

Keeping malicious intruders out isn't the biggest issue.

Knowing what changed—and why—IS.

If you're spending most of your IT resources keeping unwanted intruders out of your systems, you're missing the biggest threat of all. The most significant security threat to your information systems could be sitting next to you. Up to 80 percent of all system problems and downtime is caused from within your agency by unintended errors and the unforeseen impact of system changes. Assuring security and system availability requires having visibility into changes—whether they're the result of malicious attacks from the outside or innocent mistakes made by staff members and consultants.

Security is Knowing What Changed—and What to Do About It

Only when you know what changed, and how it changed, can you evaluate the impact and take appropriate action. And, only an Integrity Assurance solution can give you immediate visibility into IT infrastructure changes with the critical information required for problem diagnosis and rapid recovery.

Security is Control and Confidence

Tripwire® Integrity Assurance solutions give government agencies greater control over their IT infrastructures. By establishing a solid security foundation for servers and network devices, Tripwire software and services support the *President's Management Agenda* and the *National Strategy to Secure Cyberspace*. Not only does Tripwire provide you with a secure line of defense that reduces risk—it saves time, reduces cost, and significantly improves the stability of IT operations.

We're on a Mission. Yours.

Mission-critical. Mission-ready. Mission Accomplished.

Common Criteria Certified, Tripwire Integrity Assurance software is used by world-leading corporations, academic institutions, and many government agencies to assure system integrity. In fact, Tripwire solutions are installed in prominent government organizations that we can't discuss. Regardless of the IT environment, our software ensures integrity across multi-vendor networks and common operating systems.

Certified and proven in demanding enterprise environments, Tripwire delivers confidence in your data and systems. Tripwire is also recommended as a best practice by SANS, CERT, leading security advisory groups, and is featured in the NSA's 60 Minute Security Guide.

For more information about Tripwire solutions, call 1-800-TRIPWIRE or your local Tripwire sales representative.

Information systems are key to your mission.
Having them change without your knowledge
is critical.

TRIPWIRE



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

©2003 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. All other trademarks and company names are property of their respective owners. All rights reserved.

TRIPWIRE

Layer Your Defenses to Secure Systems against Cyber Attacks

Changes initiated by insiders are far more prevalent than attacks from the outside because many more insiders know where valuable data resides. To protect your systems from cyber attacks of any origin, your comprehensive layered security strategy must be able to identify integrity breaches from within the organization as well as from outside intrusions.

Because Tripwire software detects any change—whether from inside or outside the organization—it creates an essential foundation for layered security strategies. If an undesired change or cyber attack does occur, Tripwire quickly detects, identifies, and reports it, enabling the fastest possible recovery. Tripwire solutions help government agencies comply with *National Strategy to Secure Cyberspace* objectives, providing certainty that servers or network devices have not been compromised, maximizing system uptime, and minimizing risk.

Ensuring Mission Readiness and Peace of Mind

Tripwire software forms the foundation of a layered security strategy because, unlike other security solutions, it detects external and internal compromises and monitors at the file level. When used with other measures such as personnel policies, password controls, firewalls, and anti-virus and authentication software, Tripwire software enables IT managers to control changes across their network and server infrastructures. In fact, Tripwire software will verify the integrity of other security products themselves.

Mitigate Risk with a Blanket of Security across Your Network

With Tripwire software running across your network, undesired changes to monitored systems are quickly detected. Once detected, change information can be delivered in several ways to authorized staff members who need to know. The appropriate IT staff can be notified by email or pager. Change information can be sent to the syslog or via SNMP traps for integration with other enterprise management systems and reporting packages.

No Threat Can Hide

Detailed reports outline specific changes from any monitored server or network device. Staff can view reports from the Tripwire Manager console or receive them via email. Finally, executive summary reports can be exported as HTML files and viewed from any web browser. Once Tripwire knows of a change, everyone else who needs to know, will.

Pre-empt Negative Impact

With visibility into exactly what changed, when, where, and by whom, your staff can minimize damage and act decisively. Tripwire enables a consistent change management process with flexibility for taking action—such as automatic restoration, scripted responses to specific alerts, and verification of intended changes back to authorized IT processes and personnel.

Stabilize IT Operations. Control Costs. Meet Objectives.

With visibility into activity across your network, Tripwire software gives you far greater control over your IT environment. Immediate detection and rapid notification enable you to quickly diagnose changes—slashing troubleshooting time from hours or days to minutes. Now you can quickly restore files and configurations and limit potentially costly damage and downtime. Tripwire gives you confidence that nothing can change without your knowledge.

Tripwire also enables you to verify software patches or upgrades implemented across your network in minutes. By freeing staff from continuous manual monitoring, tedious verification tasks, and hours of troubleshooting, you can re-direct valuable technical talent to manage proactive, value-added initiatives. When every taxpayer dollar counts, Tripwire enables you to maximize productivity for every dollar spent.

Demonstrate Compliance with Confidence and Accountability

Managing system compliance for the Office of Management and Budget, NIST regulations, or internal audits is far easier and more efficient with Tripwire software. It records a history of changes, greatly simplifying change tracking and reporting. Detailed reports provide data demonstrating that no unauthorized changes have occurred over a set time period. With Tripwire software, you'll have peace of mind—and proof—that servers and network devices are, and have remained, in a known good state.

- 1 Tripwire software establishes a "digital inventory" of known, good file attributes and uses it as a baseline for monitoring changes.
- 2 User-scheduled integrity checks monitor file attributes and compare them against the baseline. Changes are immediately pinpointed and integrity alerts are reported to authorized staff.
- 3 Tripwire shows exactly which files were added, deleted, or modified, reducing troubleshooting time to minutes and enabling rapid restoration.

