



PCI for Retailers

CONFIGURATION INTEGRITY FOR STORES AND DATA CENTERS



The pressure on retailers to achieve and prove compliance with the Payment Card Industry Data Security Standard (PCI DSS) is intensifying. Data security breaches are on the rise, with seemingly a new horror story every month—stolen credit card data, huge restitution costs, heavy fines, and irreparable reputation damage. And that’s just the tip of the iceberg; in a recent study of 50 U.S. retailers, Gartner found that 21 of the retailers were certain they had had a data breach. However, just three of the retailers had disclosed the incident to the public.

“Throughout our 34-year history, we have made a priority of putting the customer first. Ensuring that our customers’ data are secure, and that our website is consistently available to them, is mission critical for us—and Tripwire is the right solution for that job.”

— Jeff Bingaman
Senior Director of IT,
Crutchfield

Retailers face a unique challenge when it comes to protecting sensitive customer data and maintaining PCI compliance: their distributed network of stores. Customer data is captured, stored and transmitted from in-store POS systems, and protecting this data can be just as important as protecting the information maintained in corporate databases. Two recent, high-profile thefts of credit card data—Hannaford Brothers, a grocery chain headquartered in Portland, Maine, and Dave & Buster’s, a restaurant/entertainment chain based in Dallas, Texas—were the result of security breaches of in-store POS systems.

Tripwire has created customized solutions specifically for retailers that address these unique needs. These PCI-specific solutions not only cover the corporate data center but go beyond, encompassing POS systems efficiently and cost-effectively, whether you have a single register per store or a hundred. Having provided PCI solutions to

a majority of the top 100 retailers, Tripwire also brings its extensive professional services experience to bear with “PCI Foundation for Retailers” consulting engagements that ensure your implementation is simple, fast and successful.

It’s this expertise and proven product capabilities that are the reason seven of the nation’s top ten retailers and over 300 organizations in total have already turned to Tripwire to achieve, prove and sustain PCI compliance.

MEETING THE PCI REQUIREMENTS

The PCI DSS lists 12 requirements for achieving compliance. Taken together, they are a powerful combination of security best practices that protect the confidentiality of customer data. The more these requirements are automated, the more secure you will be, the better you will be able to stay in compliance, and the easier it will be to pass

SOLUTION BRIEF

| Tripwire Out-of-the-box PCI Policies | |
|--|--------------|
| Platform | Version |
| Servers | |
| AIX (PowerPC) | 5.1 |
| HP-UX (PA-RISC) | 11 |
| Red Hat Linux | 4 |
| Solaris (SPARC) | 8 |
| Solaris (SPARC) | 9 |
| Solaris (SPARC) | 10 |
| SUSE Linux | 9 |
| Windows Server DM | 2003 |
| Windows Server | 2000 |
| Network Devices | |
| Cisco IOS | 10–12.3 |
| Cisco PIX | 5.2–6.4 |
| Databases | |
| MS SQL Server | 2000 |
| MS SQL Server | 2005 |
| Oracle 9i | Solaris |
| Oracle 9i | Windows |
| Oracle 10g | Solaris |
| Oracle 10g | Windows |
| Active Directory | |
| Windows Server DC | 2003 |
| Applications | |
| MS Exchange | 2003 |
| MS IIS | 6 |
| VMware | ESX v2.x/3.x |

your PCI audit. Tripwire can help you address 11 of the 12 PCI requirements, by instilling file integrity monitoring and configuration assessment capabilities.

Configuration control is the foundation of sustainable PCI compliance and impacts nearly all PCI requirements. Without control, improper configuration of in-scope systems and the risk of unauthorized changes creates significant security risk and diminishes the integrity of your IT systems, which can lead to damaging business consequences. Automated configuration control enables retailers to take proactive measures to minimize these risks by ensuring continuous configuration integrity across the data center and in-store infrastructures.

One of the most difficult requirements to fulfill and least satisfied among merchants according to recent research is the PCI DSS 11.5 category, which calls for “alert on unauthorized modification of critical system and content files...” This “file integrity monitoring”, also referred to as “change auditing”, is a core function of Tripwire Enterprise, the recognized leader in this market for over a decade. In addition, Tripwire Enterprise provides configuration assessment, which allows you to proactively assess and validate critical configuration settings and values against PCI DSS and the Center for Internet Security (CIS) benchmarks, which are needed to comply with requirements throughout the PCI standard.

Tripwire delivers out-of-the-box PCI configuration assessment policies across your IT infrastructure. Tripwire leverages industry standards and benchmarks, such as CIS, to proactively assess configurations for PCI DSS compliance across 21 different elements within your infrastructure, including operating systems, network devices, directory servers, databases and applications.

ASSESS, ACHIEVE AND MAINTAIN A COMPLIANT STATE

Assess your current state: The starting point for any compliance activity is to proactively assess the configuration state of the corporate and in-store infrastructure components that are in-scope for PCI compliance.

