



Tripwire ExpertOps Security Configuration Management and File Integrity Monitoring (SCM/FIM) Services Description



Instant Expertise with Managed Cybersecurity

Strengthen security and compliance rapidly with industry leading file integrity monitoring (FIM) and security configuration management (SCM) capabilities with Fortra's Tripwire® ExpertOpsSM SCM/FIM managed services. Tripwire ExpertOps is a managed service that helps organizations address cybersecurity challenges by providing trained experts to help with critical day-to-day solution management. Our team of experts are ready to help organizations quickly achieve and ensure cyber integrity across their unique environments and stay aligned with frequently changing compliance regulations.

Tripwire ExpertOps SCM/FIM helps effectively monitor IT assets for unplanned changes to identify security misconfigurations or indicators of compromise. With a comprehensive library of policy and platform combination tests organizations are equipped to provide auditors with evidence of compliance and have greater visibility into policy status for heightened security. Tripwire ExpertOps can also provide a designated Tripwire expert to provide personalized advice, incident assistance, and audit support.

ExpertOps offers SCM/FIM through either hosted operations or remote operations. Knowing when a change occurs on a critical file or in a critical configuration allows for prompt intervention on unauthorized changes, or validation of forensic details when authorized changes occur and research is being performed later. This information is also useful amid regulatory audits, where Tripwire can provide audit-ready reporting.

Hosted and Remote Operations

Hosted Operations

The ExpertOps Service offering can be hosted by Tripwire in the cloud (“Hosted”) and data protection is a top priority. From the moment a scan leaves an asset to providing the reports of detailed information organizations need, the ExpertOps solution ensures that only the right people have access to the right data at the right time. Data is encrypted in motion and at rest; the ExpertOps single-tenant environment ensures data is segregated, and least-privileged controls limit access to only those authorized. The environment is continuously monitored for both security and operational incidents to identify and respond to any potential threats. To learn more about the ExpertOps cloud environment controls, request a copy of our compliance reports: SOC 2 and PCI DSS AoC.


Remote Operations

ExpertOps Services are also available via remote management of on-premises software, licensed to the customer, including monitoring and reporting, as described in an order (“Remote Operations”). Remote Operations does not include software license fees, implementation services or maintenance support services which customers must purchase separately.

Data Center Location and Business Hours

Regionally located data centers are currently available in the US, UK, EU, and Canada. Unless otherwise stated by Tripwire, the console and customer content will be hosted in a regional data center closest to the customer’s primary business location.

The Managed Services team is available Monday–Friday, excluding public and company-designated holidays. Please check the ExpertOps Service Portal for a detailed list of the public and company-designated holidays, which will be updated annually. Technical Support is additionally available off-hours for Severity 1 events as described below.

Priority Level Help					
 After hours "Severity 1 — System Down" issues <i>must</i> be reported by phone in order to page an engineer.					
Severity	Description	Contact us	Response	Relief	
1 System down	Product is inoperable or non-functional; Business outage; Data is lost.	Phone, email, portal	1 hour ^{‡‡}	1 business day	
2 High	Major business impact; Product is crippled but somewhat usable; Very difficult work around.	Phone, email, portal	1 hour [‡]	2 business days	
3 Medium	Moderate business impact; Production is proceeding but impaired; Workarounds are available.	Email, portal	4 hours [‡]	5 business days	
4 Low	Minimal business impact; Cosmetic problems; Usage questions; Feature Q&A; Issue doesn't require resolution.	Email, portal	4 hours [‡]	Next product release	
[‡] During business hours only.					
^{‡‡} After hours, "Severity Level 1 — System Down" requires a report by phone.					

ExpertOps SCM/FIM Service Tiers

The Tripwire ExpertOps SCM/FIM Service offering includes three subscription services tiers to choose from. All tiers include: a Tripwire Enterprise (TE) Console, licensed Tripwire Enterprise software for all in-scope assets, and system administration services provided by Tripwire's Managed Services team. ExpertOps Service is offered on an annual basis, and includes standard implementation, monitoring, reporting and support during the term based on the customer's configuration instructions and policies.

Hosted

The Hosted tier includes best-in-class FIM and SCM plus basic operation and monitoring. This is ideal for mature organizations with a preference toward minimal support in a highly reliable environment. The Hosted tier is for organizations that want Tripwire to host and maintain the underlying infrastructure but want to remain in control of the day-to-day FIM and SCM program themselves. It provides essential maintenance of in-scope assets as a managed service for customers that need change management or compliance information. It includes access to Tripwire authored Change Rules, but any tuning, customization, or reporting by the ExpertOps team is not included.

Managed Services

The Managed Services tier gives the option of utilizing the Tripwire managed environment to host or hosting in the customer environment with remote management services for policy creation, custom app monitoring, additional change requests, and analysis needs. In addition to the ExpertOps Service provided at the Hosted tier, the Managed Services tier includes:

- ▶ Tactical tuning assistance to ensure that the most important information is highlighted for action
- ▶ Customized reporting and dashboards, with a more detailed analysis of results
- ▶ Designated problem resolution support
- ▶ Status meeting interval is increased to weekly
- ▶ Service Performance Review interval increased to semiannual
- ▶ Content tuning
- ▶ Custom FIM content creation for up to four applications
- ▶ Dashboards and reports to display and alert on changes detected
- ▶ Assistance with the configuration of two standard policies and custom compliance reporting

Integrated Strategy

The most robust and comprehensive Tripwire ExpertOps subscription is the Integrated Strategy tier which includes long term cybersecurity planning and execution through an assigned Strategic Consultant. With the Integrated Strategy tier, the ExpertOps Service team is even more involved with the customer's internal team. Waiver creation, policy tuning, and remediation assistance can be prioritized at the customer's request. In addition to the services above, the Integrated Strategy tier includes:

- ▶ Development of an operational use plan with best practice recommendations
- ▶ Assistance with reconciliation of change and prioritization of remediation activities
- ▶ Custom FIM content creation for applications
- ▶ Setup and maintenance of a change reconciliation integration with supported ticketing systems
- ▶ Assistance with the configuration of an unlimited number of Tripwire standard policies, as well as custom benchmarks
- ▶ CISO and executive reviews

Service Tier	Delivery
Hosted	Hosted
Managed Services	Hosted or Remote
Integrated Strategy	Hosted or Remote

Professional Services

The ExpertOps Service fee does not include other Professional Services, which are available on a time and expense basis, and which must be ordered separately. Efforts not specifically included in the Services Agreement would require Professional Services to implement.

Examples include:

- ▶ Development of custom policies
- ▶ Custom integrations with unsupported integration targets, e.g., Git, Zendesk
- ▶ Integration with third-party products

Certifications and Audit Reports

Copies of the current PCI DSS Attestation of Compliance and the SOC 2 audit for ExpertOps Service are available upon request under a non-disclosure agreement.

ExpertOps SCM/FIM Service Task Descriptions

Note: See table below for the features that apply to each service tier.

Key Roles

Customer Lead

Primary point of contact at the customer for the Managed Services Engineer (MSE); provides guidance to the MSE on asset configuration, classification and priorities, and compliance policies to be monitored; receives status reports and updates from the MSE.

Tripwire Managed Services Engineer

Primary administrator of the ExpertOps Service for the customer; responsible for regular operational and maintenance activities.

Tripwire Service Delivery Manager

Primary point of escalation within Tripwire; responsible for the management and delivery of all ExpertOps Service accounts, and the successful execution of all standard activities; works with the MSE and the customer Lead to establish strategic goals for customer and Tripwire.

Tripwire Strategic Consultant

Dedicated Tripwire expert who partners with Integrated Strategy tier customers to develop forward looking, customized operational use plans and delivers best practice recommendations.

Onboarding Support

ExpertOps will provide Onboarding Services based on the Services Agreement.

Management

Service Status Updates

On a frequency aligned with the service tier (monthly or weekly), a status report will be delivered to the Customer Lead and the Tripwire Service Delivery Manager. This report will contain a high-level overview of the daily and weekly activities completed. This report will also include any noteworthy issues encountered (with resolution, if any), event tickets created, and status of change requests submitted by the customer.

Proxy Maintenance (*Hosted Only*)

A proxy virtual appliance is required by the ExpertOps service to serve as a secure gateway between the customer's environment and the Tripwire hosted environment. This proxy appliance is typically deployed to a customer's DMZ that has IP and port limited access to the customer's environment.

- ▶ **Proxy onboarding:** A proxy deployment in the customer's environment is the responsibility of the customer. This will typically require augmentation of firewall rules and processor, memory, and disk resources provided from a customer's virtual host. The number of proxies required will depend on the customer's physical network configuration. Additional details on proxy requirements are available in the ExpertOps Onboarding Checklist.

- ▶ **Proxy updates (including Apps):** Once a secure link between the proxy appliance(s) and the Tripwire hosted solution has been established, updates to the proxy device will be maintained by the customer with binaries provided by Tripwire.

