1touch.io
Data Aware Security

Solution Guide

A Retailer's Guide to PCI DSS v4.0

Navigating the New Era of Payment Security

This guide aims to help retailers navigate the complexities of PCI DSS v4.0 with confidence and efficiency. It provides a roadmap for understanding the key changes in PCI DSS v4.0, assessing your compliance readiness, and implementing a sustainable, data-centric approach to payment security. It also examines how AI-powered data discovery solutions like 1touch.io Inventa™ can dramatically accelerate your PCI DSS v4.0 journey by providing real-time visibility into the location, volume, and flow of payment data.

Harness the Power of AI and Automation for Continuous Compliance

The Payment Card Industry Data Security Standard (PCI DSS) v4.0, released in March 2022, marked a significant shift in the payment card industry's approach to data security. This updated standard introduces over 60 new requirements designed to address the challenges of safeguarding payment data in an increasingly complex and threat-laden environment.

For organizations that process, store, or transmit payment card data, meeting PCI DSS v4.0 is not just a regulatory mandate—it's a business imperative. Data breaches can lead to financial penalties, legal liabilities, operational disruptions, and irreparable damage to customer trust and brand reputation. In today's unforgiving business environment, no organization can afford to be lax about payment security.

But achieving and maintaining compliance with PCI DSS v4.0 is no simple task. The updated standard demands a level of data visibility, control, and agility that many organizations struggle to achieve with traditional security tools and manual processes.

This guide provides a roadmap for navigating the complexities of PCI DSS v4.0 with clarity and confidence. We'll explore the key changes in the standard, outline strategies for implementing critical security controls, and share best practices for embedding compliance into your day-to-day operations.

You'll learn how AI-powered data discovery solutions like 1touch.io Inventa can dramatically simplify and streamline your compliance efforts.

Whether you're just starting your PCI DSS journey or looking to optimize an existing program, this guide will equip you with the knowledge and tools you need to protect payment data efficiently and effectively.

Let's dive in.

The Role of PCI DSS in Protecting Sensitive Payment Data

Payment card data is the lifeblood of commerce, but it's also the primary target for cybercriminals. Verizon asserts that "Payment card data is one of the most highly sought after data types by external and internal threat actors, because it's one of the easiest data types to monetize." In fact, **84% of data breaches involved payment account data**, according to Verizon's 2022 Payment Security Report.

Last year, the Federal Trade Commission (FTC) received 2.6 million fraud reports, with consumers losing over $10 billion to fraud—a staggering increase of over $1 billion compared to 2022. Specifically, more than **$676 million in financial losses were reported due to credit card, debit card, and payment app fraud.**

These alarming statistics underscore the critical importance of the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS provides a robust framework for protecting payment account data throughout its lifecycle. By adhering to PCI DSS, organizations not only safeguard their customers' sensitive information but also mitigate the risk of costly breaches.

Understanding the PCI DSS Data Security Standard

At its core, PCI DSS is a global information security standard designed to prevent fraud by increasing payment account data controls. It advances cardholder protection, establishes an early warning system for policy violations, and supports agreements with payment processors and financial institutions.

The data security standard applies to all entities that store, process, or transmit payment cardholder data and/or sensitive authentication data, including merchants, service providers, issuers, and acquirers. It requires secure acceptance, storage, processing and transmission of cardholder data to prevent fraud and breaches.

PCI DSS compliance is not a one-time event, but an ongoing process that requires continuous monitoring, assessment, and optimization. Organizations must not only meet all applicable PCI DSS requirements at a given point in time, but also demonstrate the ability to sustain a secure payment environment over time.

Who Must Comply with PCI DSS?

PCI DSS applies to any entity that accepts, transmits, or stores any cardholder data, regardless of size or transaction volume.

This includes:

- Merchants of all sizes, from small businesses to global enterprises
- Payment processors, gateways, and other service providers
- Financial institutions that issue payment cards or acquire transactions
- Third-party organizations that handle cardholder data on behalf of others
- Systems that store, process, or transmit cardholder data or sensitive authentication data included in or connected to the cardholder data environment

If your organization touches payment card data in any way, you are likely required to comply with PCI DSS.

The Six Objectives of PCI DSS

At a high level, PCI DSS has six overarching objectives:

1. Build and maintain a secure network and systems
2. Protect account data
3. Maintain a vulnerability management program
4. Implement strong access control measures
5. Regularly monitor and test networks
6. Maintain an information security policy

These objectives encompass 12 granular requirements that prescribe specific technical and operational controls for safeguarding payment data. Organizations must meet all applicable requirements within each objective to achieve and maintain compliance.

