TRIPWIRE® ENTERPRISE

# TRIPWIRE ENTERPRISE 8.5 DETECT. RESPOND. PREVENT.

◆ Tripwire has nearly two decades of experience in the security and compliance industry, with foundational technology essential for detecting cyber threats, rapid and real-time response, and prevention against future attacks. Tripwire Enterprise has kept over half of the Fortune 500 and many of the most sensitive networks in the world secure and compliant, with its capabilities fulfilling many security and policy compliance requirements. ◆

Tripwire® Enterprise is a security configuration management (SCM) suite that provides fully integrated solutions for policy, file integrity and remediation management. Organizations can use these solutions together for a full, end-to-end SCM solution, or use its file integrity monitoring or policy management solutions on their own to address today's pressing security and compliance challenges, while building a foundation that positions them to address tomorrow's. The suite lets IT security, compliance, and IT operations teams rapidly achieve a foundational level of security throughout their IT infrastructure by reducing the attack surface, increasing system integrity and delivering continuous compliance. Plus, because Tripwire Enterprise integrates with enterprise applications to automate workflow with additional security point solutions like SIEMs and change management tools, organizations can broaden their security worldview and gain even greater efficiencies.

A key IT enterprise security and compliance solution, Tripwire Enterprise supports a *detect, respond and prevent* strategy by:

- **Detection** of cyber threats and possible breach activity by highlighting possible indicators of compromise
- **Response** to deviations with high value, low volume alerts with guidance on what to do to return the system to a known secure state
- **Prevention** through adapting and prioritizing threats and change deviations to maintain a consistently hardened and objective view of overall security posture across all devices and systems

## HOW IT WORKS: TIGHTLY INTEGRATED CONTROLS

Tripwire Enterprise delivers four integrated capabilities that work in concert to create an enterprise-class SCM solution:

- **Tripwire File Integrity Manager (FIM)** is the world's first and best file integrity monitoring solution. It checks across large heterogeneous environments to provide threat detection and instant insight into configuration vulnerabilities while increasing operational efficiency by reducing configuration drift and unauthorized change. Tripwire's FIM can be used stand-alone to provide granular endpoint intelligence with rapid insight to security and compliance posture. If used in conjunction with Tripwire Policy Manager, it delivers change-triggered configuration assessment and other system configurable responses. This turns a "passive" configuration assessment into a dynamic, continuous, and real-time defensive solution that immediately detects deviations from expected, secure configuration standards and hardening guidelines.

- **Tripwire Policy Manager** establishes and maintains consistent compliance agent-based and agentless continuous configuration assessment against over 650+ combinations of platforms and security and compliance policies, standards, regulations and vendor guidelines. The Policy Manager also offers complete policy customization, waiver and exception management, automated remediation options, and prioritized policy scoring with thresholds, weights and severities. It does all this while providing auditors with evidence of compliance and making policy status highly visible and actionable for compliance teams.
- **Remediation Manager,** a value-add component of Tripwire Policy Manager, provides built-in guidance to IT security and compliance teams to repair drifted, misaligned security configurations while retaining role-based management, approvals and sign-offs for repairs. This helps operations teams more easily and efficiently know what failed and how to return systems into a production-ready state—and once they're in production, keep them there.
- **Investigation and Root Cause Drill-down** capabilities give IT Security and Operations teams the ability to rapidly and effectively investigate to determine root causes. Systems inevitably change as enterprises constantly revise and change their people, processes and technologies. Tripwire Enterprise can deliver granular drill-down, side-by-side comparisons, historic baselines and comparisons to quickly provide investigative teams what they need to know: what changed, when, by whom and how often, with "how" information.
- **Tripwire Axon™ Platform** enables flexible data collection and resilient communication across a broad range of devices, cloud and virtualized assets. The Tripwire Axon platform addresses collection challenges by utilizing an extensible and resource-efficient agent, asynchronous messaging techniques, and product- and platform-neutral message definitions. The Tripwire Axon Agent and its plugins are designed to operate efficiently, optimized for minimal overall system resource utilization and network bandwidth. The entire set of agent binaries is implemented in C++ to minimize footprint and maximize performance for their specific data collection objectives.

## INDUSTRY-LEADING IT SECURITY AND COMPLIANCE CAPABILITIES

As part of an industry-leading security platform, Tripwire Enterprise can leverage these components to meet key IT security and compliance needs.

