirements with the PCI Council's recommended 4-step continuous process of Assess, Remediate, Report, and Monitor and Maintain will place your organization on a proven path toward full compliance and reduce the risks of brand damage, fines, and litigation. As a major additional benefit, your organization will also ensure a strong cybersecurity posture across the enterprise IT environment. When used as an enabler of this process, the Qualys Compliance Solution Set offers integrated applications to simplify and help automate the compliance process and keep your cardholder data environment secure. To learn more details about PCI DSS, read the full text of PCI DSS 4.0 and other supporting documents in the PCI DSS v4.0 Resource Hub on the PCI Council website. We also invite you to learn more about how you can use Qualys to achieve PCI DSS 4.0 compliance and start your free trial.

Contributors:

Bill Reed, Qualys Product Marketing