TRIPWIRE CONFIGURATION COMPLIANCE MANAGER

CONFIGURATION AND PATCH AUDITING, FIM AND CHANGE ANALYSIS

HIGHLIGHTS

- Patch compliance auditing
- Agentless file integrity monitoring including checksum, change originator, file size, version creation date and modified date
- Sophisticated risk prioritization algorithms identify the most urgent problems
- Flexible reporting and dashboards provide compliance data to the appropriate audience

Ensuring that systems are always properly configured is critical for compliance and security initiatives. But gaining visibility into system configurations and their compliance status is a significant challenge, especially with the rapid rate of change in enterprise networks. Additionally, demonstrating to auditors that systems are compliant can be a manual, time consuming project that is inefficient and potentially ineffective.

Tripwire Configuration Compliance Manager (Tripwire CCM) automates enterprise-wide configuration auditing, patch compliance auditing, change analysis and file integrity monitoring, providing continuous visibility into the compliance of IT system configurations and the impact of changes. Its integrated policy engine compares actual configurations to internal policy or best practice benchmarks, and prioritizes the risk and compliance impact of configuration changes.

Automating configuration auditing enables a greater level of security and dramatically reduces preparation time for IT audits conducted for regulations such as PCI, Sarbanes-Oxley and HIPAA. Tripwire CCM's continuous change-centric process lowers costs and increases uptime by ensuring that systems also remain configured in compliance with organizational policies.

COMPREHENSIVE AUDIT SUPPORT

Using innovative agentless technology, Tripwire Configuration Compliance Manager continuously identifies all IP-enabled systems that are active on a network, including servers, desktops, laptops, routers, switches and firewalls. The solution then enumerates the applications and configuration of each system, providing detailed information on thousands of configuration variables. Tripwire CCM identifies and assesses virtually everything on the network, from routing table entries and access control lists to Active Directory group policy objects and application misconfigurations, all without requiring agent software on the endpoints.

Tripwire CCM continuously 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 and HIPAA.

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

patches and can proactively alert the system owners to help reduce your attack surface and harden your systems.

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.

Tripwire Configuration Compliance Manager's robust reporting capabilities and web-based dashboards provide details on the compliance of system configurations through a range of customizable reports—from technical reports designed for IT and security teams to compliance framework reports such as CobiT, SAS-70 or ISO 17799—for managerial and audit audiences. The automated reports make preparation for IT audits efficient and comprehensive while the dashboards give administrators a variety of real-time perspectives into the compliance status of every system on the network.

Tripwire CCM can also be integrated with configuration or change management processes to address any configuration compliance deviations identified. When the solution identifies out-of-compliance configurations or changes it can immediately notify administrators, open trouble tickets and update the CMDB. Additionally, issues can be prioritized based on the business value of the assets affected.

FASTER AUDIT PREPARATION THROUGH COMPLIANCE MANAGEMENT

The Tripwire CCM agentless configuration auditing solution provides four key technology breakthroughs that enable fast and effective audit preparation:

- **Agentless Architecture**—Because it does not require the installation of software agents on devices, Tripwire Configuration Compliance Manager can monitor a wide variety of systems not typically supported by some agent-based applications, including routers, switches, and firewalls. Monitoring of mobile devices can be made operational by a small team in a matter of hours. Tripwire CCM even provides file integrity monitoring without the use of agents.

- **Integrated Policy Engine and Rich Policy Library**—Tripwire CCM comes with a rich library of pre-built policies, including prescriptive policies from NIST, CIS and Microsoft and regulatory policies including PCI, SOX and HIPAA. The policy engine enables easy customization of these policies and for creating new ones. With just one click, you can even create a policy based on the configuration of a particular system (such as the "gold" image for new servers).

- **Configuration Change and Patch Audit Analysis**—Tripwire CCM not only enumerates the configuration of IT systems in detail, it identifies how these configurations are changing and whether these changes require attention—including if patches are missing. When Tripwire CCM identifies a compliance deviation, it can escalate the issue in a number of ways, including alerting administrators or opening a trouble ticket. Further, all configuration changes are recorded for audit and control purposes.

- **Open Architecture**—Tripwire Configuration Compliance Manager can operate standalone or as part of a federated CMDB, such as the HP Universal CMDB and the IBM Tivoli CCMDB. Tripwire CCM is the authoritative source of policy and compliance data for the HP Universal CMDB, and it provides the sole source of policy and compliance status into the IBM Tivoli CCMDB.