Ease the Burdens on Your Cybersecurity Team

Boost Your Cybersecurity Program with Tripwire ExpertOps

> **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, Tripwire VP of Product Management and Strategy

Few industries have undergone as drastic a change in recent years as cybersecurity. The proliferation of new types of cyberattacks, in addition to rapid progress in cloud computing and automation, sets organizations and agencies up to need more cybersecurity professionals than they can possibly find and retain given the shortage of qualified talent on the market.

This leaves security managers, directors, and CISOs in a dangerous position if they place non-security IT professionals in security roles and hope for the best, as many organizations have done out of a lack of better options. One solution organizations can turn to is a managed service. It is possible to maintain powerful security operations with small teams if you know where to look.

Training and Retaining Cybersecurity Staff

There simply aren't enough cybersecurity professionals to meet industry demand. In order to manage the shortage of cybersecurity talent on their teams, organizations and agencies often leverage IT professionals with no cybersecurity background into cybersecurity positions.

Overwhelmed Security Teams

Small security teams are often overburdened with managing complex security tools to handle their most important responsibilities, like 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 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.

How Managed Services Help

No organization or agency has the power to drastically alter the supply-to-demand ratio of qualified candidates in the cybersecurity industry. Managed services can solve staffing and resource challenges within your organization, arming your team with the necessary security expertise to thwart cyberattacks and maintain optimal compliance configurations.

Consolidate Vendors and Tools

If your security team is underprepared, crowding their processes with too many tools and vendors is not going to help. Vendor and tool consolidation takes some time up front, but it's well worth the effort to narrow your toolkit down to the products and services that actually help do the heavy lifting of security operations—rather than flood your team's inboxes with unnecessary notifications.

Extend the Efficacy of Stretched Teams

Less is more when it comes to using the resources of a stretched team wisely. Strategically implementing managed services is the best way to get your security operations where they need to be. Rather than trying to recruit and train in a scarce talent market, extend your team with a dedicated engineer from your security solutions vendor. This security-as-a-service model means you'll have an expert who stays in sync with your team, offering customized advice for improvement every step of the way.

How to Evaluate Managed Services

Once you've made the decision to seek out a managed services solution, how do you evaluate it to ensure that it meets all of your criteria? What will the total cost of ownership be compared to keeping security operations in-house—and the hiring and training that would require?

Here are the most important considerations you must keep top-of-mind when assessing the overall value of a managed services cybersecurity solution:

- » Advanced FIM, SCM, and VM, with enforced policy compliance
- » Advice, incident assistance and audit support
- » A designated expert assigned to your team
- » A vulnerability and exposure expert assigned to your team to help you mature your VM program

Tripwire ExpertOps

Tripwire® ExpertOps^{SM} provides a cloud-based managed services model of the industry's best FIM, SCM, and VM, along with several other key foundational security controls. A single subscription includes both 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 provides you with continuous staffing to operate and manage your Tripwire solution at peak efficiency. 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.

Together you will jointly develop a service plan that outlines communication practices, escalation procedures, and any specialized requests.

The Tripwire Expert will then tune and operate the solution and provide:

- » Prescriptive policy and content guidance
- » Recommendations for maximizing automation capabilities
- » Prioritized remediation to reduce risk and efficiently improve compliance posture
- » Organizational grading for visibility into groups needing additional resources and attention
- » Quarterly CISO and executive review of achievements and insight into ongoing improvement

Tripwire ExpertOps FIM & SCM

Get the maximum security benefits of industry-leading FIM and SCM right away with Tripwire ExpertOps SCM. Quickly achieve and ensure 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 also includes options for cloud account configuration management via Tripwire Configuration Manager, which monitors Amazon Web Services and Azure accounts using the Center for Internet Security (CIS) benchmarks.

Tripwire ExpertOps VM

Tripwire ExpertOps Vulnerability Management provides you with continuous staffing to deliver a cloud-hosted managed services model for VM, including the lowest false-positive rate. And the solution adapts to your objectives:

reports and profiling tasks are customized to meet your organizational objectives and priorities. You will regularly receive expert guidance to ensure that your environment is secure and that critical vulnerabilities are remediated. You will also receive personalized feedback from the Tripwire Vulnerability and Exposure Research Team (VERT) to help you mature your VM program.

Tripwire ExpertOps Industrial Visibility

The IT/OT convergence is driving the need for new security capabilities and integrations. The breadth of new OT security tools adds to security teams' already overburdened task of managing their environment. Tripwire ExpertOps Industrial Visibility is a managed services version of the Tripwire 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.

Tripwire ExpertOps Federal

Tripwire ExpertOps Federal provides a FedRAMP-certified cloud-based managed services model that includes the industry's best FIM and SCM. Tripwire ExpertOps Federal is hosted within our partner, Databank's, FedRAMP certified environment. 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.

A Subscription Tier That Matches Your Needs

Tripwire ExpertOps saves organizations the additional costs of licenses, training, and hardware, and can reduce total cost of ownership by 30 percent or more compared to a typical Tripwire product deployment. Annual subscription pricing includes a base fee for the service. For existing customers, you no longer need to pay for support and will receive a discounted subscription price.

Tripwire ExpertOps offers three subscription service tiers:

Essential

Essential includes best-in-class FIM plus one standard policy, basic operation, and monitoring. It also includes day-to-day maintenance of the VnE console and ensures that vulnerability scans are executed on a predefined cadence for clients that need this information. This tier provides day-to-day maintenance of the console and managed nodes for clients that need change management, compliance, and vulnerability information. This is ideal if you're just getting started with change management or compliance practices.

Advanced

Tripwire ExpertOps Advanced builds on the essentials with two standard policies, custom app monitoring, additional change requests, 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. In addition, this tier provides proactive risk monitoring and assessment, dedicated problem resolution support, and vulnerability remediation recommendations.

Advanced Plus

The most robust and comprehensive Tripwire ExpertOps subscription also includes custom policies, process assistance, and unlimited change requests, as well as DSR and the Tripwire Enterprise Integration Framework. With Advanced Plus, 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. This tier also provides integrations with threat intelligence, change management, incident management, and configuration management database (CMDB) tools.

Summary

Many cybersecurity teams struggle with a skills gap. It might be that your team is too small for their responsibilities, or that you're finding it difficult to attract, train, and retain talent. Turnover is a common problem, with organizations and agencies often losing skilled individuals to new opportunities. Fortunately, strategically selecting a comprehensive managed services solution closes the skills gap and allows constrained teams to successfully run cybersecurity programs. Tripwire ExpertOps equips such teams with the advice and support needed to protect your data from cyberattacks while maintaining regulatory compliance.

Schedule Your Demo Today

Let us take you through a demo of Tripwire security and compliance solutions and answer any of your questions. Visit **tripwire.me/demo**

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