



Enforcing Federal Cyber Security Strategies with Tripwire Configuration Control



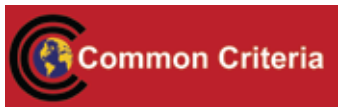
Protecting computer systems, IT networks, and information assets against unauthorized access and loss is one of the most critical forms of Federal cyber security. Security breaches are high-profile risks. Hackers from outside the network, or employees and contractors with means, motive and opportunities, bypass or defeat security defenses, and make malicious changes to software files and system configurations. These unauthorized changes can have dire consequences, including financial loss, disruptions to IT operations, and threat to national security.

Whether for economic advantage or national security purposes, government and civilian agencies are experiencing exploits of an unprecedented scale. Federal IT security response must include a broad strategy to cover the full range of information security threats. This means security managers need tools to track incremental changes to the network that could cause—or allow—irreparable damage to occur. Misconfigured systems, for instance, can present potential vulnerabilities that introduce risk to the organization. Intrusions may occur and remain undetected for months. Discovering compromise quickly is of utmost importance so that remedial action can be taken immediately.

As a recent example, unauthorized access to a computer within a Federal

agency network may have exposed the personal information of employees and retirees of the agency. Though the agency claims the server was not connected to operational data, confidence is understandably low that critical federal information is adequately protected.

Poor oversight and lack of enforcement for change configuration management policies also create risk of system compromise. Unfortunately, it's hard to enforce policies without the ability to assess the state of your IT systems and continuously locate and identify incremental changes, when they occurred—and who was responsible. Consequently, despite the best intentions, most change and configuration management policies are good in theory, but poorly practiced.



SOLUTION BRIEF

"A Chief Security Architect was interested in virtualization but wasn't convinced adequate security controls could be implemented. We brought in Tripwire to verify the VMware ESX configuration and showed how Tripwire's server agent could be installed onto virtual servers. He was convinced and now both VMware and Tripwire are installed."

— Government Integrator

According to Gartner, "an effective vulnerability management program requires projects and processes that span the IT security organization and the organizations that provide network management, desktop management, server management and software distribution."

In other words, you need an overall guard to watch over all the other guards.

Why? Because even with all of today's sophisticated security measures, breaches still occur. Any network with an internet connection is by definition an open network; it's not easy to determine where the perimeter is in today's environment of distributed technology. VPNs, extranets, tunneling, and simply the many technical possibilities of e-commerce and the Web make it virtually impossible to support a truly contained network with a definable "outside" and "inside." Today's virtualization technologies create yet another point of entry and more connection complexity.

"Configuration drift" refers to another kind of risk to the integrity of systems that cannot be stopped at the perimeter. It describes movement away from a desired state. Configuration drift is the result of several factors, including the diversity of platforms, applications and processes operating in any typical IT organization; the complexity introduced by mergers and acquisitions; and the ongoing pressure on IT by business users to "just get it up and running quickly." A recent analyst report indicates that more than 65% of security vulnerabilities in an organization are a result of system misconfiguration.

It's obvious that in order to truly defend the data center in an affordable manner, IT needs a way to:

- Continually assure the integrity of the IT infrastructure;

- Assess systems against security standards to assure their compliance;
- Identify and trace intrusions and misuse; and
- Detect unauthorized or incorrectly implemented changes and repair them quickly.

THE SOLUTION IS TRIPWIRE

Tripwire, the recognized leader in configuration control with over 6,500 customers worldwide, provides a comprehensive solution that enables you to mitigate security risks, automate compliance, and increase operational efficiency.

Tripwire is the first company to effectively combine configuration assessment with the automated change auditing required for successful configuration control. The result is a complete solution that can proactively assess configurations across your data center to ensure they comply with internal and external policies as well as identify and validate all changes to ensure your configurations remain in a known and trusted state.

Trust in a data center begins with the certainty that everything is in a known good state. Only by monitoring your IT infrastructure against a trusted baseline state can you discover security breaches fast enough to avoid serious damage and respond effectively.