Tripwire Enterprise quickly provides a scorecard that shows the pass/fail status of a specific infrastructure as it relates to key configuration settings, and also weights the scores based upon the most critical failures. You can easily drill down on any test and find out exactly why it is failing and receive prescriptive remediation guidance to rapidly fix all non-compliant configurations. Knowing the actual configuration state of your infrastructure is of great value from a sound security perspective, as well as accomplishing a successful audit.

Tripwire configuration assessment will quickly show the state of compliance of your critical infrastructure compared to internal and external best practices.

Achieve a compliant state: Tripwire not only detects non-compliant settings, it also helps remediate the failed tests so that a higher level of compliance can quickly be achieved. Tripwire provides:

- **Golden Policies:** Maximize the value of your IT investments by codifying internal IT configuration best practices.
- **Remediation Advisor:** Out-of-the-box prescriptive steps required to remediate a non-compliant setting to a compliant state.
- **Policy Waivers:** Streamline compliance processes by applying temporary waivers to failing tests that are being addressed by planned projects.

Unlike most configuration control solutions, Tripwire Enterprise captures and permanently retains the current state of PCI-required critical system, content and configuration settings. This “current-state” version of the data is stored in the central repository of the Tripwire Enterprise Console as a “baseline”.

Maintain a compliant state: From that point of initial capture, any change that is detected to the baseline is captured and stored in the central repository as a version to the corresponding baseline. The “baseline + versions” model represents the current approved state of each monitored item. And because change is continuously captured and analyzed, there is never a need to perform a

SOLUTION BRIEF

TRIPWIRE'S EXPERTISE AND PROVEN PRODUCT CAPABILITIES ARE THE REASON SEVEN OF THE NATION'S TOP TEN RETAILERS AND OVER 300 ORGANIZATIONS IN TOTAL HAVE ALREADY TURNED TO TRIPWIRE TO ACHIEVE, PROVE AND SUSTAIN PCI DSS COMPLIANCE.

“mega-scan” to re-capture the baseline data so that it can be analyzed for compliance.

Using the Tripwire baseline architecture, file integrity monitoring and configuration assessments are continuously performed. As incremental change is detected, it is streamed into the central repository and that change data is automatically reevaluated against compliance requirements. This process provides a continuous view of the state of compliance of your environment with negligible impact to systems, applications and network. And because Tripwire is constantly monitoring the integrity of your files, you can be assured that your compliance state will not drift.

TRIPWIRE ENTERPRISE FOR STORES

More and more, retailers and auditors are considering their POS systems to be within the scope of their PCI compliance efforts. This introduces a number of potential new issues, including efficiently deploying the agents, managing the software, and collecting the data across geographically dispersed networks. Equally important, store system configuration management must be done at an economical price. Tripwire Enterprise for Stores meets that requirement by providing

coverage of registers and in-store servers at a low per-store fixed price.

Because infrastructure size and network topology can vary greatly among retailers, Tripwire provides two architectures for reaching PCI compliance goals. In the centralized architecture all changes made to registers or to the store server are reported directly back to the Tripwire Enterprise Console. The distributed architecture option consolidates all changes at the store server before being communicated to the console, providing the benefit of reducing network traffic and better matching with some large store configurations. Tripwire's professional services group will work with you to determine the architecture that's optimal for your needs.

EXPERT ASSISTANCE

There's usually no time to delay when it comes to PCI compliance efforts, and Tripwire has the experience and expertise to minimize the time, cost and risk of your implementation. Tripwire Professional Services offers a standard “PCI Foundation for Retailers” consultation that provides our recommended level of design, customization, training and deployment assistance for a successful PCI implementation.

The first step is a complementary two-hour assessment by a Tripwire Professional Services consultant to understand your specific requirements and to scope the project. Once approved, the consultant will work with you to develop a foundational set of rules, tests, reports and dashboards, customized for your environment, including both corporate and store assets. Tripwire will then deploy and test the software to an initial set of devices, both within your corporate location and a retail location, and provide you with the training and documentation you need to deploy throughout the rest of your infrastructure—or provide complete deployment services.

For more information on how Tripwire can help you achieve and maintain PCI compliance across your retail operations, please visit tripwire.com/retailers or contact your Tripwire sales representative.

