TRIPWIRE®
WHITELIST PROFILER

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 Whitelist Profiler extends these capabilities for Tripwire customers around the globe, across many industries, including those who need to adhere to strict NERC CIP and PCI compliance requirements. It is also a powerful tool to address many of SANS Critical Security Controls.

Tripwire customers across many industries, including those who need to adhere to strict NERC CIP and PCI compliance requirements, benefit from Tripwire Whitelist Profiler. It's also a powerful tool to address many of the SANS CIS Critical Security Controls.

TRIPWIRE WHITELIST PROFILER

AUTOMATED "WHY" REPORTING FOR SECURITY AND AUDIT EFFICIENCY

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 WHITELIST PROFILER

Tripwire® Whitelist Profiler works in tandem with Tripwire Enterprise and Tripwire IP360™ to offer an automated, flexible solution to this security challenge.

With Tripwire Whitelist Profiler you can:

- Define records in centralized whitelist configuration files that contain approved configuration items (e.g., network ports, services, local users, etc.)
- Automate the validation of detected system configurations against your whitelist configuration files
- Generate detailed system configuration reports of authorized and unauthorized configurations. Tripwire Whitelist Profiler supports the collection and reconciliation of the following configuration items:
  - Network Ports
  - Local Users
  - Local Groups
  - Services
  - Installed Software
  - Local Shares
  - Persistent Routes

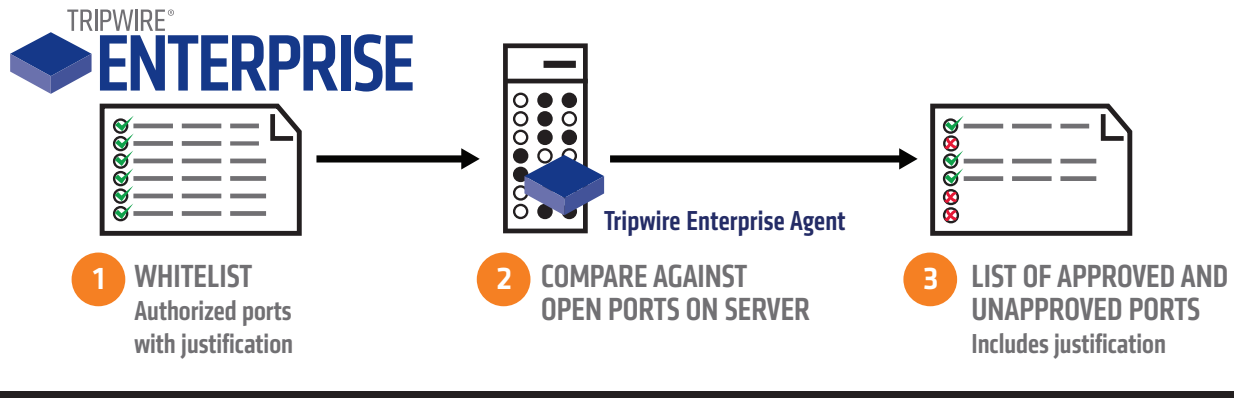


FIG. 1 *Overview of the Tripwire Whitelist Profiler process flow in the context of network port whitelisting.*
Step 1: User defines a whitelist of authorized network ports
Step 2: Tripwire Whitelist Profiler interrogates the system and compares any open ports to the list of authorized ports
Step 3: Report is generated, listing authorized and unauthorized open ports

HOW DOES TRIPWIRE WHITELIST PROFILER HELP YOU?

With Tripwire Whitelist Profiler, 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 Whitelist Profiler 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

Tripwire Whitelist Profiler 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

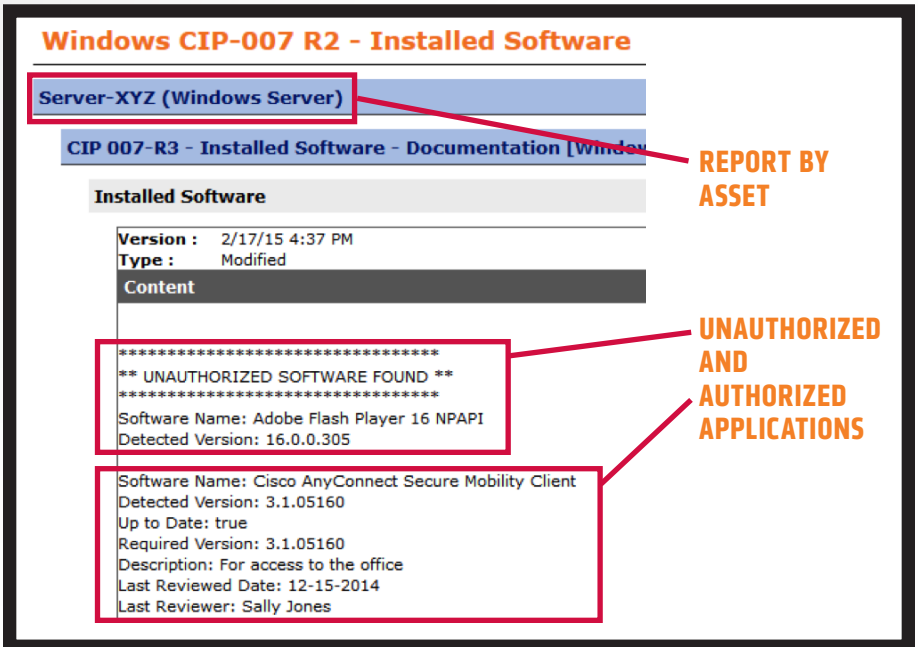
PCI 3.2 REQUIREMENTS

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. Tripwire Whitelist Profiler 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 CRITICAL SECURITY CONTROLS

The SANS CIS Critical Security 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 Whitelist Profiler is a powerful tool to address the following CIS CSC:

2) Inventory of authorized and unauthorized software
3) Secure configurations for hardware and software in mobile devices, laptops, workstations and servers
6) Application software security
10) Secure configurations for network devices such as firewalls, routers, and switches
11) Limitation and control of network ports, protocols and services
12) Controlled use of administrative privileges
16) Account monitoring and control



◆ **FIG. 2** *Tripwire Whitelist Profiler reports on approved as well as unauthorized system settings, regardless of type.*

Tripwire Whitelist Profiler is a powerful tool that, in conjunction with Tripwire Enterprise, Tripwire IP360 and Tripwire Log Center, helps you address the requirements contained in the NERC CIPv6 standards:

» **CIP-007 R1:** Ports and Services – Tripwire's Whitelist Profiler 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 – Tripwire's Whitelist Profiler 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 BCA's.

» **CIP-007 R5.2:** System Access Controls – Tripwire's whitelist profiler can verify only approved accounts exist on systems, as codified in an authorized user whitelist.

» **CIP-004:** Access Management & Access Revocation Programs – Tripwire's Whitelist Profiler can verify only approved accounts exist on systems, as codified in an authorized user whitelist.

For a full description of the Tripwire NERC Solution Suite, visit tripwire.com and search "NERC CIPv6"

◆ Tripwire is a leading provider of endpoint detection and response, security, compliance and IT operation solutions for enterprises, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. Learn more at tripwire.com ◆

SECURITY NEWS, TRENDS AND INSIGHTS AT TRIPWIRE.COM/BLOG ◆ FOLLOW US @TRIPWIREINC ON TWITTER

TAPPWLP2a 201605