WHITEPAPER

# PCI DSS 4.0: Three Critical Compliance Considerations

## Contents

If your company is a merchant, processor, acquirer, issuer, or other related service provider, it must comply with the Payment Card Industry's Data Security Standard (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.

PCI DSS version 4.0 introduced sixty-four new requirements, most designed to ensure compliance for cybersecurity by preventing the exposure of customer Personally Identifiable Information (PII).

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 – even if you're just selling T-shirts on a company website, and even if your credit card company provides transaction tokenization.

This whitepaper describes what PCI DSS means for payment data security, where risks reside, what's required for compliance, and how three critical compliance considerations should not be overlooked to help prevent audit failures, security breaches, brand damage, and litigation.

## Why PCI DSS Matters Today

Compliance can be challenging, but it can also be rewarding if it helps you avoid serious consequences. If you fail to comply, credit card companies may restrict or remove your ability to accept credit card payments. The brand damage and revenue risk for PCI DSS compliance failures can include fines of up to $100,000 per month for larger firms or $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.

Many experts say PCI DSS sets the bar for cybersecurity. The scope of the latest version, 4.0, is enormous. There are six tactical goals, twelve primary requirements, and hundreds of sub-requirements and testing procedures covering 356 pages. 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 to best fit your organization’s needs.

For security and compliance professionals, perhaps the most frustrating aspect of pursuing PCI DSS compliance is no single solution provides everything required to fully comply. 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.

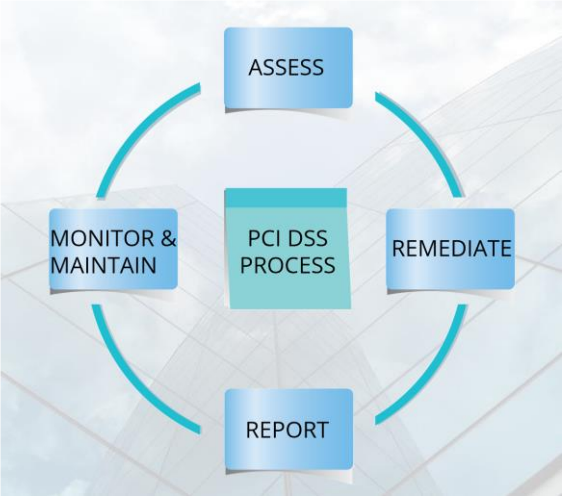
- Cloud-based systems
- Endpoint devices (mobile, laptop, PC)
- Paper-based storage systems
- Point-of-sale devices
- Remote access connections
- Windows and Linux servers
- Transmission of cardholder data to service providers
- Vulnerabilities in systems operated by service providers and acquirers
-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

## PCI DSS 4.0 Four Step Process

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.

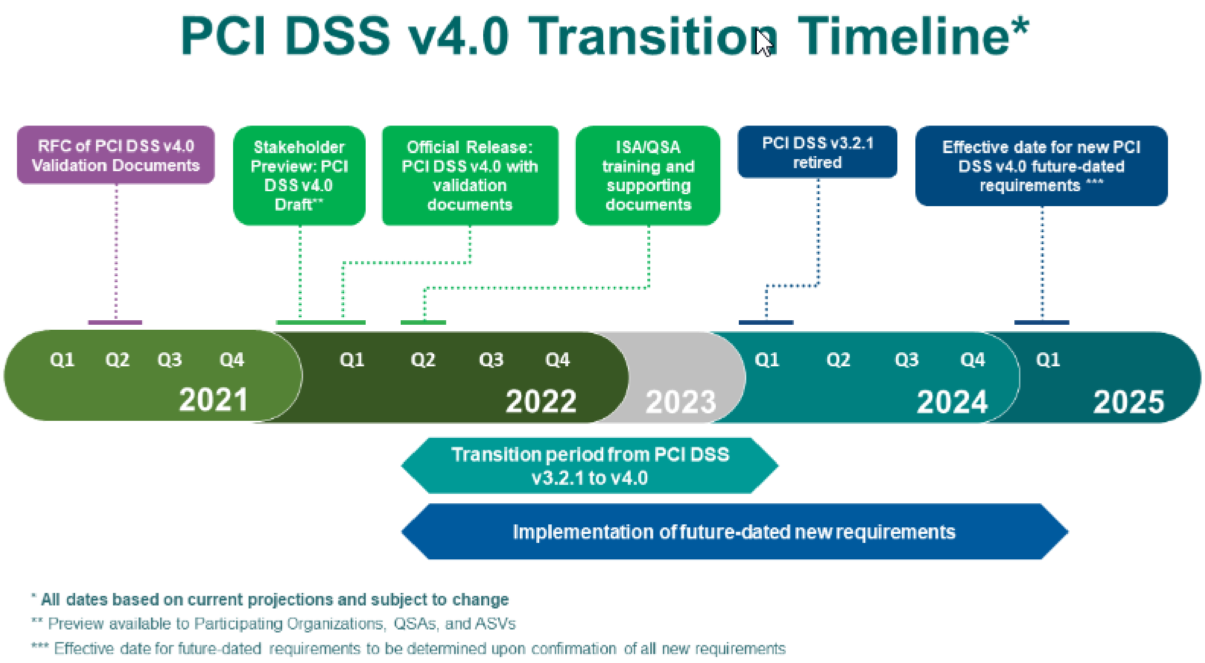


Note that process methodologies for using Qualys Vulnerability Management, Detection and Response (VMDR) and other applications for the Qualys Cloud Platform are completely aligned with the PCI Council's four-step process. We'll address specific synergies below.

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

## The Qualys PCI DSS 4.0 Compliance Trio

The Qualys TruRisk Enterprise Platform can help you take a giant step toward ensuring 97 percent compliance for PCI DSS 4.0 by starting with three key apps. These include Policy Compliance (PC), File Integrity Monitoring (FIM), and Endpoint Detection and Response (EDR). These three Qualys apps are designed to augment Qualys Vulnerabilty Management Detection and Response (VMDR) which comes with the Qualys PCI Approved Scanning Vendor (ASV) app. Today, the Quays Cloud Platform provides more than two dozen integrated applications for security and compliance addressing a broad spectrum of requirements. As such, Qualys is well-suited for addressing a robust range of security control requirements for PCI DSS 4.0.

Describing every requirement and sub-requirement addressed by Qualys is beyond the scope of this whitepaper. If your security team needs more details, please click here to contact Qualys for a detailed map showing how Qualys applications meet each PCI DSS 4.0 requirement. Here are examples of how we can do this through the Qualys Cloud Platform by using a single agent:

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. It even performs authenticated scans, such as for certificate inventory, which other scanners are unable to do. Qualys VMDR also includes Qualys PCI ASV, which is an important component but will not ensure full PCI compliance.

## 1. Qualys Policy Compliance

Qualys Policy Compliance (PC) includes a comprehensive PCI DSS 4.0 dashboard that lets you identify and remediate issues efficiently, manage mandates within a single pane of glass, and generate audit-friendly reports. 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 of the standard. Regulatory-centric reporting templates make it easy to produce custom reports quickly to satisfy "on-demand" auditor requirements.

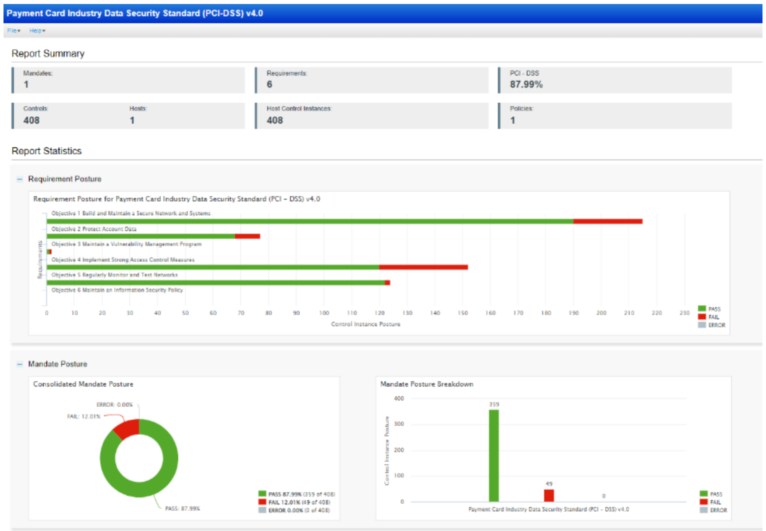
Qualys PC offers over 900 policies, 20,000 controls, 350 technologies, and 100 regulations for compliance. For cybersecurity, it also helps you gain up to 81 percent coverage against MITRE ATT&CK tactics and techniques compared to only 53 percent with Vulnerability Management alone. Misconfigurations account for most security breaches. Now you can simplify, expand, and automate compliance for the latest mandates while increasing your security hardening score to 79 percent compared to only 51 percent with other solutions.

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 for PCI DSS 4.0 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 PC now includes tight integration with Qualys EDR. When threats are detected with Qualys EDR, one click directs you to a tab in PC to initiate an automated remediation workflow.



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

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

− Mandate Posture

Consolidated Mandate Posture

🟩 PASS 87.99% (359 of 408)
🟥 FAIL 12.01% (49 of 408)
▨ ERROR 0.00% (0 of 408)

Mandate Posture Breakdown

## 2. Qualys File Integrity Monitoring

Qualys File Integrity Monitoring (FIM) is an essential layer of defense for any small, medium, or large enterprise network. FIM solutions identify illicit activities across critical system files and registries, diagnose changes, and send alerts. Selecting the right FIM for your organization is critical for achieving compliance and cybersecurity best practices. The best FIM solutions should include noise cancellation, File Access Monitoring (FAM), and agentless support for network device monitoring. 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.

FIM addresses these specific PCI DSS 4.0 requirements:

- 10.2.1.1: Need to capture all individual user access to cardholder data as A record of all individual access to cardholder data can identify which accounts may have been compromised or misused.
- 10.2.1.2: Need to capture all access by administrators as Accounts with increased access privileges, such as the "administrator" or "root" account, have the potential to significantly impact the security or operational functionality of a system.
- 10.2.1.3: Need to capture all access to audit logs as Malicious users often attempt to alter audit logs to hide their actions. A record of access allows an organization to trace any inconsistencies or potential tampering of the logs to an individual account.
- 10.2.1.4: Need to ensure that all invalid access attempts are captured.

File Access Monitoring (FAM) is uniquely included with Qualys FIM and is a security practice that involves tracking and logging access to sensitive files. FAM should be included with any FIM solution to trigger alerts when critical host files, not intended for regular use, are accessed. Any FIM solution should include FAM to also ensure cybersecurity best practices and meet minimum compliance requirements. For example, many PCI DSS 4.0 requirements now specify access monitoring. FAM solutions should be designed to capture comprehensive information about access to sensitive information, which include:

**User information**
Users that attempt to access specific files. This information is crucial for accountability and to identify authorized or unauthorized users.

**Timestamps**
Exact timestamp of when a file access occurs.

**Accessed File Details**
Information about the specific file being accessed, including the name and location. This allows for more granular on file interaction.

**Processes**
Details about processes or methods used to access a file.

**Host details**
Host where the file access takes place. This granular detail helps strengthen user identification and hold users accountable for their actions.

FAM represents both a major gap and an opportunity for organizations looking to identify threats and achieve compliance. It's a gap because organizations may determine that systems need the capability to log every file access as successful or unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance.

