Beyond FIM:

10 More Tripwire Capabilities to Give Your Cybersecurity Program the Edge

Introduction

Tripwire is best known for being the originator of file integrity monitoring (FIM), the security control based on the idea that every cybersecurity breach and compliance misconfiguration, at its core, begins with a single thing: change. FIM is the process of detecting system changes and alerting on those that present an increased security risk. It works hand in hand with security configuration management (SCM), which identifies misconfigurations by establishing and monitoring trusted system baselines.

FIM and SCM are the fundamental features of Tripwire's best-known solution, Tripwire Enterprise. But over the course of our 20+ year history, we've expanded our portfolio to provide much more. You can now look to Tripwire for cloud account configuration security, vulnerability management (VM), industrial visibility, and managed services—alongside sophisticated solutions for many other essential security and compliance needs.

This guide presents 10 additional Tripwire capabilities that you may not be aware of. Both individually and combined, they're a powerful and effective means for improving the security posture throughout your organization—from the shop floor to the top floor, from on-prem to the cloud, and throughout blended IT/OT environments.

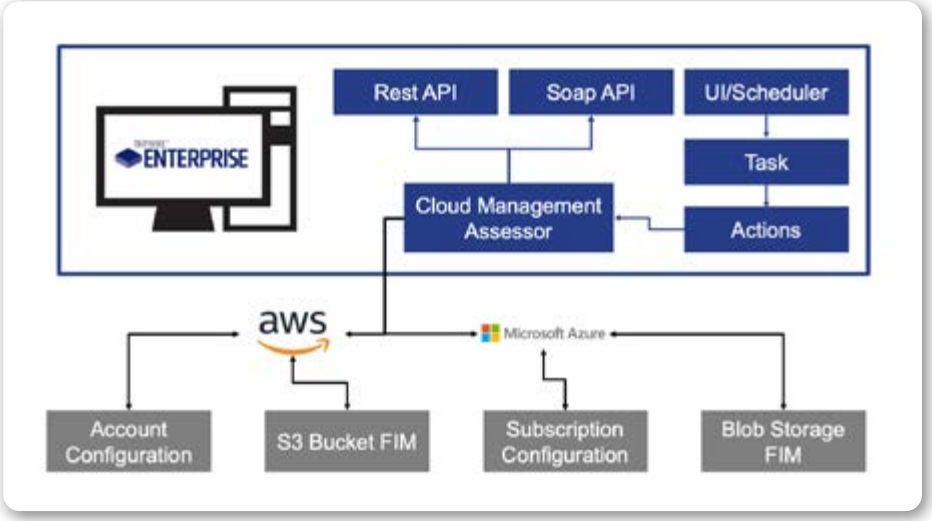
1. Cloud Infrastructure Monitoring

TRIPWIRE® CONFIGURATION MANAGER

Attackers use automated tools to find misconfigured Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) accounts and storage, including AWS S3 buckets and Azure/GCP Blobs. Deploy your own automated monitoring to detect—and even automatically correct—misconfigurations before attackers gain an opening with Tripwire® Configuration Manager, which corrects human error and indicators of compromise automatically.

Tripwire Configuration Manager provides periodic assessment of security settings compared with industry standards, specifically the Center for Internet Security (CIS) Foundations Benchmarks. You are immediately alerted to non-compliant settings that could be exposing your company. This stand-alone SaaS solution does not require a separate installation of Tripwire Enterprise.

Tripwire Cloud Management Assessor is another cloud and multi-cloud solution delivered as an add-on to Tripwire Enterprise that extends your traditional on-premises SCM controls to your public cloud infrastructure.



2. Available from Amazon and Azure Marketplaces

Tripwire joined the global partner program for AWS. As a new Advanced Technology Partner of the AWS Partner Network (APN), Tripwire's primary VM solution, Tripwire IP360™, available on the AWS Marketplace. You can find it on the Microsoft Azure marketplace as well. Tripwire IP360 is an enterprise-class vulnerability and risk management solution that enables cost-effective reduction of cyberthreat risk by focusing remediation efforts on the highest risks and most critical assets. The solution is built upon a scalable architecture that delivers risk-based vulnerability assessment across modern hybrid infrastructure—including data centers, private clouds, and public clouds—with support for container environments and DevOps toolchains.

