

Tripwire Remote Operations

Stop Operating, Start Analyzing

Count on Tripwire Remote Operations

- » Free up time for more strategic projects
- » Benefit from Tripwire's in-house expertise
- » Achieve faster and greater ROI
- » Know your implementation is running smoothly—always

Your Tripwire implementation captures data from thousands of systems with millions of unique elements. Figuring out which configurations, security events or changes need your attention can distract from more strategic business tasks—or from using the valuable intelligence it provides to manage IT risk throughout your enterprise. So if you'd like to spend more time managing your business and less managing software, Tripwire Remote Operations is just the ticket.

Move From Tactical to Strategic

With Tripwire Remote Operations, a Tripwire-certified team manages daily operation of your Tripwire® Enterprise, Tripwire Configuration Compliance Manager, Tripwire Log Center® and/ or Tripwire IP360™ implementation, keeps it up-to-date and makes sure it's operating optimally. Most importantly, we put critical security information in your hands when—and exactly how—you need it.

By letting us handle the day-to-day maintenance and long-term health that keeps your Tripwire implementation

running smoothly, you'll have more time to address mission-critical tasks like:

- » Measuring and reporting on your organization's changing and evolving risk posture;
- » Maintaining hardening guidelines and perimeter security;
- » If a breach should occur, being able to quickly provide relevant forensics data to identify what changed, related security events—and how to prepare for next time;
- » Demonstrating progress toward security and compliance goals; and

» Reviewing only unexpected changes rather than business-as-usual changes.

No Job Too Big—or Too Small

Of course we do the smaller tasks like ensuring your implementation is always up-to-date and that important systems don't slip through the cracks. But we can also help with more complex needs, like creating new rules to address emerging security threats, managing the health of integrations, meeting compliance and change management/remediation goals and maintaining accurate risk profiles for monitored assets. We work closely with you to focus our efforts and expertise where they're needed most.

No More Sleepless Nights

Because we live and breathe security and have deep expertise with Tripwire solutions, you'll have confidence that your systems and data are continuously protected. And that means no staying up at night worrying about a breach showing up on the front pages.

What to Expect From Your Tripwire Team

Your Tripwire remote operators perform a series of daily, weekly, monthly and annual tasks. This support is provided using a combination of secure remote connections, email, and telephone, making it both convenient and cost-effective. Review the list of provided activities to learn just how your Tripwire team can help. And remember: we're here for you, so count on us to be flexible enough to provide the help you need—the way you need it.

Gigabytes of Data Missing, But No Harm in the End

Hundreds of gigabytes of data went missing from a critical file server of an energy utility. Tripwire Remote Operations was able to identify the user who was responsible, determine that the activity was not malicious, and help restore the data. We also showed the client how to avoid a recurrence of the issue by tightening user permissions.

Web Site Defaced, But No Customer Data Lost

When an intruder used an unsecured administrator account to hack into a web server and deface a public-facing web page, we helped an international finance firm determine the changes caused by the hacker. We also determined, to the relief of the client, that no customer data had been compromised.

Stop Operating, Start Analyzing

Before starting the Remote Operations service, we update your applications and policies, apply mission-critical security rules and then co-develop your operational procedures. These steps help us best align your Tripwire implementation with your business policies and various needs.

At this point, you can stop operating your Tripwire installation, and start analyzing the wealth of data it provides. Rest assured that we're taking care of the day-to-day operational needs and long-term maintenance of your implementation, so you can reap the benefits of a secure, stable and compliant IT infrastructure.

Tripwire Remote Operations Essentials

If our standard Tripwire Remote Operations offering provides more than your organization needs, consider this alternative: combine a set of pre-defined core services with à la carte service selections. Tripwire Remote Operations Essentials provides only the services you need. No more. No less. Ask your sales representative for more details.



Remote Operations Performed With a Tripwire Enterprise Implementation

Weekly Tasks

Produce Trend Reports	Generates weekly trend reports that give you the insight you need to think proactively and strategically, and ensures reports are delivered to appropriate individuals.
Verify System Health	Reviews, adjusts and corrects operational settings to optimize Tripwire Enterprise Console, including scheduling scans and other actions.
Verify Promotion of Changes	Verifies that all detected changes are promoted based on your rules and processes—critical for producing the digital paper trail you need for forensic evidence if situations ever call for it.
Tune Change Monitoring	Identifies and excludes any noisy, business-as-usual changes from your monitoring process. Helps identify unmonitored resources that should be monitored and modifies rules accordingly, including adjusting their severity, parameters, descriptions or options.
Tune Configuration Assessment Policies	Examines and adjusts Tripwire Enterprise regulatory and operational policies and tests to accurately reflect your current and future needs.
Review Compliance Reporting	Ensures compliance reports run as required, have proper scope and are being delivered to the key stakeholders.
Verify Successful Backups	Checks the integrity and efficiency of backups of your Tripwire Enterprise database.
Manage User Access	Ensures appropriate user access and permissions, creates any necessary custom roles and helps develop User Home Pages.

