FORTRA™

SOLUTION BRIEF (TRIPWIRE)

Tripwire ExpertOps and PCI 4.0

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 a customer's personal and financial credit information.

The Challenge

Credit card data has long been a prime target for attackers. Research and multiple forensic investigations show that it can take attackers only 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 have often been exfiltrated.

The Goal: Continuous PCI Compliance

Organizations, struggling to address ever-growing cybersecurity risks with limited resources—the lack of cybersecurity talent and high turnover on cybersecurity teams—typically focus their energies by employing 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 passed their audit. As IT security professionals know, compliance is no guarantee of security. However, the PCI Security Standards Council states "to ensure security controls continue to be properly implemented, PCI DSS should be implemented into BAU (business as usual) activities as part of an entity's overall security strategy." BAU translates into continuous compliance every day. Fortra's Tripwire® ExpertOps℠ can help organizations achieve continuous PCI DSS compliance while insulating their teams from the challenges of turnover and the cybersecurity talent gap.

HIGHLIGHTS

- Quickly achieve compliance for PCI 4.0
- Addresses 11 of the 12 PCI 4.0 requirements
- Support from designated Tripwire Experts
- Cloud-hosted infrastructure combined with consulting services
- Broadest depth and breadth of compliance policy and platform coverage

Your Solution: Tripwire ExpertOps

Tripwire ExpertOps combines managed services with the industry's best File Integrity Monitoring (FIM) and Security Configuration Management (SCM) and addresses 11 of the 12 PCI DSS requirements. The solution provides personalized consulting, audit support, and cloud-based infrastructure to help you achieve and maintain compliance. The solution is easy to deploy and use, with simple subscription pricing and a low total cost of ownership.

Tripwire ExpertOps enables you to rapidly achieve compliance with PCI 4.0 throughout your environment by reducing the attack surface, increasing system integrity and delivering continuous compliance. Plus, because Tripwire ExpertOps includes personalized consulting, you receive ongoing support from a designated Tripwire Expert.

Benefits

- PCI DSS 4.0 audit support
- 24/7 compliance visibility via a customized dashboard
- Alerts and reports in your inbox
- Waivers and change requests made easy
- No more awkward or incomplete hand-offs when your staff changes

How It Works

Tripwire ExpertOps provides you with continuous staffing to operate and manage Tripwire-provided PCI DSS controls at peak efficiency. The solution adapts to your unique environment—reports and profiling tasks are customized to meet your specific needs. You will receive expert guidance to configure your system and policy configurations to best align with your requirements. And you'll gain visibility via 24/7 access to compliance information via a tailored dashboard and management console.

A Tripwire Expert will act as an extension of your team by prioritizing work efforts and managing critical escalations. Together you will jointly develop a Service Plan that outlines communication practices, escalation procedures and any specialized requests.

The Tripwire Expert will then tune and operate your Tripwire-provided PCI DSS controls to provide:

- Prescriptive policy and content guidance to enable PCI DSS compliance for your specific network or system security requirements
- Recommendations for maximizing automation capabilities for compliance and event alerting practices, change management process integrations, and audit prep activities
- Prioritized remediation to identify opportunities to efficiently improve compliance posture
- Organizational grading for each accountable department to provide visibility into groups needing additional resources and attention

Get 24/7 visibility without deploying additional hardware, databases and back-end software. Tripwire ExpertOps is built on a cloud computing platform, allowing the service to quickly scale to meet your needs while maintaining high levels of security. The service uses a single-tenancy model to ensure that data remains segregated between customer accounts. Tripwire applies multiple controls for security and privacy of your data, including secure configurations, vulnerability scanning, data encryption, malware defenses, access control, log management, multi-factor authentication, VPN and much more.

Ready to Take the Next Step?

Get in touch with your Tripwire Account Manager—or visit www.tripwire.com/contact-us—to develop a custom Service Plan for Tripwire ExpertOps.

Migrating from Tripwire Enterprise?

We can help with migration services and pricing. Contact your Tripwire Account Manager for details.

PCI DSS 4.0 – Six Objectives & 12 Requirements	Tripwire ExpertOps Coverage
BUILD AND MAINTAIN A SECURE NETWORK	
Requirement 1: Install and Maintain Network Security Controls	Tripwire continuously detects unauthorized changes and compliant configuration setting changes, providing evidence that network traffic uses only approved protocols and routes
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
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
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. Tripwire Expert prioritizes remediation to identify opportunities to reduce risk and efficiently improve compliance posture, and provides audit-ready evidence of compliance and ongoing monitoring
MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM	
Requirement 5: Protect All Systems and Networks from Malicious Software	Tripwire can validate that anti-virus is installed and running
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
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
Requirement 8: Identify Users and Authenticate Access to System Components	Many of the sub-controls for this requirement are procedural and documentation. However a great many of the requirements can be enforced using Tripwire. Multi-factor authentication and password policies are part of Tripwire's compliance audit capabilities
Requirement 9: Restrict physical access to cardholder data	
REGULARLY MONITOR AND TEST NETWORKS	
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data	Tripwire 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
MAINTAIN AN INFORMATION SECURITY POLICY	
Requirement 12: Support Information Security with Organizational Policies and Programs	Tripwire can discover unexpected change to critical systems as well as provide audit-ready reporting to demonstrate compliance with procedures and practices in force

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.