



What Changed? Leveraging the Power of Change Auditing

USING TRIPWIRE ENTERPRISE TO DETECT CHANGE AND MAKE IT ACTIONABLE



With pressure on IT departments to remain lean and efficient, comply to policies and regulations, and also provide reliable 24/7 service, it is imperative that companies large and small adopt solutions and processes to ensure a known and trusted state at all times. With the reliance on technology to conduct business, interact with customers, and meet auditing requirements, “store doors” need to remain open at all times. That’s why more than 6,000 organizations worldwide have turned to Tripwire’s configuration audit and control solutions to detect and identify the changes that can jeopardize compliance, security and operations.

“A major IT risk is improper oversight and processes to manage change, leading to compromised integrity and availability of systems.”

— Michael Rasmussen
Forrester Research, 2006

DO YOU KNOW WHAT CHANGED, WHO CHANGED IT, AND WHEN?

Change auditing is a method for tracking every change made across the data center. Some IT managers may wonder why it is important to know about every change, especially given that most systems experience hundreds, thousands, or even tens of thousands of changes every week. To auditors, tracking every change is crucial, as uncontrolled change means risk. A handful of risky changes that can cause system failure, and just one ill-advised change can lead to compliance degradation, security vulnerabilities and service availability issues.

With change auditing, there is complete visibility to all change, a record of who made changes, and an audit trail that gives you the data to quickly troubleshoot problems—suspect changes can be quickly identified

and resolved. Being able to quickly pinpoint problem changes and streamline the troubleshooting process is one of the most effective uses of change auditing. But as Tripwire’s customers have discovered, the benefits an IT organization receives from their configuration audit and control solutions are much more far-reaching.

TRIPWIRE — THE PIONEER IN CHANGE AUDITING

Tripwire, the recognized leader in configuration control, provides software solutions to help you achieve and maintain the integrity of all your IT configurations. Change auditing makes change visible by detecting all changes across the breadth and depth of the data center, including virtual environments. It scans systems to create a baseline report, then compares subsequent scan results to

SOLUTION BRIEF

that baseline and reports changes, resulting in a verifiable audit trail and version history of each system's state.

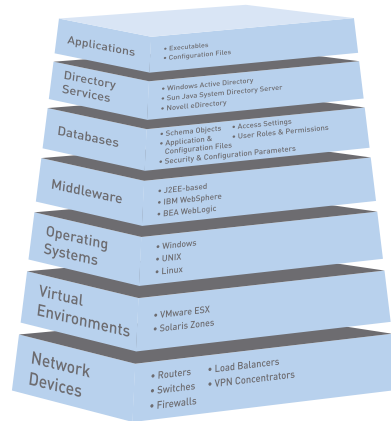


Figure 1: Tripwire's change auditing capabilities ensure that all changes are detected across the entire datacenter, no matter the source. From business-critical applications to operating systems, databases, network devices, virtual environments and hypervisors, one point of control provides the visibility and control necessary to automate compliance, mitigate security risks and increase operational efficiency.



COMPLIANCE CAN NO LONGER BE CONSIDERED A ONCE A YEAR EVENT, BUT RATHER AN ONGOING, CONTINUOUS PROCESS

Tripwire® Enterprise accommodates a broad range of user-defined policy criteria to enable its automated filtering of changes. Authorized changes can be defined in a variety of ways: those made within specified time windows, made by authorized users, correlated to change tickets and/or matching pre-tested changes, etc. Tripwire Enterprise also takes into account that not all changes are equal. It can enforce specific criteria based on the type of change (e.g. "Business As Usual" vs. Emergency) and type of system (e.g. a SOX server vs. email server).

Those customers wishing to complement their change and configuration automation tools with Tripwire Enterprise do so by using Tripwire's integrations with popular enterprise change ticketing systems, such as BMC

Remedy and HP OpenView. A flexible API is also available to facilitate integration with home-grown solutions. Tripwire's standard integration methods, including Tripwire Reconcile Express, make it easy to align configuration audit and control with your existing processes.

THE ROLE OF CHANGE AUDIT IN COMPLIANCE, SECURITY, AND IT OPERATIONS

High performing IT organizations know that to help avert data center problems, they must have complete visibility of change. This visibility helps them maintain a known and trusted state for compliance, security and IT operations.

Compliance

Compliance can no longer be considered a once a year event, but rather an ongoing, continuous process. With Tripwire's change auditing capability, the audit process is automated and streamlined, expedited through detailed change history and reporting. Because all change is tracked and an audit trail created, auditors can quickly be given proof of how changes are managed. When combined with Tripwire Enterprise's out-of-the-box configuration assessment capability, each change is proactively tested to ensure it is within internal and/or external policy. Tripwire makes this powerful information actionable by alerting you when a change does not meet policy and can go as far as to create a new incident request within your existing change management system so it can be investigated further. Whether you are facing PCI, SOX, FISMA, GLBA, Basel II, JSOX, NERC or internal audits, Tripwire's market-leading Configuration Audit and Control solution can make the process easier, more accurate and cost effective.

SOLUTION BRIEF

“Now, instead of spending as many as 28 man-days over a year providing manual proof of change control, we simply review our Tripwire implementation and show evidence of compliance across the infrastructure with on-screen Tripwire reports. As a result, we now spend about an hour per audit answering questions about our change processes. That’s a reduction of nearly 90%!”

— EdFinancial Services

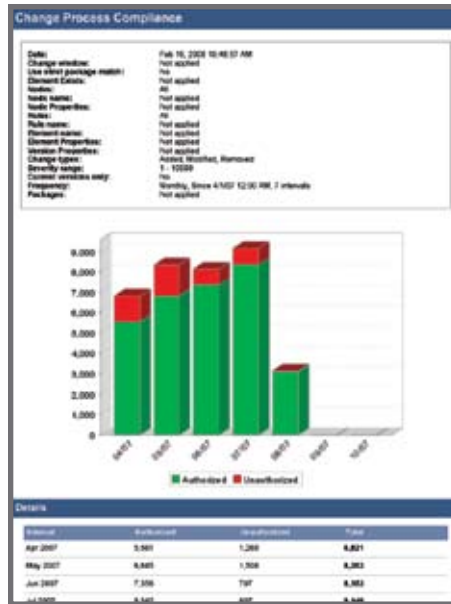


Fig. 2: The Change Process Compliance report identifies authorized and unauthorized changes to nodes over time, showing effectiveness of change process controls.

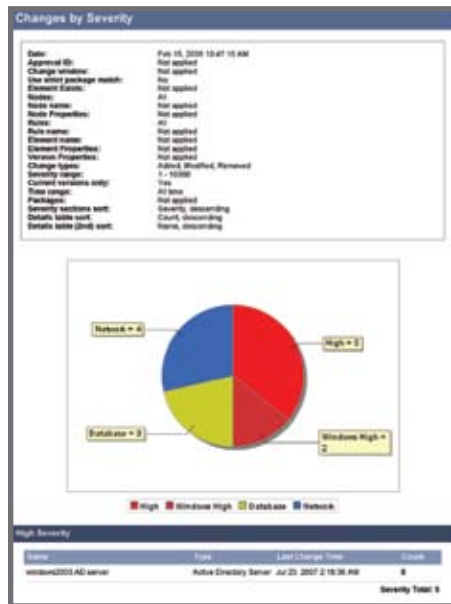


Fig. 3: The Changes by Severity report identifies configurations that have deviated from their baseline by user-defined severity levels.

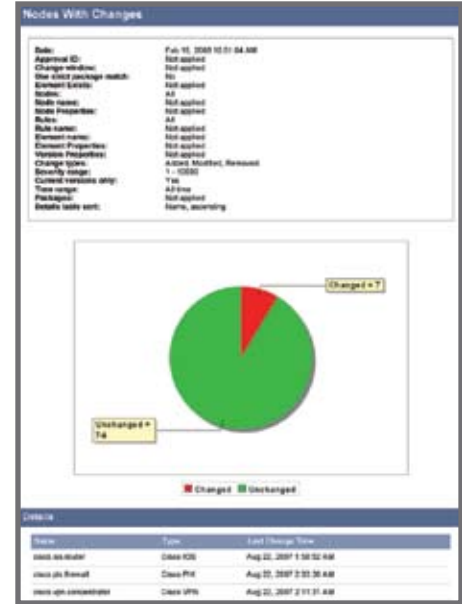


Fig. 4: The Changes by Severity report identifies configurations that have deviated from their baseline by user-defined severity levels.

