Tripwire Enterprise 8.8

Detect. Respond. Prevent.

Tripwire has over two decades of experience in the security and compliance industry, with foundational technology essential for detection and rapid, real-time response to cyber threats, and protection 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 of the most essential and recommended 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 complete 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 security, compliance and operations teams rapidly achieve a foundational level of security across your entire enterprise, including on-premise, cloud and industrial assets, 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.

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

- **Detecting** cyber threats and possible breach activity by highlighting possible indicators of compromise
- **Responding** to deviations with high value/low volume alerts, along with guidance on what to do to return the system to a known secure state
- **Prevention** through adapting and prioritizing threats and change deviations in order 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 features and capabilities that work in concert to create an enterprise-class SCM solution:

- **Tripwire File Integrity Manager** is the world's first and best file integrity monitoring (FIM) 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. When used 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 1000 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** works alongside Tripwire Policy Manager to provide 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 quickly and effectively determine root causes. Systems inevitably change as enterprises constantly revise and change their people, processes and technologies. Tripwire Enterprise delivers 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, along with "how" information.

Industry-leading Security and Compliance Capabilities

Tripwire is continuously adding new capabilities to Tripwire Enterprise to meet evolving security and compliance challenges. Tripwire Enterprise now has new capabilities to monitor cloud assets, protect industrial devices, and, using the MITRE ATT&CK framework, discover evidence of adversarial behavior in your environment.

» **Cloud Management Assessor** The primary cause of security incidents with public cloud services is caused by configuration errors. Tripwire's Cloud Management Assessor monitors for changes to Amazon Web Services, Microsoft Azure and Google Cloud Platform configurations, as well as SaaS account configurations such as Salesforce, and alerts you to unauthorized or unexpected changes. Cloud Management Assessor also can evaluate if your public cloud management account is securely configured, based on best practices (e.g. the Center for Internet Security AWS Foundations v1.1.0 Benchmark).

Storing files in cloud file storage services such as AWS S3 Buckets or Azure Storage can be risky because a simple configuration change can result in sensitive data being exposed publicly. Cloud Management Assessor will alert you when permissions or other file attributes change, enabling you to take immediate corrective action.

» **Tripwire Connect** Tripwire Connect enables CISOs and security and compliance teams to connect their enterprise security details with their business context while answering: What is our current security posture? How is it trending? Can we achieve our corporate objectives for risk reduction? With Tripwire Connect you can visualize your security and risk trends across your enterprise—whether it's the entire organization or within business units or single departments. Tripwire Connect empowers CISOs and IT security directors with actionable reporting of their IT infrastructure to reduce the cyber threat attack surface, assuring system integrity and delivering continuous compliance.

» **MITRE ATT&CK Framework** Developed by the MITRE corporation, the ATT&CK framework is a useful cybersecurity model illustrating how adversaries behave and details the tactics you should use to mitigate risk and improve security. Using ATT&CK policy content for Tripwire Enterprise, you can detect and report on adversarial behavior in your environment—adding a new layer of defense to your security strategy.

Tripwire has taken its original host-based intrusion detection tool, 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. Additional enterprise integrations provide granular endpoint intelligence that supports threat detection and policy and audit compliance. Years have been spent honing Tripwire Enterprise's ability to detect and judge change with policy and security risk prioritization and integration refinements to achieve high value/low volume change alerts—helping even 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, CentOS, Ubuntu, SUSE and Debian
- **Many vendor-specific OSes:** AIX, Solaris, HP-UX, etc.
- **Directory Services:** Active Directory, LDAP, etc.
- **Network Devices:** Firewall, IPS and IDS configurations, routers, etc.
- **Databases:** Oracle, MS SQL, DB2 and PostgreSQL
- **Industrial Devices:** Data acquisition controllers, human-machine interfaces (HMIs), programmable logic controllers (PLCs), relays, remote terminal units (RTUs), etc.

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 cloud and virtualized environments, applications and industrial devices—Tripwire Enterprise provides the capability to assess, validate and enforce policies and detect all change, no matter the source.

Tripwire Enterprise Supports the Entire Service Stack

Applications	Tripwire Enterprise 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.
Directory Services	Tripwire Enterprise 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.
Databases	Tripwire Enterprise 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.
File Systems and Desktops	Tripwire Enterprise assesses the configurations of physical and virtual server and desktop file systems, including security settings, configuration parameters and permissions.
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.
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.
VMware	Tripwire Enterprise provides visibility across the VMware virtual infrastructure, enabling continuous configuration control of virtual environments.
Network Devices	Tripwire Enterprise assesses configuration settings of the broadest range of network devices in the industry, including any device running a POSIX-compliant operating system.
Industrial Devices	Tripwire Enterprise supports monitoring industrial devices via a variety of protocols, including Modbus TCP, Ethernet/IP CIP and SNMP. In addition, agentless scanning of industrial systems running Windows or Linux is supported. For devices that cannot be scanned directly, configuration information can be collected through integrations with Rockwell Automation FactoryTalk AssetCentre, MDT AutoSave and Kepware KEPServerEX. Configuration data can also be collected using the Web Retriever, which can scrape configuration data from web pages.

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 Enterprise Policy Manager
- Tripwire Enterprise Remediation Manager
- Tripwire Enterprise Platform Support
- Tripwire Connect
- Tripwire Enterprise for Industrial Devices

Tripwire Enterprise Features and Benefits

Updated data collection and communication platform	Tripwire Enterprise delivers best-in-class security, integrity monitoring, and configuration and compliance management with Tripwire Axon, a pluggable, extensible and high-performance endpoint data collection and communication platform. Users benefit from unparalleled visibility and cyber-resilience while reducing operational burdens and improving responsiveness.
Support for hybrid environments	Tripwire Enterprise can monitor both on-premise and cloud environments for security and compliance. Customers can reduce costs and provide better visibility by using a single solution for both environments.
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 collected information. Administration APIs allow automation of tasks like enable real time monitoring, or run policies.
OT network monitoring	Using the Tripwire Data Collector with Tripwire Enterprise, users can monitor their industrial network for change and compliance, resulting in a more secure environment without compromising availability.
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.

tripwire®

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*: Security news, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

TEDS88a 1907