netwrix

File Integrity Monitoring Best Practices

Introduction

File integrity monitoring (FIM) is the process of continually monitoring and reporting on any change to your system and configuration files. FIM is an essential security control for one simple reason: Any unauthorized or improper change to your system and configuration files could weaken security and indicate that the system has been compromised. In other words, FIM is vital for two main reasons:

- **Breach prevention** — Security defenses are strongest when all systems maintain the most secure configuration at all times. FIM monitors for any drift from the hardened state.

- **Breach detection** — Changes to files could represent a malware infection or other threat in progress. While many other security controls (such as antivirus software, next-generation firewalls and SIEM systems) promise intelligent detection of malware and cyberattacks, they usually leverage known threat profiles or trusted access rules, which leaves them largely blind to zero-day threats, polymorphous malware, insider attacks and ransomware. FIM, on the other hand, provides comprehensive breach detection because it highlights any potentially harmful file changes.

This article explains the key best practices that organizations should keep in mind when choosing and implementing a FIM solution.

Despite its name, file integrity monitoring must not be limited to a narrow range of files

Don't let the term "file integrity monitoring" mislead you — FIM should not be limited to a select few types of files, such as executables. For example, configuration and registry files are critical for the security and proper functioning of applications and operating systems.

Therefore, ensure that the FIM solution you choose is capable of monitoring all system, program, application and configuration files and directories, across a range of platforms, from the datacenter to the network to the desktop, on premises and in the cloud.

At a minimum, a FIM solution must track all file attributes, including file contents, and generate a secure hash value (at least SHA2) for each file as a 'DNA fingerprint' to expose trojan file insertions. Capturing who made each change is also an essential requirement.

FIM must filter out the noise and zero in on harmful changes

IT ecosystems are highly dynamic. Every minute, documents are being created, log files and database records are changing, updates and patches are being installed, applications are being installed and enhanced, and much more.

The vast majority of these changes are normal and legitimate. To avoid overwhelming security teams with a flood of notifications that result in alert fatigue, a SIM solution must filter out the noise of harmless activity. Specifically, a FIM solution needs to distinguish between four types of changes:

- **Approved and good** —These are legitimate changes that are executed properly, such as properly applied patches and additions to audit logs.
- **Approved but bad** — Sometimes people make mistakes. FIM solutions need to be able to recognize when an approved change was not implemented as anticipated and alert the security team.
- **Unexpected but harmless** — Unplanned changes that are harmless do not require investigation by the security team so they need to be filtered out as change noise.
- **Unexpected and bad** —Any change that can't be correlated with a legitimate cause and that could be malicious or harmful needs to trigger an immediate alert so it can be promptly investigated and remediated.

FIM solutions are even more effective when integrated with other technologies

To further reduce the amount of change noise, look for a FIM solution that can integrate with your other security processes and technologies, especially your security information and event management (SIEM) and IT service management (ITSM) tools:

- ITSM tools like ServiceNow and BMC maintain a record of approved changes that an integrated FIM solution can use to better assess whether each change it detects was planned and executed properly.

- SIEM integration provides the context of activity around the changes detected by FIM, facilitating alert triage and investigation. You may also want to feed all FIM alerts into your SIEM solution as part of your security operation center (SOC).

Threat intelligence further enhances FIM capabilities

Threat intelligence can provide additional context around changes to support alert triage, incident investigation, and response and recovery. In particular, threat intelligence can help FIM discern between "unexpected harmless" and "unexpected bad" changes by providing whitelists of known good changes and blacklists of known harmful changes.

The best FIM tools can improve over time

As explained above, integration with an ITSM system can dramatically improve a FIM solution's ability to distinguish between expected and unplanned changes. But the best FIM technology also provides intelligent analysis of changes to improve in this area over time. This feature, which is often called "intelligent change control," uses previously observed activities to consider factors such as the who, when and where of changes and deliver more accurate analysis of whether a change is harmful.

Baselining capabilities help you quickly establish strong configurations

State-of-the-art FIM systems can establish a gold-standard baseline configuration from a live system and compare similar systems to that baseline to ensure consistency.

Similarly, FIM technology can establish standard configurations based on CIS benchmarks or DISA STIG guidance and audit for any deviations from that baseline to ensure that all systems remain secure.

