FORTRA®

DATASHEET

Tripwire

Take control of your digital environment and detect cyber threats in real time

Security, compliance, and IT operations leaders need a powerful and effective way to accurately identify security misconfigurations and indicators of compromise. Tripwire® is the leading integrity and compliance monitoring solution, using file integrity monitoring (FIM) and security configuration management (SCM). Backed by decades of experience, it's capable of advanced use cases unmatched by other solutions.

This fully integrated suite of solutions for policy compliance, system integrity, and remediation management reaches far beyond simple compliance. It enables teams to rapidly achieve an increased level of security across the entire enterprise, including on-premises, cloud, and industrial assets.

How It Works

Tripwire delivers four core capabilities in a single interface that work in concert as an enterprise-class security and compliance solution:

- **System Integrity Monitoring** scans across large heterogeneous environments to detect threats and provides an instant view into configuration vulnerabilities — boosting ecosystem security by reducing configuration drift and unauthorized change. Tripwire File Integrity Manager is the world's first and best file integrity monitoring (FIM) solution and it can also be used stand-alone for granular endpoint intelligence. 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, delivering customized contextual information to accelerate effective response.
- **Policy Management** establishes and maintains continuous agent and agentless configuration assessment against 4,000+ combinations of platforms, security and compliance policies, standards, regulations, and vendor guidelines. Tripwire Policy Manager offers complete policy customization, waiver and exception management, automated remediation options, and prioritized policy scoring. It does all this while providing auditors with easily accessible evidence of compliance, making policy status highly visible and actionable for compliance teams.

KEY BENEFITS

- Powerful integrity monitoring and security configuration management workflow
- Unparalleled visibility into misconfigurations and suspicious changes
- Compliance monitoring backed by decades of experience
- Threat prioritization with guidance on returning a system to a secure and compliant state
- Monitoring for adherence to regulatory policy requirements (PCI, NIST, CIS, and dozens more), with delivery of auditor-friendly reporting

KEY INTEGRATIONS

- Tripwire LogCenter®
- Splunk
- ServiceNow
- Active Directory
- SAML 2.0
- Cherwell
- JIRA
- ChangeGear
- CyberArk
- Thycotic

- **Advanced Use Cases** are available thanks to the highly customizable monitoring options, real-time change detection for your most critical assets, enterprise-wide detection of emerging vulnerable files (Log4J, Spring4Shell, Text4Shell, etc.), and continual review of networking devices to meet strict hardening standards. Tripwire is unmatched in advanced monitoring use cases, fortifying your security ecosystem.
- **Remediation Management** works alongside Tripwire Policy Manager to supply built-in guidance to IT security and compliance teams to repair drifted, misaligned security configurations while retaining role-based management, approvals, and signoffs for repairs. This helps operations teams quickly understand what failed and how to return systems to a production-ready state — and once they're in production, keep them there.
- **Investigation and Root Cause Drill-down** gives IT security and operations teams the ability to quickly and efficiently determine what happened. Systems inevitably change as enterprises constantly revise and change their people, processes, and technologies. Tripwire delivers granular drill-down, and side-by-side 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, giving unparalleled visibility into the forensic details of changes to the environment.

