Tripwire ExpertOps

Cloud-Based Managed Services for Monitoring Compliance, Configurations and Integrity

Cybersecurity Skills Gap *By the Numbers*

- **1.5 million:** The worldwide shortfall of information security professionals by 2020.
- **91%:** The amount of IT security professionals planning to outsource security skills to address the gap.
- **1 in 5:** The number of IT security professionals who say their organization hires talent without adequate experience to run security operations.
- **$1 trillion:** The projected global spending for cybersecurity by 2021.
- **Every 40 seconds:** The frequency of ransomware attacks against businesses.

Finding a powerful set of security solutions to protect your organization'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.

The high demand for recruiting, training and retaining competent cybersecurity personnel poses a serious challenge to most organizations. There simply aren't enough experts to fill those roles—and this skills gap leaves you vulnerable to attacks because of improper enforcement of security best practices.

Tim Erlin, VP of Product Management and Strategy at Tripwire explains, "The skills gap doesn't have to be an operational gap. 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."

The Skills Gap Problem

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.

Operational challenges: Security teams are often overburdened with managing other security tools in their environment to handle the breadth of their most important responsibilities, like file integrity monitoring (FIM) and security configuration management (SCM). They have too many tools to manage, and not enough bandwidth to get up to speed in time to meet their compliance needs. When staff transitions, a lack of proficiency with security tools makes for awkward and incomplete hand-offs.

Increased vulnerability: The skills gap is much more than an HR problem. It pits IT professionals against cyber adversaries using sophisticated and ever-changing plans of attack. No effectively leveraging the full capabilities of security tools can lead to breaches going undetected for months, costing organizations and agencies untold resources in short periods of time.

Enter Tripwire ExpertOps

Tripwire® ExpertOps℠ provides a 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.