Security

Security professionals widely recognize that IT configuration integrity is fundamental to a sound security strategy. Change auditing is core to a security plan since intrusions may occur for an indefinite amount of time without change auditing actively monitoring the enterprise. Tripwire Enterprise not only tracks every change made across the IT infrastructure, in both physical and virtual environments, it lets you know what changed and who made the change. This information is provided through Tripwire reports and dashboards, which can be customized to your needs (such as severity of risk). Knowing who makes the changes can also be used to review access privileges.

Operations

80% of unplanned downtime is caused by unauthorized change and 80% of the time taken to restore services is spent discovering what changed in the first place. Therefore, system availability is dependent upon how well an organization manages change. Tripwire Enterprise tracks every

SOLUTION BRIEF

“With Tripwire we were able to discover and correct configurations or disable options that represented potential threats. This ability helped us improve our overall security posture.”

— Colorado Housing Authority

“Tripwire acts like a radar gun, constantly on the alert for unauthorized and undocumented change. It’s nice to know I don’t have to worry about unknowns. All I have to do is look at the Tripwire report.”

— VML

change across the data center—and identifies who made each change. This enables organizations to enforce a zero-tolerance for unauthorized change, thereby quickly eliminating the number one source of downtime. If a system outage does occur, change auditing can help the organization immediately pinpoint the problem and inform rapid remediation.

SUMMARY

Change is necessary not only to keep up with day-to-day operational evolution, but also to enable IT to transform the

organization. As the business continues to demand change, it’s in its own best interest to get control of the changes that pose potential risk. Tripwire’s change auditing solution empowers IT professionals with the capability to improve and enforce change and configuration management policies and procedures to ensure compliance with internal governance, external regulatory requirements, and industry best practices. By adopting Tripwire configuration control solutions, organizations achieve a known and trusted state by automating compliance, mitigating security risk and improving operational efficiency.

CHALLENGE	HOW TRIPWIRE HELPS
80% of unplanned downtime is caused by unauthorized change	Tripwire tracks every change across the data center, alerting you to unauthorized or suspect changes that can cause downtime. Tripwire change auditing is completely tunable to your processes.
80% of the time taken to restore services is spent discovering what changed	Tripwire lets you know what changed, when it changed and who made the change. This drastically reduces firefighting, troubleshooting and mean time to repair.
Intrusions may occur for an indefinite amount of time without notice	Tripwire’s change auditing function automatically and actively monitors the enterprise for suspect changes, alerting staff for immediate investigation and remediation.
Change and configuration management processes are frequently circumvented, leading to unauthorized change that increases the risk of system compromise	Tripwire ensures all changes are made through expected tools and processes by automatically correlating changes with other configuration and change automation systems in order to better identify authorized and unauthorized change.
Auditors are increasingly aware that strong IT controls are predicated on strong change and security controls	Tripwire’s automated change detection, ongoing documentation of change history and online reporting capabilities provide preventive and detective controls that continuously ensure safeguards are in place and working effectively.
Auditing processes are now frequent and numerous, eating up resources and increasing IT costs.	Auditors recognize Tripwire and its reputation as a proven automated control, and consequently spend less time questioning and inspecting. They know that with Tripwire in place, there is proof whether or not change is properly managed.



ABOUT TRIPWIRE

Tripwire helps over 6,000 enterprises worldwide reduce security risk, attain compliance and increase operational efficiency throughout their virtual and physical environments. Using Tripwire’s industry-leading configuration assessment and change auditing solutions, organizations successfully achieve and maintain IT configuration control. Tripwire is headquartered in Portland, Oregon, with offices worldwide.