Superior Security, Continuous Compliance

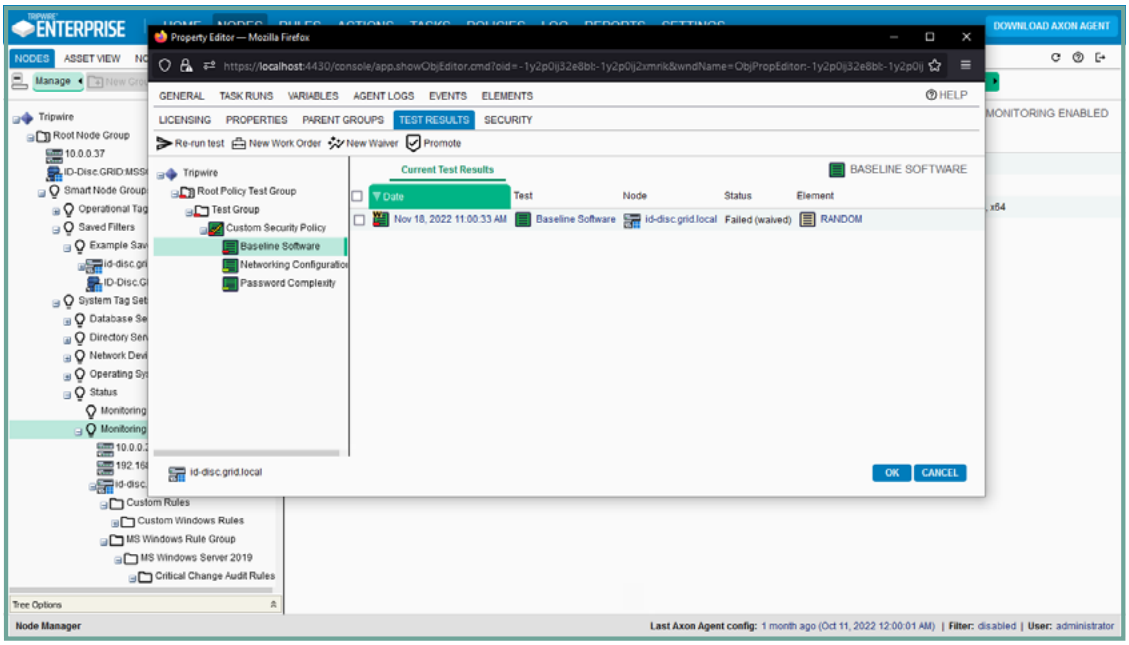
Tripwire continuously adds new capabilities to meet evolving security and compliance challenges. Tripwire now has capabilities to protect industrial devices, and, using the MITRE ATT&CK framework, discover evidence of adversarial behavior in your environment.

Reporting and Integration

Between the included audit-ready reporting, our advanced security use cases, and our integrations to leading platforms such as ServiceNow and Splunk, Tripwire enables you to efficiently connect security details with business context: Always know your current security posture (and how it's trending) to achieve corporate objectives for risk reduction. Get visibility into the security and risk trends across your enterprise — from the entire organization down to business units or single departments.

MITRE ATT&CK Framework

Developed by the MITRE corporation, the ATT&CK framework is a cybersecurity model illustrating how adversaries behave and details the tactics you should use to improve security. Using ATT&CK policy content for Tripwire, you can detect and report on adversarial behavior in your environment — adding a new layer of defense to your security strategy. And this is only one of dozens of frameworks available in our comprehensive content library.



Tripwire Difference Viewer displaying additions and changes to the approved baseline.

Key Features and Benefits

Support for Hybrid Environments

- Monitors both on-premises and cloud environments for security and compliance
- Reduces costs and gives better visibility via a single solution for both environments

Updated Data Collection and Communication

- Enables best-in-class security, integrity monitoring, and configuration and compliance management
- Event generator that leverages eBPF technology for greater stability and accuracy

Auto Onboarding/Offboarding for Cloud Assets

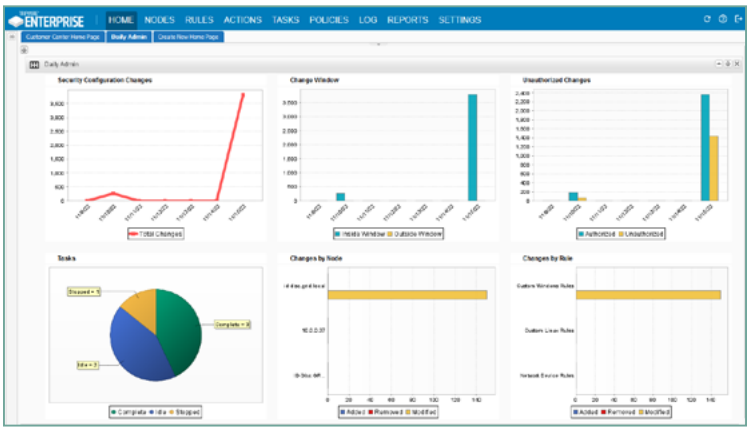
- Classifies and scans assets as soon as they are connected in dynamic environments
- Delivers immediate baseline state to monitor changes through the life of an asset even when short-lived
- Provides automatic offboarding that lets you define how long ephemeral assets data should be retained

Single Point of Control for All IT Configurations

- Supports 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

- Enables programmatic automation of Tripwire, extraction of collected information, and custom integrations with other solutions
- Allows automation of routine tasks through administration APIs, to integrate workflows with other business processes and tools



Tripwire's customizable dashboard showing Security and Change compliance.

