

---

## Proactively Reduce Risk and Improve IT Security in Physical and Virtual Environments

---

- page 2** Executive Summary
- page 3** Environmental Challenges for Security Professionals
- page 4** Sources of Security Compromise
- page 5** Tripwire as Part of a Proactive Security Strategy
- page 8** Putting It All Together: Benefits of Configuration Audit and Control
- page 9** Ensuring a Strong Security Posture for Your IT Infrastructure

## Executive Summary

Securing the IT infrastructure in today's computing environment may well be the biggest challenge faced by organizations. Not only must organizations ensure the integrity of their systems and data, but often they must also prove that their security processes and policies measure up against standards and regulations established and enforced by national standards-developing entities. In addition, the recent popularization of virtualized environments adds a new layer of complexity to the security picture. Businesses are just beginning to comprehend the security implications of these environments.

To tackle these security issues, many organizations adopt a security approach that addresses vulnerabilities through security policy and systems designed to protect the integrity of the IT infrastructure. This approach recognizes that the integrity of the IT infrastructure may be easily compromised by malicious attacks from external sources, but often lacks a means of addressing compromises that originate from within the organization through both intentional and inadvertent employee actions. And ironically, the very systems responsible for providing security—the firewalls, intrusion detection systems, and others—often go unmonitored.

Configuration Audit and Control solutions from Tripwire play a critical role in an organization's security approach, starting with configuration assessment of all systems and devices, including those with the primary function of protecting the computing environment and data. Tripwire software assesses the infrastructure against established, consensus-based security standards, providing a scorecard that security, compliance and IT operations staff can use to get the infrastructure into compliance with security standards—even with virtualized machines as part of the environment. Once the organization achieves a known and trusted state with its computing infrastructure and data, Tripwire helps organizations stay there, with continuous monitoring and alerting for any configuration changes—whether they originate from inside or outside the organization, and whether they represent proper or improper change.

In this paper you'll learn more about the security risks and vulnerabilities faced by organizations. You'll also learn about the elements of a proactive security approach. Finally, you'll learn how Tripwire helps organizations attain and maintain a good security posture using industry-leading configuration assessment and change auditing to harden systems against security breaches, automate compliance with security standards and policies, identify configuration changes, and resolve vulnerabilities.

## Environmental Challenges for Security Professionals

Those whose job it is to protect the security of the organization's IT infrastructure work within an ever-changing landscape. Challenges arise from Internet connectivity, e-commerce, a global workplace, virtualized environments, and the ever-increasing complexity of today's enterprise network. Top that with people who inadvertently introduce risk to the infrastructure and individuals out to cause mischief or trouble, and it's obvious that security professionals have a big job on their hands. Some of the major challenges security professionals face are discussed below.

### Unclear Perimeter

In the past, the line between what is inside versus outside the organization was fairly clear. By connecting to the Internet though, businesses connect to the public networks of the entire world, exposing business infrastructures to the possibility of exploitation by thousands of people in the outside, online, global community. VPNs, extranets, tunneling, and the many technical aspects of e-commerce and the Web make it virtually impossible to support a truly contained network, further blurring the line between what constitutes inside and outside the network.

### Integrity Drift

IT must continually contend with integrity drift—the movement of the IT infrastructure away from a known and trusted state. Factors leading to integrity drift include a departure from the homogenous environments common in the past to environments that include a wide diversity of platforms, applications and processes. Mergers and acquisitions also add layers of unanticipated complexity, as does the ongoing pressure by business users to “just get it up and running quickly.”

### Virtualized Computing Environments

Virtualization of the computing environment is a more than a passing fad. Virtualization allows organizations to do more with fewer physical machines and to realize tremendous cost-savings if these virtual environments are well managed. However, virtualized machines introduce numerous possibilities for security compromise. They increase the number of entry points and connections for attackers to zero in on per physical machine, and virtual machines can easily be brought online and offline in a short timeframe with little or no oversight from IT. In addition, disk images of virtual machines are extremely portable, meaning that employees can easily copy a disk image, email it or save it to a file, and take it off site. Whether introduction of risk through these environments is intentional or accidental, keeping track of these machines and the vulnerabilities they introduce is an issue security professionals cannot afford to ignore.

### A Sea of Security Products

The organization now requires a whole host of security-related products to reduce risk of system compromise. Security professionals need time and training to achieve optimal results with these security products, and they also need to know how to use security information management solutions—tools that help them manage the numerous security products. And of course, they now need to ensure that these management product themselves don't introduce risk.

