Tripwire Enterprise

File Integrity Manager

File integrity monitoring was invented by Tripwire. But that's only one reason why so many consider "Tripwire" synonymous with this critical security control. Tripwire Enterprise has taken FIM far beyond basic change auditing. It not only collects highly detailed change data in real-time, it also adds change intelligence and automated remediation and then integrates this data with the other critical security controls provided by Tripwire solutions.

Changes to configurations, files and file attributes throughout the IT infrastructure are just part of everyday life in today's enterprise organizations. But hidden within the large volume of daily changes are the few that can impact file or configuration integrity. These include unexpected changes to attributes, permissions and content, or changes that cause a configuration's values, ranges and properties to fall out of alignment with security or compliance policies. To protect critical systems and data, you need to detect all changes, capture details about each instance, and use those details to determine if a change introduces security risk or non-compliance. You also have to do that in real time to stop an attack from succeeding—or minimize the impact of a successful one.

But with constant changes to files and configurations occurring, how do you tell the difference between "good" and "bad" ones? Or in a more pragmatic sense, between business-as-usual changes and the ones that spell trouble?

That's what file integrity monitoring (FIM), a critical security control, is supposed to do. Unfortunately, most FIM solutions simply determine that a change occurred—and stop right there. Only a few capture change in real time and with enough detail to show you who made it. Even fewer provide the option to trigger remediation of an undesirable configuration change.

Organizations need "true" FIM—file integrity monitoring that detects each change as it occurs and uses change intelligence to determine if a change introduces risk or non-compliance. File Integrity Manager, a core component of Tripwire® Enterprise, offers exactly this by combining Tripwire's industry-leading change detection with ChangeIQ™ change intelligence and automated responses.

Agent-based FIM for Change Data in Real Time

One of the big differentiators between File Integrity Manager and other FIM solutions is Tripwire's use of agents to continuously capture detailed who, what and when change details in real time, with little impact on systems and network traffic. Tripwire's lightweight, easy-to-manage agents mean you don't miss the changes that occur between scans that can leave systems and data exposed.

While some solutions claim to be agentless, they actually install and uninstall an agent each and every time they collect change data, which increases overhead and risk. And the truly agentless solutions only collect a subset

of the change data that File Integrity Manager collects, which reduces your knowledge of system states as well as your overall security posture. Other solutions rely on periodic megascans to collect detailed change data, but due to the impact these scans impose on systems, they're usually only scheduled to occur weekly, monthly or even quarterly.

ChangeIQ Change Intelligence

In addition to capturing highly-detailed change data in real time, File Integrity Manager uses ChangeIQ™ change intelligence to differentiate between "good" change and "bad" change, or at least between expected changes versus undesired and potentially harmful ones.

ChangeIQ:

- Determines if changes takes configurations out of policy
- Reconciles changes against change tickets or a list of approved changes in a text file or spreadsheet
- Automates responses to specific types of changes—for example, flag the appearance of a DLL file (high-risk) but auto-promote a simple modification to a DLL file (low-risk)
- Triggers a user-tailored response when one or more specific changes reaches a severity level threshold that one change alone wouldn't trigger—for example, a minor content change accompanied by a permission change that was done outside change window hours.

In short, ChangeIQ turns raw change "noise" into actionable information.

Automation Helps Organizations Keep Up with the Workload

Most IT organizations have too much to do and not enough time or staff to do it. Automation is essential to keep up with the workload. File Integrity Manager uses automation to detect all changes and to remediate those that take a configuration out of policy. At the same time, ChangeIQ auto-promotes countless business-as-usual changes, so IT

What makes FIM "true" FIM?

True FIM detects change by first establishing a highly detailed baseline version of each monitored file or configuration in a known and trusted state. Using real-time monitoring, it detects change to any aspect of the file or configuration and captures these in subsequent versions. Versions provide critical before-and-after views that show exactly who made the change, what changed, and more. True FIM also applies change intelligence to each change to determine if it impacts integrity (for example, rules that determine if the change takes a configuration out of policy or is one that is typically associated with an attack). File Integrity Manager is true FIM.

Fig. 1 Tripwire Enterprise allows you to see before and after differences in precise detail through continuous versioning and baselining.

has more time to investigate changes that introduce risk and may truly impact security.

