
What's Good for Security is Good for Operations

Why Configuration Assessment Followed by Change Auditing Is Key to Operational Stability

- page 2** Establishing a Good, Secure Starting Point
- page 3** The Need for Complete Coverage for Detecting Change in the Data Center
- page 5** Proving Compliance: The Need for Trusted Audit Data
- page 5** Circumventing Attacks
- page 6** Configuration Assessment and Change Auditing for IT Infrastructures
- page 7** Conserving a Valuable IT Resource: People
- page 8** Security and Operations—Fundamental Business Controls

Whoever coined the phrase “a small change can make a big difference” probably had no idea how much that phrase would resonate with today’s network administrators and IT managers. The ramifications of one small change to a company’s critical servers or network devices like routers, switches, and firewalls, depend on whether the change is desired or not. Without a way to know when change occurs and whether it’s intentional or accidental, benign or malicious, or originates from inside or outside, IT teams have few options for preventing negative consequences and minimizing damage. More importantly, it’s difficult to know whether a change was good or bad, no matter its origins or intent, if IT and security have no way of establishing a trusted, secure state as a baseline for a before and after comparison. And with the increasing popularity of meeting business needs through rapid deployment of virtual machines, achieving and maintaining the integrity of the data center in the face of change is becoming even more complicated.

Fortunately, solutions are available to meet these challenges. IT can employ a configuration assessment solution that assesses the data center against trusted industry standards and internal operational policy, informing IT of security issues detected in both physical and virtual environments and providing details so they can modify files and configurations to get the data center into a trusted state. IT can also use a change audit solution to monitor the entire data center, detecting any departure from the trusted state, and alerting IT of unauthorized or out-of-compliance change. When such change is detected, IT can pinpoint where it occurred, rapidly restore critical systems when necessary, and preserve service quality in the production environment.

Tripwire offers an industry-proven configuration audit and control solution—Tripwire Enterprise—which includes both configuration assessment and change auditing, enabling organizations to achieve and maintain a sound security posture for the entire data center, even the virtual elements. By employing sound security practices that include Tripwire Enterprise, organizations reduce IT costs, significantly improve operational stability, and minimize security risk.

Establishing a Good, Secure Starting Point

In the past, it was fairly accurate to say that each server and network device was deployed with a known configuration. The reality for today’s business is that they contend with virtual environments that allow virtual machines to spin up and down without IT ever knowing. IT also assumes responsibility for servers and devices inherited through mergers and acquisitions. Add that to remote workers working through VPNs, the company network being connected to the Internet, and complex e-commerce systems, and it’s easy to see why IT often feels as though they’ve lost control over the data center.

Case in Point

One company’s information security executive related that when he came on board, each of his organization’s 200+ machines were configured differently from the rest and were not properly maintained. While the company had a lot of operations staff focused on deployment, there were no system administrator resources dedicated to maintaining machines. The CIO summed up what many CIOs feel by stating that, “when I joined, it was clear that, well, the machines weren’t really ours anymore.”¹

Regaining a Sense of Control

Gartner Group states that, “Operational change management is a prerequisite to providing high IT service quality. It is not optional.”² While most IT managers would agree with that statement, they have been unable to fully and effectively manage change that affects operations because they lack a means of establishing a good state—a secure starting point from which to manage change.

Tripwire Enterprise addresses the need for configuration assessment, providing out-of-the-box policies that proactively test systems against benchmarks from the Center for Internet Security (CIS), the National Institute of Standards and Technology (NIST), and the Defense Information Systems Agency (DISA). These benchmarks include tens of thousands of configuration assessments for configurations, enabling automatic and sustainable security policy testing. In fact, the CIS policies alone block 80 to 95 percent of known security vulnerabilities, providing IT a powerful jumpstart in securing the data center. In addition, CIS recently released security policies for VMware ESX Server to address the numerous security vulnerabilities introduced by virtualized environments. With proactive configuration assessment, IT enables automatic, sustainable policy compliance testing that assists IT in getting the data center into a trusted and secure state.

But getting the data center into a known and trusted state is just half the battle. Once IT has accomplished that, the second half is maintaining that state.

