

---

## Managing Change in IT Infrastructures

Using Tripwire Software to Gain Visibility and Close the Verification Loop in Change Management Strategies

---

- page 2**      The Impact of Change—Good or Bad?
- page 2**      Visibility or Lack Of?
- page 3**      Managing Change for Positive Service Impact
- page 5**      Integrating Tripwire Configuration Audit and Control into Change Management Processes
- page 5**      Tripwire Configuration Audit and Control and Remedy Change Ticket Logging
- page 8**      Closing the Loop

## The Impact of Change—Good or Bad?

Changes to a server, router, or switch configuration can have a major impact on the level and quality of IT services delivered. The question is what kind of impact? As enterprise network infrastructures become geometrically more complex, IT teams are burdened with demands, and budgets dwindle, costs and operational risk increase. Without a way to know when change occurs and whether it's desired, not desired, accidental, benign, malicious, intentional, or originating from inside or outside, IT teams had few options for preventing negative consequences and minimizing damage.

Today however, Tripwire® configuration audit and control solutions deliver visibility into service-affecting changes, as well as the capabilities to quickly detect change, assess its impact, and mitigate risk. As a vital component of operational best practices, Tripwire solutions are integrated with a wide range of enterprise systems to close the verification loop on change management. And in the process, enable organizations to increase security, instill process accountability, and improve system availability.

## Visibility or Lack Thereof?

How does the IT team know when something changes on a router or server? Usually, only when negative consequences result. At that point, the team is forced to react quickly, without much visibility into what caused a change. During the time it takes to troubleshoot, isolate the problem, and respond appropriately, the potential for serious damage to an organization increases dramatically. Traditional security solutions have been focused on identifying security breaches originating externally to the organization. For that reason, they are not able to detect or pinpoint internal changes, report exactly what changed, how it changed, or who originated the change.

## One Small Change, One Major Disaster

While external hackers represent a threat, a far larger threat is change initiated from inside the organization. Industry analysts IDC and Gartner Group estimate that 70 to 80 percent of all changes resulting in downtime or reduced operational capabilities are initiated by people within the organization, and most of those changes are accidental or unintentional.

## Causal Factors of IT Downtime

Percentage of Incidents



One small change to a server or network device can result in a huge impact to business operations. For example, in January 2001, a technology company's technician changed a router configuration in its edge network. The router's performance remained stable, packets still reached the DNS servers, and internal networks still worked properly. However, outside traffic wasn't getting through, and millions of users couldn't reach any of the firm's public sites. It took 22 hours for network technicians to track down the mistake and fix it—even with a layered security strategy in place. When networks are compromised—even accidentally—they can't work.

### Configuration Audit and Control Sees *All* Change

Change to an IT infrastructure is—and will continue to be—constant. The goal is not to minimize or prevent change, but to maintain systems' operational integrity by recognizing when change occurs and verifying that it is both authorized and purposeful. Tripwire configuration audit and control solutions monitor key files and configurations of servers and network devices, detect external and internal changes, alert IT staff, and provide detailed reports for rapid restoration of systems to a known good state. By providing visibility into change, Tripwire software allows IT teams to proactively plan for change, monitor for unexpected change, and validate that desired change does indeed occur. As a result, operations managers can manage based on fact rather than faith.

Tripwire software provides configuration audit and control capabilities through:

- Establishing state—Tripwire software establishes a digital inventory of known good files and their attributes and uses it as a baseline for monitoring changes.
- Discovering state change—the software monitors files and their attributes, comparing them against the baseline. Changes are immediately pinpointed and appropriate IT staff can be notified by email or pager.
- Recovering from undesired change—detailed reports and audit logs provide IT with a fast recovery path when change occurs. Desired changes can be verified and rolled into the baseline. If a change is not desired, the software enables rapid restoration of files to a known good state.
- Guarding the guard—Tripwire software can be used with measures such as personnel policies, change and configuration management, identity management, and perimeter security products to control change across the enterprise, as well as to verify the integrity of other security products themselves.

Implementing Tripwire configuration audit and control solutions allows the IT team to establish policies and gather information for tracking planned changes. The Tripwire policy file can be configured to define which attributes to monitor, identify who makes changes, identify when a file has changed, prioritize change severity, and specify where to route integrity alerts. When a change does occur, Tripwire software can report it using email, SNMP, text output, sys/event log, or a combination of methods. Rapid notification enables the IT team to take quick action to minimize risk.

### Managing Change for Positive Service Impact

“Operational change management is a prerequisite to providing high IT service quality. It is not optional,” says the Gartner Group (*Best Practices for Operational Change Management*, March 6, 2003). Organizations typically implement infrastructure changes to improve overall service, correct service-affecting deficiencies, or reduce service costs. Having a plan for proposing, approving, implementing, and verifying changes helps ensure that desired changes are made successfully and undesired changes are quickly caught and remedied. When change management is implemented at a high level, the benefits radiate out to all enterprise applications and users.

