File Integrity Monitoring (FIM): Best Practices for Compliance and Data Integrity

Sudden unexpected changes to system files, host files and configuration files are inevitable in a humongous IT environment. All these intentional and unintentional file changes might result in IT operational hazards, resulting in systems behaving in an unexpected manner due to their loss of integrity. ARCON File Integrity Monitoring (FIM), an integral component of ARCON | Endpoint Privilege Management (EPM) identifies these changes and helps organizations to track and roll back such unauthorized file changes and preserve the desired integrity for files.

Table of content

Overview

Endpoints present the biggest attack vector for today's organization. Unmanaged and uncontrolled endpoints are the main sources of malware infections. Misuse of endpoints through privilege elevation or privilege abuse also augments endpoint threats. Against the backdrop of persistent increase in number of endpoints, it becomes increasingly critical to grant endpoint access based on "need-to-know" and "need-to-do" basis. Therefore, security, risk management and compliance leaders find great merit in deploying endpoint security solution- ARCON Endpoint Privilege Management (EPM) as it provides a solid layer of endpoint security.
A unified endpoint governance engine, the solution offers a rule and role-based controlled access to business-critical applications, ensuring adherence to the principle of least privilege.

Importantly, what sets ARCON EPM apart from other endpoint governance tools Is the fact that it offers File Integrity Monitoring (FIM) as well. FIM as a standalone solution is not that easy to manage, and often results in ineffective deployment. ARCON EPM is embedded with FIM capability to enhance the compliance posture of an organization.

In March and April 2021, the department of police in one of the cities in Texas suffered massive data loss as one of its employees deleted 8.7 million critical files (approx. 23TB of data) by mistake. These files included crucial evidence of many criminal cases in video, photos, audio, case notes, and other items the police department collected. It resulted in slowing down the process of prosecutions impacting around 17,500 cases with the County District Attorney's Office.

This is an ideal instance where a government department faced an IT disaster though there were no malicious or fraudulent activities. The employee was unable to manage and verify the existence of the files before deleting them and there were no backups.

"File Integrity Monitoring (FIM)" feature of Endpoint Privilege Management (EPM) solution could have averted the disaster by checking and identifying any modifications or changes made to any file or directory. Once it detects any sudden unauthorized changes, it sends instant alerts to the IT administrator who investigates and takes prompt action.

In this paper, we have discussed how FIM enables IT compliance teams in maintaining an organization's audit and compliance policy by adhering to prescribed mandates.

Why is FIM a Critical Component of Endpoint Security

Infrastructural changes in the enterprise IT environment are unavoidable and uncontrollable. Continuous additions and alterations of new users, devices, and servers generate unexpected changes or additions to system files, host files or configuration files.

Simultaneously, new risks emanate from organizations' changing IT infrastructure. IT administrators' challenges revolve around continuous monitoring of the end-users' activities, detection of malicious activities by analyzing who is accessing which file for what purpose and when. Even a single anomaly in the network can be very risky and raise questions on audit and compliance.

In this context, endpoint security management is comparatively a less-discussed area. Malicious insiders or even third-party users can compromise business information assets by misusing endpoints like deleting or changing files in systems. And these unauthorized changes on files can happen at any time, and by any means.

Non-detection of such changes (both intentional or unintentional) can be catastrophic from a regulatory compliance and security perspective. Hence, IT administrators need a solution that offers everything under one roof. File Integrity Monitoring (FIM), a critical component of endpoint security, fits in the role because -

- FIM is crucial to complying with IT standards
- FIM is also important to ensure IT operational effectiveness as without this tool organizations can face operational challenges
- Many approved and unapproved changes in the files can create confusion, risks, and IT negligence

We believe that FIM as a standalone feature can seldom help to achieve the desired security level and compliance standards. If data integrity needs to be managed effectively, FIM security features must be integrated with endpoint security platforms for better risk assessments and risk management.

Role of File Integrity Monitoring as Additional Security Layer

IT infrastructure is constantly changing and complex. File Integrity Monitoring continuously assesses the changes or transitions happening in the enterprise network, especially to the critical file servers, devices, important applications, or other IT systems.

FIM is a tool that finds out the change and records it with further analysis to determine whether the activity is authorized or not. Not only that, the most revolutionary and remarkable feature of FIM is that it can also reverse the action by transforming the system or application to the earlier baseline configuration. As a result, the IT administrators get a chance to rectify any unprecedented or anomalous action. The tool raises an alert for the entire change as an official intimation to the IT security team.

Gartner® in its report "Best Practices for File Integrity Monitoring" (ID: G00368216) clearly explains the types of changes in an organization and whether it is desired/ acceptable or not.

Change	Description	Desired Outcome
Expected Change	This is a change triggered by internal management or operational activities, such as patches or progressive/ planned alteration, and it is usually well-executed.	✅
Expected Bad Change	This change is not solicited, but can be linked to a legitimate change, and includes requests that did not plan out well or did not result in an anticipated change. Such changes lack a malicious intent but may lead to system malfunctions.	❌
Unexpected Change	This is an unexpected change that is okay (i.e., there is no malicious intent); however, it creates a lot of noise.	❌
Unexpected Bad Change	This type of change cannot be linked to an internal or legitimate trigger. It may have malicious intent or be an early indicator of attack or compromise, internally or externally.	❌

File Integrity Monitoring with ARCON Endpoint Privilege Management (EPM)

The File Integrity Monitoring (FIM) tool in ARCON | EPM keeps a thorough check on any unauthorized file changes/transfers on end-user devices and identifies if the 'change' is an unauthorized one. If required, the entire action is rolled back. Indirectly, it works as a threat predictive tool by indicating a warning that some malicious/ unexpected action has taken place. If any organization is unaware of the activities, then it could remain unaware of the possible threats to the IT infrastructure.