- **Tripwire Search by Hash API** provides API commands within the Tripwire Enterprise Data API. This command set API will let IT teams test systems being monitored by Tripwire Enterprise for bad file hash values in an automated way, using scripts or programs to leverage the Search by Hash API commands, and use large lists to search large numbers of assets.
- **Point-of-Sale (POS) Threat Content** is now available to protect Windows and Windows Embedded OS. These systems are especially vulnerable to digital tampering, malicious insiders, and RAM scraping, and once breached, privilege escalation and data exfiltration. Tripwire has released specialized content with tests for many of the most common attack changes that occur on POS.
- **Tripwire Asset View** helps organizations manage their Tripwire-monitored assets through their unique business lens by assigning tags that can reflect risk, priority, relevance and organizational alignment. Now Tripwire Enterprise can provision assets with pre-assigned asset tag files, shortening the time it takes to provision and have assets up, labeled and functioning. And now, Tripwire IP360 vulnerability assessments can deliver risk-prioritized asset tags to Tripwire Enterprise for increased risk visibility and remediation.
- **Tripwire Connect** is a new product from Tripwire that integrates with Tripwire Enterprise to deliver advanced, customizable— yet easy-to-use—reporting.

◆ Tripwire has taken its original host-based intrusion detection system, which could simply detect changes to files and folders, and expanded it into a robust file integrity monitoring (FIM) solution, able to monitor detailed system integrity: files, directories, registries, configuration parameters, DLLs, ports, services, protocols, etc. And enterprise integrations provide granular endpoint intelligence that supports threat detection and policy and audit compliance. Years have been spent honing Tripwire's ability to detect and judge change with policy and security risk prioritization and integration refinements to achieve high value, low volume change alerts. Tripwire Enterprise helps the largest enterprises manage system configuration integrity, security and compliance. ◆

## ENTERPRISE SUPPORT

Tripwire Enterprise can operate with agents or agentlessly, and supports:

- All major OSes: Windows, Red Hat, SUSE, Solaris, MacOS, Debian, CentOS, etc.
- Many vendor-specific OSes: AIX, HP-UX, etc.
- Directory Services: Active Directory, LDAP, etc.
- Network Devices: Firewall, IPS and IDS configurations, routers, etc.
- Databases: Oracle, MS SQL, DB2, etc.

## READY TO DIG DEEPER?

**To learn more about Tripwire Enterprise capabilities, reports, available policies, platform support and more, click on or visit tripwire.com for the following datasheets:**

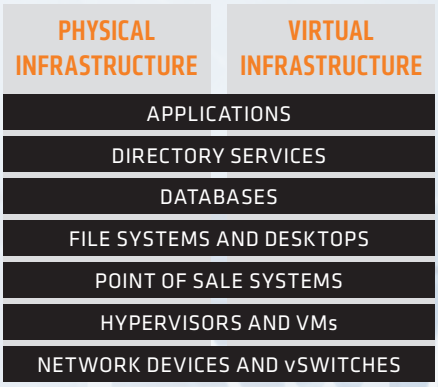
- Tripwire Enterprise Report Catalog
- Tripwire File Integrity Manager
- Tripwire Policy Manager
- Tripwire Connect
- Tripwire Remediation Manager
- Tripwire Enterprise Platform Support
- Tripwire Axon
- Tripwire Axon Platform Support