Robust Asset Views

- Supports classification of assets with business-relevant tags, such as risk, priority, geographic location, regulatory policies, and more
- Offers provisioning with an asset tag file, increased scale for large numbers of assets, and imported asset tagging from integrations with other Tripwire products

Workflow Tools for Managing Failed Configurations

- Delivers the Remediation Manager module for role-based workflows that let users approve, deny, defer, or execute manual and automated remediation of insecure and non-compliant configurations

Integration with Change Management Systems

- Integrates with leading change management system (CMS) solutions such as ServiceNow, Cherwell, JIRA and others
- Automatically reconciles detected changes against change tickets and change requests

Support for Maintaining a Secure, Compliant State

- Automates compliance with industry regulations and standards such as PCI DSS, SOX, FISMA, DISA, NERC, and many others
- Combines security configuration assessment with real-time FIM to detect, analyze, and report on changes as they happen to keep configurations continually compliant and fix issues before they result in a major data breach, audit finding, or long-term outage

Centralized Allowlisting

- Monitors drift from known good configuration of ports, services, software, and users
- Automates compliance for key NERC CIP requirements, including CIP-007 and CIP-010
- Verifies only approved accounts exist on systems as codified in an authorized user allowlist

- Complies with Internet Protocol version 6 (IPv6) requirements for federal agencies and organizations pursuing FedRAMP

Faster, Easier Audit Preparation

- 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
- Includes reports designed with auditors in mind to ensure you can confidently supply justifications

Active Directory and SAML Integrations

- Integrations between Tripwire and Active Directory or your preferred IDP reduces administrative overhead and minimizes human error with auto-created users, groups, and roles for secure and efficient access management

Broad Support for your IT Stack

Keep watch over mission-critical servers or the entire IT infrastructure, including cloud and virtualized environments, applications, and industrial devices. Tripwire provides the capability to assess, validate, and enforce policies while detecting all changes — no matter their source.

It supports out of the box agent and agentless monitoring for:

- **Physical, Virtual, Cloud and Hybrid Environments:** Works in both physical and virtualized environments, including private, public, and hybrid clouds. The Tripwire console can operate as a virtual machine and its agents can monitor any supported virtualized or physical endpoint.
- **Network Devices:** Assesses configuration settings of the broadest range of network devices in the industry, including any device running a POSIX-compliant operating system. Monitors network devices with modern Secure Shell (SSH) ciphers. With custom connection parameters, most devices can be monitored.
- **Applications:** Compliance policy management and integrity monitoring capabilities ensure supported applications are configured properly for security, compliance, functionality, and availability.
- **Directory Services**: Includes 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:** Keeps Oracle, Microsoft, and IBM database servers and instances in a secure, continually high-performing state.
- **File Systems and Desktops:** Assesses configurations of physical and virtual server and desktop file systems, including security settings, configuration parameters, and permissions with forensic-level insight.
- **VMware:** Provides visibility across the VMware virtual infrastructure, enabling continuous configuration control of virtual environments.
- **Customizable and Flexible Device Support:** Tripwire maintains a content library with over 4,000 out-of-the-box configurations. The customizable monitoring capabilities give you the flexibility to monitor assets that are critical to your operation — even when those assets are developed in-house or custom solutions not widely available on the market.

SYSTEMS MONITORED

Major OSes: Windows, Red Hat, Oracle, AIX, SUSE, Debian, Ubuntu, Solaris, CentOS, Rocky, Amazon Linux, HP-UX

Directory Services: Active Directory, LDAP

Network Devices: Firewall, IPS and IDS, routers, SSH devices

Databases: Oracle, MS SQL, Maria DB, DB2, AWS Aurora MySQL, PostgreSQL

Virtual Infrastructure: VMware

Ready To Dig Deeper?

To learn more about Tripwire capabilities, reports, available policies, and platform support, visit fortra.com.

FORTRA

fortra.com

Copyright © Fortra, LLC and its group of companies. Fortra®, the Fortra® logos, and other identified marks are proprietary trademarks of Fortra, LLC.