Asset Onboarding

Additional monitored assets can be added during the ExpertOps service term with a purchase order. The MSE will review any new assets that are added and, upon guidance from the Customer Lead, classify the assets for monitoring and reporting using the appropriate tagging.

Client Requests

Customer configuration or informational requests will be made through the ExpertOps Service Center. The number of requests included in ExpertOps Service varies by ExpertOps Service tier.

User Management

To support effective separation of duties within the customer environment, Tripwire Enterprise offers full role-based access control. There are several built-in roles that can be assigned to individual users; additional custom roles can be constructed as well. Customers may request additional user access through the ExpertOps Service Center. ExpertOps also supports integrating with Customer ADFS to utilize SSO authentication.

Dashboard and Reporting Maintenance

The standard ExpertOps implementation includes standard reports, created, and configured by the MSE based on direction from the Customer Lead. The MSE will adjust the standard reports from time to time at the Customer Lead's request to keep pace with the customer's changing environment and monitoring needs.

Dashboard and Report Creation

For customers at the Managed Services and Integrated Strategy tiers, ExpertOps Service includes creating new reports and dashboards at the Customer Lead's request to keep pace with the customer's changing environment and monitoring needs.


FIM Content Tuning

For customers at the Managed Services and Integrated Strategy tiers, the MSE and the Strategic Consultant will work together to identify potential candidate deviations to be tuned out as noise. In this context, noise is considered changes that do not provide meaningful information and should be excluded from monitoring.

Content Maintenance

Tripwire releases updates to SCM and FIM based on industry benchmark availability and the urgency of updates for a particular platform. The MSE will work with the customer to determine the applicability of available SCM and FIM content to the customer's requirements as applicable.

- ▶ **Content updates—Build:** Tripwire is responsible for the creation and publication of new and updated core operating system FIM rules for Tripwire supported operating system releases.
- ▶ **Content updates—Installation:** Tripwire will install the newly available rules as published when requested by the customer.

- 
- ▶ **Content updates—Validation:** The MSE will validate the installation of the new rules. Validation includes any rule tuning and severity setting at the direction of the customer.
 - ▶ **Update applicability determination:** The MSE will work with the customer to determine if the newly available rules are applicable to their requirements.

Custom Policy Maintenance

For customers at the Integrated Strategy tier, Tripwire Enterprise can be configured with custom policies. When a new and distinct custom policy test is necessary the MSE will deliver a custom policy questionnaire to the Strategic Consultant. This questionnaire will be completed by the customer and returned to the MSE for the test structure.

Custom policy tests may include specific directories, database queries, or scripts to identify important configuration to test against. It is critical that accurate and detailed information be provided by application subject matter experts to ensure the effectiveness of the custom policy. Overarching policy tests will require an additional and separately purchased Professional Services engagement.

ExpertOps MSEs will maintain custom policies and tests as configured or created during the term of service. In addition, ExpertOps is capable of tuning requirements for custom policies. Tripwire is not responsible for the quality of customer-defined policy tests.

Monitoring

Implementation Monitoring

As with any enterprise-class application, Tripwire software benefits from occasional maintenance activities and performance review. The Managed Services Lead will regularly review the operational metrics of the solution and make any adjustments or corrections considered necessary or advisable.

- ▶ **Application health monitoring:** Tripwire will monitor applications provided by Tripwire as part of this service. Tripwire will notify the customer in the event of a complete loss of a service.
- ▶ **Customer environment health:** Tripwire will monitor the health of the customer's environment that is necessary for the communication between the Tripwire service and the assets. This would include any Tripwire supplied appliances.
- ▶ **Tripwire hosted environment health:** Tripwire will monitor the hosted infrastructure including the supporting database and VPN terminus at the hosted solution site. Tripwire will notify the customer in the event of a complete loss of a service.

Asset Health

Tripwire will verify that all monitored nodes are communicating with the TE Console on a daily basis and will verify that the monitored nodes are completing their scans as expected. Tripwire will analyze node health error conditions and provide tactical troubleshooting assistance to improve the completeness of monitoring results. Any identified errors or unexpected behavior will be investigated and remediated by Tripwire with the guidance and assistance of the customer.

Proxy Appliance Health (*Hosted Only*)

The proxy appliance is the gateway to the Tripwire ExpertOps service. The proxy resides in or close to the customer's network. The proxy appliance is virtual and is hosted by the customer. The MSE can monitor the proxy appliance via the TE Console. The MSE will work with the customer to ensure the availability of the proxy appliance as it is a key component of the service.