### Compliance Pressure

With the numerous data security breaches in recent years, standards and regulation-developing bodies such as the Center for Internet Security (CIS), National Institute of Standards and Technology (NIST), and the Defense Information Security Agency (DISA), have developed and issued security and standards that amount to best practices for security. Whether voluntary or mandatory, organizations should achieve compliance with these standards to optimize their security posture. In fact, as the line between who is responsible for what increasingly blurs between IT governance, IT risk management, and IT compliance, many organizations are beginning to realize that by addressing regulatory and compliance requirements, they end up improving their organization's overall information security posture.<sup>1</sup>

## Sources of Security Compromise

More and more, organizations are beginning to see that risk to the IT infrastructure's security stems from poor judgment by employees, failure to follow established processes, and sadly, intentional sabotage by dissatisfied employees. Inadvertent or ill-advised employee actions tend to manifest themselves in poorly configured applications, servers, routers, and access levels—a host of potential misconfigurations that typically compromise the integrity of the computing infrastructure. While according to a recent analyst report, misconfigured systems introduce more than 65 percent of security vulnerabilities, both the usual and sometimes not-so-usual suspects command attention.

The most common security issues facing the organization include:

- **System Misconfiguration.** Misconfigured systems present potential vulnerabilities and introduce unnecessary business risk, making configuration integrity fundamental to a sound security strategy. Misconfigurations can occur from experimentation, accidental employee actions, allowing security fixes to get out of date, failure to periodically review risks and policies, and changes in services and service level offerings.
- **Security Policy Shortcomings.** An effective security policy explicitly states the risks that a business foresees and discusses how to address those risks. Such a policy also sets implicit standards of practice that must be adhered to. If an organization does not have a security policy, has an outdated or inadequate security policy, or fails to enforce its policy, then unnecessary risk may be introduced through employee misconduct, experimentation, hacking, and other improper actions.
- **Virtualization.** With more organizations leaning toward virtualizing a significant portion of their computing infrastructure, security experts are beginning to see the critical implications of these virtualized environments to their security posture.
- **Hacker Attacks.** Viruses, worms, denial-of-service attacks, web-defacement, and hacker penetration are still common issues that lead to downtime and loss of reputation and business, especially when publicized by the media.
- **Theft or Other Computing Resource Loss.** Organizations that don't give enough importance to physical security may quickly learn that computers and their components are valuable physical assets ripe for theft. Theft leads to downtime, embarrassment, loss of business, and leakage of proprietary information and data. Theft of computer assets is often an inside job, resulting in system downtime and loss of proprietary information and sensitive data such as credit card information. More insidious theft involves non-destructive copying that leaves no trace behind. Other sources of data and computing resource loss include accidental deletion or destruction from fire, flood, or other disasters.
- **Fraud.** Security professionals face at least two fraud-related risks that impact e-commerce businesses: bogus payment and liability due to theft of customer payment data such as credit card details.
- **Human Error.** Perhaps the broadest, yet mildest form of threat, is lack of security awareness amongst employees which can lead to leakage of proprietary data through personal emails and vulnerability to con artists and "social engineering" schemes.

With data at the heart of today's business, a company's ability to compete and survive depends upon the integrity of its IT infrastructure—an infrastructure that is increasingly vulnerable to unintentional misuse and malicious attacks. A proactive security strategy is one approach many organizations employ to help plug the organization's security holes.

## Tripwire as Part of a Proactive Security Strategy

In a proactive security approach, a company may deploy many data security technologies to address the sources of security risk and fulfill specific security objectives and functions. However, many of these security approaches fall short when it comes to dealing with attacks or compromise that come from within the organization. Tripwire shores up many existing security technologies—firewalls, authentication solutions, and others—through its industry-leading configuration assessment and configuration audit and control. With Tripwire, organizations can get IT infrastructures into a known and trusted state, and keep them there.

### Firewalls/VPNs

A firewall is a system or group of systems that enforces an access control policy between two networks. Some firewalls place a greater emphasis on blocking traffic, while others emphasize permitting traffic. Usually, a firewall's purpose is to keep intruders out of your network while still letting you get your job done. The firewall's configuration is the mechanism for enforcing policy and imposes that policy on everything behind the firewall.

Unfortunately, a firewall is only effective if it is configured properly. What's more, firewalls can't protect against attacks that don't go through them; they only detect intrusion attempts from outside the firewall. That means that internal attacks, where most security risk originates, are never a part of the firewall equation. In addition, firewalls can only detect and protect against known vulnerabilities.

Tripwire software's configuration assessment and change auditing reinforces firewalls in two ways:

- Tripwire ensures that the firewall configuration starts off in a known good state. Tripwire assesses firewall configurations against established, proven benchmarks from national standards organizations such as CIS, NIST, and DISA. Based on the assessment, Tripwire provides a scorecard that identifies security weaknesses, allowing security professionals to remediate these issues and get the firewall configuration into a known and trusted state.
- Tripwire monitors and detects all changes to firewall configurations, operating systems, applications, and other elements of the IT infrastructure. By quickly identifying misconfigured elements, Tripwire enables immediate remediation—whether those changes originated from inside or outside the organization, and whether the vulnerability introduced was previously known or entirely new.