Hosting Tripwire solutions on the AWS and Azure platforms speeds the delivery and implementation of your cybersecurity solutions.

3. Cloud-hosted Managed Services for IT Security and Federal Government

Managed services are a cost-effective and high-impact way to strengthen your cybersecurity program when resources and personnel are spread thin. Tripwire ExpertOps℠ provides a cloud-based managed services model of Tripwire's SCM and VM solutions. A single subscription includes personalized consulting from trained experts and hands-on tool management to help you achieve and maintain compliance and critical asset security. It provides stretched IT teams an alternative to the difficult process of purchasing, deploying, and maintaining products.

Tripwire ExpertOps enables organizations to quickly achieve and maintain cyber integrity across large heterogeneous environments instead of sinking time and resources into training and administering another tool. Stay aligned with frequently-changing compliance regulations with a comprehensive library of policy and platform combination tests—all while providing auditors with evidence of compliance and highly visible and actionable policy status for security. Tripwire ExpertOps Federal provides a FedRAMP-certified cloud-based managed services model that includes the industry's best FIM and SCM.

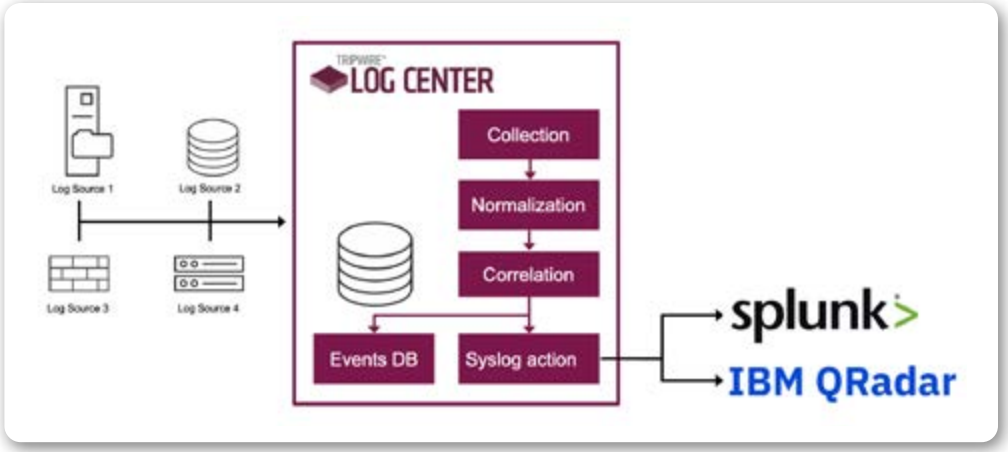
Your security team can perform at a much higher capacity thanks to ongoing support, guidance, and customized reporting that adapts to meet organizational objectives. Your designated Tripwire expert will serve as an extension of your team—no recruiting or training required. You'll receive prioritization of your team's work efforts and present progress to key stakeholders within your organization.

5. Filter Log Events Into a SIEM or Analytics Tool

Organizations now have the ability to visualize the current security status of their IT environments by adding Tripwire's deep configuration and change data with IT information stored in Splunk Enterprise. Adding Tripwire data to Splunk analytics helps identify the highest-priority threats. The Tripwire Enterprise App for Splunk Enterprise pulls in data from Tripwire Enterprise and offers built-in dashboards, reports, and fast access to critical system and application data through workflow actions. And integrating Tripwire IP360 with Splunk Enterprise enables visualization into vulnerability risk data.

Security teams collect large quantities of data for security intelligence, but gaining valuable insights from this data can be very challenging given the volume, velocity and variety of that data. The challenge is getting high-quality information with the necessary business context to make good decisions in time. The Tripwire Enterprise App for Splunk Enterprise pulls in data from Tripwire Enterprise, uniting two of your most important workflow tools into one intuitive display.

In addition, Tripwire Log Center™ can take the data you would normally send to Splunk and first filter and correlate the data then forward only events of interest, which cuts down on Splunk usage costs.



6. Scan Docker Containers for Vulnerabilities

Containers (lightweight self-contained virtual images designed to execute specific tasks or applications repeatedly and reliably), are often switched from non-running to running and back, according to need. It's important to scan containers for vulnerabilities no matter what state they are in—and to do so regularly—because they can be updated often, even in production.