What's New in PCI DSS v4.0?

PCI DSS v4.0, released in March 2022, is the first major update to the standard since 2018 and, introduces significant updates to address emerging threats and technologies. It includes 64 new requirements, of which 13 are effective immediately for v4.0 assessments and 51 are considered best practices until March 31, 2025.

New focus areas include enhanced roles/ responsibilities, encryption, authentication, vulnerability management, change detection, and targeted risk analysis. Service providers have several additional requirements around separation of customer environments, penetration testing, and incident reporting.

Key changes include:

1. **Continuous Process:** Stronger focus on security as a continuous process, rather than an annual event
2. **Customized Approach:** Allows organizations to design their own security controls to meet the intent of PCI DSS requirements.
3. **Increased Flexibility:** Accommodates a broader range of technologies and methodologies to meet the security objectives of certain requirements.
4. **Enhanced Validation Procedures:** More stringent controls around user identification, authentication (including expanded multi-factor authentication), and access for any user with non-console administrative access.
5. **Targeted Risk Analyses:** Enables organizations to define how frequently they perform certain activities to allow for flexibility when meeting requirements based on their own targeted risk analyses.
6. **Expanded Applicability:** Focuses on security for payment operations, not just the Cardholder Data Environment (CDE), to promote broader data security.
7. **New Threat Considerations:** Addresses new threats like malware, phishing, and cloud-based environments, including containerization and serverless technologies.
8. **Enhanced Testing Procedures:** More rigorous testing procedures to validate the effectiveness of security controls, including greater frequency of vulnerability and penetration testing.

These changes help organizations keep pace with new cybersecurity threats and strengthen their payment data defenses.

Comparing PCI DSS v3.2.1 vs. v4.0 Requirements

While PCI DSS v4.0 builds upon the foundation of v3.2.1, it includes several significant updates and new requirements. Here are some of the key changes:

Requirement Area	PCI DSS v3.2.1	PCI DSS v4.0
Multifactor Authentication	Required for remote access to the cardholder data environment (CDE).	Required for all access to the CDE (effective March 31, 2025).
Passwords	Minimum length of 7 characters.	Minimum length of 12 characters (or 8 characters plus compensating control until March 31, 2025).
Encryption	Required for transmission of cardholder data (CHD) over open, public networks.	Also required for storage of sensitive authentication data (SAD) prior to authorization (with some exceptions).
Risk Assessments	Annual risk assessment required.	Targeted risk analyses required for requirements with flexibility in frequency or customized implementation.
Vulnerability Management	Internal and external scans required quarterly.	More frequent scanning required for high-risk and critical systems.
Penetration Testing	Required annually and after significant changes.	Also required after organizational and infrastructure changes; more rigorous testing procedures.
Service Providers	Quarterly review of service providers' PCI DSS status.	Documentation of service providers' PCI DSS responsibilities; prompt notification of changes impacting PCI DSS scope.
Security Awareness Training	Required for personnel with security breach responsibilities.	Targeted security awareness training required for all personnel with access to account data.
Monitoring and Responding	Reviews of logs and security events required daily.	Prompt detection and response to failures of critical security controls required.

PCI DSS v4.0 Compliance Checklist

PCI DSS v4.0 contains over 400 individual requirements and sub-requirements. They roll up into 12 main requirements, organized under the six main objectives described earlier.

To achieve compliance with PCI DSS v4.0, organizations must meet 12 core requirements:

1. **Install and maintain network security controls**
- Establish and implement firewalls and network security controls
- Secure and synchronize router configuration files
- Protect all system components and software

2. **Apply secure configurations to all system components**
- Always change vendor-supplied defaults
- Develop and maintain secure configuration standards
- Securely store system configuration files

3. **Protect stored account data**
- Protect stored cardholder data
- Protect stored sensitive authentication data
- Mask PAN when displayed
- Render PAN unreadable anywhere it is stored

4. **Protect cardholder data with strong cryptography during transmission over open, public networks**
- Use strong cryptography and security protocols
- Never send unprotected PANs by end-user messaging
- Encrypt all non-console administrative access

5. **Protect all systems and networks from malicious software**
- Deploy anti-malware software
- Ensure all anti-malware mechanisms are current and perform periodic scans
- Configure anti-malware software to generate audit logs

6. **Develop and maintain secure systems and software**
- Establish a process to identify and fix security vulnerabilities
- Protect public-facing web applications against attacks
- Develop software applications in accordance with PCI DSS and based on industry best practices

