Tripwire State Analyzer App

Automated "why" reporting for security and audit efficiency

Tripwire Enterprise is a strategic business tool. Organizations around the world leverage its capabilities for better, faster and more cost effective cyberthreat protection and compliance.

The Tripwire State Analyzer app extends these capabilities for Tripwire customers around the globe, across many industries, including those who need to adhere to strict NERC CIP and PCI DSS compliance requirements. It is also a powerful tool to address many of the Center for Internet Security's CIS Controls.

Get Safe and Compliant

Keeping your organization safe and compliant is challenging and complex. Security is more effective when you have documented baselines for a system's configuration, usually in the form of a security policy. These policies specify recommended or required system configurations, including applications, ports, services, and security basics. But ask yourself: How can I validate that my systems are configured according to my security policy? Can I automate that process? Can I provide justification for my established policy? Can I easily manage my policy, especially as it applies to assets and groups of assets? This reconciliation process poses a significant challenge that often involves lots of time, resources, manual checks, cross-system comparisons, and approval processes.

The Solution: Tripwire State Analyzer App

The Tripwire® State Analyzer app works in tandem with Tripwire Enterprise and Tripwire IP360™ to offer an automated, flexible solution to this security challenge.

How Does the Tripwire State Analyzer App Help You?

With the app, you manage your policies centrally and get reports on approval, as well as unauthorized system settings of multiple types. In addition, you can automatically include the justification

With the Tripwire State Analyzer app you can:

- Define records in centralized allowlist configuration files that contain approved configuration items (e.g., network ports, services, local users, etc.)
- Automate the validation of detected system configurations against your allowlist configuration files
- Generate detailed system configuration reports of authorized and unauthorized configurations

The app supports the collection and reconciliation of the following configuration items:

- Network Ports
- Local Users
- Local Groups
- Services
- Installed Software
- Local Shares
- Persistent Routes

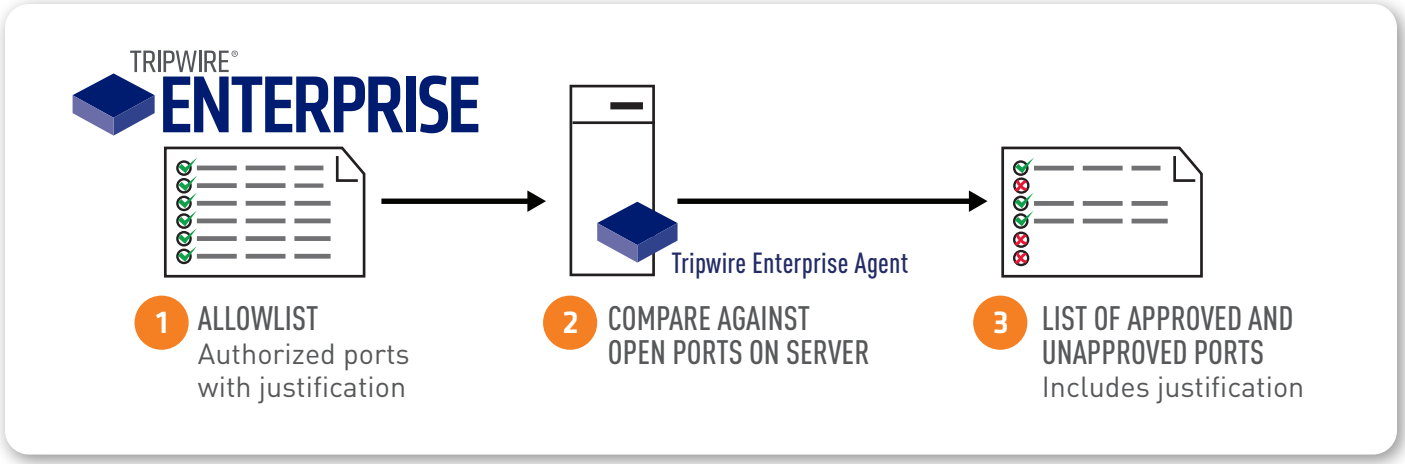

Fig. 1 Overview of the Tripwire State Analyzer app process flow in the context of network port allowlisting.
Step 1: User defines a allowlist of authorized network ports
Step 2: The app interrogates the system and compares any open ports to the list of authorized ports
Step 3: Report is generated, listing authorized and unauthorized open ports

for a given setting in the same report to speed up the auditing process.

