SERVICES BRIEF

Tripwire ExpertOps Federal

FedRAMP-Certified Cloud-Based Managed Services for Compliance, Configuration and Integrity Monitoring

Quote

Security teams shouldn't overburden themselves by trying to do everything on their own. They can partner with trusted vendors for managed services or subscribe to service plans where outside experts can act as an extension of the team.

— Tim Erlin, VP of Product Management and Strategy at Tripwire

Finding a powerful set of security solutions to protect your organization or agency's data isn't enough on its own. You also need talented cybersecurity professionals who can leverage those tools correctly and have the expertise needed to remediate security incidents immediately, while you focus on the operational tasks that matter the most.

Security teams are overburdened trying to do everything on their own. This leaves security managers, executives, and CISOs in a dangerous position, hoping for the best as many organizations have done out of a lack of better options.

Overburdened Security Teams

Security teams are often overwhelmed with managing complex security tools to handle their most important responsibilities, such as file integrity monitoring (FIM), security configuration management (SCM), and vulnerability management (VM). They often have too many tools to manage and not enough bandwidth to focus on strategic cybersecurity initiatives. When staff transitions, a lack of proficiency with those security tools makes for awkward and incomplete hand-offs. Training new cybersecurity tool administrators can quickly become a resource drain as well.

Ineffective Security Operations

The current threat landscape pits underprepared IT professionals against cyber adversaries that use sophisticated and ever-evolving plans of attack. Not effectively leveraging the full capabilities of security tools can lead to breaches going undetected for months, costing organizations and agencies untold resources.

Training and Retaining Cybersecurity Staff

There simply aren't enough cybersecurity professionals to meet industry demand. This skills gap leaves organizations and agencies vulnerable to attacks because of improper enforcement of security best practices.

Tripwire ExpertOps Federal

Tripwire® ExpertOps℠ Federal provides a FedRAMP-certified cloud-based managed services version of the industry's best FIM and SCM. 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 provides stretched IT teams an alternative to the difficult process of purchasing, deploying and maintaining products.

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. And you'll receive recommendations and best practice guidance 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 Federal provides you with security and compliance visibility via customized reporting.

FedRAMP-Certified, Cloud-Hosted Infrastructure

Tripwire ExpertOps Federal is hosted in a FedRAMP-certified cloud computing platform, provided by our partner, DataBank. That means service can scale quickly to meet changing needs while complying with FedRAMP requirements. A single-tenancy model ensures your data remains distinct from all other accounts.

Licensing

Tripwire ExpertOps Federal saves organizations the additional costs of licenses, training and hardware, and can reduce total cost of ownership by up to 30 percent or more compared to a typical Tripwire Enterprise deployment. Annual subscription pricing includes a base fee for the service. Existing customers no longer need to pay for support and will receive a discounted subscription price. Tripwire ExpertOps Federal offers three subscription service tiers:

1. **Essential:** Essential includes best-in-class FIM plus one standard policy, basic operation, and monitoring. This tier provides day-to-day maintenance of the TE console and managed nodes as a managed service for those who need change management or compliance information. This is ideal if you're just getting started with change management or compliance practices.
2. **Advanced:** The Advanced tier builds on the essentials with two standard policies, custom app monitoring, additional change requests, expert analysis, and Dynamic Software Reconciliation (DSR). Receive tactical tuning assistance to ensure the most important information is highlighted for action. View customized reporting dashboards with detailed analysis and results, and get dedicated problem resolution support.
3. **Advanced Plus:** Advanced Plus, our most robust and comprehensive tier, also includes custom policies, process assistance and unlimited change requests, as well as Tripwire Dynamic Software Reconciliation and the Tripwire Enterprise Integration Framework. With this tier, an assigned program coordinator will work with you to develop an operational use plan with best practice recommendations, as well as assistance with change reconciliation and prioritization of suggested remediation activities.

Summary

Overburdened security teams, ineffective security operations, and training/retaining qualified staff leaves most organizations in a challenging position. Tripwire ExpertOps Federal equips your teams with the expert support needed to maximize the full benefits of best-in-class File Integrity Monitoring and Secure Configuration Management.

Request a Demo

Let us take you through a demo of Tripwire ExpertOps Federal and answer your questions. Visit **tripwire.com/contact/request-demo/**

Tripwire ExpertOps Federal Features

Single point of control for all IT configurations	Centralized control of configurations across the entire hybrid IT infrastructure, including servers, devices, applications, and multiple platforms and operating systems.
Robust Asset View capabilities	Classify assets with business-relevant tags such as risk, priority, geographic location, regulatory policies and more. Asset View capabilities now offer provisioning with an asset tag file, increased scale for large numbers of assets, giving a sharper view of risk across the entire organization.
Workflow tools for managing failed configurations	Role-based workflow tools that let users approve, deny, defer or execute remediation of failed configurations.
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.
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.
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.
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 posture.
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.

DataBank has a strong pedigree in deploying secure and compliant solutions for mission-critical business systems governed by FedRAMP or FISMA requirements. DataBank has undergone a 3PAO audit and validation process utilizing the latest NIST 800-53 security framework. DataBank's Authorization to Operate, or ATO, includes traditional and enhanced IaaS and PaaS services.

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

CBTXOFED2a 2101