The Need for Complete Coverage for Detecting Change in the Data Center

Numerous change and configuration management solutions are available for pre-approving and scheduling requested changes such as device reconfigurations, software patches, and upgrades. However, when it comes to detecting and analyzing *unwanted* changes on systems *after* they occur, most organizations have no solution in place or expect traditional security tools—perimeter defenses, authentication servers, and physical measures—to handle the risks unauthorized changes introduce. This is where well-intended security efforts fall short. Most security solutions assume that changes are the result of activities by malicious outsiders. In truth, industry analysts IDC and Gartner Group estimate that 70 to 80 percent of all change resulting in downtime or reduced operational capabilities *is initiated by people within the organization*, and most of those changes are accidental or unintentional. As a result, many traditional security solutions cannot detect internal changes, pinpoint them, or report what changed, how it changed, and who made the change.

One Minor Change, One Major Disaster

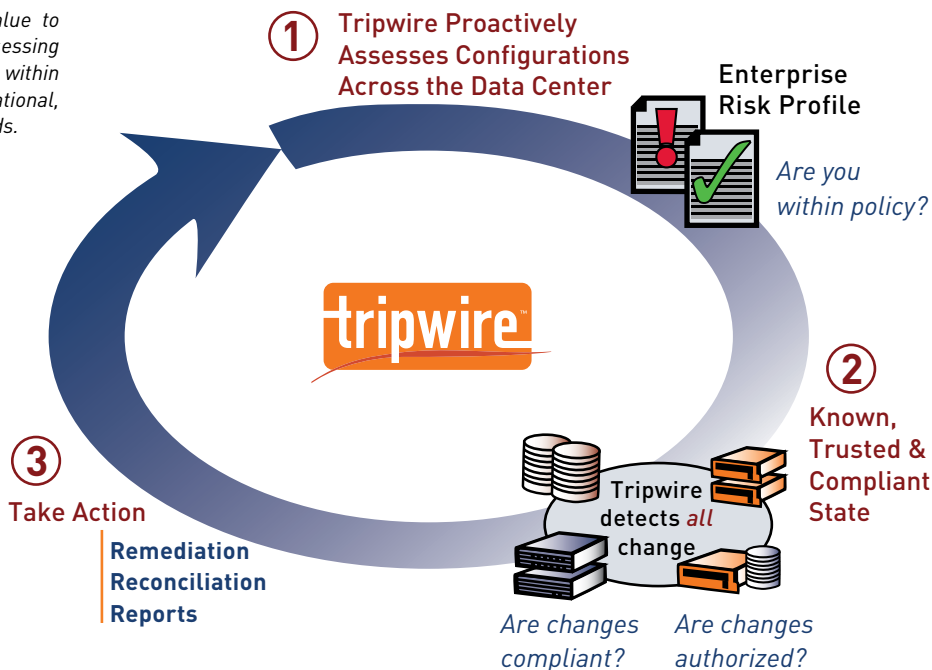
Several years ago, a technician at a major technology company changed the configuration of a router in its network border. The router's performance remained stable, packets could still reach the DNS servers, and the internal networks still worked properly, yet outside traffic wasn't getting through and 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. The company employs a layered security strategy, but as the example illustrates, that's not always enough. When configuration change compromises a network—even accidentally—the network still doesn't work. IT staff need to know when change occurs, and they have to be able to figure out exactly what changed and whether that change complies with operational policy and industry standards.

Stability Depends on Integrity Assurance

Stable business operations rely on both security *and* the ability to manage desired and undesired change. In short, they rely on integrity assurance best practices—best practices that form the foundation for the configuration assessment and change auditing provided by Tripwire Enterprise.

Had the technology company with the problem described above had Tripwire, the company first would have configured the router in a known and trusted state based on an initial configuration assessment against industry and operational standards. This assessment would provide the company detailed information about any security compromise the router's configuration introduced so that if needed, IT could modify the configuration to achieve a secure state. Once the router was configured in a trusted and secure state, Tripwire would capture a snapshot of that state as a baseline for change auditing. Tripwire would then automatically detect change in the network device or server from that caused it to depart from that baseline state, alerting administrators to *any* change, good or bad. Tripwire would test those changes against authorized business activity and change policy, alerting IT to any unauthorized or out-of-policy change so that they could initiate corrective action.

Tripwire delivers immediate value to your compliance efforts by assessing every change as authorized, within policy and compliant with operational, regulatory and security standards.



Contending with Integrity Drift

Even when configurations start in a known, good state, over time and with each change, these configurations are subject to integrity drift. Without change control practices in place, as configurations change, patches are installed, communication settings adjusted, and software is upgraded, IT loses visibility into exactly what is running on a given system. And, the ability to restore or rebuild a system to a known good state is eventually lost. Loss of visibility equals loss of control. IT staff may not be able to tell immediately when systems have been compromised or administered inappropriately. When downtime *does* occur, it is extremely difficult to diagnose and remedy the correct cause. Not only must extra time and staff be dedicated to fix the problem, unplanned downtime subjects the business to revenue loss, increased vulnerability to attack, damaged customer relations, and even fines or customer concessions.

The value of configuration assessment followed by change auditing is not to minimize or prevent change—but to maintain the operational integrity of IT systems by recognizing when change occurs and verifying that it is both authorized and purposeful.

Proving Compliance: The Need for Trusted Audit Data

The ramifications of limited visibility reach beyond having to deal with an attack or outage. Most large organizations perform regular audits of their IT systems, and many must demonstrate compliance with outside regulators, agencies, and even customer requirements. Visibility of all change activity—with associated metrics—is quickly becoming an IT audit requirement. With configuration assessment against industry standards, compliance regulations, and internal policy, IT can first ensure that the data center achieves a known and compliant state. When followed up with audit and control solutions, IT can manage by fact instead of managing by myth or assumption. And equally important, an audit trail that shows detailed information on all changes, including those that deviated from the compliant state, and a record of how IT resolved any improper change greatly simplifies proving compliance.

Consistent, Reliable Proof

Configuration audit and control solutions capture system changes, providing a common repository of change data so that IT management can produce a history of change activity and a complete, documented audit trail. The ability to record and time-stamp changes enables users to verify that necessary changes were indeed implemented correctly and demonstrate that systems have remained in a known good state over a set period of time. In addition, data is automatically secured for forensics investigations and incident response—all without requiring human intervention, so auditors and investigators can trust audit data. Tripwire enables consistent change and configuration control across production systems with the ability to implement automated actions. The software provides capabilities such as automatic recovery, scripted responses to specific alerts, and notification of intended changes back to authorized IT processes and personnel, giving IT the powerful tools it needs to know exactly what has changed across an infrastructure. And prove it.

Circumventing Attacks

Security systems have difficulty fending off malicious denial of service (DoS) attacks. DoS attacks can flood servers and networks with traffic or modify system configurations in order to deny access to legitimate users. According to information released in October 2001 from the U.S. government-funded Computer Emergency Response Team/Coordination Center (CERT/CC), DoS attacks are increasingly focusing on routers, which can be easily taken over when poorly configured or administered.

Router Misconfiguration—an Open Invitation

An organization's network routers communicate with routers in communication carriers' infrastructures to move traffic efficiently over the Internet. A compromised or misconfigured router can "cause chaos by advertising itself as the best path to an unrelated network. That's because routers using Border Gateway Protocol (BGP) implicitly trust their neighbors on the Internet—they don't ask for any sort of digital identification. Using such digital forgery could allow an attacker to redirect traffic, to wiretap data, to create an information black hole and even to masquerade as another server."³ Far from being a theoretical "what-if," this scenario played out for a small Virginia Internet service provider. A router misconfiguration led the router to advertise that it was the best route to the entire Internet. The ensuing avalanche of data took down the router and disrupted major segments of the Internet, causing an outage that in some places lasted as long as two hours.

Scary Server Scenarios

These techniques have also been used successfully in recent years to take down popular e-commerce sites and cause enormous losses. Typically a hacker finds a "hook" into a target server that provides access to administrative privileges. To subvert the server, the attacker may use a "root kit," a toolkit containing software that replaces system programs controlling critical server operations. With access to the root functionality, a hacker now can shut the server down, steal data, or alter confidential information.

