DATASHEET

Tripwire Configuration Compliance Manager 5.17

Asset discovery, configuration and patch compliance auditing, risk and prioritization reporting

Highlights

- Asset Discovery—Find all the IP-addressable assets within your environment and create a hardware and software inventory
- Configuration Compliance Audit—Agentlessly assess and audit compliance of network infrastructure devices and other key systems
- Patch Compliance Audit—Assess what patches have been applied and know what is missing or available
- Audit-Ready Reporting and Dashboards—Different, flexible views of compliance and audit data based on role

Enterprises in many regulated industries must comply with rapid regulation and compliance updates and increasingly complex audit requirements. Global compliance standards in 2014 underwent over 40,000 compliance updates. In addition, increased risk from escalating cyber threats brings significant new challenges to enterprise compliance, IT Security, and IT Operations teams.

Challenges include:

- Compliance Policy Change and Complexity
- Gap Analysis
- Limited Resources
- Sustaining Audit
- Growing Cybersecurity Risk
- Financial Risk
- Increasing Audit Costs and Short Timelines

The Tripwire CCM Solution

Tripwire® Configuration Compliance Manager (CCM) delivers innovative agentless compliance and security audit that has proven to be light touch on most enterprise infrastructure and quickly provides value and insight through a risk-prioritized view of enterprise compliance and security posture.

Tripwire CCM Capabilities

Asset Discovery

Upon installation of Tripwire CCM, asset discovery can be rapidly enabled to discover all IP-addressed active assets such as routers, switches, gateways, firewalls, desktops, laptops, servers and printers. Tripwire CCM then enumerates the configuration and applications discovered on each system and provides detailed information on thousands of configuration variables. It identifies and assesses virtually everything on the network, from routing table entries and access control lists to antivirus and system logging status, all without requiring agent software on the endpoints.

Configuration Compliance Audit

Tripwire CCM audits each system's configuration and compares any configuration changes with relevant best practice and industry standard policies from NIST, CIS and Microsoft. Tripwire CCM also provides policies for specific regulations such as PCI, SOX, HIPAA, NERC CIP and more.

The current release of Tripwire CCM significantly increases Linux policy coverage by incorporating over 100 Tripwire Enterprise Linux policies.

Patch Compliance Audit

Patch compliance auditing is a critical step in reducing security risk and achieving compliance. Tripwire CCM includes a powerful audit capability to find missing and unapplied patches. Whether managed through the Tripwire CCM console or an easy-to-use report, you can quickly identify which systems have missing patches that take systems out of compliance.

Reporting and Dashboards

Tripwire CCM compliance audit scan results within enterprise environments can deliver a detailed and actionable view of asset compliance and security posture. The system also delivers prioritized guidance on which findings to address first.

Complete Enterprise Coverage—Agent and Agentless Technologies

Tripwire CCM can monitor a wide variety of systems not typically monitored using agent-based methods (e.g. routers/wireless routers, switches, gateways, firewalls). Tripwire CCM provides scheduled and on-demand audits.

Tripwire CCM is complementary to Tripwire's agent-based solution, Tripwire Enterprise. Often, enterprise customers may opt for a blended technology approach allowing them to place agents such as those used by Tripwire Enterprise on their interior and critical servers, Active Directory servers and key databases, and use the agentless technology of Tripwire CCM to monitor and audit network infrastructure devices, edge, and desktops—all of which can be more challenging to monitor and maintain using agents.

Tripwire CCM and ICS

Industrial control systems (ICS) monitor and control industrial and physical infrastructure processes and include a wide range of devices and processes, such as supervisory control and data acquisition (SCADA) systems, process control systems (PCS), process control domains (PCD), and building automation and control systems (BACS).

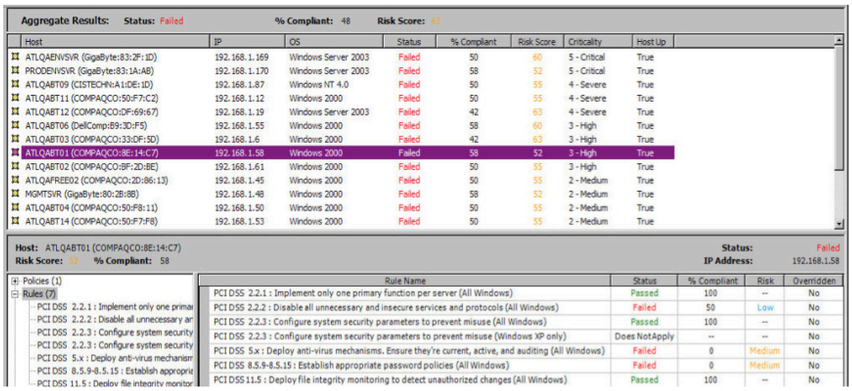

Fig. 1 Tripwire CCM Aggregate Results of enterprise scan with Percent Compliant and Risk Scores, plus actionable details.