7. **Use change control procedures for all system and software configuration changes**
- Restrict access to system components and cardholder data by business need to know
- Limit access to system components and cardholder data
- Establish an access control system for systems components
- Ensure proper user authentication and password management

8. **Identify users and authenticate access to system components**
- Assign all users a unique ID before allowing them to access system components or cardholder data
- Use at least one of these to authenticate all users: something you know, such as a

password; something you have, such as a token; or something you are, such as a fingerprint

- Implement multi-factor authentication for all non-console access to the CDE
- Render all passwords unreadable during storage and transmission using strong cryptography

9. Restrict physical access to cardholder data

- Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment
- Develop procedures to easily distinguish between onsite personnel and visitors
- Make sure all visitors are authorized before entering areas where cardholder data is processed or maintained
- Physically secure all media containing cardholder data
- Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution

10. Log and monitor all access to system components and cardholder data

- Implement audit trails to link all access to system components to each individual user
- Implement automated audit trails for all system components to reconstruct events
- Record audit trail entries for all system components for each event
- Synchronize critical system clocks and times
- Secure audit trails so they cannot be altered
- Review logs and security events daily

11. Test security of systems and networks regularly

- Implement processes to test for the presence of wireless access points and detect unauthorized wireless access points
- Run internal and external network vulnerability scans at least quarterly and after any significant change in the network
- Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification
- Use network intrusion detection and/or intrusion prevention techniques
- Deploy file integrity monitoring or change detection software

12. Maintain an information security policy

- Establish, publish, maintain, and disseminate an information security policy that addresses all PCI DSS requirements
- Review the security policy at least annually and update when the environment changes

These requirements encompass over 400 individual controls, making compliance a significant undertaking.

Best Practices for Meeting New Requirements

To streamline compliance with PCI DSS v4.0's updated requirements, organizations should:

- Conduct a comprehensive gap assessment against the v4.0 standard
- Implement an automated data discovery and classification solution
- Automate compliance activities and controls to reduce manual effort
- Encrypt sensitive data at rest and in transit using strong cryptography
- Adopt a zero trust approach to access management and authentication
- Deploy automated vulnerability scanning and penetration testing tools
- Integrate compliance requirements into existing risk management and security frameworks
- Document all policies and procedures related to payment data handling
- Provide ongoing PCI DSS training and awareness programs for all personnel

The Challenges of Maintaining Compliance

Achieving PCI DSS compliance is hard; maintaining it is even harder. According to Verizon's Payment Security Report, **only 43.4% of organizations achieve full PCI DSS compliance during interim validation**, with over half struggling to maintain effective security controls on a consistent basis. Common challenges include:

- Lack of visibility into the location and flow of payment data across complex environments
- Reliance on manual, resource-intensive processes for compliance activities
- Difficulty keeping pace with evolving threats and changes to the PCI DSS standard

The Costs of PCI DSS Noncompliance

Failing to comply with PCI DSS can have severe financial, legal, and reputational consequences for an organization:

Monetary Fines and Penalties

- Non-compliance fines ranging from $5,000 to $100,000 per month until compliance is achieved
- Increased transaction fees and potential termination of card processing privileges
- Liability for fraud losses and recovery costs in the event of a breach

Legal and Regulatory Consequences

- Mandatory forensic investigations that can cost over $50,000
- Federal and state regulatory fines for violations of data protection laws
- Class action lawsuits and settlements related to consumer harm

Operational and Reputational Damage

- Loss of customer trust and loyalty after a publicized data breach
- Significant operational disruption and remediation costs
- Potential loss of business partners and revenue streams

To close this gap, organizations need a new approach to PCI DSS compliance—one that is data-centric, automated, and continuous. Organizations need a robust compliance program that emphasizes continuous monitoring, automated control validation, and data-driven risk management.

1touch.io Inventa provides a comprehensive, forward-looking solution for navigating the complexities of PCI DSS compliance. By automating core compliance activities, Inventa enables organizations to maintain a robust security posture while achieving operational efficiency and cost savings. It doesn't just meet the requirements of today; it prepares you for the complexities of tomorrow.