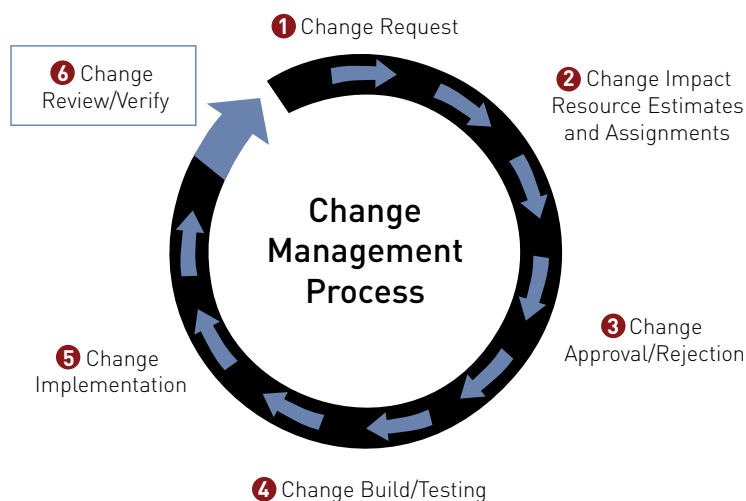
The benefits of change management include:

- Increased staff efficiency because they can immediately detect change and act to minimize consequences
- Reduced server and network device downtime because service-affecting change can be remedied quickly
- Reduced Mean Time to Repair (MTTR) because enforcing consistent configurations and repeatable builds results in increased reliability
- Improved security because all threats can be accurately detected and identified
- Reduced IT costs because validated changes eliminate the need for manual configuration and rework
- Trusted audit data because it is measured against a known good state
- Increased control over *ad hoc* changes and accountability for undocumented changes

### Establishing Change Management Processes

Typically, the first question of someone diagnosing a problem is "what changed?" With a change management process in place, that question is far easier to answer.

#### Closed Loop CM Process



Change management is a process made up of people, software, and procedures. Properly followed, the process results in the above-mentioned benefits. The process works as follows:

- (1) A change is requested—for example, install a security patch to a Windows XP server
- (2) Requested changes are reviewed, the impact assessed, and resources estimated and assigned
- (3) Changes are either approved or rejected
- (4) If approved, changes are developed and tested
- (5) Change is implemented into production
- (6) Changes are verified and reconciled

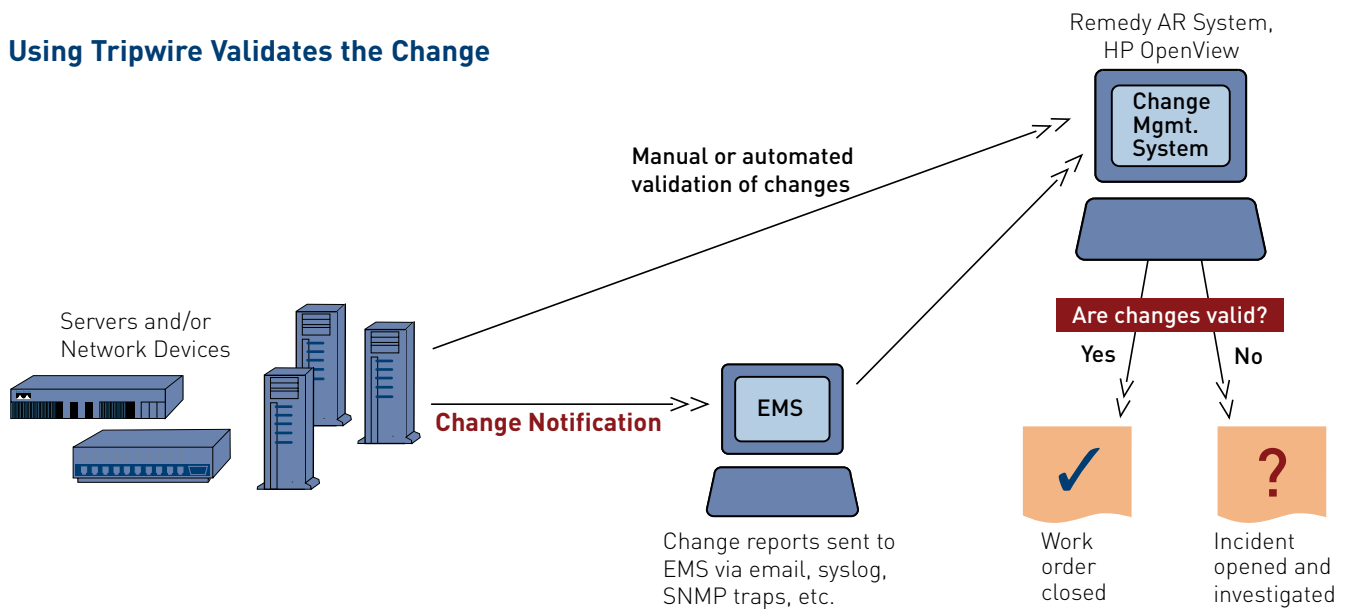
## Integrating Tripwire Configuration Audit and Control Solutions into Change Management Processes