Monthly Tasks

Update Implementation As Appropriate	Seamlessly applies newly released patches or updates issued from Tripwire, with no loss in operational efficiency or coverage of your Tripwire Enterprise implementation.
Review Database Growth Rate	Checks the Tripwire Enterprise change database to ensure proper growth rate and database integrity.
Construct New Rules	Imports or adjusts platform rules for emerging security and auditing needs.
Construct New Reports	Reviews and customizes the reports you depend on, ensuring that they continue to meet your needs. This review ensures you get the “gold” from Tripwire Enterprise—reports with critical, detailed information like ratio of approved to unapproved changes, or your trends in compliance scoring over a specific time period.
Review Waivers and Exclusions	Examines waived tests and excluded assets or tests to ensure they are still relevant and within the grace period.
Adjust Tripwire Enterprise Reconciliation	Ensures changes detected in Tripwire Enterprise are properly reconciled with your existing change ticketing system or other relevant systems and processes.

Annual Tasks

Evaluate Database Health and Capacity	Evaluates the data stores in the Tripwire Enterprise database to ensure it’s healthy, free of corruption, and can grow at the forecasted rate. These data stores hold the change information key for a successful audit, review trends, and for support forensic data investigations.
Upgrade Console	Upgrades the Tripwire Enterprise console to the latest version so you can benefit from every new and improved capability.
Archive/Cycle Out Old Data	Ensures your Tripwire Enterprise data store is appropriately archived or cycled out so you have more time to pay attention to your business needs.
Evaluate the Role of Tripwire Enterprise	Discusses the role of Tripwire Enterprise in your organization based on your organization’s needs and long-term goals. The findings of this evaluation help you achieve those goals and further your organization’s change process maturity.
Evaluate the Role of Tripwire Enterprise	Performs a comprehensive review of your implementation, including current usage, scope, the status of reports, and any other topic that can help you get more value from your implementation.
Help Prepare for Audits	Gathers and refreshes reports, reviews the coverage of your critical assets, and helps you prepare for annual audits.



Remote Operations Performed With A Tripwire Configuration Compliance Manager Implementation

Weekly Tasks

Produce Trend Reports	Generates weekly trend reports that give you the insight you need to think proactively and strategically, and ensures reports are delivered to appropriate individuals.
Verify System Health	Reviews, adjusts and corrects operational settings to optimize the Tripwire Configuration Compliance Manager (CCM) CCM Console, including scheduling scans and other actions.
Tune Change Monitoring	Identifies and excludes any noisy, business-as-usual changes from your monitoring process. Helps identify unmonitored resources that should be monitored and modifies rules accordingly, including adjusting their severity, parameters, descriptions or options.
Tune Change Monitoring	Identifies and excludes any noisy, business-as-usual changes from your monitoring process. Helps identify unmonitored resources that should be monitored and modifies rules accordingly, including adjusting their severity, parameters, descriptions or options.
Tune Configuration Assessment Policies	Examines and adjusts Tripwire CCM regulatory and operational policies and tests to accurately reflect your current and future needs.
Review Compliance Reporting	Ensures compliance reports run as required, have proper scope and are being delivered to the key stakeholders.
Verify Successful Backups	Checks the integrity and efficiency of backups of your Tripwire CCM database.
Manage User Access	Ensures appropriate user access and permissions, creates any necessary custom roles and helps develop User Home Pages.

Monthly Tasks

Update Implementation As Appropriate	Seamlessly applies newly released patches or updates issued from Tripwire, with no loss in operational efficiency or coverage of your Tripwire CCM implementation.
Review Database Growth Rate	Checks the Tripwire CCM change database to ensure proper growth rate and database integrity.
Construct New Rules	Imports or adjusts platform rules for emerging security and auditing needs by using the Tripwire CCM policy editor.
Update Reporting	Reviews and optimizes the reports you depend on, ensuring that they continue to meet your needs. This review adjusts filters and creates custom search queries that help you get the right information from your Tripwire CCM Console.
Review Waivers and Exclusions	Examines waived tests and excluded assets or tests to ensure they are still relevant and within the grace period.
Review Integrations	Ensure that external product integrations are working as expected.

Annual Tasks

Evaluate Database Health and Capacity	Evaluates the data stores in the Tripwire CCM database to ensure it's healthy, free of corruption, and can grow at the forecasted rate. These data stores hold the change information key for a successful audit, review trends, and for support forensic data investigations.
Upgrade Console	Upgrades the Tripwire CCM Console to the latest version so you can benefit from every new and improved capability.
Archive/Purge Out Old Data	Ensures your Tripwire CCM data store is appropriately archived or cycled out so you have more time to pay attention to your business needs.
Evaluate the Role of Tripwire Configuration Compliance Manager	Discusses the role of Tripwire CCM in your organization based on your organization's needs and long-term goals. The findings of this evaluation help you achieve those goals and further your organization's change process maturity.
Review Use of Tripwire Configuration Compliance Manager	Performs a comprehensive review of your implementation, including current usage, scope, the status of reports, and any other topic that can help you get more value from your implementation.
Help Prepare for Audits	Gathers and refreshes reports, reviews the coverage of your critical assets, and helps you prepare for annual audits.