Leveraging AI-Powered Data Discovery to Simplify Compliance

The Need for Continuous Data Visibility

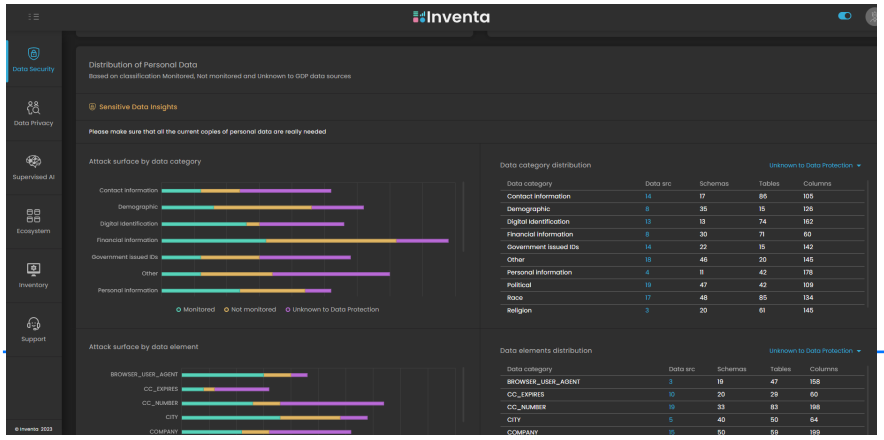
One of the biggest challenges in achieving and maintaining PCI DSS compliance is keeping track of payment data across an organization's environment. With data constantly moving and proliferating, traditional discovery methods can't keep pace.

1touch.io Inventa is purpose-built to help organizations meet this challenge. Leveraging advanced AI and machine learning techniques, Inventa provides organizations with real-time visibility into the location, volume, and flow of payment data.

Continuously scanning structured and unstructured data sources, Inventa builds a dynamic map of an organization's cardholder data environment, making it easier to ensure appropriate controls are in place. By providing a centralized, always-up-to-date view of sensitive data, Inventa dramatically simplifies many of the most challenging aspects of PCI DSS v4.0 compliance.

This empowers organizations to:

- Streamline PCI DSS scoping and segmentation
- Identify and remediate compliance gaps in real-time
- Demonstrate compliance to auditors with comprehensive reporting
- Integrate payment data intelligence with existing security and compliance tools
- Continuously monitor the CDE for potential security incidents



1touch.io Inventa reduces sensitive data risk through Contextual AI that provides insurers relevant information to inform prioritized decision-making.

How 1touch.io Inventa Maps to PCI DSS Requirements

Here is how 1touch.io Inventa maps to the 12 main requirements of PCI DSS v4.0:

PCI DSS Requirement	How Inventa Helps
Requirement 1: Install and maintain network security controls	Inventa's network-centric approach to sensitive data discovery helps organizations identify all systems and network segments where cardholder data resides. Inventa continuously analyzes network traffic to detect the flow of cardholder data, aiding in proper network segmentation and security control implementation.
Requirement 2: Apply secure configurations to all system components	Inventa's comprehensive discovery of cardholder data across all systems—including on-premises, cloud, and mainframe environments—ensures each system handling cardholder data adheres to secure configuration standards. It can identify misconfigurations or unsecured instances of cardholder data.
Requirement 3: Protect stored account data	Inventa directly supports requirement 3.2 to minimize cardholder data storage, identify opportunities for secure deletion, and trigger remediation workflows like encryption, redaction, and deletion through third-party integrations.
Requirement 4: Protect cardholder data during transmission	While Inventa is not an encryption solution, its network scanning capabilities can detect instances of unencrypted cardholder data transmission. This visibility helps organizations identify and rectify gaps in their encryption controls for cardholder data transmitted over open, public networks.
Requirement 5: Protect all systems and networks from malicious software	Although not an anti-malware tool, Inventa integrates with endpoint protection and network monitoring solutions. It can correlate malware or cyberattack events with attempts to exfiltrate sensitive data, bolstering an organization's malware defenses.
Requirement 6: Develop and maintain secure systems and software	Inventa scans an organization's custom-developed software, including payment applications, to identify storage of cardholder data, violating requirement 6.5.3. This empowers prompt remediation of insecure cardholder data handling in the software development lifecycle.
Requirement 7: Restrict access to cardholder data	Inventa's automated classification of discovered cardholder data enables granular enforcement of role-based access controls and least privilege through integration with identity and access management (IAM) solutions. This ensures access to cardholder data is granted only to roles with a legitimate business need, satisfying requirement 7.2.
Requirement 10: Log and monitor access to cardholder data	Inventa integrates with SIEM and log management tools to enrich security event data. By linking access events to the presence of sensitive data, Inventa enables more efficient detection and investigation of suspicious cardholder data access.
Requirement 11: Test security of systems and networks	Inventa automates discovery-related testing procedures, such as requirement 11.3.3 to detect unprotected PANs, and can feed updated asset inventories to penetration testing tools.
Requirement 12: Maintain an information security policy	Inventa reinforces several requirement 12 procedures, including maintaining a current cardholder data flow diagram (12.5.2), conducting data discovery for incident response (12.10.7), and informing employee security awareness training (12.6) with data insights. Reporting capabilities maintain compliance evidence of these practices.