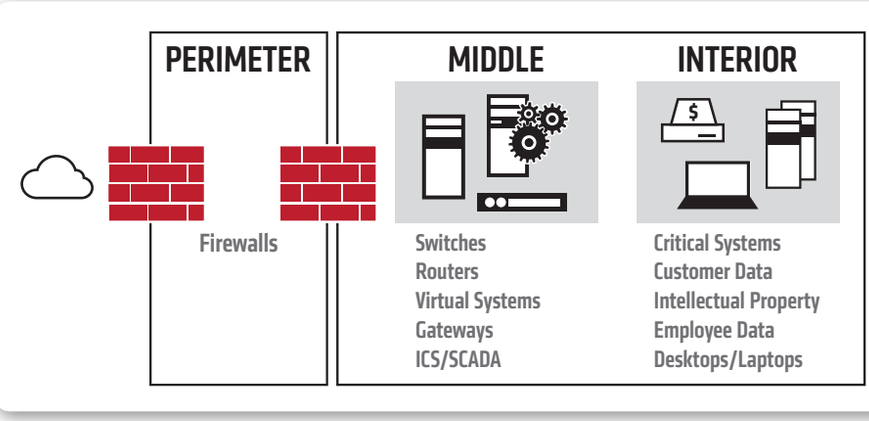

Fig. 2 Tripwire Security Configuration Management—Tripwire CCM and Tripwire Enterprise—covers the entire enterprise.

Tripwire CCM provides customers with a simple path to add effective security monitoring and assessment without touching ICS or SCADA equipment, putting operational availability at risk or requiring a complicated deployment. Rather than retrofitting security tools built for IT, Tripwire CCM for Industrial Automation is a purpose-built low/no-touch solution for industrial security with configuration assessment, change and threat detection for industrial environments.

Tripwire CCM supports the industry standard ANSI/ISA 62443-3-2 for network segmentation and secure zones and conduits, securing zone ingress/egress and ICS system security. Tripwire CCM assures that required network segmentation configurations are set and do not "drift" from the policy. This reduces the risk of industrial automation system and critical infrastructure disruption and downtime due to cyber threats from external attacks, malicious insiders and human error.

Summary

Tripwire CCM's agentless ease-of-management lowers cost of compliance for enterprise regulatory audits and minimizes risk while increasing uptime by ensuring that systems also remain configured in compliance with organizational policies.

Features and Benefits

Asset Discovery	Quickly find all assets within your environment, create and maintain a hardware and software inventory—most organizations find at least 10–15% more assets than they realized were present in their environment.
Configuration Compliance Audit	Easily assess network infrastructure devices, desktops and servers for audit compliance, with visualized and actionable color-coded prioritization.
File and System Integrity Monitoring	Most compliance standards require some type of file and system integrity monitoring for assets "in-scope." Tripwire CCM's monitoring is on-demand or scheduled, and provides change deltas from prior assessment, giving trends and insight as to how the environment is maintaining compliance.
Patch Compliance Audit	Know if your critical systems have the latest security patches applied and fulfill many compliance requirements to keep systems current, patched and hardened against possible cybersecurity threats.
Audit-Ready Reporting and Dashboards	Different audiences within the organization need different views of compliance, trends and audit data; Compliance, IT Security, IT Operations, and executives all have specific information needs that can be flexibly and visually presented based on roles.
Continuous Compliance	Overall these capabilities combine to help enterprises achieve continuous compliance rather than a highly variable status as they prepare for "point-in-time" compliance, and has been shown to reduce compliance and audit readiness costs by 25–40%.

SCAP Scans

With Tripwire CCM you can easily view Security Content Automation Protocol (SCAP) scan results all in one place, produce a compliance report and confidently assure our agentless technology leaves zero trace on the systems scanned, demonstrating SCAP compliance and report results for a Continuous Diagnostics and Mitigation (CDM) program.

Supported Platforms

- RHEL 4–7
- SUSE 9.3–11
- Solaris 7–11
- VMware ESX Server 3.0–5.x
- VMware ESXi 3.5–5.x
- Fedora 7–14
- IBM AIX 4.3–6
- IBM i5 OS
- HP-UX 10.20–11
- Debian
- Cisco IOS 11–15
- Cisco ASA
- Cisco PIX
- Check Point Firewall
- Juniper Network Infrastructure
- Windows XP, 8
- Windows Server 2000–2012
- Microsoft Active Directory
- Microsoft SQL Server 2000–2012
- Oracle 9i–12c
- Apache 2
- Microsoft IIS 6–7.5
- Microsoft Office 2007
- Symantec AntiVirus
- Trend Micro AntiVirus
- McAfee Virus Scan
- PatchLink Update Agent
- Microsoft Exchange Server 2007
- MySQL 4.1–5.1
- DB2

ISO · NIST · SANS · DISA Defense Information Systems Agency, Department of Defense · NERC North American Electric Reliability Corporation · COBIT 5 An ISACA Framework · Center for Internet Security · PCI Security Standards Council · HIPAA Health Insurance Portability & Accountability Act · FISMA

tripwire®

Tripwire is a leading provider of security, compliance and IT operations solutions for enterprises, industrial organizations, 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

The State of Security: Security News, Trends and Insights at tripwire.com/blog
Follow us on Twitter @TripwireInc » **Watch us at** youtube.com/TripwireInc

TCCM517j 201610