PCI DSS 4.0 requirements state that audit logs must record the Success and Failure Indication of the event. Qualys FAM demonstrates a proactive approach by logging events for unsuccessful access attempts. For instance, if a regular user tries to access a highly restricted file and faces denial from the operating system due to insufficient permissions, Qualys FAM promptly generates an event within the Qualys FIM app. This event clearly indicates the outcome with the Success Status marked as "No."

Most FIM solutions are considered “noisy” in that they generate a great deal of false positive alerts. They promote their ability to generate more alerts with increasingly customized risk ratings. This alert storm burdens compliance and security analysts with hundreds of thousands of events that lack accurate or meaningful prioritization. The truth is that most alerts require no action, dramatically taxing SOC teams and compliance audit resources and thwarting efficient incident response and analysis. Qualys FIM includes unique noise cancellation technology that reduces false alerts by 90%+, which could help prevent a PCI DSS audit failure for ignoring alerts. Qualys FIM enriches event data with threat intelligence by adding Trusted Source and File Reputation context to control noise and prioritize events. With intuitive dashboards, you can continuously track your change posture, as well as view insights on change events with ‘what-who-when’ context.

Qualys also offers agentless FIM, including FIM for network devices like JuniperOS, Arista, and PaloAlto. This capability triggers alerts that precisely pinpoint the differences in network configurations during routine scan intervals, offering detailed insights into 'what' changed in the configuration.

You can learn more about how Qualys FIM helps support PCI DSS 4.0 compliance here:
PCI DSS 4.0 FIM Requirements Simplified with Qualys File Integrity Monitoring

## 3. Qualys Endpoint Detection and Response

Qualys Multi-Vector Endpoint Detection and Response (EDR) – Qualys EDR integrates vulnerability management of the CDE with endpoint threat detection and response (Req. 5, 12). Qualys EDR goes beyond the endpoint protection silo by empowering security teams to reduce risks and eliminate alert fatigue. Qualys EDR monitor endpoints to detect suspicious activity in real time, hunt for sophisticated threat actors across your environment, and act quickly with automated response workflows.

Qualys EDR protects systems from malware and other forms of attack with multi-layered prevention including mature and well-trained machine learning and behavior-based blocking, memory protection, network attack defense, Anti-phishing protection. Qualys EDR also prevents malware from encrypting personal or sensitive data, keeping your organization safe. Automatically create a backup of target files that are restored after the malware is blocked. Device control is included to stop malware and leakage of sensitive data via attached devices such as USB flash drives, Bluetooth devices, and other storage devices.

Remediation is a weakness for many EDR solutions, but as noted earlier, Qualys PC now includes tight integration with Qualys EDR, allowing you to automatically remediate threats discovered in EDR with PC. Automatic Incident Prioritization, Visualization and Root Cause Analysis allows security administrators to focus on the most important activities. Threat forensics and Remote shell is included for thorough endpoint investigations. Qualys EDR leverages the existing Qualys Cloud Agent, making it drop-dead simple to get started.

# Conclusions

The Qualys Enterprise TruRisk Platform provides you with a unified view of your entire cyber risk posture so you can efficiently aggregate and measure all Qualys & non-Qualys risk factors in a unified view, communicate cyber risk with context to your business, and go beyond patching to eliminate the risk that threatens the business in any area of your attack surface.

Following the requirements with the PCI Council's recommended four-step continuous process of Assess, Remediate, Report, and Monitor and Maintain can ensure your organization is on a proven path toward full compliance to reduce the risks of brand damage, fines, and litigation. Your firm can also ensure a stronger cybersecurity posture across the enterprise IT environment. When used as an enabler for this process, the Qualys Compliance Trio for PCI DSS 4.0 can simplify and automate the compliance process and keep your cardholder data environment secure.

Learn more about how Qualys supports PCI DSS 4.0.

We also invite you to start your Qualys PCI DSS 4.0 compliance free trial.

**Contributors:**

Bill Reed, Qualys Product Marketing

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of disruptive cloud-based Security, Compliance and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings. Qualys, Qualys VMDR® and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.

For more information, please visit **qualys.com**