FIM is a core security control, not a compliance checkbox

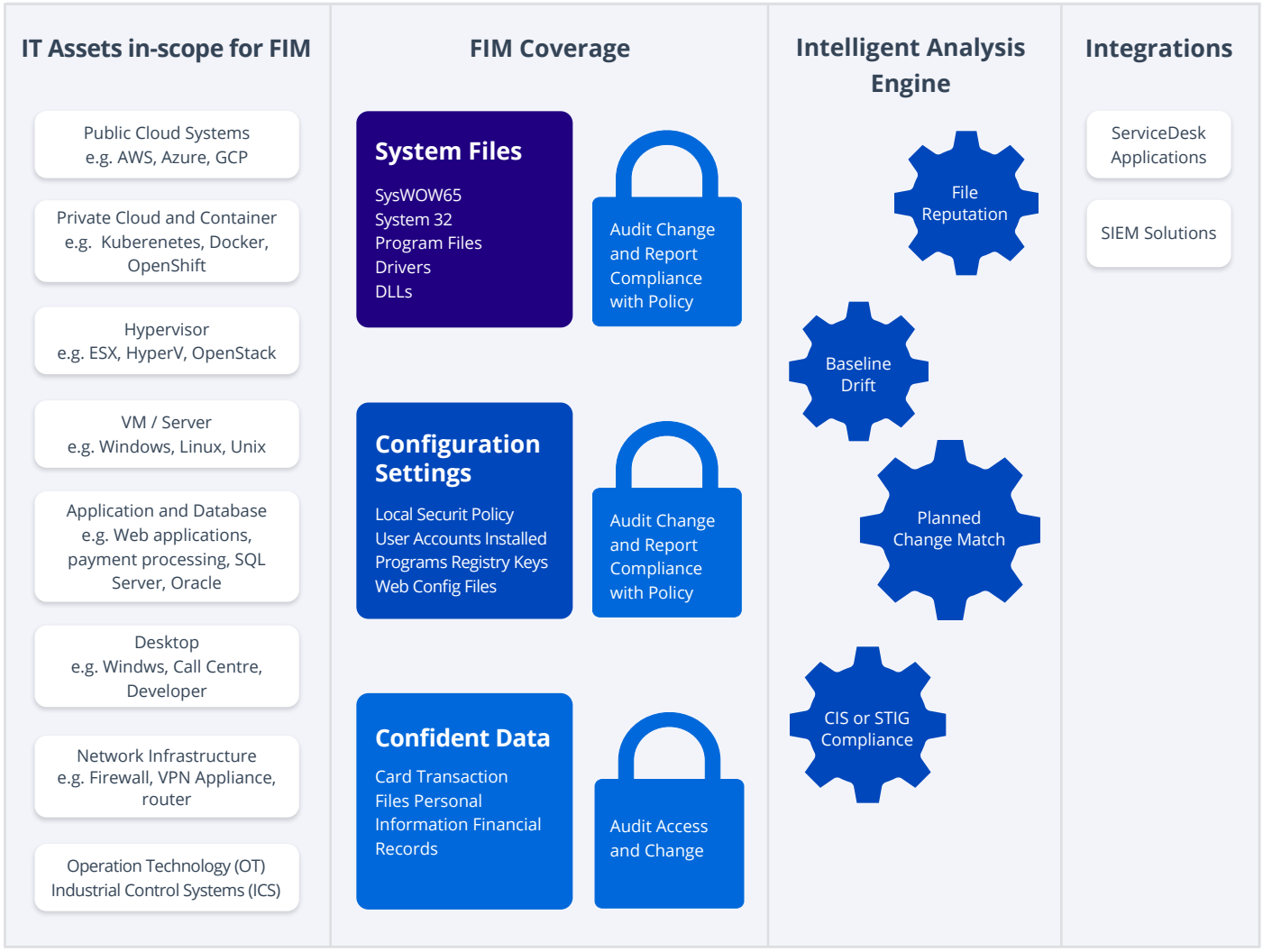
It's true that FIM is required by a number of mandates, including the Payment Card Industry Data Security Standard (PCI-DSS), NIST 800, North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) and the Sarbanes Oxley (SOX) Act. Nevertheless, organizations should not adopt FIM merely to tick a compliance checkbox.

Instead, it's important to remember that FIM is listed as a mandatory security control for good reason — it is vital to strong security. Indeed, FIM helps with all 5 pillars of security described in NIST: Identify, Protect, Detect, Respond and Recover. Therefore, plan your FIM deployment to improve cybersecurity, and compliance will follow.

Conclusion

By following the best practices laid out here, you can dramatically strengthen cybersecurity across your IT ecosystem. Figure 2 provides a convenient summary of the key elements to include in your FIM strategy:

Recommended File Integrity Monitoring Architecture



Implement File Integrity Monitoring to Strengthen Your Security with Netwrix® Change Tracker

- Detect indications of data breaches and malware infections in real time.
- Remove change noise and empower operations teams to focus on truly anomalous events.
- Get full visibility into changes to critical system files across your entire infrastructure.
- Reduce the time and effort you spend on compliance reporting using 250+ reports covering CIS, NIST, PCI DSS, CMMC, STIG and NERC CIP.

Request Free Trial

About Netwrix

Netwrix® makes data security easy by simplifying how professionals can control sensitive, regulated and business-critical data, regardless of where it resides. More than 11,500 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers.

Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more information, visit www.netwrix.com

Next Steps

See Netwrix products — Check out the full portfolio of Netwrix products: netwrix.com/products

Get a live demo — Take a personalized product tour with a Netwrix expert: netwrix.com/livedemo

Request a quote — Receive pricing information: netwrix.com/buy

CORPORATE HEADQUARTER:

300 Spectrum Center Drive
Suite 200 Irvine, CA 92618

565 Metro Place S, Suite 400
Dublin, OH 43017

5 New Street Square
London EC4A 3TW

PHONES:

1-949-407-5125
Toll-free (USA): 888-638-9749

1-201-490-8840

+44 (0) 203 588 3023

OTHER LOCATIONS:

Spain:	+34 911 982608
Netherlands:	+31 858 887 804
Sweden:	+46 8 525 03487
Switzerland:	+41 43 508 3472
France:	+33 9 75 18 11 19
Germany:	+49 711 899 89 187
Hong Kong:	+852 5808 1306
Italy:	+39 02 947 53539

SOCIAL:

netwrix.com/social