Virtual private networks (VPNs) are another potential weak point. VPNs allow remote employees, partners, and customers to securely access a corporate network by establishing an authenticated, secure connection. Tripwire augments VPN security by first assessing the VPN against established industry security standards to ensure that it is properly configured. Once the VPN is configured in a trusted state, Tripwire monitors and detects change to systems and data to help ensure that any changes made through the VPN are authorized and do not introduce risk.

### Antivirus

Antivirus companies have made virus protection the best-known defense against network invasion. Certainly, no proactive security strategy is complete without it. However, virus protection software works primarily by looking for known virus signatures, coming from the outside in. That's why virus definitions must continually be updated—the software won't find what it hasn't been told to look for. Nor can it report file changes not associated with virus signatures.

Tripwire software complements antivirus solutions, assisting in system or file recovery caused by viruses undetected by an antivirus solution. For example, many worms change or delete Windows Registry values—changes that would be nearly impossible to detect if a user didn't know where to look. With Tripwire, a user can quickly detect exactly which registry entries were changed or deleted and replace only those files that were affected.

### **Authentication**

Authentication is the process of determining whether someone or something is who or what they claim they are. The most common form of authentication, logon passwords, can often be forgotten, stolen, or accidentally revealed. To provide stronger security, passwords are often combined with tokens to provide two-factor authentication. To gain access, users must correctly identify both elements (token and password). If an individual steals legitimate authentication information, that person can access the enterprise network without anyone knowing.

Tripwire software complements all forms of authentication by identifying any changes to a machine—changes that may have been introduced by an individual or a program without access rights. For example, an attacker could steal the token and password to access a machine from a person with legitimate access rights. The attacker could then access the machine or server and plant a backdoor program that allows them to continue to access the machine undetected. If the attacker returns the token to the person he or she stole it from, no one even knows the server has been accessed. The attacker then later returns to compromise and/or steal critical company files.

In this scenario, Tripwire configuration assessment followed by configuration audit and control would provide three things. First, Tripwire would enable the organization to assess all files against industry security and compliance benchmarks to get the system into a known and trusted state. Second, Tripwire's continuous monitoring would detect the additional backdoor files that were installed on the server in a hidden directory. The administrator could then quickly delete the files, preventing future access by the attacker into the system. Finally, Tripwire would identify the specific company files the attacker tampered with, so the organization can take measures to recover or restore those files. No authentication product can provide such extensive capabilities for recovering from a security breach.

### **Intrusion Detection Systems (IDS)**

Intrusion detection systems (IDS) send alerts or notifications when someone attempts to gain unauthorized access to the datacenter. Two primary kinds of intrusion detection systems exist:

- **Host based** – Software that monitors a system or application log files and responds with an alarm or a countermeasure when a user attempts to gain access to unauthorized data, files, or services.
- **Network based** – Software that monitors network traffic and responds with an alarm when it identifies a traffic pattern as either a scanning attempt or a denial of service or other attack.

Intrusion detection is a vital facet of proactive security; however, when an intrusion occurs, it will not tell you how data has been compromised, what's changed on your system, or what your data baseline was before the attack. In addition, an IDS does not look for internal threats. Only integrity assurance software like Tripwire monitors data for change, whether initiated internally or externally, regardless of the cause or motive.

### **Additional Security Technologies to Consider**

Firewalls, authentication systems, anti-virus software, and intrusion detection systems can be considered the basic layers of defense for any organization. All work fairly effectively against identified attacks, but hackers continue to employ these “tried and true” attack techniques simply because so many companies fail to implement these defenses.

Of course, persistent and devious hackers constantly develop new and innovative ways to penetrate network resources. And when they do, the vendors who supply firewall, IDS and anti-virus technologies upgrade their solutions. But what happens to the organization that is the first one to experience a new form of attack? Or to the organization that doesn't have the latest defense against a known attack patched into the network? To fully protect themselves, smart organizations add a few more layers of defense.

### **Vulnerability Assessment Scanners**

These tools check the settings on systems to determine whether they are consistent with corporate security policies and to identify “holes” or vulnerabilities that attackers could exploit. Many products simulate the behavior of attackers to learn which of as many as 600 possible weaknesses possibly present on a system could get attacked.

Tripwire adds to this assessment effort by leveraging industry standards, such as policies from the Center for Internet Security (CIS) that block 80–85 percent of known security vulnerabilities. By testing against these benchmarks, which include tens of thousands of assessments for configurations, and by testing against operational policies, Tripwire enables automatic and sustainable security policy testing.

