tripwire®
ENTERPRISE

FILE INTEGRITY MANAGER

Changes to configurations, files, and file attributes across the IT infrastructure are just part of everyday life in today's enterprise organization. But hidden within the large volume of daily changes are the few that can impact file or configuration integrity. These include unexpected changes to a file's credentials, privileges, or hash value, or changes that cause a configuration's values, ranges and properties to fall out of alignment with security policy. To protect critical systems and data, you need to detect all change, capture details about each one, and use those details to determine if it 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 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. Fewer still provide the option to automatically remediate 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 remediation.

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 found in the Tripwire VIA™ platform.

CHANGE DATA IN REAL TIME WITH AGENT-BASED FIM

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. 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.

CHANGE INTELLIGENCE WITH ChangeIQ

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

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.

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 hosted—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
- Provides automated remediation of changes that cause non-compliance with any Tripwire security policy or a custom, internal policy.
- Captures highly-detailed change data in real time without notable impact on systems.

FILE INTEGRITY MANAGER AND THE TRIPWIRE VIA PLATFORM

The Tripwire VIA platform lets you integrate File Integrity Manager with all your Tripwire security controls—security configuration management (SCM), log

LOOKING FOR ADDITIONAL INFORMATION?

.: To learn more about Tripwire Enterprise's fundamental controls and robust reporting capabilities, visit www.tripwire.com for the following datasheets

Tripwire Enterprise Policy Manager

Tripwire Enterprise Remediation Manager

Tripwire VIA Asset View

Tripwire Enterprise Report Catalog

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 before. For example, the VIA 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 Tripwire VIA components and capabilities, you can easily and effectively manage the security of your modern IT enterprise.

NEED A BASIC, STANDALONE FIM SOLUTION? TRIPWIRE CAN HELP.

tripwire® FILE INTEGRITY MANAGER

.: What if you're not ready for an end-to-end enterprise SCM solution, but you still need FIM? Maybe for an audit, or maybe you need integrity checking as you implement other controls or decide what policy your organization will use. If that's the case, there's Tripwire File Integrity Manager, our FIM-only solution. Later, when you're ready for policy capabilities or need automated remediation, you can easily upgrade to Tripwire Enterprise. Contact Tripwire Sales to learn more about Tripwire File Integrity Manager.

.: Tripwire is a leading global provider of IT security and compliance solutions for enterprises, government agencies and service providers who need to protect their sensitive data on critical infrastructure from breaches, vulnerabilities, and threats. Thousands of customers rely on Tripwire's critical security controls like security configuration management, file integrity monitoring, log and event management. The Tripwire® VIA™ platform of integrated controls provides unprecedented visibility and intelligence into business risk while automating complex and manual tasks, enabling organizations to better achieve continuous compliance, mitigate business risk and help ensure operational control. :.

LEARN MORE AT WWW.TRIPWIRE.COM OR FOLLOW US @TRIPWIREINC ON TWITTER.

TEFIM1n 201109