FORTRA™

SOLUTION BRIEF (TRIPWIRE)

Automated Change Monitoring

Streamline Compliance Reporting and Allowlist Management with Tripwire State Analyzer

Changes occur nearly every second in the typical network. These changes most commonly include those made to group memberships, which ports are open, software patches, and a variety of other categories. That is precisely why it is so important to remain compliant with standards that regulate change monitoring, such as North American Energy Reliability Corporation Critical Infrastructure Protection (NERC CIP).

Many of the most popular cybersecurity compliance frameworks require the creation of allowlists for installed software, network ports, network services, local users, local shares, and persistent routes. This includes the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the Payment Card Industry Data Security Standard (PCI DSS), and NERC CIP, to name a few.

Maintaining compliance to these policy frameworks requires proof that unauthorized changes are detected and remediated quickly. Audits that verify compliance require extensive and time-consuming documentation and can potentially result in costly fines if there are any findings.

Product Overview

Fortra's Tripwire® State Analyzer ensures the compliance and security of your network by monitoring the system against lists of what's allowed to run. Invalid changes to the monitored items are detected and reported so they can be returned to a compliant state.

Tripwire State Analyzer then generates audit reports detailing both authorized and unauthorized configurations. To improve audit efficiency, the application also permits the justification for the approvelist test for any setting to be included in the audit report. To reduce the false positive rate of reporting, Tripwire State Analyzer enables you to define required versus permitted system settings. Violations are flagged only if required software is not present or if software that is not explicitly permitted is present.

Key Benefits

Remaining compliant with security frameworks is of the utmost importance. However, doing so is made especially difficult if the system put in place to assist with compliance is overly complicated and requires a great deal of manual monitoring and creation of audit artifacts. Beyond remaining compliant with security frameworks, thoroughly securing your network is impossible if your change detection software cannot rapidly detect changes—especially if they are quickly returned to a compliant state.

HIGHLIGHTS

Tripwire Enterprise is a leading security solution that provides file integrity monitoring (FIM) and security configuration monitoring (SCM). Organizations worldwide leverage its capabilities for better, faster and more cost effective cyberthreat protection and compliance. Tripwire State Analyzer extends these capabilities for Tripwire customers—including those who need to adhere to strict NERC CIP and PCI DSS compliance requirements. It also addresses many of the Center for Internet Security's CIS Controls.

For these reasons, Tripwire State Analyzer provides the following:

- **Automated Monitoring** – Tripwire State Analyzer allows users to manage allowed lists for group memberships, open ports, routes, services, shares, software, and users on the systems in their environment. It then automatically compares items such as open ports, group memberships, etc. to the allowed lists and makes note of any unauthorized differences.
- **Rapidly Detect Allowlist Changes** – Tripwire State Analyzer can be scheduled to monitor allowlist items for change as often as desired.
- **Easy-to-Use, Secure Interface** – Tripwire State Analyzer has an easy to operate user interface where allowed items can be managed as individual objects, rather than as lines in a CSV file. You can determine which users are able to access Tripwire State Analyzer and what level of access they should have. Authentication can also be integrated with Active Directory.

Conduct Audits Efficiently

Although automated compliance monitoring will assist your organization in securing your network, this is not the same as passing an audit to ensure compliance with the same cybersecurity frameworks. These frameworks exist to protect your organization as well as the customers you serve, which is precisely why remaining compliant and passing audits is so important. A failed audit implies negligence on an organization's behalf and can result in extensive liability should a breach occur. Additionally, the penalties for failing an audit are costly, possibly resulting in multi-million dollar fines.

Conducting an audit is not an easy task either. When done manually, preparing the various artifacts necessary for deeming your business compliant can be painstakingly slow, costing your business hours of lost productivity. Additionally, conducting an audit manually leaves room for human error. If the auditors' questions cannot be answered concisely and completely there will be follow up requests, resulting in even more lost productivity and an even more costly experience. Tripwire State Analyzer was designed to reduce audit findings and penalties while simultaneously reducing the staff time required to prepare for audits and answer any requests.

Automated Report Generation

When a system is examined, a comprehensive report of authorized and unauthorized settings is generated by Tripwire State Analyzer along with the justification information. This report enumerates the settings that are out of compliance, and can be configured to provide justification for why the change was allowed. This provides an automatic audit trail of changes, waivers and justifications, as well as unauthorized changes, as they happen. This process can also be customized to each unique enterprise and its individual compliance needs. Overall, this automated process serves as a direct substitute to the hours of manual work required by staff to produce a report that has a greater potential for errors.