Closing the Door on External and Internal Threats

Tripwire is the first solution to effectively combine configuration assessment with change auditing, enabling IT to take a deliberate and controlled approach to achieve and maintain data center operational and security integrity. Being able to act quickly and effectively minimizes the potential for loss, downtime, and costly consequences in the form of customer concessions and Service Level Agreement (SLA) or legal penalties. And, Tripwire software also captures attack data for investigations for use as evidence to prosecute attackers.

Tripwire's independent broad coverage provides a single point of control to manage change with 24/7 tunable change detection across millions of elements, including files, directories, registry settings, directory server objects, and configuration files. Tripwire's customizable reports and dashboards offer drill-down capability into specific change events. IT can use this detailed information to ensure adherence to change management policies and to rapidly recover from improper change.

Configuration Assessment and Change Auditing for IT Infrastructures

Tripwire software assures the integrity and security of the entire data center—the physical servers, virtual servers, guest operating systems, host operating systems, desktops, network devices, directory servers and more—through five key steps.

1. Assesses the State

Tripwire software first assesses the files, configurations, and policies of the data center elements against established industry standards, including those developed by the Center for Internet Security (CIS), the National Institute of Standards and Technology (NIST), as well as the Defense Information Systems Agency (DISA). The configuration assessment provides detailed information about any areas of potential compromise, enabling the organization to make necessary changes to get the data center into a known and secure state.

2. Establishes a Baseline State

Once the organization achieves a known and trusted state, Tripwire software takes a snapshot of files and configurations in that state and uses this snapshot as a baseline against which it automatically monitors for change.

3. Discovers Any State Change

User-scheduled integrity checks monitor files and their attributes, comparing them against the established baseline state. Tripwire detects changes immediately, notifies IT staff, and provides sufficient detail so that IT staff can determine the exact change. Tripwire also verifies whether that change is in compliance with operational policy, flagging inappropriate change so that staff can investigate further. Change event information also can be integrated with enterprise management systems such as BMC Remedy, HP OpenView, CA Unicenter Service Desk and others.

4. Aids in Fast Recovery from Undesired Change

Detailed reports and audit logs provide IT with a fast recovery path when change occurs. If the change is desirable—a scheduled software patch, for example—Tripwire makes it easy to verify these changes and roll them into the baseline for future monitoring. If the change is not desired, Tripwire software not only alerts IT of the change, but also enables rapid restoration of files to a known good state. In fact, Tripwire allows IT to put in place controls that not only identify changes, but also restore systems automatically when undesired change occurs—immediate remediation that avoids costly system outages, unhappy customers, and loss of reputation. In addition, this record serves as an audit trail IT can use to prove compliance with the many standards and regulations organizations are increasingly subject to.

5. Guards the Guard

When used with other measures such as personnel policies, change and configuration management, identity management, and perimeter security products, Tripwire software enables IT managers to control changes across their enterprise networks. In fact, Tripwire software verifies the integrity of other security products, including Tripwire, because these systems are at risk for malicious and unintentional change just as general business systems and applications are. Tripwire configuration audit and control software secures the IT infrastructure, giving IT organizations visibility into changes made to the entire network infrastructure, automating manual processes to restore to a known and trusted state, validating change against established policy, and increasing overall system security and availability.

Conserving a Valuable IT Resource: People

As business relies increasingly on technology systems to operate, fewer and fewer IT staff have more and more infrastructure to administer. Even armed with an arsenal of scripts and network management applications, IT professionals must continually reconfigure, install, and patch software across a myriad of systems—servers, network devices, databases, workstations and applications. Obviously it makes sense to plan and execute these changes in an orderly fashion. In reality, however, this is frequently not possible. As a result, staff spends an extraordinary amount of time manually updating and modifying system configurations in an ad hoc, reactive—and costly—way. For example, one corporate IT department manages 1,200 Unix systems that each contains 10–15 configuration files, all of which are monitored nightly on 10 percent of the machines. Files have to be manually downloaded and a Unix “diff” is used to find changes. If differences are found, the staff must manually restore or repair the files. Night in and night out, this task never changes. And the possibility of introducing an accidental error is significantly increased. With Tripwire the department can install configuration audit and control capabilities on 100 percent of its systems, eliminating costly and manual tasks while increasing visibility, control, and confidence.