Even armed with an arsenal of scripts, network management applications, and change management policies, IT professionals must continually reconfigure, install, and patch software across a myriad of systems—servers, network devices, databases, workstations and applications. Yet many existing change management or ticketing systems cannot effectively verify, validate, and reconcile changes.

As part of operational best practices, Tripwire software provides scalable, centralized management for thousands of Tripwire systems, enabling staff to quickly verify that desired changes, reconfigurations, and software patches or upgrades are implemented correctly across a network.

Many customers deploy Tripwire into their change management processes by integrating it with systems such as HP OpenView, Remedy, IBM Tivoli, Micromuse Netcool and others. Tripwire’s standard integration methods and specially designed “plug-ins” make it relatively easy to implement configuration audit and control with existing systems.

### Using Tripwire Validates the Change

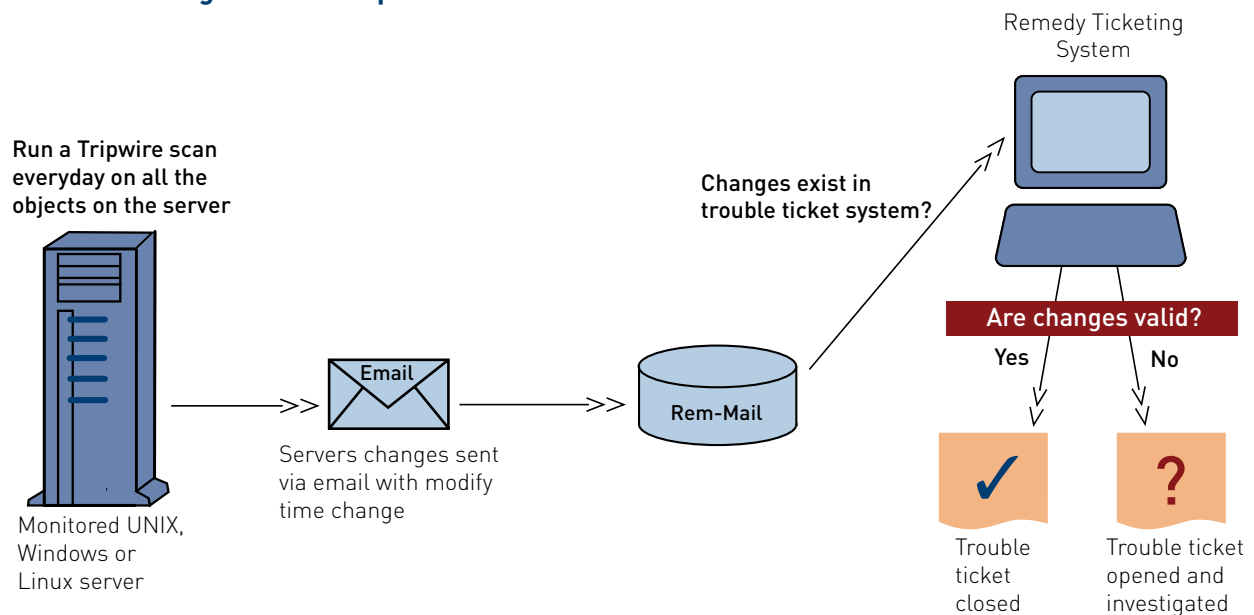


Tripwire uses email, syslog, SNMP traps, plug-in modules, or XML reports to send file change information to EMS or change management systems. Upon receiving the Tripwire violation report, the change management system looks at the changes for each host and attempts to match file changes with open work orders. If a match occurs and is verified, then the work order is closed and the Tripwire baseline database is updated. If there is no open work order, then an incident is issued and investigated to identify the cause of the change. Once the change is satisfactorily explained, the new incident is closed.

### Tripwire Configuration Audit and Control and Remedy Change Ticket Logging

One Tripwire customer uses Remedy software to manage changes and service incident tickets. The company deployed Tripwire software to alert, track, and close the loop on verifying these changes. This customer uses email integration to send integrity alerts to the Remedy system for validation and reconciliation.