Remote operations performed with a tripwire Log Center implementation

Weekly Tasks

Review New Assets	Ensures that new assets are properly grouped, configured and integrated with Tripwire Log Center®.
Tune Correlation Rules and Alerts as Necessary	Identifies potential events to exclude from monitoring and identifies those not being monitored that should be. Adjusts associated event alerts as needed to ensure you receive the proper notifications.
Verify Console Health	Reviews operational metrics of the Tripwire Log Center Console and makes any necessary adjustments or corrections.
Review Database and Audit Logger Growth Rate	Regularly checks the Event database and Audit Logger data store growth rate to ensure early detection of potential issues as evidenced by abnormal storage consumption.
Verify Backup Run	Where possible, verifies successful backup of the Console application and Event Database(s).

Monthly Tasks

Patch Application Managers and Consoles	Determines the impact and criticality of any available patches and installs as recommended.
New Asset Construction	Adds, groups, and configures new assets, and creates normalization rules, as needed.
New Correlation Rule and Alert Construction	Creates or enables correlation rules and develops new alerts to keep pace as your environment and monitoring needs change.
New Report and Dashboard Construction	Creates additional reports and/or dashboards to keep pace as your environments and monitoring needs change.
User Administration Tasks	Adds or adjusts users and roles as needed to support effective separation of duties within the environment.

Annual Tasks

Comprehensive Review of Application Scope	Performs a review of all aspects of the Tripwire Log Center implementation to ensure that its monitoring the desired systems, capturing useful information, and notifying the proper individuals.
Evaluate the Strategic Role of Tripwire Log Center	Performs an evaluation to ensure that Tripwire Log Center supports your strategic business goals and continuous improvement initiatives.
Upgrade Managers and Consoles	Performs application upgrades and assists you with migration and training issues.
Archive/Cycle out Historical Log Data	Cycles out data that is no longer considered valuable (retired assets, logs, etc.) in accordance with your organization's data retention policy.



Remote Operations Performed With a Tripwire IP360 Implementation

Weekly Tasks

Perform on-demand validation scans	On-demand vulnerability scans will be executed to help validate that remediation has occurred.
Report Generation	Technical detail reports will be generated on a weekly basis and provided to the customer lead and/or designated network owners. (Requires Tripwire Security Intelligence Hub (SIH))
Network Configuration Updates	Creation of new networks and balancing of scan activity between device profilers for optimal scan performance and accuracy. Review and adjust overlapping IP ranges and resolve duplication.
Review Scan Accuracy	Review any concerns about vulnerability coverage and accuracy. Engage necessary resources to resolve and improve.
Adjust Scan Profiles	Adjust scan profiles to alleviate scan performance problems or improve asset discovery and fingerprinting.
Perform ASPL Content Updates	Tripwire provides ASPL updates on a weekly basis. Tripwire Remote Operations will ensure that updates are applied properly and that important changes are identified to the customer.
Verify Successful Backups	Checks the integrity and efficiency of backups of your Tripwire IP360 VnE. Validate that backups are pushed off of the VnE Manager.
Manage User Access	Add and remove users, updating permissions as needed.
Perform VnE Maintenance	As with any Enterprise-class application, Tripwire IP360 benefits from occasional maintenance activities and performance review.
Update to Global Excludes	Review and update global exclusions to scanning.

Monthly Tasks

Update Implementation As Appropriate	Seamlessly applies newly released patches or updates issued from Tripwire, with no loss in operational efficiency or coverage of your Tripwire IP360 implementation.
Review Database Growth Rate	Checks the Tripwire IP360 vulnerability result database to ensure proper growth rate and database integrity.
Construct New Rules	Consultation on the creation of custom vulnerability rules.
Device Profiler Changes	Review and revise Device Profiler configuration and placement.
Review Console Logs	Review daemon and service logs to identify potential problems.
Adjust Alerting	Tripwire IP360 has the capability to alert on various host, score, and scan conditions. Tripwire Remote Operations will review these alerts and adjust thresholds and configurations based on customer feedback.
Monthly Reporting	Tripwire SIH differential reports will be delivered to the customer designated network owners.

Annual Tasks

Strategic Review	Review of organizational initiatives and review any product or coverage gaps. Perform a comprehensive review of your implementation, including current usage, scope, the status of reports, and any other topic that can help you get more value from your implementation.
Upgrade Console	Upgrades the Tripwire IP360 to the latest major version so you can benefit from every new and improved capability.
Review of Integration	Review integrations to determine how Tripwire can more effectively distribute data as well as leverage external data. Consider relevant changes to integration configurations.
Configuration Data Export	For many Tripwire Customers, Tripwire IP360 operates as an authoritative record of networks and asset locations. In essence, we are the network system of record. Tripwire Remote Operations will work with the customer to export configurations to ensure the availability of this configuration information long term.
Major VnE Changes	Often, organizational changes will introduce challenges with accountability and associated Network configurations. Year-end is an excellent time to consider these changes and make updates to Tripwire IP360 that will support the natural course of business. Tripwire Remote Operations will work closely with the customer to adjust configurations based on goals for the upcoming year.



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](#)