FORTRA™

SOLUTION BRIEF (TRIPWIRE)

Automated, Continuous PCI 4.0 Compliance with Tripwire

Comprehensive Protection of Customer Card Data

The Payment Card Industry Data Security Standard (PCI DSS) was created to help organizations that process credit card payments secure the cardholder environment to prevent credit card fraud, cyber threats, and other security vulnerabilities. The latest version, 4.0, provides specific security guidance on handling, processing, transmitting, and storing credit card data to minimize the theft, exposure, and leakage of personal and financial credit information. Businesses who process credit card transactions are required to comply with the new PCI 4.0 requirements by March 2024.

The Challenge

Credit card data and the systems processing it remain a valuable target for attackers. Research and many forensic investigations have shown that it can take attackers mere seconds to minutes to breach an organization's defenses, but it takes an average of eight months to discover a breach—and by that time, millions of records could have been exfiltrated. With the continuing rise of ransomware threats, the need to provide a minimum baseline for security standards has become even more important.

ATTACK TARGET: CARDHOLDER DATA

Only 27.9 percent of organizations achieved full compliance with PCI DSS during their interim validation in 2019. As expected, within the retail industry, 99 percent of incidents were financially motivated, with payment data remaining the most sought-after and lucrative commodity by threat actors. The report indicates that web applications, rather than point-of-sale (POS) devices, are now the main vector for retail breaches.

—**Verizon Payment Security Report, 2019**

The Goal: Continuous PCI Compliance & Security

Unfortunately, many organizations focus their energies on a "check-box" mentality for passing each PCI compliance audit and then simply return to business as usual after the administrative scramble. This is when configurations can "drift" out of compliance, even though at a particular point in time the organization may have undergone third-party penetration testing and vulnerability assessments and had passed an audit. As IT security professionals know, minimum adherence to compliance standards has been no guarantee of security. However, the PCI v4.0 Standards seek to enforce continuous compliance and security oversight. PCI DSS should be implemented into BAU (business as usual) activities as part of an entity's overall security strategy. This continual operational focus on compliance and security will lead to improved system integrity and reduced risk.

PCI DSS 4.0 Compliance Highlights

Even if you are already PCI 3.2.1 compliant, progressing to v4.0 will require some extra effort. Fortra's Tripwire has the tools to streamline PCI 3.2.1 compliance and determine readiness for 4.0. The scope of the changes for 4.0 may take organizations more time to adopt operational process changes. Tripwire recommends reviewing the updated standards early to maximize the time available to plan for the new standards that take effect in March 2024.

Tripwire's PCI Compliance Solution

Tripwire is the leading domain expert and provider of continuous PCI compliance and automation, delivering a suite of products and services that enable merchants, banks, and payment processors to create and enforce a comprehensive PCI security policy. Our solutions can proactively discover, harden, and secure all systems that store credit card data.

Tripwire also helps companies prepare and respond effectively to audits.

Tripwire® Enterprise delivers award-winning policy management and tightly integrated file integrity monitoring

- Real-time alerts on change audit or detection of threat indicators or anomalies
- Establishes a known and trusted configuration baseline for your security policy, hardening configurations and catching configuration drift
- Remediation guidance built in, speeding resolution of issues for your IT Security and SOC teams
- Agentless options available

Tripwire LogCenter® with event correlation

- Ingests security information from a variety of sources to correlate information and alert on "events of interest"
- Tripwire IP360™ delivers vulnerability assessment
- Auto-discovery of your environment provides visibility of hardware and software—whether in- or out-of-scope
- Scans your environment using vulnerability intelligence to find the risks you need to act on

Tripwire IP360™ delivers vulnerability assessment

- Auto-discovery of your environment provides visibility of hardware and software—whether in- or out-of-scope
- Scans your environment using vulnerability intelligence to find the risks you need to act on

PCI DSS 4.0 — Six Objectives & 12 Requirements

Each of Tripwire's PCI solutions can operate either independently or together, offering file integrity monitoring, security configuration management, intelligent event logging, and vulnerability management. When deployed together, Tripwire offers "out-of-the-box" immediate value to validate and enforce good security measures, as well as provide audit-ready compliance reports.

Please note that PCI DSS v4.0 was released March 2022, but it will not be mandated until March 2024. Tripwire is preparing our solutions so you will have complete coverage of all 12 PCI 4.0 requirements well in advance of the mandate. This table represents the features currently being developed.

		Tripwire Enterprise	Tripwire LogCenter	Tripwire IP360
Objective 1:	**Build and maintain a secure network and systems**			
Requirement 1: Install and Maintain Network Security Controls	Tripwire continuously detects unauthorized changes and compliant configuration settings changes, and collects firewall logs, providing evidence that network traffic uses only approved protocols and routes. Tripwire can scan and test accessible services, improper network traffic, current status of all monitored network devices (firewalls, routers, switches), and support change approval systems, workflows, and processes.	✔	✔	✔
Requirement 2: Apply Secure Configurations to All System Components	Tripwire automates and validates security configurations for access control, protocol settings, audit/log settings, and privileges to ensure compliance with standards. Tripwire's solutions are aligned with most security frameworks, such as PCI, NIST, CIS Controls, ISO, etc.	✔		✔
Objective 2:	**Protect account data**			
Requirement 3: Protect Stored Account Data	Tripwire checks and reports on the removal or change in encryption, keys, data files and database tables. Alerts can be generated on suspicious access activity to sensitive data. Logging can provide history of activities, who changed what and when, as well as provide an automatic record for forensic value.	✔	✔	
Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks	Tripwire checks for data encryption and can alert and show specifics on weak encryption, services running without encryption and changes to encryption algorithms. Built-in remediation advice is provided to return settings to a compliant state. Tripwire can check for current certificates, record and report on crypto and cipher use in a variety of applications and operating systems, and offers automation, audit-ready evidence of compliance and ongoing monitoring.	✔	✔	✔
Objective 3:	**Maintain a vulnerability management program**			
Requirement 5: Protect All Systems and Networks from Malicious Software	Tripwire can validate that anti-virus and endpoint monitoring software is installed and running, as well as detect systems running with out-of-compliance signatures. Tripwire is effective against zero-day attacks through its ability to detect damaged systems through tracking, alerting, logging and reporting on system changes affecting integrity.	✔	✔	✔
Requirement 6: Develop and Maintain Secure Systems and Software	Tripwire can enforce development and production environment change control procedures with tailored rules and tests to fit specific security and audit requirements. Tripwire captures system logs, validates proper error handling and checks for secure cryptographic storage and communications. Tripwire can also enforce role-based access control, PAN, and other requirements for protecting cardholder data in the development and testing environment prior to release to production. Tripwire assesses if there are any vulnerabilities and risk and prioritizes the vulnerabilities so IT security can quickly and effectively reduce overall network risk. This can be deployed on-premises or in the cloud.	✔	✔	✔

		Tripwire Enterprise	Tripwire LogCenter	Tripwire IP360
Objective 4:	**Implement strong access control measures**			
Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know	Tripwire helps ensure use of strong access control, including authentication, permission settings and supplemental audit evidence of monitored change. Tripwire can detect common and custom settings in third party products. Tripwire can monitor local logins to machines that house PCI data, and capture log information about login attempts, generating alerts based on suspicious login behavior.	✔	✔	
Requirement 8: Identify Users and Authenticate Access to System Components	Many of the subcontrols for this requirement are procedural and documentational. However, a great many of the requirements can be enforced, logged and alerted upon using Tripwire solutions. Multi-factor authentication and password policies are part of Tripwire's compliance audit capabilities, and additionally Tripwire can check for strong cryptography and valid credentials, and alert on all types of retries, terminated employees seeking access, verifying unique IDs for each employee, etc.	✔	✔	
Requirement 9: Restrict Physical Access to Cardholder Data	Tripwire supports security procedures such as physical access control by monitoring features of custom applications used for physical monitoring or alarm software. As such, Tripwire can automate detection of non-typical behavior. Tripwire captures logs of access control mechanisms that can be correlated with other data to detect improper physical access.		✔	
Objective 5:	**Regularly monitor and test networks**			
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data	Tripwire meets log collection, reporting and retention requirements and can encrypt them for secure storage. This prevents log tampering as well as provides all the features of detecting who accessed cardholder data, what security events occurred, and when. Tripwire also monitors configuration and security settings for audit purposes, verifying they are in compliance and alerting within seconds if they are altered.	✔	✔	
Requirement 11: Test Security of Systems and Networks Regularly	Tripwire's enhanced file integrity monitoring detects changes and programmatically analyzes each change to determine whether authorized and compliant. This can be set to customer-specific policy and processes. Tripwire can automatically remediate when detected changes cause failures in policy tests, repairing by bringing systems back to a secure and compliant state.	✔	✔	*
Objective 6:	**Maintain an information security policy**			
Requirement 12: Support Information Security with Organizational Policies and Programs	Tripwire can be used to provide evidence of compliance for policy (such as acceptable use, system configuration settings and changes and administrative events). Tripwire can discover unexpected changes to critical systems as well as provide audit-ready reporting to demonstrate compliance with procedures and practices in force.	✔	✔	

* Tripwire IP360 does not do penetration testing but can assist by finding exploitable vulnerabilities and by validating remediations through a subsequent scan.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.