## FEATURES AND BENEFITS

| | |
|---|---|
| **Updated data collection and communication platform; Tripwire Axon** | Tripwire Enterprise delivers best-in-class security, integrity monitoring, and configuration & compliance management with a pluggable, extensible, and high-performance endpoint data collection & communication platform; Tripwire Axon. Tripwire customers' benefit from unparalleled visibility and cyber-resilience while reducing operational burden and improving responsiveness. |
| **Increased threat detection for changes that indicate threats or breach activity.** | Tripwire Enterprise has a number of threat detection and response capabilities, with a new Search by Hash API, Point-of-Sale (POS) device protection, and integrated threat intelligence services in addition to our own integration for adaptive threat intelligence from Tripwire IP360. |
| **Single point of control for all IT configurations** | Tripwire Enterprise provides centralized control of configurations across the entire physical and virtual IT infrastructure, including servers and devices, applications, and multiple platforms and operating systems. |
| **Advanced Integration through Rest APIs** | Updated Rest APIs allow Tripwire Enterprise value to be integrated with other applications. Rest APIs enable programmatic command and control of applications such as Tripwire Enterprise and also extraction of information collected. Administration APIs allow automation of tasks like enable real time monitoring, or run policies. |
| **Robust Asset View capabilities** | Asset View lets you classify assets with business-relevant tags such as risk, priority, geographic location, regulatory policies, and more. Tripwire Enterprise's asset view capabilities now offer provisioning with an asset tag file, increased scale for large numbers of assets, and imported asset tagging from integration with Tripwire IP360, giving a sharper view of risk across the entire organization. |
| **Workflow tools for managing failed configurations** | The Remediation Manager module provides role-based workflow tools that let users approve, deny, defer or execute remediation of failed configurations. |
| **Integration with change management systems** | Because Tripwire Enterprise integrates with leading Change Management System (CMS) solutions, as change happens Tripwire Enterprise automatically reconciles detected changes against change tickets and change requests. |
| **Faster, easier audit preparation** | Tripwire Enterprise dramatically reduces the time and effort for audit preparation by providing continuous, comprehensive IT infrastructure baselines along with real-time change detection and built-in intelligence to determine the impact of change. |
| **Support for maintaining a secure, compliant state** | Tripwire Enterprise combines configuration assessment with real-time file integrity monitoring (FIM) to detect, analyze and report on changes as they happen and keep configurations continually compliant. This immediate access to change information lets IT fix issues before they result in a major data breach, audit finding or long-term outage. |
| **Automated IT compliance processes** | Tripwire Enterprise automates compliance with the industry regulations and standards organizations are now subject to—from PCI, to NERC, SOX, FISMA, DISA and many others. |

# BROAD, DEEP SUPPORT FOR COMPONENTS IN THE IT STACK

**Whether IT needs to keep watch over mission-critical servers or the entire IT infrastructure—including virtualized environments and applications—Tripwire Enterprise provides the capability to assess, validate and enforce policies and detect all change, no matter the source. Tripwire supports the following components in the IT stack:**




| | |
|---|---|
| **Tripwire Enterprise for Applications** | Tripwire Enterprise for Applications provides compliance policy management and file integrity monitoring capabilities to help ensure that supported applications are configured properly for security, compliance and optimal performance and availability. |
| **Tripwire Enterprise for Directory Services** | Tripwire Enterprise for Directory Services provides independent compliance policy management for LDAP-compliant directory server objects and attributes, such as LDAP schema, password settings, user permissions, network resources, group updates and security policies. |
| **Tripwire Enterprise for Databases** | Tripwire Enterprise for Databases works in conjunction with Tripwire's File Systems component to help organizations get their Oracle, Microsoft and IBM database servers into secure, continually high-performing states. |
| **Tripwire Enterprise for File Systems and Desktops** | Tripwire Enterprise for File Systems and Desktops assesses the configurations of physical and virtual server and desktop file systems, including security settings, configuration parameters and permissions. |
| **Tripwire Enterprise for Point-of-Sale (POS) Devices** | Tripwire Enterprise secures POS devices against cyber threats, manages security and compliance policies for these devices, and provides IT Operations with alerts, notifications and response guidance when possible breach indicators or "indicators of compromise" are suspected to exist on these devices. |
| **Tripwire Enterprise for Virtualized Environments** | Tripwire Enterprise works in virtualized environments—private, public and hybrid clouds. The Tripwire Enterprise Console can operate as a virtual machine, and its agents can monitor any supported virtualized endpoint. This includes delivering protection for cyber threats in virtualized/cloud environments, system integrity monitoring, application of security and compliance policies, dashboards, reporting and real-time alerts and notifications. |
| **Tripwire Enterprise for VMware** | Tripwire Enterprise for VMware provides visibility across the VMware virtual infrastructure, enabling continuous configuration control of virtual environments. |
| **Tripwire Enterprise for Network Devices** | Tripwire Enterprise for Network Devices assesses configuration settings of the broadest range of network devices in the industry, including any device running a POSIX-compliant operating system. |

tripwire®

◆ 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**



TEPB850a 201608