### **Security Information Management**

Security Information Management (SIM) products centrally manage security data from other security products, analyzing the data, correlating attack patterns across a network, and providing users with actionable information. A security product is only useful if the user understands the information it provides and understands how data from one security product can be used in conjunction with another security product. A SIM gathers together and presents the information in an understandable way, providing an extremely valuable higher-level view of the company.

### **Digital Video Surveillance**

One often-neglected part of a layered security solution is digital video surveillance of servers, network devices and data centers. Integrating digital video surveillance security with data security measures provides a well-rounded approach for protecting a company's critical IT infrastructure. Some video surveillance solutions can send images electronically over a wired or wireless network to centralize all computer security monitoring.

## Putting It All Together: Benefits of Configuration Audit and Control

Tripwire software for servers, desktops, network devices, as well as for millions of other elements, including directories, registry settings, and configuration files, helps companies achieve and maintain a strong security posture through comprehensive configuration assessment and continuous monitoring to detect change. Tripwire software provides the following benefits to the organization:

- **Ensures the IT Infrastructure Achieves and Maintains a Known and Trusted State.** Tripwire Enterprise can proactively test and assess a IT infrastructure against pre-configured regulatory, security, and operational policies, even policies developed for virtualized environments. Tripwire leverages industry standards—specifically benchmarks issued by CIS, NIST, and DISA. These benchmarks include tens of thousands of configuration assessments, enabling Tripwire to automatically and continuously conduct security policy testing.
- **Reduces Risk with Visibility to All Change.** Powerful change detection and reporting by Tripwire Enterprise monitors file integrity and file structures on the hardware, software, network, and all elements of the computing infrastructure. By detecting unauthorized change and non-conforming configurations, IT can quickly pinpoint, analyze and recover from any undesirable change. Tripwire ensures the integrity of systems and data.
- **Establishes a Foundation for Data Security.** Tripwire takes a snapshot of data in its known, good state, providing companies a baseline to monitor against. This snapshot allows companies to verify when changes occur and what they are by comparing the current snapshot to the last known, good state—a highly-effective means of establishing and maintaining data security.
- **Lowens Costs.** Using Tripwire lowers costs associated with troubleshooting, downtime, and change management. Instead of wasting precious time looking for individual files that have been tampered with or attempting to troubleshoot a system error, Tripwire points you directly to improper change, so you can fix it and get back to business. Tripwire reduces the time spent trying to locate the source of system problems from hours—sometimes even days—to just minutes, freeing up IT staff for more proactive, productive activities.
- **Maximizes System Uptime.** Tripwire enables companies to maximize their investments in IT by eliminating risk and uncertainty, while maximizing system uptime. Tripwire software pinpoints the exact location and nature of change to enable quick restoration of systems to a desired, good state.
- **Increases Control and Stability.** By verifying system integrity and limiting integrity drift, users gain more control over systems because they know unequivocally whether a system has drifted from a known good state.
- **Monitors the Guard.** Since even security products can introduce risk, Tripwire checks configuration files for security products *and even for itself*.

## Ensuring a Strong Security Posture for Your IT Infrastructure

In today's environment, organizations connected to the Internet must be more vigilant than ever. Networks are scanned for vulnerabilities many times a day. Viruses and worms abound. Virtualization opens up new vulnerabilities. And the threat of cyber terrorism looms.

Addressing these challenges is, and will continue to be, part and parcel of protecting the security and integrity of the IT infrastructure. Knowing that, many security professionals take a proactive security approach that helps them prevent, detect and respond to security incidents. In this approach, they implement security products designed to address one or more of these specific challenges. A common shortcoming of these products is the ability to detect security compromise introduced from inside the organization. To have a truly robust strategy, security professionals must consider complementary solutions that can address attacks and breaches from both outside the organization and inside.

Tripwire configuration assessment and change auditing software is a critical layer in such an approach, helping organizations address the security holes other security products such as firewalls, VPNs, and intrusion detection systems simply are not designed to address, particularly security risks introduced from inside the organization. In fact, Tripwire detects risk introduced from inside *and* outside the organization—changes that can have dire consequences to the organization's security posture.

Tripwire's approach is a solid one. First, Tripwire helps organizations get their IT infrastructure into a known good state by testing against industry security and operational standards, providing the organization the information it needs to eliminate security risk. Then, Tripwire continuously monitors for all change across the entire infrastructure, alerting IT if improper change has been detected, so they can quickly respond to and remediate any issues.

In combination with other security technologies, Tripwire software provides companies the assurance that they need—and their customers need—that their digital assets are protected.

### 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.

<sup>1</sup> "The Future of Information Security: 2008 and Beyond", CIO, January 2008.



[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