The Tripwire State Analyzer app enables you to define a set of required or permitted system settings. When a system is examined, a comprehensive report of authorized and unauthorized settings is generated along with the justification information. This report enumerates those 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.

Save Time with Customized Detailed Reports

The Tripwire State Analyzer app increases automation and efficiency and can be customized for each unique enterprise, enabling you to save time and resources:

- Automate the validation of detected system configurations
- Generate detailed system configuration reports of authorized and unauthorized configurations
- Increase audit preparation efficiency

PCI 3.2 Requirements

Tripwire delivers continuous and unmatched PCI 3.2 compliance by our unique integration of policy management, file integrity monitoring (FIM), vulnerability assessment and log intelligence. The Tripwire State Analyzer app specifically addresses PCI Requirement 1.1.6, which relates to the documentation and business justification for use of all services, protocols and allowed ports.

CIS Controls

The Center for Internet Security's CIS Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. The Tripwire State Analyzer app is a powerful tool to address the following:

- **Control 2:** Inventory and Control of Software Assets
- **Control 4:** Controlled Use of Administrative Privileges
- **Control 5:** Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- **Control 9:** Limitation and Control of Network Ports, Protocols, and Services
- **Control 11:** Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches
- **Control 16:** Account Monitoring and Control
- **Control 18:** Application Software Security

The app also lends its power—in conjunction with Tripwire Enterprise, Tripwire IP360 and Tripwire Log Center™—to help you address the requirements contained in these NERC CIPv6 standards:

- **CIP-007 R1: Ports and Services** — The app can monitor ports and services and compare current state against a tailored set of customer-specific approved port 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 a full description of the Tripwire NERC Solution Suite, visit tripwire.com and search "NERC CIPv6".

Schedule Your Demo Today

Let us take you through a demo of Tripwire security and compliance solutions and answer any of your questions. Visit **tripwire.com/contact/request-demo**

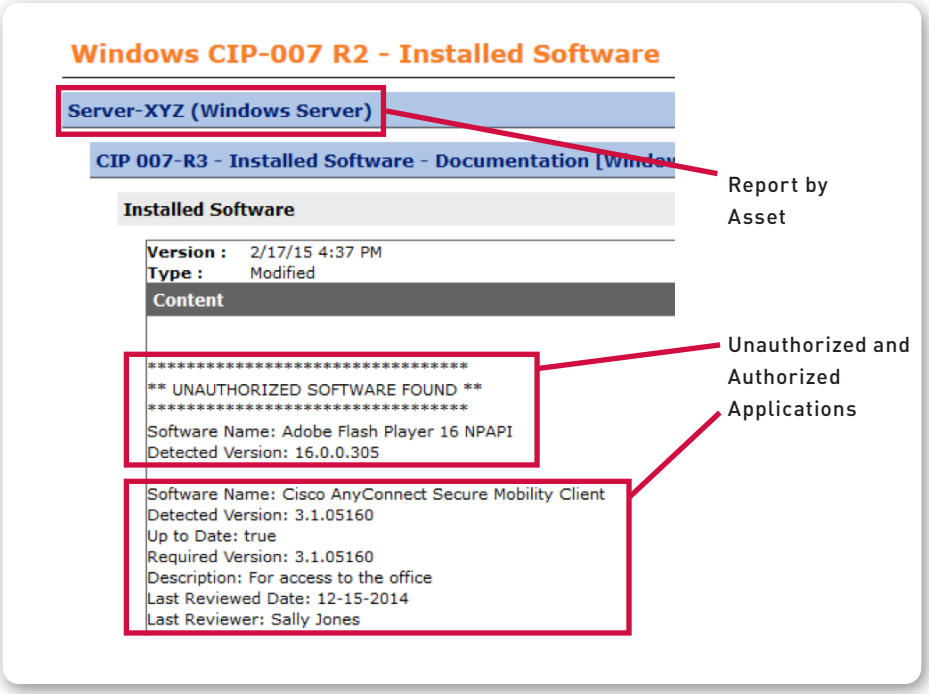

Fig. 2 The Tripwire State Analyzer app reports on approved as well as unauthorized system settings, regardless of type.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

TAPPTSA1b 2009