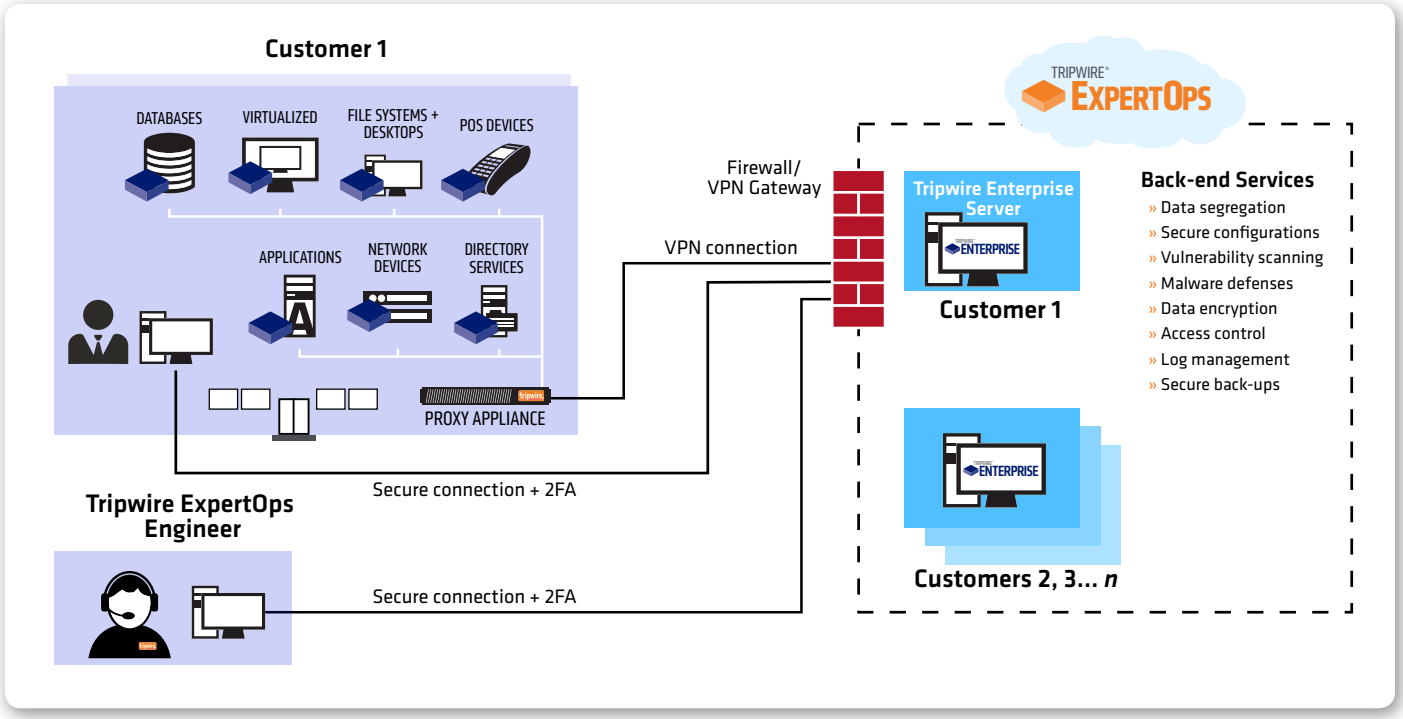

Fig. 1 Tripwire ExpertOps combines FIM and SCM software as a service, personalized consulting, administration services and a cloud-based infrastructure.

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.

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.

Tripwire ExpertOps 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.

Licensing

Tripwire ExpertOps 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. 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. This tier provides day-to-day maintenance of the TE console and managed nodes as a managed service for clients that need change management or compliance 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.

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 (TEIF). With the Advanced Plus 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.

How the Proxy Appliance Works

A proxy appliance is an integral part of the Tripwire ExpertOps architecture. Tripwire engineers will work with you to install the proxy in an appropriate location in your environment then help you configure and resource the appliance to meet your specific needs. There's no additional cost for the appliance, even when multiple appliances are necessary for your environment.

Proxy Resources

RAM: 8 GB

Hard Disk Space: 80 GB

CPUs: 4 Cores

Network Connectivity

- Proxy outbound: at 500, 4500, 4501
- Agent-to-Proxy: Port requirements depend on monitored assets and agent technology in play

Summary

The disparity between security needs and security talent leaves most organizations in a challenging position. Tripwire ExpertOps fills the skills gap by equipping your teams with the expert support needed to maximize the full benefits of best-in-class FIM and SCM.

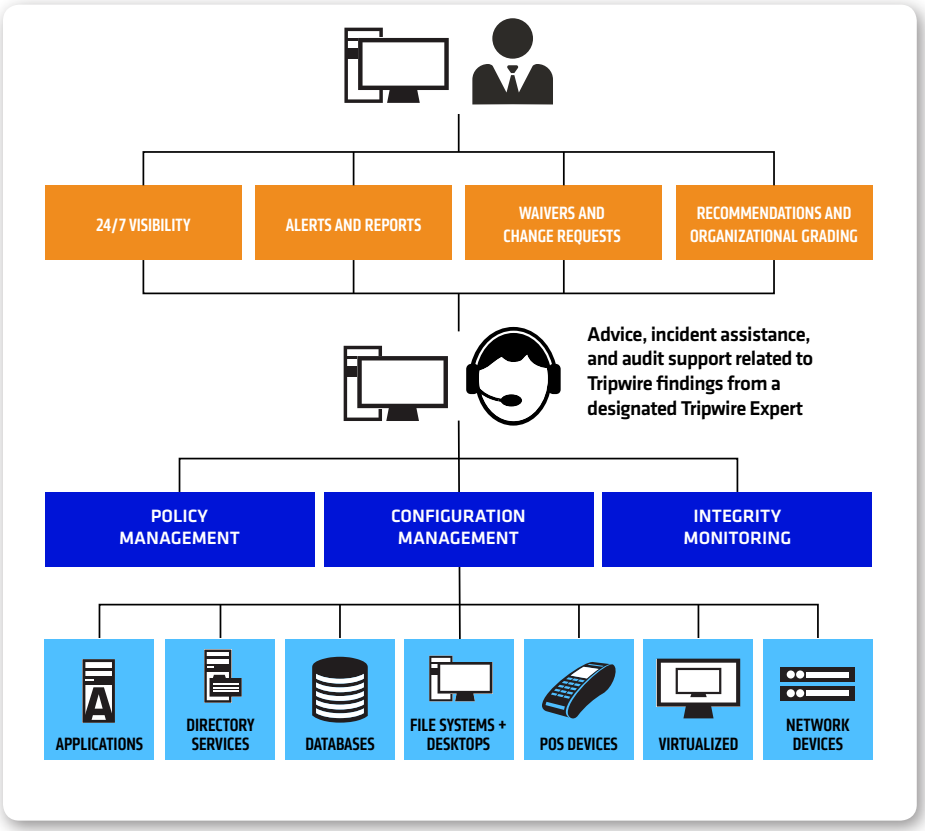

Fig. 2 Tripwire ExpertOps helps you spend less time managing tools and more time securing your organization.

Request a Demo

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

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at tripwire.com**

***The State of Security*: Security news, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook