SERVICES BRIEF

Tripwire ExpertOps

Cloud-Based Managed Service for Policy Compliance, Secure Configuration, and Vulnerability Management

Highlights

- Simple subscription pricing for best-in-class FIM, SCM and VM
- Tailored advice, incident assistance, and audit support related to Tripwire findings
- 24/7 visibility via security posture dashboard
- Broadest depth and breadth of compliance policy and platform coverage
- Comprehensive discovery and profiling of all network assets
- Waivers and change requests made easy
- Detailed understanding of good vs. bad changes
- No more incomplete or awkward handoffs when your staff changes
- Recommendations and organizational grading to maximize value

Cybersecurity, compliance, and operations teams don't always have the adequate resources or staffing to run the solutions meant to keep their environments secure and audit-ready. Tripwire® ExpertOps℠ delivers industry-leading file integrity monitoring (FIM), security configuration management (SCM), and vulnerability management (VM) as a managed service.

Personalized consulting and ongoing support from a designated Tripwire expert helps you put your focus on detecting breaches, staying in compliance, and remediating vulnerabilities. The solution is easy to deploy and use, with simple subscription pricing and a low total cost of ownership.

Tripwire ExpertOps helps organizations rapidly achieve a foundational level of security throughout their infrastructure—from on premise to cloud— by reducing the attack surface, increasing system integrity, and achieving continuous compliance—all via cloud-based infrastructure. It provides stretched teams an alternative to the difficult process of purchasing, deploying and maintaining products.

Benefits

- **Ongoing support:** You'll be matched with a designated Tripwire expert who serves as an extension of your team by providing personalized advice, incident assistance and audit support. You'll receive recommendations and organizational grading to maximize the value of Tripwire Enterprise, as well as regular alerts and reports in your inbox.
- **System transparency:** How can your security team prioritize which system

changes to address if they don't have deep visibility, let alone a detailed understanding of which changes are relevant? Tripwire ExpertOps provides you with 24/7 security and compliance visibility via a customized dashboard.

» **Cloud-hosted infrastructure:** Tripwire ExpertOps is built on the Microsoft Azure cloud computing platform. That means service can scale quickly to meet changing needs while maintaining the highest standards of security—no extra hardware required. A single-tenancy model ensures your data remains distinct from all other accounts.

How it Works

Tripwire ExpertOps provides you with continuous staffing to operate and deliver core cybersecurity controls like FIM, SCM, and VM. The solution adapts to your objectives—reports and profiling tasks are customized to meet your organizational priorities. You will regularly receive expert guidance to ensure that your environment is secure and that critical vulnerabilities are quickly remediated. You'll gain visibility via 24/7 access to security, compliance, and vulnerability information via a detailed yet easy-to-understand dashboard.

Your Tripwire expert will act as an extension of your team by prioritizing work efforts, managing critical escalations, and presenting results to stakeholders. Together, you will jointly develop a service plan that outlines communication practices, escalation procedures, and any specialized requests.

» Prescriptive policy and vulnerability remediation guidance to ensure the most critical changes and vulnerabilities are identified quickly

» Recommendations for maximizing automation capabilities for security and event alerting practices, change management process integrations, and audit prep activities

» Prioritized remediation to identify opportunities to reduce risk and efficiently improve security posture

» Quarterly CISO and executive review of achievements towards objectives, insight into ongoing improvement, and utility of the environment

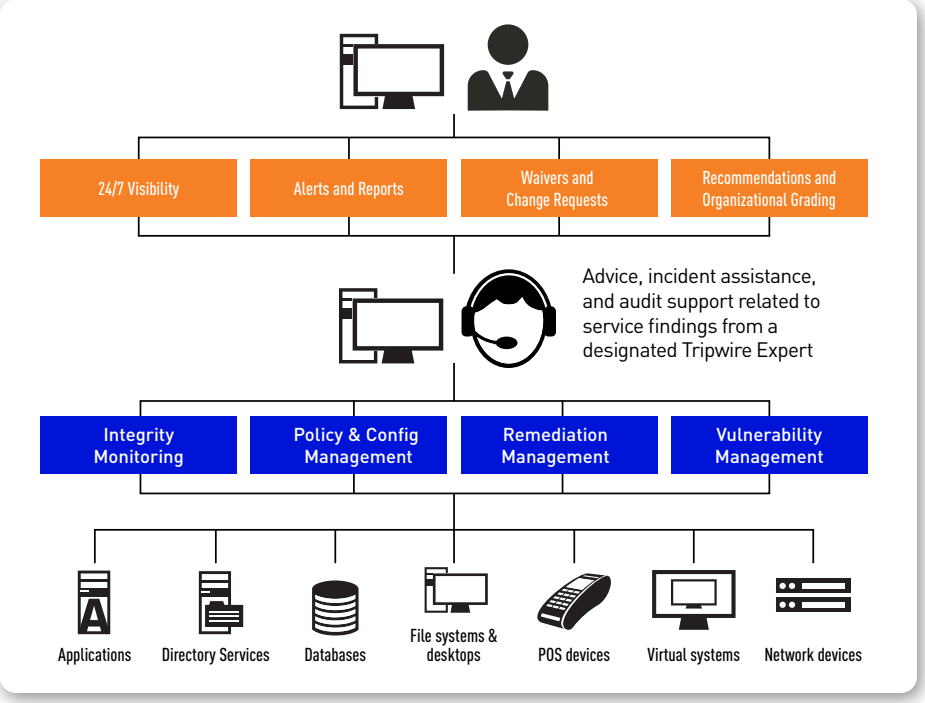
» Organizational grading for each accountable department to provide visibility into groups needing additional resources and attention

Best-In-Class Security with No Additional Resources

Tripwire ExpertOps combines four foundational capabilities to help organizations improve and maintain their security posture without adding resources:

Tripwire File Integrity Manager is the world's first and best FIM technology. 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. Combined 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. Your Tripwire expert will refine FIM results so that reporting is actionable and that the most important configuration lapses drive work activity.

Tripwire Policy Manager establishes and maintains continuous monitoring and configuration assessment across large heterogeneous environments using a comprehensive library of policies and platforms. Tripwire Policy Manager also offers customizable policies, waiver and exception management, automated remediation guidance, 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. Your Tripwire expert will work closely with auditors to provide reusable reporting that answers Tripwire-related questions in the proper context without requiring an auditor that understands the technology.

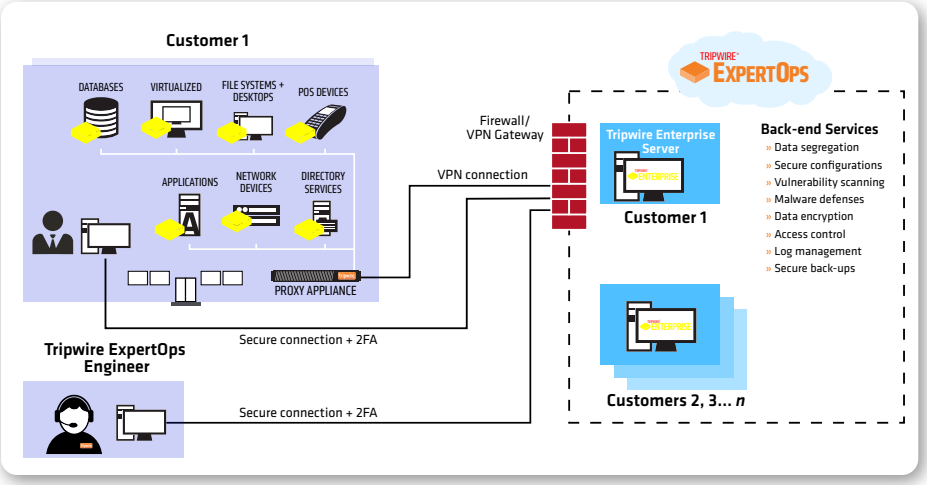


Tripwire ExpertOps helps you spend less time managing tools and more time securing your organization.

Tripwire Remediation Manager provides built-in guidance 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 drill-down capabilities give teams the ability to rapidly and effectively determine root causes. Systems inevitably change as enterprises constantly revise and change their people, processes, and technologies. Tripwire ExpertOps delivers granular drill-down, side-by-side comparisons, historic baselines and comparisons. These capabilities quickly provide investigative teams what they need to know: what changed, when, by whom and how often, along with "how" information.

Tripwire IP360™ uses advanced analytics and a unique quantitative scoring algorithm based on several factors—including the ease and impact of exploit—to prioritize vulnerabilities for remediation. This capability, delivered along with expert advice from your designated Tripwire expert, results in actionable data that enables IT security teams to focus on the tasks that will quickly and effectively reduce overall risk. Tripwire ExpertOps gives you all the security benefits of a mature VM program without the resource strain.

Tripwire Configuration Manager provides periodic assessment of your cloud accounts, storage buckets, and blobs, and then compares them with the Center for Internet Security (CIS) Foundations Benchmarks. It gives you the ability to monitor the configuration of Amazon Web Services (AWS) and Azure-based assets from a single console. Automated enforcement and risk scoring help maintain secure configurations in your cloud accounts.



