FORTRA

Beyond the Basics: Tripwire Enterprise Use Cases

Introduction

Security, compliance, and IT operations leaders need a powerful and effective way to accurately identify security misconfigurations and indicators of compromise. Fortra's Tripwire® Enterprise is the leading file integrity monitoring (FIM) and security configuration management (SCM) compliance monitoring solution—and delivers security capability far beyond compliance.

If you're already familiar with Tripwire® Enterprise, you may know it as the most powerful FIM compliance solution of its kind. But there are several other key use cases you can take advantage of to maximize the efficacy of your organization's security and compliance programs.

Use this guide to explore the many ways Tripwire Enterprise can protect your organization with superior security and continuous compliance.

FIM for Compliance

Differentiate between normal versus suspicious file changes for in-scope assets when monitoring with Tripwire Enterprise. Visibility into which file changes affect your compliance equips you with the ability to act fast and return your systems to a compliant state.

As the inventors of file integrity monitory (FIM), Tripwire has had 20+ years to develop an unmatched depth and breadth of detection to help organizations:

- Identify "good" versus "bad" changes
- Speed up the audit process with a solution well-known among compliance auditors
- Cover numerous platforms, policies, standards, regulations, and vendor guidelines with a content library of more than 4,000 combinations

For Instance

A large banking institution needed to comply with PCI DSS Requirement 11 to have a change detection solution in place. Knowing our reputation as the leader in this space, they purchased Tripwire Enterprise to monitor the PCI in-scope assets. Using our broad platform coverage and the benefit of our content library to help them jumpstart quickly, they were able to realize their compliance state with minimal time and effort. Using our continuous compliance workflow within Tripwire Enterprise, management was able to receive continual progress reports as configurations were updated across the environment as they worked to improve their compliance scores. When the time came for their PCI audit, the auditor immediately recognized the Tripwire solution and had few questions about the deployment—they knew the results could be trusted to be accurate.

Learn More

Watch it in action

Explore compliance standards

FIM for Security

Since FIM is such an integral security control for compliance, there is a common misconception that it's for compliance only. In reality, the FIM powering Tripwire Enterprise supports advanced security use cases—and advanced security—as well. Customize what you monitor to include environment-specific software and devices outside the standard platform set (e.g., threats inside the data center, not just protecting the perimeter). And this data can be integrated with other solutions such as Splunk and ServiceNow for aggregation and a complete picture of your security status.

Tripwire Enterprise helps:

- Gain extensive additional visibility across your ecosystem, including change over time
- Reduce mean-time-to-repair (MTTR) with advanced forensic analysis
- Protect against the reputational and financial risk posed by breaches or outages

For Instance

An insurance company has web servers to host a customer portal, accept payments, and access account information. Interested in protecting these systems from activity that could impact the security and integrity of the portal, they purchased Tripwire Enterprise to monitor for unauthorized changes to the web server application, payment card processing application, and the customer information database. They set up Tripwire Enterprise to collect forensic information to enable their security team to protect customer data, the integrity of their payment processing application, and to respond to security issues in real-time. Since they had a mature change control and approval process in place for these critical systems, they implemented an integration with their ServiceNow system to correlate detected activity in Tripwire Enterprise with approved change tickets. When changes are detected that do not have a corresponding ticket, an Incident ticket is created, assigned to the SOC team for immediate review, and a playbook was written to ensure appropriate business response to any unauthorized activity on these systems.

Learn More

[FIM for comprehensive integrity management]

[Supported platforms]

Policy Monitoring for Compliance

Tripwire Enterprise combines two essential security controls: FIM and security configuration management (SCM). This combination eases the burden on organizations to prove their systems are compliant with regulatory compliance frameworks via audit-ready reporting. With unmatched breadth and depth in terms of compliance framework coverage, you can align your systems with multiple standards simultaneously without time-consuming manual effort. The SCM workflow leverages pre-defined policy content and simplifies waivers and remediation processes.

Tripwire Enterprise:

- Keeps policy content automatically up to date
- Gives clear remediation advice or automates remediation workflows
- Monitors open ports and services as well as installed software
- Enables comprehensive multi-regulatory compliance

For Instance

A financial institution processing transactions for their customers across many industries is required to keep servers compliant with the same regulations that their customers adhere to. Due to the nature of their industry mix, this financial institution needed to ensure compliance with PCI, SOX, and even HIPAA standards on their own servers. When identifying solutions, Tripwire stood out with the most comprehensive selection of policy coverage. They purchased Tripwire Enterprise to collect information and provide reports for their internal audit and GRC team showing the compliance state of servers to all relevant regulations within the same powerful tool. When the need arose to satisfy requests during customers' audits, this institution would run more narrowly scoped reports in Tripwire Enterprise to provide compliance proof to the specific standards needed. The rest of the time, Tripwire's reporting was used to provide the broad level compliance data to the audit and GRC teams for their own compliance proof.

Learn More

Read a case study

Explore Tripwire compliance capabilities

Policy Monitoring for Security

In addition to regulatory compliance, policy monitoring is crucial for security in organizations, especially those with internal audit, compliance, or GRC (Governance, Risk, Compliance) teams—after all, the reason regulatory compliance mandates exist is to set a required standard or baseline for best-practice security in order to protect sensitive data. Along with standards like PCI DSS (Payment Card Industry Data Security Standard), Tripwire Enterprise also offers policy content for unenforced security frameworks such as the Center for Internet Security's CIS Controls and the MITRE ATT&CK framework to tighten security.

With Tripwire Enterprise you can:

- Create your own customized internal policy content supporting additional high priority security frameworks
- Use configuration management database (CMDB) and IT service management (ITSM) ticketing integrations
- Increase your security efficacy, and reduce risk of a breach or service outage

For Instance

A regional retail bank with a small IT team outsources the configuration of networking infrastructure for the hundreds of branches and ATMs within their business. When they started noticing inconsistencies in configuration among the networking devices, they wanted more visibility into the changes made by their outside vendor, so they purchased Tripwire Enterprise to help monitor the configuration of these devices. Once they saw that the vendor was inconsistently applying their security standards, they set up a custom policy within Tripwire Enterprise to enforce their specific hardening standards in network configuration. Then they used reporting to highlight security gaps caused by the outside vendor when devices were being reconfigured monthly. Thereby, they hardened their security posture despite changes beyond their immediate control. The Policy Manager in Tripwire Enterprise allowed for continuous comparison to their hardening standards with every daily scan of the devices that was configured. This let them know of security issues with a reasonable delay as defined by their risk tolerance.

Learn More

Policy customization executive brief
CIS Controls executive guide

Advanced Monitoring

Use Tripwire Enterprise as a powerful search tool within the IT environment to find where files do (or do not) exist on each machine. The flexibility of its monitoring capabilities allows you to collect important data quickly, which is especially valuable in the presence of a major new security vulnerability (e.g., Log4j), malware, or indicators of compromise, enabling a rapid search of all monitored assets down to the specific file level. Also, this capability can easily validate configurations across sets of machines to make sure they've been updated correctly when closing out a change ticket during a deployment window.

Tripwire Enterprise allows you to:

- Specify any file name and find all instances of that file on assets with the agent installed
- Deploy a script in any programming language with COCR (Command Output Capture Rules) to greatly expand the monitoring options for less accessible devices
- Assess exposure to potential vulnerabilities—even before a fix has been released (e.g., Log4j)

For Instance

When a new critical security vulnerability was publicly announced (caliber of Log4j, Spring4Shell, etc.), a government agency used the coverage of Tripwire Enterprise across their environment to quickly scan for files related to the vulnerability. The easily customizable rules and results filtering allowed them to identify all areas of exposure in less than an hour after disclosure. They then produced a report showing all the affected servers in their environment for leadership—days before their vulnerability management vendor had published new scanning updates to even detect the same vulnerability.

Learn More

Best practices for ransomware prevention and detection

Watch Tripwire Enterprise overview

Advanced Control

The Tripwire Axon® agent used with Tripwire Enterprise is a powerful endpoint data collection agent, that allows you to execute arbitrary commands or scripts on the assets monitored by Tripwire Enterprise—meaning it's possible to operationalize ad-hoc sysadmin functionality. For example, if a server needs to be restarted, a configuration updated, or even restart of the service of another tool that is failing to respond, Tripwire Enterprise can assist. This broadly applicable, highly extensible capability saves admin teams a significant amount of time when trying to perform an ad hoc set of commands on several remote machines.

Tripwire Enterprise can help:

- Update configurations on thousands of servers and reboot them as needed
- Create an ad hoc script to be deployed, run, and reported upon
- Manage complex and varied IT infrastructure with flexibility

For Instance

An insurance company with datacenters across the globe had purchased Tripwire Enterprise to ensure compliance with their industry regulations. When the endpoint monitoring team kept detecting failures of other security software agents to check in, the team used Tripwire Enterprise to establish a custom policy to identify when the other tools' agents were out of sync. They set up an automated remediation workflow so the Tripwire Axon agent could send a command to restart the other vendor's agent. This workflow enabled the endpoint team to maintain the functionality of all their security tools without having hours of delays and incident tickets with multiple sysadmin teams.

Learn More

See it in action

Download the Tripwire Enterprise datasheet

Talk to an Expert

Contact one of our security and compliance experts. We look forward to learning about your specific needs and answering any questions you have about taking advantage of these Tripwire Enterprise use cases to overcome your biggest security and compliance challenges.

CONTACT US

FORTRA

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.