FORTRA™

GUIDE (TRIPWIRE)

Five Myths and Misconceptions About FIM

How File Integrity Monitoring Fits Into a Successful Cybersecurity Program

File integrity monitoring (FIM) is the cybersecurity process that monitors and detects changes in your environment to alert you to threats and helps you remediate them. FIM was first introduced in 1997 when Gene Kim launched Tripwire and its "Change Audit" solution. Just a few years later, Change Audit became FIM, which worked with the 12 security controls identified in Visa's Cardholder Information Security Program (CISP). In fact, Tripwire software was mentioned by name in the original CISP requirements. CISP led to the development of the Payment Card Industry Data Security Standard (PCI DSS), and other compliance mandates that included various forms of change monitoring continued to evolve from there.

While monitoring environments for change sounds simple enough, there are plenty of misconceptions about how exactly FIM fits into a successful cybersecurity program. It's essential to address those common myths now so that organizations don't forsake this security practice and thereby leave themselves exposed to avoidable risks.

1. FIM Generates Too Many False Positives

The first misconception is that implementing a FIM solution will generate too many false positives and alerts. While it's conceivable that FIM could generate this alert overload, this is an issue only if monitoring is enabled for everything. FIM tools that don't help you differentiate expected from unexpected changes lead to excess "noise," which does actually distract security teams from important risks.

The purpose of FIM is to zero in on critical system files of different operating systems, including important files associated with key applications. If you use FIM on all your systems, the monitoring process will become onerous and time-consuming and generate too many alerts. You can automate processes here by integrating your FIM capabilities with other security systems such as IT Service Management (ITSM) solutions for change reconciliation. This will help reduce the number of alerts you receive when something does change, thereby enabling your security teams to focus on unauthorized changes without having to deal with too much noise from the network.

2. FIM Overloads Endpoints

Another common FIM myth is that implementing it leads to endpoint overload. We can look at Fortra's Tripwire® Enterprise as an example of low-resource use FIM. It uses agents that sit on endpoints and monitor real-time changes while using minimal network resources by only communicating differences. At the same time, it helps organizations access other crucial security features, such as security configuration management (SCM), and maintain their compliance with specific policies and standards, all with very little impact on the endpoint.

3. FIM Doesn't Help Security Posture

When teams aim their efforts toward security posture improvements, FIM often isn't one of their top priorities. However, consider that one of the main functional purposes of a FIM solution is to make sure that changes occur as the result of a patch or other legitimate reasons. If the change is unapproved, then an organization can initiate a response against malware or another perceived digital threat. Through these means, organizations can safeguard themselves against zero-day attacks for which there are no known signatures. A FIM tool lets you detect changes and remediate them before they evolve into an incident.

4. FIM Doesn't Provide Context

People who aren't well-versed in FIM may be concerned about the amount of context (or lack thereof) provided to explain unexpected changes. This myth does have a bearing in reality, because some "checkbox" FIM solutions don't do enough to provide the situational awareness surrounding any given unexpected change. An advanced FIM solution gives you the context around each change, such as who made the change, when, and—most importantly—what the change was, along with tools that differentiate between good and bad changes.

5. FIM is Only for File Systems

Lastly, some are inclined to think that FIM monitors only file systems. But that's not true either. FIM can also monitor databases, active directory, virtual infrastructures, network devices and cloud storage.

Databases: On the surface, it might not make sense to monitor a database, especially one that's changed often. But you can use a FIM tool to monitor a database's access control lists, schema, database configuration and permissions lists, etc. This will help to identify unauthorized individuals accessing the database. Additionally, FIM enables the monitoring of typically static content found in certain databases.

Network devices: Using a Command Line Interface (CLI) such as SSH or telnet, you can review firewall rules, access control lists and configurations on network devices such as routers, switches and firewalls. You can then report on what's changed if there have been any modifications.

Active Directory: FIM allows you to monitor changes to any element in Active Directory. For example, monitor group memberships for new users that are added or removed from restricted groups, such as "Domain Admins." This functionality gives users visibility over all changes that are made to their directory services.

Virtual infrastructures: This monitors the host infrastructure for change. For example, a new virtual machine is created, modified or deleted.

Cloud Storage: You can also detect changes in cloud storage, such as Amazon S3 Buckets and Azure Blobs.

Fortra's Approach to FIM

Tripwire Enterprise, Fortra's flagship FIM solution, focuses on adding business context to data for all changes that occur in an organization's environment. As such, it provides IT and security teams with real-time intelligence that they can use to identify incidents that are of real concern. Tripwire Enterprise also provide insight into the who, when, where the change was made, and, through baselining, it can identify what changed within the file as well. This information enables users to understand more about a given change so that they can verify whether it's legitimate or not. As cybersecurity professionals begin to see past the common misconceptions around FIM, they'll be able to better take advantage of the wide range of applicability that advanced FIM solutions offer.

Request a Demo

Ready to learn more? Let us take you through a demo of these industrial security solutions. We'll show you powerful features and answer any of your questions. **Visit** tripwire.com/demo

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.