FORTRA

WHITE PAPER (TRIPWIRE)

The Value of True File Integrity Monitoring

A Critical Control for Protecting Data Integrity

File integrity monitoring (FIM, and often referred to as "change audit") was around long before its early reference in the ever-evolving PCI standard. So, here we are years later… Where is FIM now? Is it still relevant or important? Does it really protect data and improve security?

The answers, in order, are:

- **FIM isn't going away**—in fact, it's now part of almost every IT compliance regulation and standard as well as every IT security standard. And some still refer to it as change audit.
- **Yes, FIM is still relevant and important**—although many organizations that must use FIM solutions complain that the term "FIM" is now synonymous with "noise," due to the huge volume of changes these solutions detect and report on.
- **Yes, FIM protects data and improves security**—but only when FIM has specific capabilities and only when the information it provides is truly actionable.

In this paper, we give an overview of FIM, an explanation of how it provides data protection and improves security, and what capabilities it must offer to effectively provide those benefits.

An Overview of FIM

File integrity monitoring is technology that monitors and detects changes in files of all types—changes that can lead to increased risk of data compromise. Unfortunately, many organizations subject to FIM in their regulatory requirements have lost sight of its intent and spirit. For them, FIM means noise: too many detected changes, no context around those changes, and very little insight into whether or not a given change poses a risk or is just business-as-usual. It's hard to argue with this criticism given their experience with typical FIM tools.

FIM actually is a critical control in the fight against data compromise. However, a true FIM tool must provide additional information. That information—or intelligence—would allow it to alert security teams only to changes that pose increased threat to protected data, and not to the hundreds of thousands (or even millions) of changes that occur daily across large, enterprise-level IT infrastructure.

Making FIM an Effective Security Tool

To guarantee FIM's rightful place at the security table we must change how we use it, and ensure the solution has specific capabilities. We must decide what in the infrastructure needs to be monitored and how to manage the changes that are detected. We also need a solution that gives us more information than the basic "something changed." Finally, we need to analyze each change to identify if it introduces risk.

Determining What to Monitor—and Managing Detected Changes

Monitoring every file on every device or application all the time is impractical and unnecessary, so the first step for effective file integrity monitoring is controlling what gets monitored. Ideally, a FIM solution would provide a way to control which files are monitored and the appropriate level of monitoring. In other words, the solution would let you determine how much information about these files—their properties—you want to capture. You would make those determinations based on the type of file and how much risk changes to a file might introduce. For example, a permissions file for a financial application represents a high-risk file. You would likely want to harvest enough properties about changes to this file to help you determine if a change is expected or suspicious.

Although you will limit the scope of the files you monitor, as well as the properties you capture, even a medium-sized organization will generate a large amount of change data. Managing the large volume of change data captured by a FIM solution requires a version-based architecture that is compact and fast, and that stores data permanently. One approach that has proven highly successful is to capture the initial state, or baseline, of every monitored file or element and store it in a database. From that point on, the solution detects any changes to an element, including its previously determined properties, and stores that change data as the original baseline version plus these typically minor changes. These "delta" versions (where delta means incremental change to the element's properties) must be stored indefinitely. But to truly add value, the solution must allow this captured history of each element to be accessed, analyzed and acted upon at any time in the future.

Determining What Changed and Who Made the Change

Knowing only that a file has changed is of little value unless you know what about or within the file has changed. Each file has dozens of attributes that, if changed, could indicate or cause trouble. Capturing these attributes can provide information essential in determining if the change is harmful or harmless—it tells you exactly what within a file changed so you can quickly determine if the change was high-risk and provides the information required to fix the issue. A true FIM solution will be able to harvest this level of information, including changes to configuration files and even character-for-character differences to human-readable file types like Word documents or PDFs.

In addition, knowing who made a change is often key to determining if a change is suspect or low-risk. But capturing the "who" data is not easy, and most FIM solutions are unable to provide this important information. Most FIM solutions available today need to enable OS Auditing on the monitored device to harvest this information; yet most IT professionals will not allow this due to concerns about security. The use of real-time detection agents installed on each monitored device overcomes this issue.