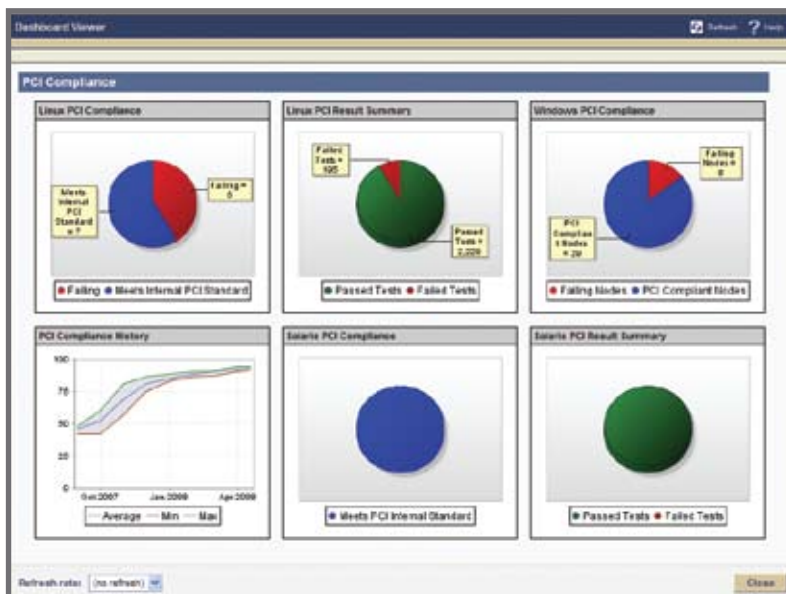


Fig. 1: Tripwire Enterprise dashboard showing PCI compliance status

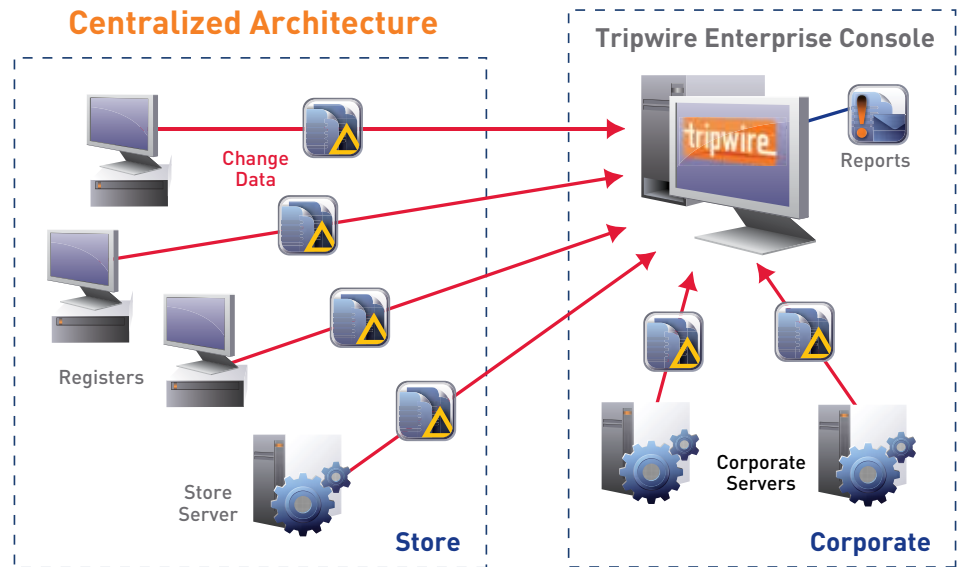


Fig. 2: Changes to registers and store server (if applicable) are reported directly to the Tripwire Enterprise Console.

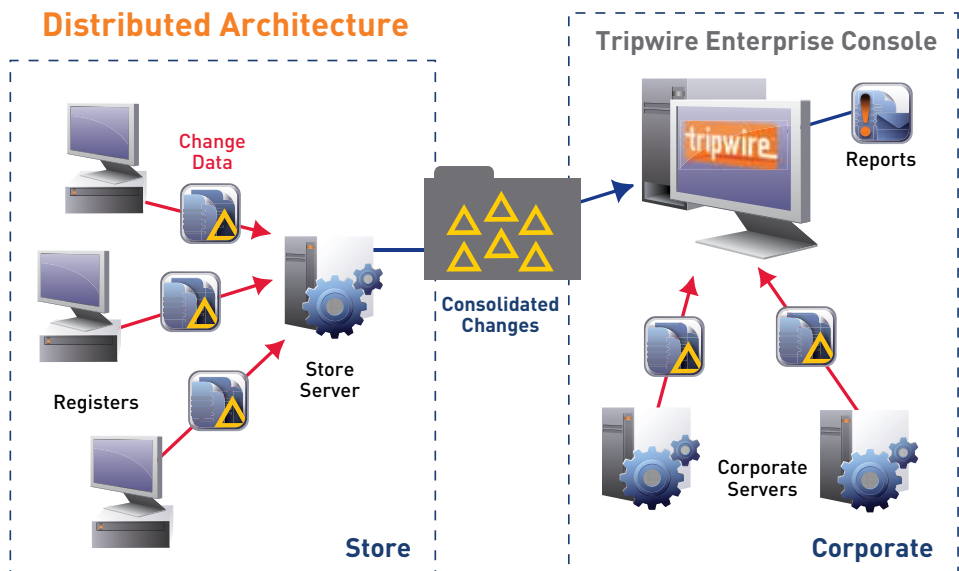


Fig. 3: Changes are consolidated on the store server, and then reported to the Tripwire Enterprise Console.



ABOUT TRIPWIRE

Tripwire helps over 6,000 enterprises worldwide reduce security risk, attain compliance and increase operational efficiency throughout their virtual and physical environments. Using Tripwire's industry-leading configuration assessment and change auditing solutions, organizations successfully achieve and maintain IT configuration control. Tripwire is headquartered in Portland, Oregon, with offices worldwide.