FORTRA™

DATASHEET (TRIPWIRE)

Tripwire State Analyzer

Automated "why" reporting for security and audit efficiency

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

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

How Does Tripwire State Analyzer Help You?

With Tripwire State Analyzer, 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 for a given setting in the same report to speed up the auditing process.

Tripwire State Analyzer 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 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 and justifications, as well as unauthorized changes as they happen. Tripwire State Analyzer saves time and increases accuracy for both business- and audit-driven compliance policies.

With Tripwire State Analyzer you can:

- Define records in centralized Allowlist configurations that contain approved configuration items
- Automate the validation of detected system configurations against your Allowlist configurations

PRODUCT SUMMARY

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.

Tripwire State Analyzer 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.

- Generate detailed system configuration reports of authorized and unauthorized configurations
- Integrate with FoxGuard to improve the process of validating software and patches

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

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

PCI Requirements

Tripwire delivers continuous and unmatched PCI compliance by our unique integration of policy management, file integrity monitoring (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

The application also lends its power—alongside 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 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-010 R1: Configuration Change Management** — The app can identify and authorize application software/ versions, custom software, logical network accessible ports, and security patches.

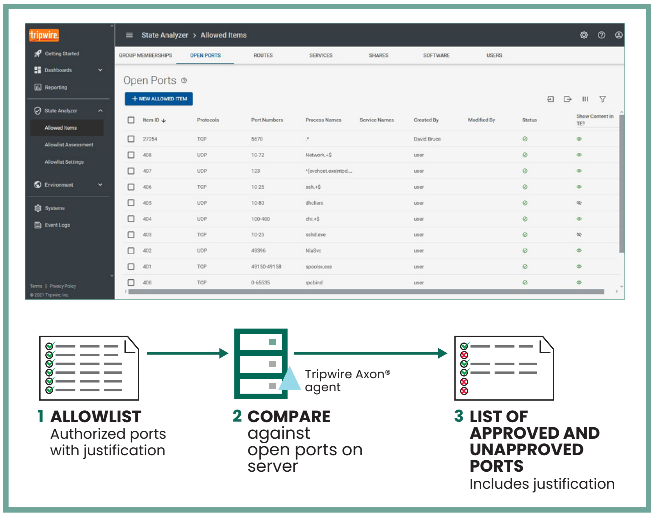
For more information on Tripwire's NERC solutions, visit the NERC Compliance Solution section at tripwire.com.

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.

Tripwire State Analyzer is a powerful tool to address the following:

- **Control 2:** Inventory and Control of Software Assets
- **Control 4:** Secure Configuration of Enterprise Assets and Software
- **Control 5:** Account Management
- **Control 6:** Access Control Management
- **Control 13:** Network Monitoring and Defense
- **Control 16:** Application Software Security



State Analyzer > Allowed Items

GROUP MEMBERSHIPS | OPEN PORTS | ROUTES | SERVICES | SHARES | SOFTWARE | USERS

Open Ports

+ NEW ALLOWED ITEM

Item ID	Protocols	Port Numbers	Process Names	Service Names	Created By	Modified By	Status	Show Content in TE?
27254	TCP	5670	.*		David Bruce		✓	●
408	UDP	10-72	Network.+$		user		✓	●
407	UDP	123	^(svchost.exe|ntpd....		user		✓	●
406	TCP	10-25	ssh.+$		user		✓	●
405	UDP	10-80	dhclient		user		✓	⊘
404	UDP	100-400	chr.+$		user		✓	●
403	TCP	10-25	sshd.exe		user		✓	⊘
402	UDP	49396	NlaSvc		user		✓	●
401	TCP	49150-49158	spoolsv.exe		user		✓	●
400	TCP	0-65535	rpcbind		user		✓	●

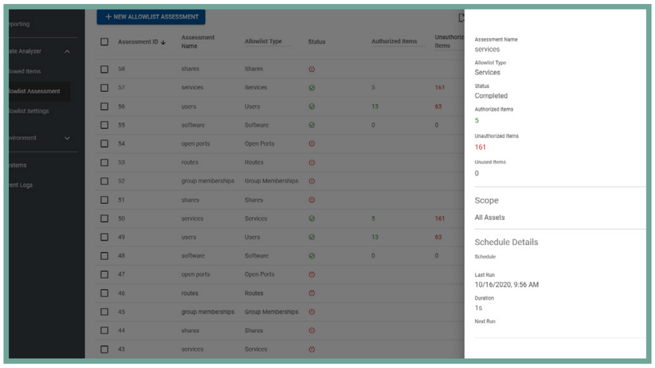
Overview of Tripwire State Analyzer's process flow in the context of network port allowlisting.

Step 1: User defines an allowlist of authorized network ports
Step 2: Tripwire State Analyzer 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

Save Time with Customized Detailed Reports

Tripwire State Analyzer 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



□	Assessment ID ↓	Assessment Name	Allowlist Type	Status	Authorized Items	Unauthoriz Items
□	58	shares	Shares	!		
□	57	services	Services	✓	5	161
□	56	users	Users	✓	13	63
□	55	software	Software	✓	0	0
□	54	open ports	Open Ports	!		
□	53	routes	Routes	!		
□	52	group memberships	Group Memberships	!		
□	51	shares	Shares	!		
□	50	services	Services	✓	5	161
□	49	users	Users	✓	13	63
□	48	software	Software	✓	0	0
□	47	open ports	Open Ports	!		
□	46	routes	Routes	!		
□	45	group memberships	Group Memberships	!		
□	44	shares	Shares	!		
□	43	services	Services	!		

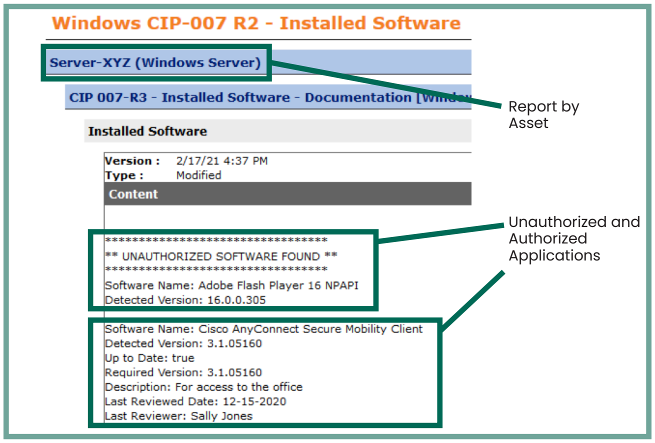
Assessment Name
services
Allowlist Type
Services
Status
Completed
Authorized Items
5
Unauthorized Items
161
Unused Items
0

Scope
All Assets

Schedule Details
Schedule

Last Run
10/16/2020, 9:56 AM
Duration
1s
Next Run

Tripwire State Analyzer allows for quick, high-level overviews of all assessment data from multiple consoles in a single source, which can be viewed in greater detail—down to the per-node level.



Windows CIP-007 R2 - Installed Software

Server-XYZ (Windows Server)

CIP 007-R3 - Installed Software - Documentation [Window

Installed Software

Version : 2/17/21 4:37 PM
Type : Modified

Content

```
*********************************
** UNAUTHORIZED SOFTWARE FOUND **
*********************************
Software Name: Adobe Flash Player 16 NPAPI
Detected Version: 16.0.0.305

Software Name: Cisco AnyConnect Secure Mobility Client
Detected Version: 3.1.05160
Up to Date: true
Required Version: 3.1.05160
Description: For access to the office
Last Reviewed Date: 12-15-2020
Last Reviewer: Sally Jones
```

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.