Tripwire proactively assesses configuration settings against internal and external security policies, then alerts you when unauthorized changes in configurations occur and provides actionable information so you can locate and identify what changed, when it changed and who changed it. This helps IT quickly restore systems to a known and trusted state. Being able to act quickly and effectively minimizes the potential for

SOLUTION BRIEF



“BEFORE TRIPWIRE, MY TEAM PUT IN 80 HOURS A WEEK INTO UNDOING THE DAMAGE CAUSED BY A VIRUS. WE HAVEN’T HAD TO DO THAT SINCE WE STARTED USING TRIPWIRE; NOW OUR SYSTEMS ARE CONFIGURED PROPERLY”
— SECURITY PROFESSIONAL

loss, downtime, and costly consequences. Tripwire data also serves as forensic evidence for use in investigations.

THE FOUR COMPONENTS OF THE TRIPWIRE SOLUTION

Tripwire’s configuration control solution helps you achieve and maintain a higher level of security in four ways:

- **Configuration Assessment.** Tripwire® Enterprise provides the broadest selection of security assessments for business-critical systems designed by industry experts such as the Center for Internet Security (CIS) and National Institute of Standards and Technology (NIST), and automatically assesses configuration settings against internal

and external policies. These assessments view all configuration settings across the infrastructure to determine the degree of risk for security vulnerabilities.

Tripwire Enterprise contains more out-of-the-box policies than any other solution to keep systems safe and secure. Tripwire includes policies for CIS and NIST standards, DISA, FISMA, and SCAP. New policies are under constant development—please refer to the Tripwire Web site for more information.

- **Change Auditing.** Tripwire Enterprise gives you broad, independent coverage with a single point of change control for 24/7 independent change detection across millions of elements (e.g. files,

SECURITY CHALLENGES	HOW TRIPWIRE HELPS
Security vulnerabilities in virtual environments	Policy-based control for hypervisor and virtual machine layers. Tripwire reports on configuration settings that could lead to weakened security states, and detects unauthorized change throughout the virtual environment.
Risks due to misconfigured systems	Out-of-box security configuration assessments to proactively assess system settings against standards derived from CIS, NIST, DISA, and internal policies. Change auditing capabilities ensure continuous compliance across the data center.
Increased risk due to lack of visibility into change	Tripwire Enterprise monitors and reports on every change made across the data center regardless of source, detecting unauthorized change and non-conforming configurations. This enables IT organizations to gain visibility into their entire network infrastructure, automate manual processes, verify desired change, and increase overall system security and availability.
Maintaining the integrity of systems and data	Tripwire provides the foundation for data security and ensures a safe, productive, stable IT environment. It can be used for change detection, file integrity assessment, IT auditing for compliance initiatives, damage discovery, change and configuration management, system auditing, and forensics.
Detecting—and recovering from—security breaches	Instead of wasting precious time looking for individual files that have been tampered with or attempting to troubleshoot a system error, Tripwire reports exactly what changed, reducing recovery times.

directories, registry settings, directory server objects, and configuration files). Tripwire even provides automated change detection throughout the virtual environment, from virtual machine to hypervisor.

- **Reports and Dashboards.** Tripwire Enterprise provides a comprehensive set of actionable reports and dashboards that enable you to drill down to explore the full chain of assessment results and change events. They provide the necessary information to reduce configuration drift, enforce change/configuration policies, correlate actual changes with change orders, and perform forensics.
- **Reconciliation.** Tripwire Enterprise categorizes changes that pose potential risk to the business. This gives your IT staff the ability to quickly reconcile changes that are unauthorized and return to a known and trusted state.

TRIPWIRE ROI

Tripwire provides solid return on investment. Tripwire helps you determine your degree of risk for security vulnerabilities and helps you monitor IT systems and data to protect them from internal and external threats.

- Spend less time assessing configurations for policy conformance.
- Dramatically reduce time spent discovering and recovering from security incidences.

Another important aspect of Tripwire's ROI to consider is what how valuable its configuration audit and control solution can be in helping your organization achieve and maintain regulatory compliance and improve overall service availability. To learn more about Tripwire's ROI in these areas, be sure to read our solution papers on Compliance and IT Operations.



www.tripwire.com

ABOUT TRIPWIRE

Tripwire helps over 6,500 enterprises worldwide, including over 700 government and civilian agencies, 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.