DATASHEET

Remediation Manager

Automate Remediation. Reduce Costs. Streamline Compliance.

Successful IT compliance requires IT Security and Compliance teams to adopt a known IT security standard and continually check the organization's compliance status against it. It also requires IT Operations to efficiently—and with low impact on availability—fix deviations from that standard. Unfortunately, these teams aren't always in synch.

Operations focuses primarily on keeping systems and services available, while Security and Compliance focus on keeping IT configurations secure, ready, and able to pass internal and external audits. When security and compliance teams detect configuration errors that introduce risk or non-compliance, they need to work with operations to remediate the issue. This process can be intricate, time-consuming and costly, and often results in delayed response or lost remediation requests.

Tripwire® Enterprise's Remediation Manager changes all that, with a work order-based system that lets users from each IT team seamlessly communicate across organizational boundaries and automatically remediate most security and compliance configuration errors. Remediation Manager provides a timesaving, cost-effective means of correcting hundreds of seemingly mundane, yet important configuration errors to keep systems secure, compliant and audit-ready.

How Does Remediation Manager Work?

Remediation Manager is an add-on module for Tripwire Enterprise that uses work orders, role-based workflow features and automated scripts to ensure that configuration errors get fixed quickly, while simultaneously tracking duties and sign-offs across various remediation activities. Users can launch Remediation Manager directly from their custom Tripwire Enterprise home page to review all current remediation work orders at a glance.

When Tripwire Enterprise's Policy Manager detects a failed configuration test, an IT Security or Compliance team member can easily create a work order and assign roles. This role-based system ensures that the right individuals approve, deny, defer or execute the work orders tracked by Remediation Manager.

Once the work order has been created, the person assigned the remediator role can execute remediation scripts to repair configurations. Work order status can be tracked in real-time through the user interface, color-coded status indicators, and a remediation report. With Remediation Manager, IT can rapidly put systems into a policy-aligned, compliant state—whether in pre-deployment or production settings—and ensure remediation requests are addressed in a timely manner and never get lost.

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

Remediation Manager Fits Modern Security strategies

Prevent-Detect-Correct is an established strategy that defines the worldview of modern IT security. With Remediation Manager, Tripwire Enterprise adds the critical "Correct" component to its already robust capabilities. It's the ideal solution for IT security teams, letting them:

- Prevent exploits and breaches by using Policy Manager to assess the security posture of almost every configuration and identify settings that introduce risk and non-compliance.
- Detect with File Integrity Manager by monitoring almost any asset in the IT infrastructure to detect even minute and seemingly insignificant changes that weaken security or indicate an attack in progress.
- Correct with Remediation Manager by automating repair and management of configuration errors identified by the Policy Manager.

Remediation Manager Features and Benefits

Automated Remediation

Depending on the platform, the Remediation Manager automates repair of up to 98 percent of the configuration errors discovered by the Policy Manager when testing configurations against policies and standards such as PCI, CIS, FISMA, DISA, NERC, and more. Built-in scripts automatically remediate failing configurations with a level of automation that rapidly and cost-effectively addresses errors without additional staff or financial resources.

Role-based Workflow

With Remediation Manager, IT teams can cross organizational boundaries to ensure configuration errors noted by IT security and compliance get in front of the correct IT operations staff. When remediation work orders are created, they can be assigned to individuals for approval, deferral, denial and execution—a feature that also supports the critical separation of duties protocols required by many security standards and regulations.

Work Order-based Remediation

Because Remediation Manager relies on work orders that are available across IT organizational boundaries, IT has an intuitive and streamlined way to track and communicate remediation issues. When someone creates a remediation work order, they assign the various roles to one or more individuals, and those individual now see their responsibilities in their Remediation Manager user interface.

Real-time Work Order Status

Losing remediation requests in the "IT black hole" is no longer an issue with Remediation Manager. When someone creates a work order, they can track its status in real time to see if it has been approved, denied, or deferred, or if remediation is running. Color-coded status indicators even provide at-a-glance status updates.

Remediation Reports

IT teams can easily access a complete set of remediation reports through Remediation Manager, while stakeholders in IT operations, security or compliance can easily receive the reports they need. Built-in reports include "Remediation Work Order Status" and "Remediation Run Details." Separate reports can also be generated for configuration assessors and remediation approvers.

Independent User Interface

As an add-on module, Remediation Manager can be launched with or without full access to Tripwire Enterprise, allowing users without knowledge of Tripwire Enterprise to effectively use Remediation Manager without extensive training and within their own workflows.

Policies and Support

Policies and security standards currently covered by Remediation Manager include:

- Payment Card Industry Data Security Standard (PCI DSS)
- Center for Internet Security (CIS)
- Defense Information Systems Agency (DISA)
- North American Electric Reliability Corporation (NERC)
- Federal Information Security Management Act (FISMA
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- And many more

Platforms supported by Remediation Manager include:

- Windows
- Red Hat Enterprise Linux
- SUSE Linux
- Solaris

For complete details on supported policies and platforms, visit www.tripwire.com.

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*: News, trends and insights at** tripwire.com/blog
Connect with us on LinkedIn, Twitter **and** Facebook