Automating Key Compliance Activities

By automating the manual, error-prone, and time-consuming process of sensitive data discovery and classification, Inventa enables organizations to achieve and demonstrate PCI DSS v4.0 compliance with unparalleled efficiency and ease. Continuous, granular visibility into payment data enables security, risk, and data leaders to make faster, more informed decisions about data protection, policy enforcement, and risk management.

Here's a checklist of key PCI DSS compliance activities that can be automated with 1touch.io Inventa:

Data Discovery and Classification

- Automatically discover and classify payment card data across your entire environment, including on-premises, cloud, and hybrid infrastructures
- Continuously monitor for new instances of payment card data and update your data inventory in real-time
- Identify and remediate data misclassification and policy violations

Scoping and Segmentation

- Automatically generate a comprehensive map of your cardholder data environment (CDE) based on discovered payment card data
- Identify systems and networks that are in-scope for PCI DSS based on their interaction with payment card data
- Monitor for changes to your CDE and adjust your scoping and segmentation accordingly

Access Control and User Management

- Automate the enforcement of role-based access controls (RBAC) and least privilege access based on data classification and business need
- Monitor for unauthorized access attempts and suspicious user activity within the CDE

Encryption and Tokenization

- Automatically apply encryption or tokenization to payment card data at rest and in transit based on policy (via third-party integrations)
- Provide intelligence to access control systems to understand the urgency of anomalous end user activity
- Integrate with key management systems to securely manage and rotate encryption keys

Logging and Monitoring

- Automate the collection, analysis, and reporting of log data from systems and applications within the CDE
- Use machine learning to detect anomalous activity and potential security incidents in real-time
- Correlate log data with user activity and data access events to investigate and respond to incidents

Vulnerability Management

- Automate vulnerability scanning of systems and applications within the CDE
- Prioritize vulnerabilities based on risk and automate the tracking and verification of remediation efforts
- Integrate with leading IT ticket systems to ensure timely deployment of security patches and updates

Third-Party Risk Management

- Automate the assessment and monitoring of third-party service providers' PCI DSS compliance status
- Use APIs to collect and analyze compliance data from service providers in real-time

Compliance Reporting and Audit Preparation

- Automate the generation of PCI DSS compliance reports and dashboards
- Collect and organize evidence of compliance controls in a centralized repository
- Use APIs to integrate compliance data with GRC systems and other reporting tools

By reducing manual effort and providing contextual data intelligence, Inventa enables organizations to achieve and demonstrate PCI DSS compliance with greater efficiency and ease.

Integrating Data Intelligence with Existing Security Tools

Inventa is designed to work seamlessly with an organization's existing security and compliance tech stack. Its API-first architecture allows Inventa to feed discovered payment data intelligence to tools such as:

- SIEM and log management platforms for enriched security monitoring
- Data loss prevention (DLP) solutions for enhanced data protection
- Identity and access management (IAM) tools for granular access controls
- Governance, risk, and compliance (GRC) systems for unified compliance reporting

These integrations allow organizations to maximize the value of their existing investments while enhancing their overall security and compliance posture.

The Path Forward

PCI DSS v4.0 represents a significant evolution of the standard to keep pace with the realities of modern payment security. By adopting a data-centric, risk-based, and automated approach to compliance, organizations can meet its requirements more efficiently and effectively.

1touch.io Inventa provides the real-time data visibility, contextual intelligence, and operational integration needed to support this approach. With Inventa, you can continually discover and protect payment data across your environment, validate controls, and demonstrate compliance—all while reducing manual effort and complexity.

The stakes have never been higher when it comes to payment data security. But with the right strategy, tools, and partners, you can protect your customers, your brand, and your bottom line in the new era of PCI DSS v4.0.

Sources:

Verizon 2023 Payment Security Report

FTC Annual Data Book 2023

PCI DSS v4.0 Quick Reference Guide, PCI Security Standards Council

PCI DSS v4.0 At A Glance, PCI Security Standards Council

PCI DSS V2.0 Best Practices for Maintaining PCI DSS Compliance, PCI Security Standards Council

Eight Steps to Take Toward PCI DSS v4.0, PCI Security Standards Council

1touch.io
Data Aware Security

Solution Guide