Tripwire ExpertOps combines FIM, SCM and VM SaaS, personalized consulting, administration services and cloud-based infrastructure

Enterprise Support

Tripwire ExpertOps operates 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:** firewalls, IPS and IDS configurations, routers, etc.

Coverage Across Physical and Cloud Infrastructure

Applications	Ensure that supported applications are configured properly for security, compliance and optimal performance and availability using compliance policy management and file integrity monitoring capabilities.
Directory Services	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	Get your Oracle, Microsoft and IBM database servers into secure, continually high-performing states.
File Systems and Desktops	Assess the configurations of physical and virtual server and desktop file systems, including security settings, configuration parameters and permissions.
Point-of-Sale (POS) Devices	Secure your POS devices against cyber threats while managing security and compliance policies for POS devices. Provide IT Operations with alerts, notifications and response guidance when possible breach indicators or "indicators of compromise" are suspected.
Virtualized Environments	Deliver protection for virtualized environments—private, public and hybrid clouds. Gain visibility across the VMware virtual infrastructure, and enable continuous configuration control of virtual environments.
Network Devices	Broad support of network devices, including any device running a POSIX-compliant operating system.

Tripwire ExpertOps supports components across the entire IT stack, so you can focus on detecting breaches and staying in compliance.

- **Databases:** Oracle, SQL Server, Db2, etc.
- **Continuous monitoring** via secure cloud infrastructure

Summary

Get 24/7 visibility without deploying additional hardware, databases, and back-end software. Tripwire ExpertOps is built on a cloud platform allowing it to quickly scale to meet your needs while maintaining high levels of security. The service uses a single-tenancy model to ensure that data remains segregated between customer accounts. Tripwire applies multiple controls for security and privacy of your data, including secure configurations, vulnerability scanning, data encryption, malware defenses, access control, log management, multi-factor authentication and much more.

Ready to Take the Next Step?

Get in touch with your Tripwire Account Manager—or visit **tripwire.com/contact**—to develop a custom Service Plan for Tripwire ExpertOps.

Tripwire ExpertOps Features and Benefits

Comprehensive coverage	Coverage across the entire hybrid IT infrastructure, including servers, devices, applications and multiple platforms and operating systems.
Prioritized remediation	Take a practical approach to gap remediation by identifying the areas of greatest impact to organizational risk and opportunities to efficiently improve overall compliance and security posture.
Designated Tripwire Expert	A Tripwire Expert that will act as an extension of your team by prioritizing work efforts, managing critical escalations and presenting results to stakeholders.
Faster, easier audit preparation	Dramatically reduce the time and effort for audit preparation by obtaining 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	Configuration assessment with file integrity monitoring to detect, analyze and report on changes as they happen and keep configurations continually compliant. This immediate access to change information lets you fix issues before they result in a major data breach, audit finding or long-term outage.
Automated IT compliance processes	Automate compliance with the industry regulations and standards that organizations are subject to—including PCI, NERC, SOX, FISMA, DISA and many others.
Custom Service Plan	Your Tripwire Expert will jointly develop a Service Plan outlining communication practices, escalation practices and any specialized requests.
Organization grading	Gain visibility into groups needing additional resources and attention through operational grading provided on a quarterly basis that's based on your KPIs.
Expert recommendations	Maximized automation capabilities for security and event alerting practices, change management process integrations and audit prep activities, based on reconditions from your Tripwire Expert.
CISO and executive reviews	A quarterly report to your key stakeholders that includes deployment health statistics as well as an overview of achievements towards your objectives. The quarterly CISO and Executive review provides insight into the ongoing improvement and utility of your Tripwire environment.
Prescriptive policies and content	Your Tripwire Expert will provide a framework for FIM and compliance content that produces a prescriptive prioritization for FIM and policy changes. This framework will be used along with your input to ensure that the most critical changes/risks are identified quickly.
Reporting analysis	Your Tripwire Expert will review FIM and policy compliance changes and look for "unusual activity" and bring it to your attention during service reviews. Urgent changes are handled based on your event ticket creation practices.
Dashboard and reporting maintenance	A full complement of tailored reports, created and adjusted by your Tripwire Expert based on your environment and monitoring needs.
Waiver creation and updates	Your Tripwire Expert will create and update waivers as directed by you. This includes the inclusion of onboarded nodes in applicable waivers as well adjustment to waiver expiration dates and/or comments.
Custom application monitoring	Monitor custom applications including specific directories to be monitored or database queries to identify important changes.
Change reconciliation assistance	Promote unauthorized changes according to the schedule defined in your Service Plan.

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

CBTX04a 2012