Types of Reports

Tripwire State Analyzer helps ensure the accurate creation of three kinds of reports and alerting, classified as follows:

- **Evidence Reporting** - Audit justification for individual configurations observed.
- **Security Alerting** - Overview of compliance with internal security controls and exceptions to them.
- **Compliance Reporting** - Audit summary of all compliance controls and adherence to them.

These are targeted for these primary use cases:

- **Users and Passwords** - In the solution for local users, multiple aspects of user accounts are reported on.
- **Ports** - Reports are generated to support two use cases: evidence reporting, and alerting for daily maintenance of compliance. Report generation is automated once the solution is fully implemented, and allows for scanning as often as desired.
- **Services** - Once the user has supplied information about normal or expected services on a system or class of systems, Tripwire State Analyzer will alert on new, unexpected services. Report generation is automated once the solution is fully implemented, and allows for reporting as often as desired.

Meet Compliance Standards

Tripwire Enterprise is used to monitor a wide range of functions. Tripwire State Analyzer takes that tool and tailors it to the specific needs created by NERC CIP and other NIST

CF-derived frameworks. The process of creating automated reports can be customized to each unique enterprise and its individual compliance needs. Tripwire State Analyzer greatly simplifies the process of ensuring that your business is compliant with your specific compliance requirements.

PCI DSS Requirements

Tripwire delivers continuous and unmatched PCI 4.0 compliance through our unique integration of policy management, FIM, vulnerability assessment, and log intelligence. Tripwire State Analyzer specifically addresses PCI v4.0 Requirement 1.2.5 (v3.2.1 Requirement 1.1.6), which relates to the documentation and business justification for use of all services, protocols, and allowed ports.

NERC CIP Requirements

Tripwire State Analyzer lends its power—in conjunction with Tripwire Enterprise, Tripwire IP360™ and Tripwire LogCenter®—to help you address the requirements contained in these NERC CIPv6 standards:

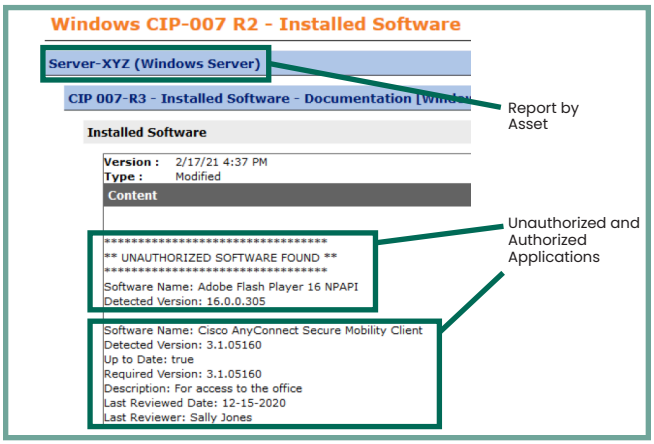
- **CIP-007 R1: Ports and Services** — The solution can monitor ports and services and compare current state against a tailored set of customer-specific approved ports and services, alerting when monitoring detects a variance.
- **CIP-007 R2: Security Patch Management** — The app can identify software versions and installed patches and compare current state against a tailored set of Patch Management customer-specific approved software versions and patches, alerting when there is a variance on specific BCAs.
- **CIP-007 R5.2: System Access Controls** — The app can verify only approved accounts exist on systems, as codified in an authorized user allowlist.
- **CIP-004: Access Management & Access Revocation Programs** — The app can verify that only approved accounts exist on systems, as codified in an authorized user allowlist.

For more information, visit Tripwire's NERC CIP compliance page.

Summary

Tripwire State Analyzer directly addresses your team's need for a high quality, time- and cost-saving change monitoring application. The application's user-friendly interface and rapid change detection ensures your organization will be able to easily define and update your allowlists while efficiently tracking any invalid changes made against them.

Aside from securing your network, the Tripwire State Analyzer's automated report generation will save you time preparing for audits and money by reducing findings from those audits.



Tripwire State Analyzer reports on authorized, unauthorized as well as unused settings, regardless of type.

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.