



Tripwire's Solutions for Automated, Continuous PCI Compliance



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, hacking and other security vulnerabilities. Unfortunately, many organizations focus their energy on simply passing each PCI audit, losing sight of the main objective of the PCI DSS—to secure the cardholder data environment. As a result, organizations still suffer security breaches and experience the negative fallout associated with a data compromise even though they passed their audit—and they can take weeks or months to determine where a breach originated because of the lack of immediate and focused evidence of system activity. To contain damage, organizations need to be alerted as the breaches are unfolding, not long after.

“Since implementing Tripwire Enterprise, we easily prove compliance for PCI audit requirements, have reduced unplanned work, and greatly improved our change management process. Now, instead of spending time on service events, we can focus more on completing our IT projects, and adding additional value and efficiency to the company.”

— Roni Wegner, Senior VP
CAPITAL Card Services

The recent security breaches at Heartland Payment Systems and Hannaford Brothers are painful examples of the lack of immediate visibility. Although Heartland suspected a breach as early as October 2008, it wasn't until mid-January 2009 that a team of outside forensic experts detected malware in Heartland's systems. However, this security breach, like most, left trails that could have been immediately detected with the right tools, thereby reducing or eliminating any damage. It's even likely that the information was captured, but not recognized as a critical event that required immediate attention.

HOW TRIPWIRE HELPS

Tripwire, the leading provider of IT security and compliance automation, provides IT organizations with proven file integrity monitoring, real time analysis of change using ChangeIQ capabilities, and log and event management that automates continuous PCI compliance. But unlike others, Tripwire solutions identify the events that matter most—those that pose the real security risks or take you out of compliance. And they help you discover those events immediately, while you can still contain the damage. Tripwire offers these capabilities in two complementary

SOLUTION BRIEF

“If you are going to purchase any one tool to help achieve PCI compliance, buy Tripwire.”

— James Summers
CISO, Vesta

“With out-of-the-box capabilities specific to PCI, purchasing Tripwire saved my staff three months of having to search out and stitch together a hodgepodge solution on our own. The time savings more than paid for the software license and training”

— Rachelle Osborn
Director of IT, Wesco

products: Tripwire® Enterprise, for configuration control, and Tripwire® Log Center, for comprehensive log and event management.

ChangeIQ CAPABILITIES FOR REAL-TIME ANALYSIS OF CHANGE

The proven file integrity monitoring (FIM) capabilities of Tripwire Enterprise help you meet the FIM requirements of PCI DSS requirement 11.5 by detecting changes to critical system, configuration and content files. As Tripwire Enterprise detects change, it subjects it to immediate analysis by a set of ChangeIQ™ capabilities that determine if that change introduces risk or causes a shift out of a compliant state. Changes that do impact security or compliance generate alerts so you can review them immediately and use the step-by-step remediation guidance to quickly return to a secure, compliant state. When changes don't impact security or compliance—the majority of changes—Tripwire Enterprise automatically promotes them, so IT can remain focused on the changes that need their attention. This real-time analysis of change is what lets Tripwire Enterprise deliver true continuous PCI compliance and is what distinguishes the solution's FIM capabilities from all others.

COMPLIANCE POLICIES BASED ON LEADING SECURITY BENCHMARKS

Tripwire Enterprise helps you get configurations into a PCI-compliant state by testing current settings against out-of-the-box policies and providing guidance to remediate non-compliant settings. These PCI policies leverage trusted industry standards, such as security benchmarks from the Center for Internet Security (CIS). Once configurations achieve a PCI-compliant state, ChangeIQ capabilities

identify and immediately alert you to changes that cause configurations to stray from that compliant state.

Tripwire Enterprise provides PCI compliance policies for a broad array of platforms, applications, systems, devices and other IT assets in your cardholder data environment. For example, Tripwire Enterprise provides coverage of most operating systems; databases like Oracle, SQL and DB2; directory services like Active Directory and SunOne; network devices like Cisco IOS/PIX; applications such as Microsoft Exchange and IIS; and even custom applications.