Determining If Expected, Acceptable Changes Were Made

Many changes are intended to make improvements or to correct problems. However, just because a change is proposed and scheduled does not mean that it was actually made or made correctly. Being able to confirm that a change has successfully been made is critical, otherwise improvements that you think were made are not always realized and problems remain when you think they have been resolved. A true FIM solution needs to detect a change and compare that change against what was expected, providing independent confirmation of change processes and policies.

While most changes are intentional, or at least not harmful, some changes simply shouldn't be made because they pose increased risk to the environment. Critical configuration files are an example. Each of these files contains configuration settings values that must be in predefined states or ranges to meet and maintain security policy. If any of these configuration files are changed, the settings values must immediately be re-evaluated to determine if they still conform to the security policy. Application executable (.exe) files of mission critical applications are another example of file types that should probably generate an alert if they change. A true FIM solution must know what has changed, what specific files are supposed to change, and if a given change is within policy. This ability to analyze changes converts volumes of change data from "noise" into actionable intelligence.

Addressing the Issue of Unauthorized vs. Undesired and Suspect Change

As an example, PCI DSS 11.5 requires merchants to "…alert on unauthorized modification of critical system, content or configuration files…" but the term "unauthorized" is fairly misleading. Many interpret the term to mean that they must measure how well the organization adheres to change process policy. In fact, the intent of the term in the requirement is for organizations to be alerted to changes that are undesirable and could put cardholder data at risk of compromise. The 11.5.b Testing Procedure that was added in version 2.0 of the security standard clarifies that it is an audit requirement to "Verify the tools are configured to alert personnel to unauthorized modification of critical files…"

Auditors have typically required proof that appropriate change data has been captured, but there has been inconsistency in verifying whether the FIM solution was also configured to determine if any of detected changes were not authorized. Too often, the change data has just been stored "in bulk" in an effort to meet compliance requirements. However, if the data is not continually analyzed for "high-risk" change, the FIM solution provides limited—or no—protection against cardholder data compromise. Even in cases where the FIM solution is being used to help determine which changes don't follow approved change process, unauthorized change differs a great deal from suspect or undesired change. Unfortunately, many presume that unauthorized change is always "bad," which is not necessarily true. While an unauthorized change may not have followed defined change process policy, it may actually resolve a critical problem. On the other hand, defining a change as authorized presumes it is a "good" change, which may be equally untrue. Many authorized changes cause problems and have to be rolled back or modified—sometimes using an unauthorized process.

The Capabilities of True FIM

- Detects changes
- Determines which changes introduce risk
- Determines which changes result in non-compliance
- Distinguishes between high- and low-risk changes
- Integrates with other security point solutions

Whether a detected change can be reconciled to some form of authorization or not fails to address the issue of a "bad" change; that is, a change that exposes a device or application to increased risk of compromise. Finding bad change is the issue that must be addressed by FIM—and that is the true intent of the PCI DSS 11.5 requirement in our example. And not only should FIM detect bad change, it should detect it immediately so the damage can be minimized. A true FIM solution helps organizations automatically determine if detected change is authorized. More importantly, a true FIM helps automatically determine if a change is suspect and needs immediate investigation, or is expected and can be considered low- or no-risk.

Conclusion: True FIM Makes FIM Relevant

So again, we ask, "Is FIM still relevant and important?" The answer is a resounding yes. FIM is a critical capability IT security and compliance need to ensure the integrity of IT infrastructure and its sensitive data. But for FIM to be relevant, it must do a lot more than just detect changes. "True" FIM must use change detection to help determine whether the changes are good or bad. It

must also provide multiple ways to distinguish low-risk change from high-risk change. And it must do this at the speed of change—in other words, immediately.

In addition, true FIM should also work with other security point solutions, like those for log and security event management. Correlating change data with log and event data allows security professionals to better protect their environment. Doing so allows security professionals to quickly see, trace and relate problem-causing activities with each other. Such visibility and intelligence provides the key for quickly remediating issues before they cause real and lasting damage.

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.