An Automatic Advantage

According to the Meta Group, organizations should migrate away from dependence on costly, error-prone manual network configuration management. By doing so they would reduce operational expenses while enjoying a robust IT infrastructure and more consistent services (*Advantages of Automation*, Meta Group, December 5, 2002). Configuration audit and control software enables IT to provide more services, with greater availability, without increasing staffing expense. It minimizes the risk and costs associated with disaster recovery, adverse business impact, and being subject to fines, violations, and liabilities imposed by regulatory agencies. At the same time, IT departments save in staffing costs because standardized tasks and processes require fewer staff members (as few as 25 percent, according to the Meta Group) and free IT experts for proactive initiatives that help the business meet high-level objectives.

More Efficiency, Less Effort

As part of operational best practices, Tripwire software provides scalable, centralized management for thousands of Tripwire systems. IT professionals throughout the organization can administer system changes from a centralized console, based on their authorized access levels, functions, and capabilities. In one example, Tripwire software revolutionized IT operations efficiency for a network services provider. According to the firm's Chief Technology Officer, the typical ratio of servers to system administrators ranges between 20 and 30:1. Best practices guidelines often set the level much higher, at 100:1. After installing the Tripwire solution, the company was able to eliminate much of the “thrash” associated with unplanned change. The server to admin ration climbed to 115:1 and the firm re-directed the efforts of its best staff to cost-saving process improvement projects. Tripwire also enables staff to quickly verify that desired changes, reconfiguration, and software patches or upgrades are implemented correctly across a network. Rapid detection, detailed reporting, and automated system recovery capabilities constitute a vital foundation for achieving high efficiency and high infrastructure stability across even the largest operations.

Security and Operations—Fundamental Business Controls

Breakdowns in security clearly affect operations, and the same is true in reverse. Accidental configuration errors and poorly managed servers can leave the door wide open to malicious attack and the resulting costly consequences. Organizations preparing for next generation security architectures are now moving to develop proactive application security programs that extend through every relevant phase of the application life cycle, from conception to operations.⁴ A complete security program proactively protects from outside attackers, internal breaches of security and mishaps caused by both innocent and malicious people on the inside.

Tripwire configuration assessment and audit and control software provides a critical foundation for a proactive security approach, working in conjunction with existing security measures and network and system management frameworks to ensure IT can provide maximum availability while enabling more services—all at a reduced cost. And when combined with Tripwire Professional Services, Tripwire creates a powerful “best practice” for mitigating risk and assuring IT integrity of the data center. With Tripwire, IT can establish a trusted, secure state, monitor for both intended and unintended changes to the entire data center, detect and deflect malicious attacks and inadvertent change that compromises integrity.

Clearly, what's good for security is good for operations and what's good for operations is good for security. Since both strategies are designed to achieve high service availability and reduce time-consuming reactions to undesired, unanticipated events, having one solution that improves both makes sense. Tripwire software enables IT to integrate configuration assessment and audit and control into operational security processes, giving an organization a fundamental business control over their infrastructures, costs, and efficiencies.

About Tripwire

Tripwire, Inc. is the recognized leader of configuration audit and control software solutions, serving over 6,000 enterprises worldwide. As the first in the industry to combine configuration assessment with configuration change auditing, Tripwire ensures organizations reduce the effort required to maintain IT configurations, mitigating risk, automating compliance and increasing operational efficiency. Tripwire is headquartered in Portland, Oregon, with offices worldwide.

¹ *Data and Network Integrity: Technology to Invoke Trust in IT*. IDC white paper, 01-104SYSTEM2930, May 2001.

² *Best Practices for Operational Change Management*. Gartner Group, March 6, 2003.

³ *Expert: Router holes threaten Net*. CNETNews.com, February 28, 2003.

⁴ *Managing Application Security From Beginning to End*. Forrester Research, August 2007.



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