LOG AND EVENT MANAGEMENT

When it comes to PCI Requirement 10, it's all about logs: demonstrating that audit trails are enabled, active and secure; that information about system and user activity is logged and stored; that logs performing a security function are reviewed at least daily; and that an audit trail is maintained for at least a year, with the most recent information easily accessible for forensic analysis. Tripwire Log Center provides all the capabilities you need to easily, efficiently, and cost-effectively meet PCI Section 10 requirements. In addition, out-of-the-box reports and queries provide proof of compliance for many other PCI requirement sections.

Most importantly, Tripwire Log Center also provides an integrated, easy-to-use security event manager to get the real-time event correlation and alerting needed to distinguish business-as-usual activities from critical security or compliance events.

COMBINING TRIPWIRE SOLUTIONS OFFERS YOU MORE

To attain the broadest compliance coverage and maximum security control, take advantage of Tripwire VIA™, the IT

SOLUTION BRIEF

VESTA USES TRIPWIRE ENTERPRISE'S FILE INTEGRITY MONITORING TO EVALUATE EACH SYSTEM'S COMPLIANCE AGAINST BOTH THE BENCHMARKS FROM THE CIS AND INTERNAL VESTA SECURITY POLICIES. THEY LIKE THE ABILITY TO COMPARE CONFIGURATION POLICIES AGAINST THEIR SYSTEMS WITH THE SAME SOLUTION THAT AUDITS THEM FOR CHANGE.

security and compliance suite that integrates Tripwire Log Center with Tripwire Enterprise to combine multiple real-time data sources—log information, change data and compliance status—and improve your ability to detect and act upon critical compliance and security threats, when they occur.

MAINTAIN AND PROVE COMPLIANCE

Together, Tripwire Enterprise and Tripwire Log Center let you monitor your compliance status and immediately receive notifications when changes or events

take you out of compliance or jeopardize security. They enable you to collect evidence and generate the reports you need to quickly and conveniently prove compliance to auditors—from how you addressed out-of-compliance settings, to evidence that you detect unauthorized and non-compliant changes, and proof that you meet the log capture, retention and reporting requirements of PCI requirement 10. With Tripwire Enterprise and Tripwire Log Center, you can pass the quarterly audit—and *continuously* maintain a high level of security.

HOW TRIPWIRE HELPS ADDRESS THE 12 PCI DSS REQUIREMENTS

PCI DSS v1.2 Requirement	Tripwire Solutions Support Summary
REQUIREMENT 1. Install and Maintain a Firewall Configuration to Protect Cardholder Data.	Tripwire continuously detects unauthorized changes, dynamically determines non-compliant configuration setting changes and provides remediation steps required to return the configuration to a compliant state. In addition, Tripwire collects firewall logs that provide evidence that network traffic uses only approved protocols and comes from or goes to only trusted networks and hosts. Tripwire alerts when improper network traffic occurs. Tripwire presents the current status of all monitored network devices (firewalls, routers, etc.) in a “live” dashboard, and generates reports that support change approval systems and processes.
REQUIREMENT 2. Do Not Use Vendor-supplied Defaults for System Passwords and Other Security Parameters.	Tripwire validates security configurations for areas such as access control, protocol settings, audit/log settings, and privileges to ensure compliance with standards. Logs collected by Tripwire also verify that vendor-supplied defaults were changed. Tripwire uses security benchmarks developed by the Center for Internet Security (CIS) and the Defense Information Security Agency (DISA) as well as vendor security guidelines.
REQUIREMENT 3. Protect Stored Cardholder Data.	Tripwire validates and reports on the removal or changes of certain types of data, such as cryptographic files and keys, data files and database tables. Tripwire can also generate alerts when log information indicates suspicious attempts to access sensitive data.
REQUIREMENT 4. Encrypt Transmission of Cardholder Data Across Open, Public Networks.	Tripwire tests security settings as they are changed, alerting on deviations from defined policy like weak encryption algorithms, and provides remediation advice to return settings to a compliant state. Once a configuration is compliant, Tripwire monitors and alerts if applications change the level of encryption during transmission. Tripwire records and reports on crypto and cipher use in a variety of applications and operating systems, providing evidence and assurance of ongoing monitoring and compliance. In addition, Tripwire provides evidence of encryption use via logs generated by encryption technologies.
REQUIREMENT 5. Use and Regularly Update Anti-virus Software or Programs.	Tripwire detects systems with out-of-compliance signatures, and reports if updates do not occur by detecting when virus definition files diverge from a compliant state. This approach complements antivirus software, which relies on pattern matching or virus definitions to operate successfully. And because Tripwire tracks and reports on system changes, if a “day zero” attack occurs, Tripwire detects damaged systems before a virus definition is even available. Tripwire captures and retains logs generated by anti-virus software and programs that provide evidence of the use of these applications and of their update status.
REQUIREMENT 6. Develop and Maintain Secure Systems and Applications.	Using Tripwire in development environments can help enforce change control procedures. Furthermore, Tripwire rules or tests can be tailored to fit specific security or audit requirements, providing a flexible and powerful tool for development, QA and automation functions. In testing and development environments Tripwire captures system logs that can be used to validate proper error handling, secure cryptographic storage, secure communications, proper role-based access control and other critical requirements for protecting cardholder data in the development and testing environment and when releasing into the production environment.