If you use Tripwire IP360 for vulnerability management with granular risk scoring and prioritization, you can extend its capabilities into the cloud and discover Docker servers. Tripwire IP360 enumerates Docker containers (both running and non-running) and scans them for vulnerabilities.

This expansion builds upon Tripwire's existing ability to scan running containers. This release provides security teams with unprecedented visibility into DevOps processes. Tripwire IP360 allows you to scan online, offline, and non-running containers for vulnerabilities, giving you an enhanced overall view and lowering the chance that vulnerabilities will slip through the cracks during the development stage and into production.

7. Help You Pass Your Next Compliance Audit

In addition to hardening your attack surface against intrusion, the SCM that powers Tripwire Enterprise also helps auditors track compliance improvements over time. When it comes time to supply your auditor with documentation, you can pull reports from any point in time to demonstrate your configurations' alignment with various compliance standards. Tripwire has the largest and broadest library of supported policies and platforms, with over 2000 policies covering the widest range of platform OS versions and devices on the market.

Configuration security is so crucial that almost all industry standards and regulations incorporate some version of an SCM mandate for specifying how configurations should be set up. SCM tools help you substantially reduce the time it takes to prepare for an audit, and speed up the actual audit process as well.

Security configuration management is also about helping you continuously maintain a compliant system state post-audit. It's not enough to know that you were aligned with your compliance mandates under the scrutiny of an auditor. The goal should be having the ability to know your exact compliance level at any point in time—audit or not. Whether you need to pass SOX, HIPAA, PCI-DSS, NERC (or many others) audit, Tripwire can make part of the process nearly painless.

8. Discover Assets on Your Network

Tripwire Asset Discovery Appliance discovers all networked hosts, applications and services. By providing a comprehensive view of devices and software on your network, you gain the foundation for effective security configuration management and compliance processes. Only this appliance provides low bandwidth, non-intrusive host and network profiling for use with Tripwire Enterprise.

Tripwire Asset Discovery Appliance can identify applications that are active on your network to help discover and inventory software and services that increase security risk, or are prohibited by policy and compliance requirements. It can also identify which ports are open on your network assets, helping you identify which services are (or are not) running on your network.

Key features of the Tripwire Asset Discovery Appliance includes:

» Comprehensive, continuous discovery and profiling of all network assets and applications

» Complete inventory of authorized and unauthorized devices and applications

» Correlation of at-risk application and asset changes in Tripwire Enterprise for proactive security

9. Secure the OT Side of Your Organization

Tripwire turns raw ICS data into actionable information. Our holistic tools span the IT/OT (operational technology) landscape, and our large ecosystem of technology integrations and vendor-agnostic solutions give ICS operators plenty of freedom of choice in the selection of automation systems that are best for their business.

Tripwire provides deep visibility through a comprehensive suite of highly-integrated products to detect ICS cyber threats and breaches, prevent future incidents by discovering and prioritizing risks, and continuous monitoring to help keep your security program on track.

Many industrial organizations also lack the personnel necessary to implement and maintain rigid ICS security controls, so Tripwire also offers a range of managed and professional services customized for industrial environments, such as security assessments, penetration testing, and even on-site resident engineers.

4. Industrial Cybersecurity Managed Services

IT/OT convergence is driving the need for new security capabilities and integrations. The breadth of new OT security tools adds to a security team's already overburdened task of managing their environment. The high effort required for recruiting, training, and retaining competent cybersecurity personnel with deep OT expertise poses a serious challenge to most organizations. There simply aren't enough experts to fill those roles—and this skills gap leaves organizations vulnerable to attacks due to lax enforcement of OT security best practices.