### Trouble Ticket Integration Example



Tripwire software scans all objects on the monitored servers daily. All detected changes are reported via email, and the report details all changes to the monitored servers, including the modify time attribute associated with each file change violation. The email is then parsed and the report sent via Rem-Mail directly into the Action Request System (ARS). Here it is reviewed to see if any violated files were issued change tickets within a specified time period of the modified time reported by Tripwire software. If the Remedy system verifies that a file change request was made within the given timeframe, then the change is verified and the ticket is closed. If Remedy does not detect a change request for the violation, a trouble ticket is opened to investigate the reason for the change.

### Implementation Workflow Instructions

When integrating Tripwire software into a change management system, the three following workflow processes should be followed to ensure maximum effectiveness and change management accuracy.

#### *Expected and Planned Changes*

- (1) A change is implemented in a test location and validated
- (2) Tripwire software conducts an integrity check on test servers or network devices
- (3) A Tripwire report describes all file changes, including modifications to existing files
- (4) The change owner provides the change control team/manager with list of files to be changed and reason/impact of change via Remedy ticket
- (5) The change is approved

- (6) The change is implemented on pre-production systems
- (7) Tripwire software runs an integrity check on pre-production systems and compares against requested change
- (8) The pre-production management or operations team reviews ticket and Tripwire report for consistency, then updates the Tripwire database
- (9) A stable check period is completed in pre-production
- (10) Change request moves to production systems along with Remedy ticket ownership
- (11) Changes occur on production systems
- (12) Tripwire integrity check is completed on production systems
- (13) Tripwire validates change and the Remedy ticket is closed, automatically or manually

#### ***Emergency Changes Workflow***

- (1) A change is required immediately in production systems
- (2) The change occurs or a Remedy ticket is opened to facilitate emergency change
- (3) Tripwire validates the change on production system
- (4) A Tripwire report is reviewed and compared against the open ticket for emergency change by operations team
- (5) Operations team closes ticket and updates Tripwire database

#### ***Unexpected Changes Workflow***

- (1) Tripwire reports violations on production systems based on a scheduled integrity check
- (2) The operations team checks Remedy for host showing violation to match open ticket
- (3) If match exists, the operations team closes ticket
- (4) If a match does not exist, the operations team changes Remedy ticket owner to operations Level 2 team
- (5) Operations Level 2 team conducts a logical investigation for file system change
- (6) Operations Level 2 team closes ticket if logical solution found
- (7) Operations Level 2 team passes Remedy ticket ownership to security/incident response team if a logical solution not found
- (8) Security/incident response team reviews the issue and resolves file issue and/or closes ticket

### Technical Information for Tripwire/Remedy Integration

The following items are required for integrating Tripwire software into the Remedy change management process:

- Tripwire is installed on the test lab, pre-production, and production systems
- Tripwire policy file has data classified by severity and owner to determine data owners
- Mail servers or relays are installed on each Tripwire-equipped system
- Remedy email incident generation is installed and properly working
- The Tripwire agent is configured properly to send integrity alerts from \$(HOSTNAME)@companydom.com
- The Tripwire agent is configured properly to send integrity alerts to tripwire servers@companydom.com
- Tripwire email report level 3, which includes information on server, timestamp, added, deleted, or changed objects and the expected state of each object compared to the observed state of each object that was changed
- Tripwire Manager console is available to management, security, and operations teams in operation center
- Management Team—Tripwire Manager install should cache no passwords, or be view only
- Operations Team—Tripwire Manager install should cache only local pass-phrases, allowing for database maintenance of agent machines, but not configuration changes
- Security Team—Tripwire Manager install should cache only site pass-phrases, allowing for configuration changes by a separate group, but not database maintenance
- Each Tripwire Manager machine should have a unique pass-phrase
- Consistent backup of console.dat, console.dat.bak, console.key, and TWManager.cert from each Tripwire Manager machine for immediate rebuild to previous state

### Closing the Loop

Tripwire configuration audit and control solutions play a pivotal role closing the loop on change in IT infrastructures. Designed to enhance IT best practices and existing change management systems, Tripwire solutions deliver greatly increased visibility into change. As a result, IT teams gain fundamental business control over their infrastructures, costs, and efficiencies—as well as provide the organization's business units with high service levels, trusted audit data, and improved security.

For more information about Tripwire configuration audit and control solutions, visit [www.tripwire.com](http://www.tripwire.com).



[www.tripwire.com](http://www.tripwire.com)

US TOLL FREE: 1.800.TRIPWIRE MAIN: 503.276.7500 FAX: 503.223.0182  
326 SW Broadway, 3rd Floor Portland, OR 97205 USA

[www.tripwire.com/europe](http://www.tripwire.com/europe)

TRIPWIRE UK: +44 207 618 6512 FAX: +44 207 618 8001  
78 Cannon Street London EC4N 6NQ UK