SOLUTION BRIEF

Tripwire Enterprise Integrations

Adding Rich Context to Improve Enterprise Security

Flexible, extensible frameworks provide the ability to combine Tripwire Enterprise's rich change and configuration data with a wide variety of security, compliance, operations and reporting/analytics solutions.

Tripwire industry-leading security solutions offer you visibility to your security data in ways that help you understand and improve your state of security and meet compliance demands. Tripwire® Enterprise provides system change, configuration and compliance information, while Tripwire Log Center™ provides log and security event information.

To further expand your visibility into your organization's security and compliance status, Tripwire offers mature, refined integration frameworks. With them, you can combine Tripwire Enterprise's rich change, configuration and compliance information with data from additional security solutions, like SIEMs, change management (CM) systems, change management databases (CMDBs), and governance, risk and compliance (GRC) systems.

Integration with SIEMs

By design, SIEMs focus on event capture and correlation. Once an incident impacts files at the system level, however, SIEMs lose much of their visibility. Tripwire Enterprise's integration with SIEMs lets you improve your incident detection abilities by adding valuable system configuration, change, user and business context data from Tripwire Enterprise to Tripwire Log Center, ArcSight, RSA Envision—or almost any other SIEM.

Combining these types of data constructs a more complete picture of what's happening, or what happened—in the case of forensics investigations—at the network and system level. For example, you could use the framework to help detect when critical files on a high value asset have changed and determine if those files were changed by an account that was supposedly disabled

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

or if the change was made outside of normal business hours. It can also tell you if file changes degraded compliance or security scores.

Integration with CMs

Change management (CM) systems help verify that changes made to a system were authorized and performed properly. The integration enables Tripwire Enterprise to query a CM system like Remedy, ServiceNow or CA Service Desk to verify that changes it detected were properly planned for and authorized—that is, if the right changes were made to the right system, at the right time, and by the right person.

Additionally, unexpected changes found by Tripwire Enterprise generate incident tickets in the CM system to notify the proper channels of a change management process violation or possible security event. For example, Tripwire Enterprise detects a system change that has no ticket in the CM system or finds that more changes were made than authorized on the ticket.

You can also use the integration framework to add information from the CM system to Tripwire Enterprise. Tripwire Enterprise can then use automation to distinguish between authorized and unauthorized changes, automatically promoting approved changes and flagging unauthorized changes for further investigation.

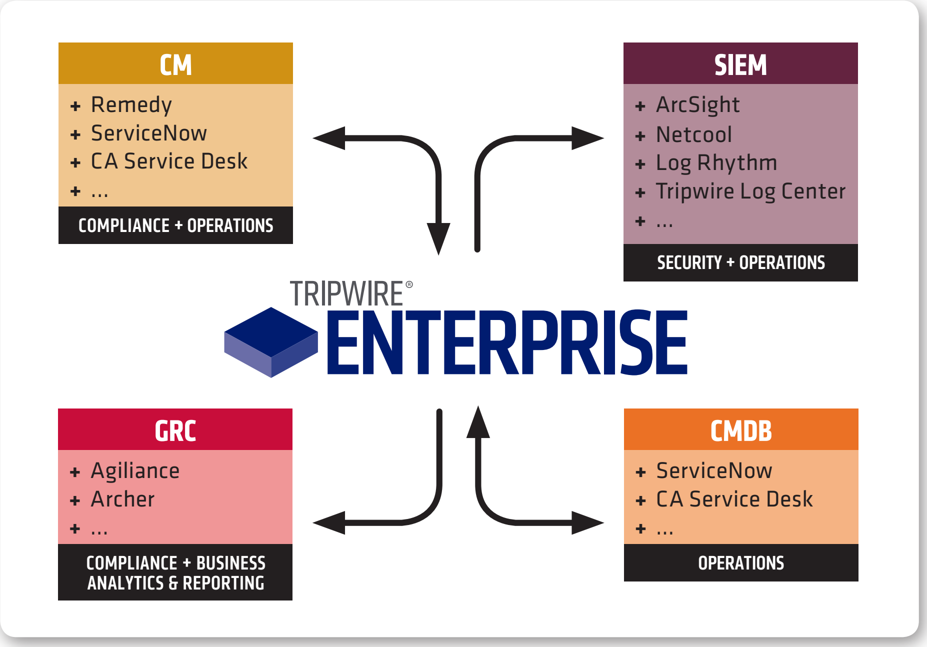

Fig. 1 Flexible, extensible frameworks provide the ability to combine Tripwire Enterprise's rich change and configuration data with a wide variety of security, compliance, operations and reporting/analytics solutions.

Integration with CMDBs

Organizations often depend on change management databases (CMDBs) as the "single source of truth" for the inventory of the systems an organization has in its infrastructure, the applications present on them, system and application owners and other associated details. While CMDBs may launch with accurate information, over time the information drifts or becomes stale, and system administrators often can't definitively state what systems they have, who owns them, what's on them, and even what data center they're in. Tripwire Enterprise's integration with CMDBs feeds and accepts change and configuration data from Tripwire Enterprise to CMDBs such as ServiceNow.

With an inaccurate CMDB, a system administrator would be hard-pressed to quickly list the applications installed on a system or the systems on which a particular application is installed. Tripwire Enterprise automatically harvests a list of every application installed on a system along with detailed system configuration information. By feeding that data into a CMDB, you could quickly produce an applications list for a system and ensure that your CMDB contains the most current information about the systems in your environment.

CMDBs typically organize and categorize assets using a structure that reflects how the business operates. The integration also lets you feed this type of CMDB information into Tripwire Enterprise and use it in the solution to automatically assign asset tags, node groupings and naming schemes. As a result, Tripwire Enterprise home pages, reports and alerts consistently represent your assets from that business perspective. Plus, when you bring new systems online, retire older systems, or update applications in the CMDB, Tripwire Enterprise reflects those changes. This helps identify situations that warrant investigation—for example, when Tripwire Enterprise detects that a retired system that should be offline is actually still recording changes.

Integration with GRC Tools

Tripwire Enterprise's integration with governance, risk and compliance (GRC) tools lets you extract high-level information from Tripwire Enterprise and feed it into GRC tools like Archer and Agiliance. That lets you keep track of important trends in security and compliance, such as whether the organization is experiencing an increase in unauthorized changes, is failing more compliance tests, or has worse or better compliance scores in some regions compared to others.

Tripwire's Professional Services Ensure Success

Tripwire delivers all the integrations through a professional services engagement. You can count on Tripwire's experienced consultants to assess your needs, effectively implement the appropriate framework, and help you gain a more complete picture of your organization's IT security and compliance status.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **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

©2019 Tripwire, Inc. Tripwire, Log Center/LogCenter, IP360 and Tripwire Axon are trademarks or registered trademarks of Tripwire, Inc. All other product and company names are property of their respective owners. All rights reserved.