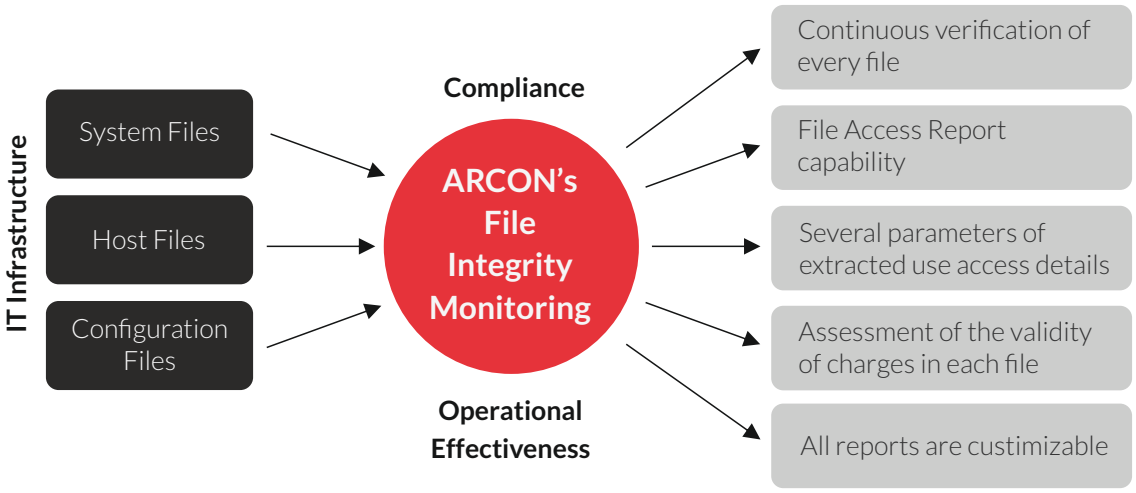
Here are the salient features of File Integrity Management embedded with ARCON | EPM -

- ARCON's FIM is an **automated process** that ensures continuous verification of every system file alteration against baseline configuration
- All the files can be **restored to the last possible checkpoint** so that there are no chances of information misuse
- ARCON's FIM has the **File Access Report capability** that enables IT administrators to know the access details of each file accessed by the IT user
- The IT user access details extracted by FIM are based on several parameters, such as access patterns, **access reasons, and the context behind the access**
- The reports generated by ARCON's FIM provide an **assessment of the validity** of the changes done to the files at a given point of time
- Incident Management **workflow can be set with tools like SNOW** and based on the classifications configured, the incidents can be identified as 'authorized' or 'unauthorized'
- **The reports are customizable** and can be downloaded in PDF, MS Word, MS Excel, and CSV formats
- Granular level filter configurations provide a **detailed summary of the activity alerts** and other subsequent activities performed by the user
- All these event data logs (alerts, text logs) are **stored in syslog and event log server** as a complete backup of logs

"The File Integrity Monitoring (FIM) capability can track unauthorized file changes on user device in real time and processes, track unauthorized changes and keep a track of file history, and roll back if needed. This level of data governance and lifecycle management is unusual in a EPM product and is very welcome, especially in the environment where remote and home working, and subsequent new data flows, is prevalent." - **Paul Fisher**, Senior Analyst from KuppingerCole explains in one of the Executive View reports titled **"ARCON Endpoint Privilege Management"** dated 11 July 2022.

Read the full Report here

Architecture of File Integrity Monitoring



FIM for Compliance and Audit

FIM is mandated by multiple global regulatory standards, that require organizations to follow best practices to maintain data integrity, data security, and data privacy.

- PCI DSS (Payment Card Industry Data Security Standard) mandates payment card organizations to have File Integrity Monitoring (FIM) to monitor and detect suspicious changes that happen to the system files regularly.
- The SOX (Sarbanes-Oxley) Act of 2002 specifies FIM as its core requirement.
- ISO 27001 (International Organization for Standardization) requires real-time FIM as the basis of data security policy.
- The NERC (North American Electric Reliability Corporation), one of the crucial American compliance bodies, mandates FIM capabilities for document security.

Conclusion

FIM is essential for ensuring data integrity, but it is also a requirement to maintain IT operational effectiveness as well. Without FIM, organizations risk facing operational challenges. If approved and unapproved changes to critical system files are undocumented or there are no alerts in place, organizations can face untoward risks resulting in IT ineffectiveness and operational challenges.

About ARCON

ARCON is a leading enterprise information risk control solution provider, specializing in Privileged Access Management (PAM) and continuous risk assessment solutions. Our mission is to help enterprises identify emerging technology risks and help mitigate them with robust solutions that predict, protect and prevent.