FORTRA

GUIDE (Alert Logic)

File Integrity and Application Attack Detection

File Integrity Monitoring (FIM) detects unauthorized change events to operating systems, content, and application files, including the integrity of the system directories, registry keys, and values on the operating system.

FIM detects and analyzes application attacks when:

- A file is accessed, created, modified, moved, or deleted
- A user accesses or modifies the file (records the login name of the user)
- Changes are made to:
  - Attributes such as read-only or hidden
  - Security access permissions
  - Directories and registry keys
  - A file's group ownership

The most effective cybersecurity solution should be tailored to your environment and organization, not based on separate features or paid upgrades, but ingrained into the product itself. Likewise, a managed detection and response (MDR) solution provider should be keenly focused on delivering an exceptional customer experience and the security outcomes you seek.

Many popular compliance guidelines require FIM for ensuring file integrity and detecting malicious attacks on secure data including Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley, National Institute of Standards and Technology (NIST), and Health Insurance Portability and Accountability Act (HIPAA).

However, many FIM solutions can be cost-prohibitive as well as add an additional layer of complexity to a security posture that can increase costs even further in terms of licensing, implementation, management, and training.

Getting the Most Out of Your Resources

When exploring FIM, one of the most common questions relates to the potential burden to existing human, technical, and financial resources. Can FIM be added efficiently?

Cybersecurity is complex and ever changing. Most companies are not equipped to meet their organization's security goals while also achieving their strategic IT commitments. It is imperative to have a security partner that delivers complete threat detection and response that is within reach and not overwhelming. To be most effective, FIM should be easy and effective.

When considering a FIM solution, many providers offer and then deliver separate, standalone tools that require additional in-house staffing and training. These tools not only require separate management, but also separate licensing and cost. With so much already on an IT team's plate, adding FIM can add complexity if not integrated as part of a larger security solution.

TIP - Before you begin the FIM selection provider process, make sure you fully understand your requirements to ensure you don't overpay for an overly complex solution that exceeds your needs.

Achieving Compliance

Regulatory cybersecurity compliance related to data protection and privacy involves a growing landscape of laws and standards. Using a single system of policies across your entire compliance program allows you to implement best practices at a lower total cost. But without a guide to assist with policy mapping, you run the risk of compliance gaps and increase the likelihood of an audit failure.

A few examples of the most common PCI DSS requirements include:

- **PCI DSS 10.5.5** — Organizations must use file-integrity monitoring or change-detection software on logs to ensure existing log data cannot be changed without generating alerts. FIM or change-detection systems should check for changes to critical files and notify when such changes are noted. For FIM purposes, an entity typically monitors files that do not regularly change, but when changed indicate a possible compromise.
- **PCI DSS 11.5** — Organizations must deploy a change-detection mechanism such as FIM to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. Change-detection solutions such as FIM tools check for changes, additions, and deletions to critical files, and notify when such changes are detected. If not implemented properly and the output of the change-detection solution is not monitored, a malicious individual could add, remove, or alter configuration file contents, operating system programs, or application executables.

Dashboard and Reporting

To detect unauthorized change events, a FIM solution should provide a dashboard (Figure 1) which monitors the integrity of all files. It also should provide intelligent alerts and reports that go beyond simple notifications to bring instant situational awareness whenever you need it.

Figure 1: The Alert Logic console dashboard provides a comprehensive view of file integrity

TIP - MDR solutions can provide the high level of coverage you need and the services of a 24/7 security operations center (SOC) to ensure you don't overextend your human and technical resources. Fortra's Alert Logic MDR® provides this comprehensive coverage and includes FIM at no additional cost.

To provide the greatest level of visibility, your dashboard should:

- Allow you to drill down directly into an issue from the dashboard page, allowing you to directly consume information
- Provide a log of file and directory change event details from the past seven days
- Offer a file integrity compliance check to ensure all regulations are met
- Provide detailed reporting that includes:
  - Top file paths
  - Top FIM event systems
  - FIM status including monitored file types and event action trends

TIP - Before selecting a cybersecurity solution, ensure your IT environment is fully up to date and compliant with the latest regulations pertinent to your industry as they pertain to FIM.

Rely on the Experts

Cybercriminals are more determined than ever to evade detection. FIM is an important capability as it monitors for file-change events that can be a precursor to a larger scale security incident. With FIM capabilities integrated into an MDR solution such as Fortra's Alert Logic MDR, organizations gain a comprehensive cybersecurity solution that delivers complete threat detection and automated response. It also includes the built-in monitoring they need without having to purchase additional, expensive point solutions.

To learn more about how to implement comprehensive coverage MDR which includes FIM at no extra cost, reach out to Alert Logic for a **demonstration**.

For more information, please visit **alertlogic.com**

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.