Report Distribution

As part of a standard implementation, customers will receive reports delivered on a regular basis. To ensure consistent distribution, the MSE will review all scheduled report executions and verify that the reports have been run.

Agent Maintenance

Tripwire provides new versions of its agent to support new features and operating systems as well as to address security and functionality issues. Agents should be kept up to date with the latest version appropriate to the customer's operating system. Tripwire will confirm the proper agent versions to use and stage those versions in the Tripwire console. Where possible, Tripwire should use the console's push functionality to upgrade the agents in place with proper approval from the customer. Tripwire will assist the customer to update any agents that cannot be upgraded by a push from the console.



Active Scan Setup and Completion

To ensure consistent and accurate functionality, the MSE will assist the customer with the setup of scheduled scans and will verify that the scans begin when expected, complete successfully, and do not run for an excessive amount of time. Collection of results for the policy tests to compare against require running certain regularly-scheduled tasks, usually on a weekly basis. Setup and monitoring of these tasks are covered by the MSE.

Operational Incident Handling

Tripwire will interface directly with the customers to address incidents with applications provided by Tripwire. If Tripwire determines the issue is related to the functions of Tripwire provided applications, Tripwire will track and resolve the incident as predefined by our SLA.

- ▶ **Service requests from customers:** Tripwire will collect requests directly from the customers. Customers will be responsible for entering a ticket into Tripwire's ExpertOps Service Center. Tripwire will be responsible for confirming the resolution and communicating status and completion back to the customer.
- ▶ **Ticketing monitoring/resolution:** Tripwire will track the service request in its ticketing system. Updates to ticket status will be available in the ticketing system and via e-mail when updates to the request are made. Depending on the severity of the ticket, different service level agreements will apply.

Business Process Integration

Tripwire Apps

Managed Services and Integrated Strategy customers can take advantage of the Tripwire Dynamic Software Reconciliation (DSR) and Tripwire Event Sender apps. Integrated Strategy also has the advantage of the Tripwire Enterprise Integration Framework (TEIF).

Tripwire Integrations Management

The Managed Services Lead will review the operation of Tripwire integrations to ensure optimal function and efficiency. Problems will be escalated as needed. For Managed Services and Integrated Strategy customers, the MSE will review the operation of Tripwire integrations to ensure optimal function and efficiency. Problems will be escalated to the appropriate Customer Lead.

Tripwire Apps Licensing

The Managed Services and Integrated Strategy service tiers include a subscription software license for the Tripwire DSR and Tripwire Event Sender apps during the ExpertOps term. In addition, Integrated Strategy customers are granted a subscription software license for the TEIF application.

Tripwire Apps Maintenance

As part of ongoing application maintenance, Tripwire R&D periodically releases patches that address emergent issues that may affect a customer's operating environment, as well as introducing new features for Tripwire Apps. Tripwire recommends that all customers' Tripwire Enterprise components remain current with official patches, and should work with the MSE to review the impact and criticality of any available patches and update Tripwire Apps in a planned maintenance window.

Change Reconciliation (Promotion)

The customer is ultimately responsible for the promotion of changes discovered by rules approved by the customer. The customer may submit formal documentation for criteria to allow the MSE to promote some or all changes on their behalf. Tripwire can also perform promotions if provided the documented criteria from the customer. For Integrated Strategy Customers, the MSE is able to promote unauthorized changes according to the schedule defined in the Operational Use Plan.

Remediation Prioritization

For Integrated Strategy, the Strategic Consultant will outline a practical approach to gap remediation, by identifying the areas of greatest impact to organizational risk and opportunities to efficiently improve overall compliance posture.

Regulatory

Audit Contribution

The MSE will provide assistance gathering application data necessary for audit preparation. In collaboration with the customer, the MSE will produce tailored reports to support audit requests. Depending on the scale of the requested reports, this may represent an additional cost provided by Professional Services (PS).

Policy Tuning and Guidance

For Managed Services and Integrated Strategy customers, the MSE will update or tune compliance policy tests as requested by the Customer Lead. This may include changes to the test condition but does not include the development of new rule logic to harvest content from Tripwire Enterprise nodes or logic to parse or filter results.

Waiver Management

For Integrated Strategy customers, the MSE will create, and update waivers as directed by the Customer Lead or Customer Escalation contact. This includes the inclusion of on-boarded nodes in applicable waivers as well as adjustment to waiver expiration dates and/or comments.

Audit Assistance

For Managed Services and Integrated Strategy customers, the MSE will review the immediately preceding audit results with the Customer Lead and will analyze the results to assist the Customer Lead to develop a plan to address findings applicable to Tripwire products. Where applicable, the plan will include adjustments to monitoring strategy, reporting strategy, changes to reconciliation processes, or changes to the ongoing remediation plan. The Customer Lead will update reports and dashboards to enable the appropriate level of detail to be made available prior to the next audit.

Analysis and Problem Support

Defect Support

Problem resolution will be managed by the ExpertOps Service Center during business hours according to Tripwire's then-current Support Policy. The Managed Services Lead will coordinate problem resolution with customers who will confirm the resolution.

Reporting Analysis

The MSE will review the observed FIM change trends and integration behavior and look for unusual activity (e.g., significant spike in change rates, unusual frequently changed nodes entries, etc.). If any such activity is observed, the MSE will inform the Customer Lead during the regular service review.

Operational and Performance Reviews

Service Performance Reviews

The MSE will conduct a periodic review of the Tripwire environment to audit configurations, reporting, dashboards, and integrations. This is to ensure that there is a continuous cycle of improvement and optimization in the managed Tripwire environment. The service review will also include an overview of all event tickets, change requests and achievements towards SLA attainment.

CISO + Executive Review

For Integrated Strategy customers, the Service Delivery Manager will provide a report to key customer stakeholders that will include deployment health statistics as well as an overview of achievements towards the customer's objectives. This report will provide insight into the ongoing improvement and utility of the Tripwire environment.

Tripwire Prescriptive Content

The Managed Services team will provide a framework for FIM content, based on the Master Agreement, that produces a prescriptive prioritization for FIM changes. This framework will be used along with customer input to ensure that the most critical changes are identified promptly. Content prioritization strategy will be documented in the Operational Use Plan.

Operational Use Plan Update

The MSE will make recommendations for updates to the Operational Use Plan to allow the customer to maximize the automation capabilities that Tripwire Enterprise can provide. This can range from security and event alerting practices to change management process integrations to audit prep activities. Guidance starts during the implementation process and extends during the ExpertOps Service term. Working closely with the customer, the Service Delivery Manager will establish an Operational Use Plan that will provide a guide to the MSE in the following areas:

- ▶ Priority systems
- ▶ Event ticket creation procedures
- ▶ Promotion and waiver creation procedures and guidelines
- ▶ Agreement on tuning rules and preferences for notification (change management practices)
- ▶ Platform ownership
- ▶ Integration ownership

Service Description Updates

Tripwire reserves the right to update or otherwise change these Service Descriptions from time to time. Any changes to these Service Descriptions shall be effective upon publication by Tripwire, by way of posting such changes at: <https://www.tripwire.com/legal/managed-service-terms/>

Specific Services Included in Each Tier

Features	Hosted	Managed Services	Integrated Strategy
Management			
Console Maintenance	Included	Included	Included
Content Maintenance		Included	Included
Service Status Updates	Monthly meetings	Weekly meetings	Weekly meetings
Service Plan Development	Included	Included	Included
Asset Onboarding		Included	Included
FIM Content Tuning		Included	Included
Client Requests	24 hours/year	20 hours/month	Unlimited
User Management	Included	Included	Included
Custom App Monitoring Configurations		Up to four	Unlimited
Dashboard and Reporting Maintenance		Included	Included
Dashboard and Report Creation		Included	Included
Monitoring			
Console Health Monitoring	Included	Included	Included
Report Distribution		Included	Included
Event Handling		Included	Included
Task Completion		Included	Included
Agent Health	Reporting only	Included	Included
Business Process Integration			
TW Apps Management		Included	Included
TW Apps Licensing		DSR, Event Sender	DSR, Event Sender, TEIF
Remediation Prioritization			Included
Change Reconciliation (Promotion)			Included

Regulatory			
Policy Tuning and Guidance			Included
Waiver Management			Included
Audit Assistance		Included	Included
Management Consulting			
Service Performance Reviews	Annually	Every six months	Upon request (recommended every six months)
CISO + Executive Review			Included
Operational Use Plan Update			Quarterly
Tripwire Prescriptive Policies and Content			Included
Analysis and Problem Support			
Software Support	Tripwire Customer Center	Tripwire Customer Center + Managed Services Engineer	Tripwire Customer Center + Managed Services Engineer
Reporting Analysis		Included	Included
Agent Health Analysis		Managed Services Engineer	Managed Services Engineer
Product Deployments			
Policies Managed		FIM + two policies (standard policies only)	Unlimited
Real-time Functionality		Included	Included
Custom Policies			Included
Custom App Monitoring		Four custom apps rules	Unlimited