SOLUTION BRIEF

PCI DSS v1.2 Requirement	Tripwire Solutions Support Summary
REQUIREMENT 7. Restrict Access to Cardholder Data by Business Need to Know.	Tripwire helps ensure use of strong access control and permission settings and provides supplemental audit evidence of change in monitored systems. Tripwire captures and retains log information about login attempts and can generate alerts based on suspicious login behavior.
REQUIREMENT 8. Assign a Unique ID to Each Person With Computer Access.	Tripwire detects settings used for proper management of User Accounts and Authentication methods, including verification of both common and custom settings in third party products. Tripwire makes it easy to generate evidence to verify that appropriate system access has been enforced. Tripwire can monitor local logins to machines that house PCI data.
REQUIREMENT 9. Restrict Physical Access to Cardholder Data.	Tripwire supports security procedures and processes, such as physical access control, by monitoring features of custom applications used for physical alarms or monitoring software. In this way, Tripwire plays a role in monitoring systems for non-typical behavior that are usually watched manually. Tripwire captures logs of access control mechanisms that can be correlated with other data to detect improper physical access.
REQUIREMENT 10. Track and Monitor All Access to Network Resources and Cardholder Data.	Tripwire meets log collection, reporting and retention requirements by collecting logs, encrypting them for secure storage, retaining them and providing real-time analysis of log and event data. These capabilities let you determine which individuals accessed cardholder data, what types of security events occurred and when, and also ensures no one can tamper with log files so you have reliable forensic evidence. Tripwire monitors system activity and can determine the specific user accounts associated with those events. In addition, Tripwire monitors configuration settings for auditing functions and security settings and verifies they are in a compliant state.
REQUIREMENT 11. Regularly Test Security Systems and Processes.	Tripwire's enhanced file integrity monitoring detects changes and programmatically analyzes each change to determine if it was authorized and compliant. Tripwire determines change authorization through reporting techniques and/or through RFC ticket matching. Tripwire determines if changes to high-risk configuration settings are compliant by testing the settings against established or customer-specific policy as changes are detected. Tripwire immediately generates alerts when detected changes cause policy test failures.
REQUIREMENT 12. Maintain a Policy That Addresses Information Security for Employees and Contractors.	Tripwire provides a solution that can be used in a variety of ways to provide evidence of compliance (such as acceptable use, system configuration changes, and administration events) and supports best practice methods of discovery of unexpected change to critical systems.
REQUIREMENT A: Additional PCI DSS Requirements for Shared Hosting Providers.	Since each installation at a Hosted provider would be unique to the client requirements, the requirements of this section would be examined for each implementation. The use of Tripwire for monitoring and compliance reporting should have the same value regardless of the location of system implementation.



867.1191
sales@nexustech.com.ph
www.nexustech.com.ph



ABOUT TRIPWIRE

Tripwire is the leading global provider of IT security and compliance automation solutions that help businesses and government agencies take control of their entire IT infrastructure. Over 7,000 customers in more than 86 countries rely on Tripwire's integrated solutions. Tripwire VIA™, the comprehensive suite of industry-leading file integrity, policy compliance and log and event management solutions, is the way organizations proactively prove continuous compliance, mitigate risk, and achieve operational control through Visibility, Intelligence and Automation. Learn more at www.tripwire.com.