Automation is especially important when it comes to reconciling large batches of changes, like the ones that occur when operating system or application patches are pushed. It's tempting to "auto-promote" these types of bulk changes, but hackers often rely on this behavior and lie in wait for a chance to insert malware. To help with this, the Tripwire Dynamic Software Reconciliation app works with Tripwire Enterprise to automate the reconciliation of changes stemming from these updates—without losing integrity or record of the change.

Another example of Tripwire Enterprise's automation capability is the way it can integrate with existing change ticketing systems like BMC Remedy, HP ServiceCenter or Service Now. This type of ticketing integration insures traceability and closes the loop between continuous integrity and uninterrupted availability.

Don't have a service management system? Check with Tripwire services consultants about implementing Reconcile Express, a simple way to automate change reconciliation against with basic change sources like Excel spreadsheets or even delimited text files.

Benefits of Tripwire Enterprise File Integrity Manager

- Captures change data with greater granularity and specificity than other FIM solutions, including who, what, when and even how details
- Continuous, real-time change detection across the enterprise infrastructure—virtual, physical and cloud—to detect and respond to malware
- Provides a reliable host-based intrusion detection system that safeguards against exploits and breaches
- Offers broad support for almost any IT asset—servers, platforms, devices, applications and more
- ChangeIQ capabilities that help determine if a change is business-as-usual or introduces risk or non-compliance
- Captures highly-detailed change data in real time without notable impact on systems.

File Integrity Manager and Tripwire Security Controls

Tripwire provides the ability to integrate FIM with all Tripwire security controls—security configuration management, vulnerability management, log management and SIEM. It also adds components that combine and manage the data from these controls more intuitively and in ways that protect data and infrastructure better than ever. For example, the Event Integration Framework (EIF) adds valuable change data from File Integrity Manager to Tripwire Log Center or almost any other SIEM. With EIF and other foundational Tripwire security controls, you can easily and effectively manage the security of your modern IT enterprise.

Need a simple, standalone FIM solution? Tripwire can do that.

What if you're looking for a FIM solution today, but want the option to easily migrate to a end-to-end enterprise SCM solution tomorrow?

Maybe for an upcoming audit, or maybe you need integrity checking while you implement other controls or decide which security policy your organization will implement.

If that's the case, you can get Tripwire File Integrity Manager as a standalone product—without policy or remediation capabilities. Later, when you're ready for an integrated SCM suite, you can easily unlock the full power of Tripwire Enterprise. Contact us to learn more.

Ready to dig deeper?

To learn more about Tripwire Enterprise capabilities, reports, available policies, platform support and more, click on or visit tripwire.com for the following datasheets:

- Tripwire Enterprise Report Catalog
- Tripwire Enterprise Policy Manager
- Tripwire Connect
- Tripwire Enterprise Remediation Manager
- Tripwire Enterprise Agent Platform Support
- Tripwire Axon
- Tripwire Axon Agent Platform Support

Fig. 2 With Tripwire Enterprise's library of pre-made, built-in reports, changes and anomalies become immediately visible.

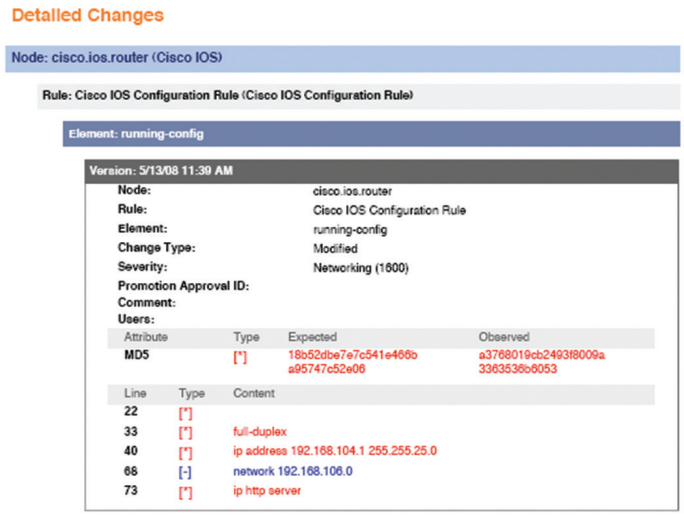

Fig. 3 Security is in the details—Tripwire Enterprise provides exhaustive detail about the Who, What, Where and When of changes.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook