FORTRA™

Five Things Your FIM Solution Should Do for You

Maximizing the Value of File Integrity Monitoring

File integrity monitoring (FIM) is such an important part of a cybersecurity program's success because it can be used to monitor the cyber integrity of the entire environment, giving you an unparalleled view of what's changed.

But what is FIM, exactly? FIM is a critical security control that helps organizations maintain a strong security posture by detecting and alerting on potential threats, allowing for rapid response and mitigation. FIM is so fundamental, it's required by many major compliance standards such as North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), the Payment Card Industry Data Security Standard (PCI DSS), the Sarbanes-Oxley Act (SOX), and the Health Insurance Portability and Accountability Act (HIPAA).

Also referred to as change monitoring or simply integrity monitoring, FIM identifies suspicious system changes to help you quickly act on potential breaches and stay in compliance. Fortunately, technology is available to help you automate monitoring for changes, but not all FIM solutions offer the same level of depth and breadth when it comes to what they monitor and how much they leverage automation. In this guide, we will look at five things your FIM solution should provide you with so you know you're getting the most value from it.

FIM Is About More Than Files

Types of Integrity Monitoring

System Integrity

- System files, configurations, and executables stay operational
- Running services aren't tampered with or disrupted
- Network access allows the system to access the environment as intended

Business Integrity

- Servers perform the work needed to keep business processes operational
- Business/customer/operational information is free of intentional or accidental damage

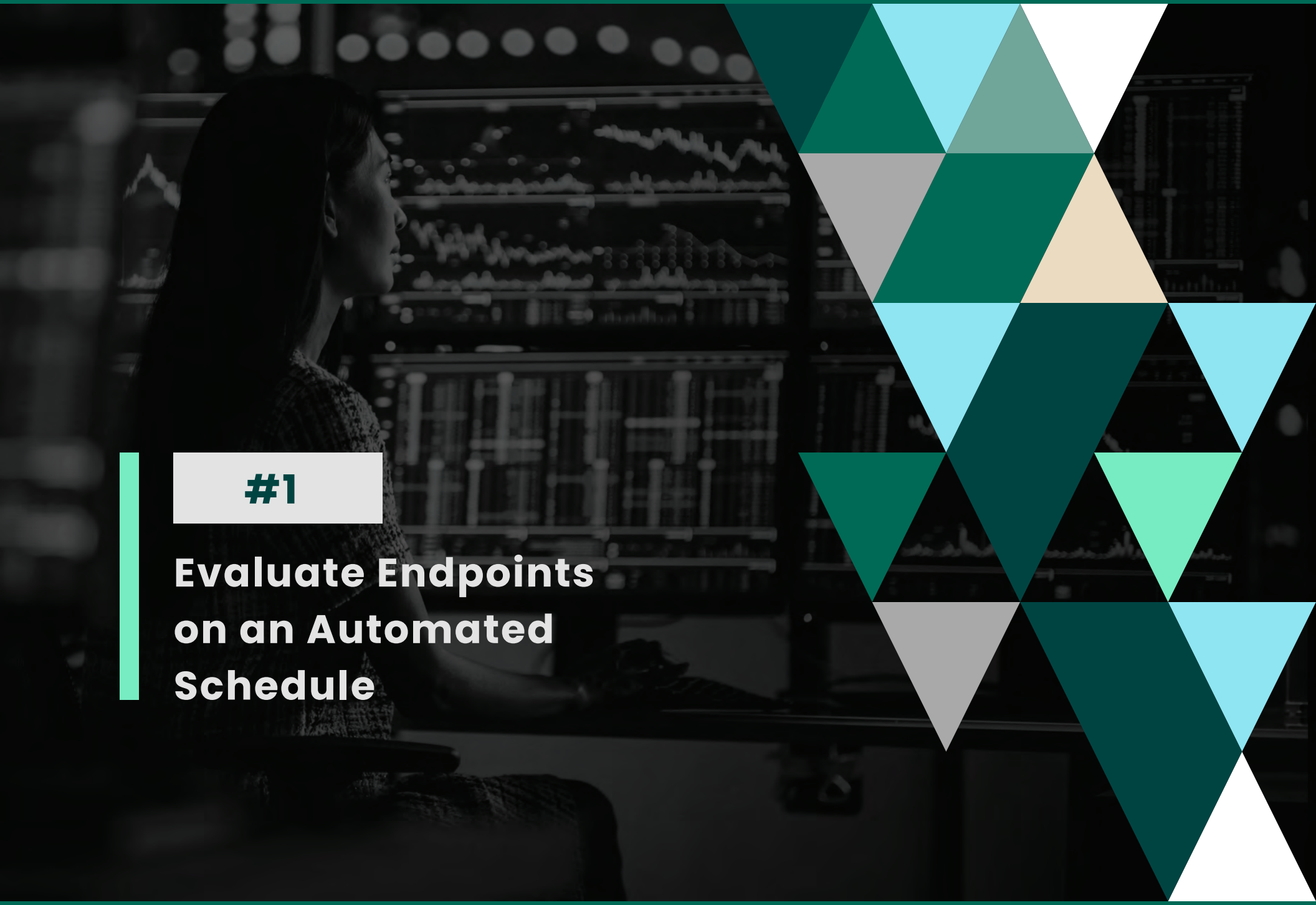
Critical Information

- Determine four of the "5 Ws": Who, What, Where, and When
- Know if a change is authorized—and whether it impacts compliance

What Is Tripwire Enterprise?

Fortra's Tripwire® Enterprise is a powerful integrity monitoring solution, building upon file integrity monitoring and security configuration management to deliver security above and beyond basic compliance. With decades of proven industry leadership, it supports advanced security use cases competitors can't.

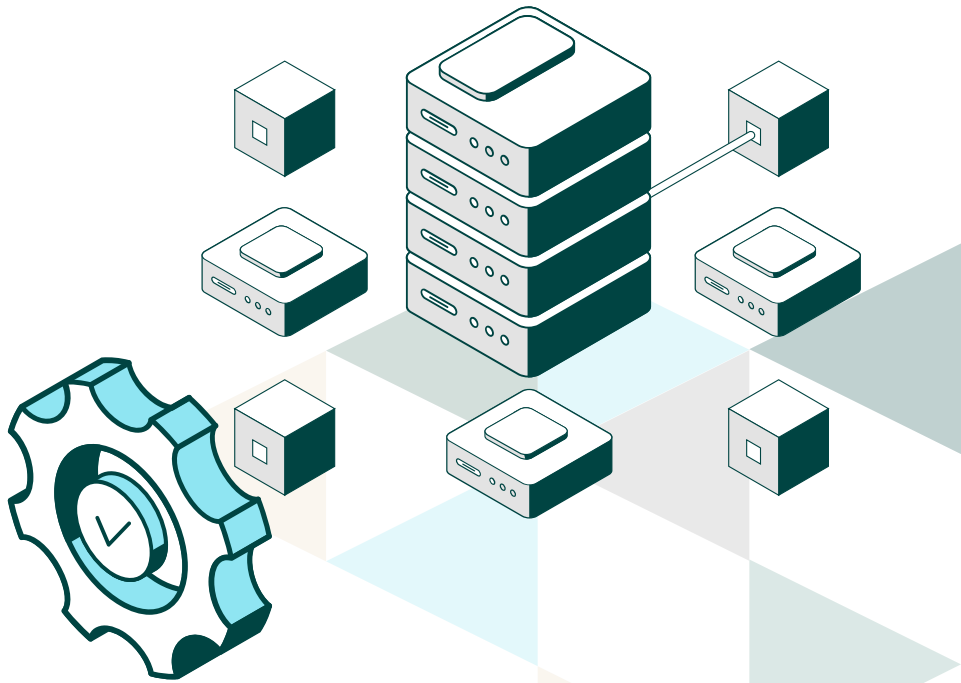
Launched in 2005, it has constantly evolved to meet growing needs while delivering the largest operating system and compliance policy content library in the industry.



#1

Evaluate Endpoints on an Automated Schedule

Your FIM solution should allow you to set the cadence at which your endpoints are evaluated. That could be every day, every hour, or every 15 minutes depending on the policies and procedures you follow. Why evaluate endpoints on an automated schedule? Changes can happen at any time, day or night. You want to "set it and forget it" so that you can quickly respond to changes that impact the integrity of your systems.



How Tripwire Enterprise Achieves This

"Tasks" within Fortra's Tripwire® Enterprise provide flexible scheduling mechanisms that can be tailored to scan your assets at your preferred cadence. Critical assets can be scanned more frequently than less critical assets. You have the same flexibility to schedule when changes are detected and alerts are generated.

#2

Identify What Changed, When, Where, and by Whom

2

Your FIM solution should tell you who was behind any given change to your system in addition to where and when it happened. By answering four of the "Five Ws," it's much easier to determine the fifth "W": *Why* it happened. The best way to identify who made a change to your system is to use kernel-level data. While there are other ways to gather "who" data, such as system logs, the kernel contains the most complete data.

There are other methods for this, including ftrace and DTrace, but these only give you after-the-fact information. Getting this information immediately allows you to investigate and remediate suspicious changes right away to better safeguard your organization against potential breaches.

How Tripwire Enterprise Achieves This

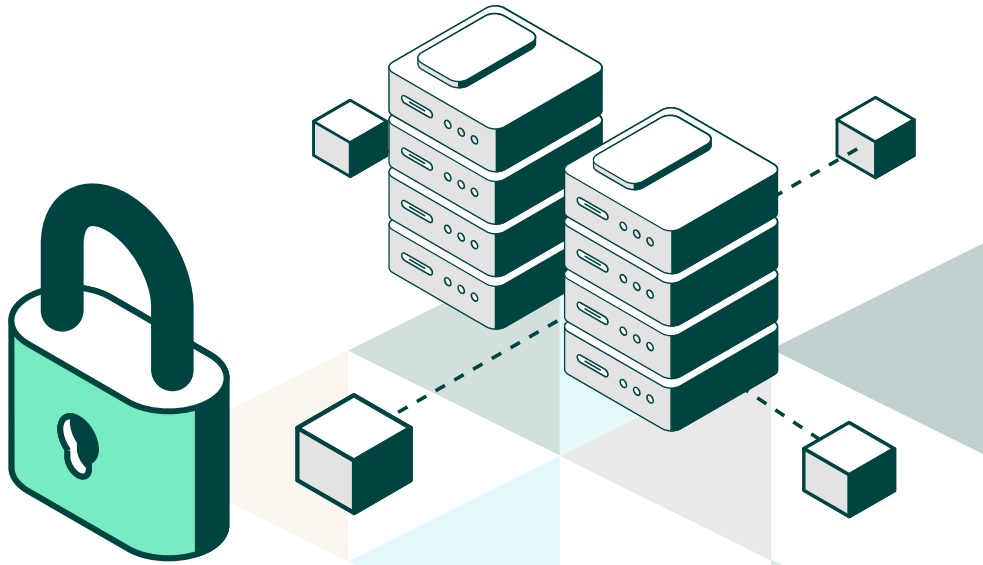
Tripwire Enterprise uses its event generator to provide real-time "who" data by way of a kernel module. System compatibility is future-proofed using a standard kernel interface called Extended Berkeley Packet Filter (eBPF).

#3

Differentiate Between Authorized and Unauthorized Changes

When your FIM solution detects a change, it should review the change and then either approve it or mark it as unauthorized. Once a change is authorized, it becomes the new baseline, or "known, good state" for the endpoint being monitored.

One method of authorization that your FIM solution should provide is via integration with service desk products such as Remedy, ServiceNow, Jira, and Cherwell. Your organization can cut down on manual ticket tracking and save substantial time thanks to the automatic change reconciliation provided by this type of integration.



How Tripwire Enterprise Achieves This

Tripwire Enterprise can utilize a module called dynamic software reconciliation (DSR) to automate the approval of changes that occur during Windows and Linux patch cycles. It also has the ability to query service desk products for change ticket data. Additionally, it can use critical change rules for operating systems and applications to promote authorized change. Lastly, it can use reference node or reference baseline data to demarcate authorized versus unauthorized changes.

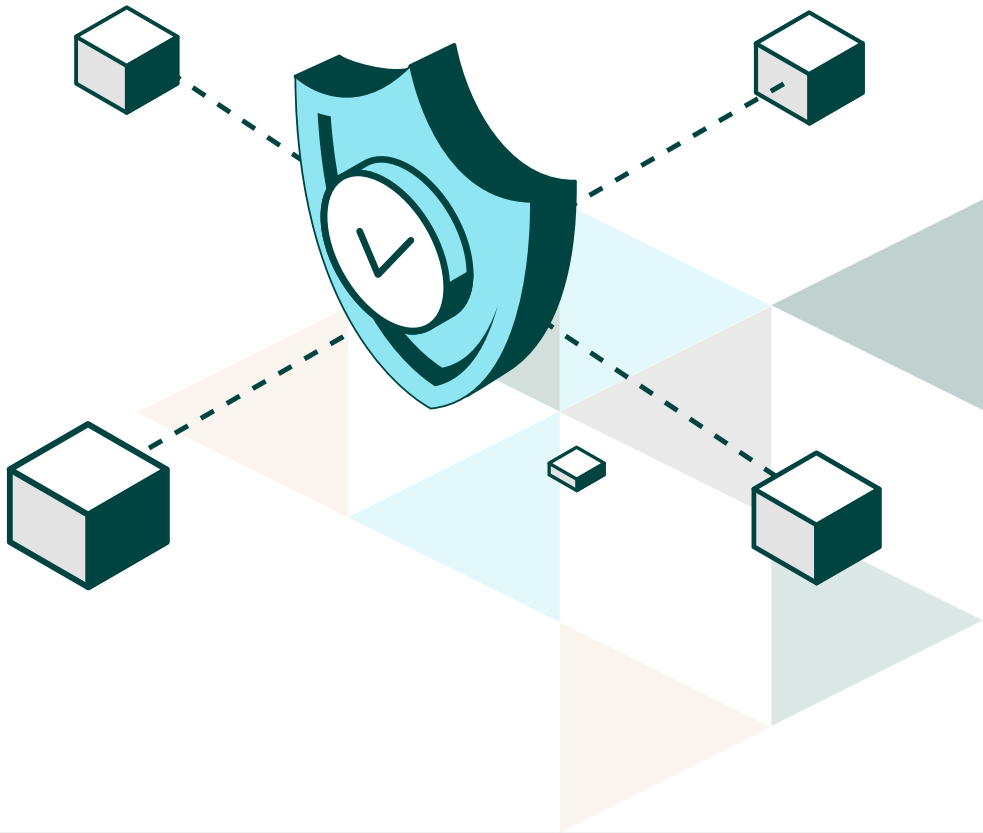
#4

Show if a Change Impacts Compliance

4

Your FIM solution should evaluate your endpoints against all the security policies and frameworks with which your organization must comply and let you know if any changes result in an impact on compliance. While some FIM solutions only monitor for compliance at specific points in time, ideally your solution should be monitoring for compliance drift continuously.

Using runbooks is a good idea for any organization, ensuring processes are documented and repeatable. Tripwire Enterprise allows the automation of computer system tasks. Service Level Agreements (SLAs) enforce response time and expected actions to drive efficiency across the organization.



How Tripwire Enterprise Achieves This

Tripwire Enterprise monitors for compliance continuously and allows you to create tag sets and assign endpoints to any set. It can evaluate the compliance level of endpoints against any policy content available from Tripwire and report on the compliance state. It supports the industry's broadest library of 4,000+ policy and platform combinations for regulations like PCI, SOX, FISMA, HIPAA, and NERC.

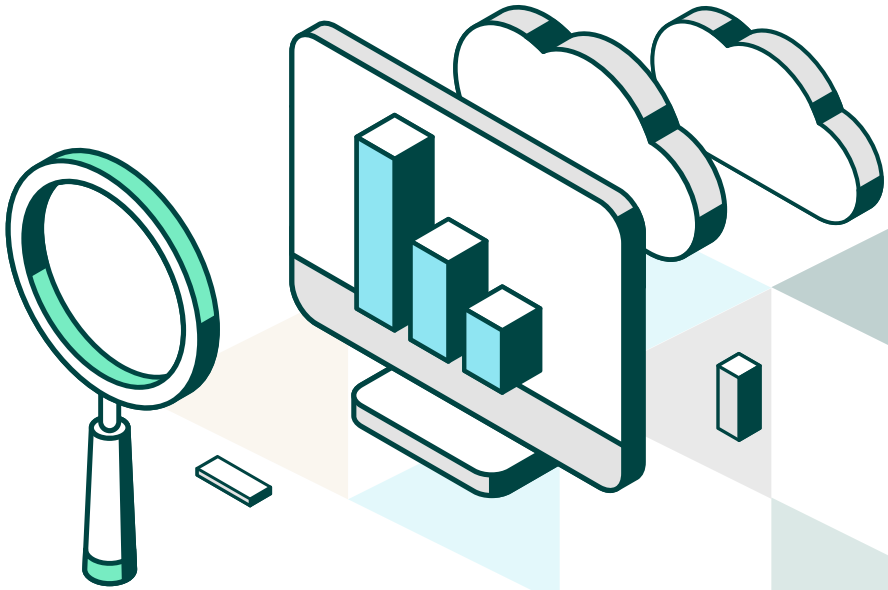
#5

Monitor an Expanded Range of Assets

The more assets encompassed within your integrity monitoring program, the more visibility you get into changes across the entire digital environment. Having deep visibility into changes on a wide range of assets makes it easier to catch intruders before they can act, as well as keep systems online and minimize costly downtime.

Besides your operating systems, servers, and endpoints, an advanced FIM solution should be able to monitor the following:

- Databases
- Network devices
- Directory services
- Boot configurations
- Certificates
- Stored procedures
- Open ports
- Firewall policies
- Cloud accounts
- Virtual desktop infrastructure



How Tripwire Enterprise Achieves This

Tripwire Enterprise monitors everything listed above. In the case of cloud accounts like AWS (Amazon Web Services), Microsoft Azure, and GCP (Google Cloud Platform), it uses a module called Cloud Management Assessor that evaluates cloud management accounts and S3 buckets.

FIM is a trusted security control required by most major cybersecurity compliance regulations. It helps organizations detect system changes in real-time that indicate impacts to compliance and potential cybersecurity incidents. Advanced FIM solutions like Tripwire Enterprise monitor more than just files and give you added context to the change data to help you achieve superior security and continuous compliance.

Learn more at www.tripwire.com.

FORTRA™

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.

fta-tw-gd-0823-r1-hm