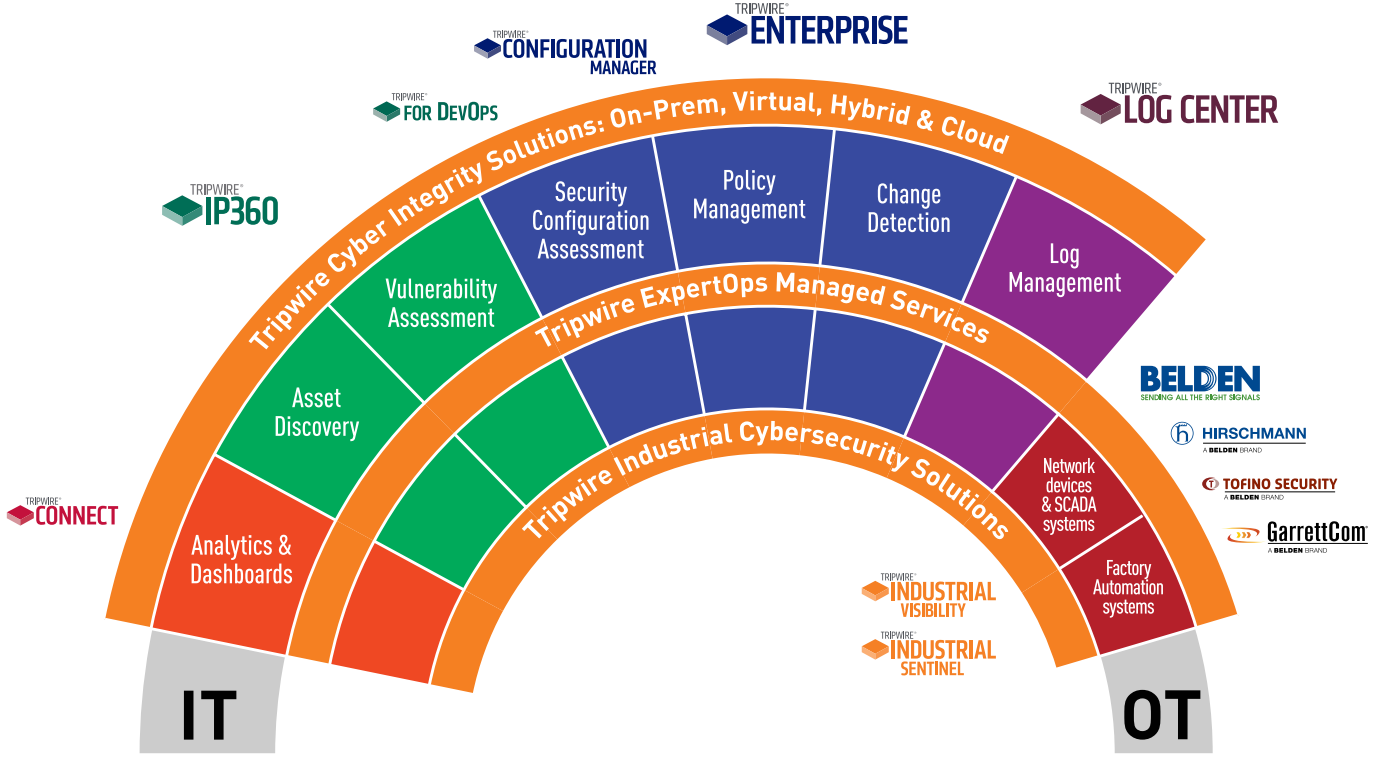
In order to manage the shortage of cybersecurity talent on their teams, industrial organizations and agencies often leverage IT security professionals with limited or no OT cybersecurity background into cybersecurity positions that oversee both IT and OT networks.

Tripwire ExpertOps for Industrial Visibility is a managed services version of the industry's best industrial visibility solution, Tripwire Industrial Visibility. A single subscription provides personalized consulting from trained experts and hands-on tool management to help you achieve and maintain compliance and critical asset security. It gives stretched security teams an alternative to the difficult process of purchasing, deploying, and maintaining additional solutions.

TRIPWIRE® EXPERTOPS *for Industrial Visibility*

10. Monitors Your Entire Infrastructure—From On-Prem to the Cloud

Continuous cybersecurity monitoring and intelligence is a necessary security control for on-premises IT operations, one Tripwire has been known for since the beginning. But large-scale, modern organizations need to track the security posture of private and public cloud accounts as well as hybridized IT infrastructure and/or OT networks. Consolidate vendors and gain confidence in your organization's cybersecurity outlook by exploring the trusted Tripwire solutions that deliver compliance and security controls to your entire infrastructure.



Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **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

BRBFIM2a 2106