ManageEngine
Log360 Cloud

File integrity monitoring

in Log360 Cloud

USE CASE DOCUMENT

Are you ready for granular visibility?

As a security manager, it is vital to gain visibility and insights into critical files within your network. A capability like file integrity monitoring (FIM) can elevate your team's potential to detect and respond to threats. Let's look at the various ways FIM can help your team.

What is FIM?

Imagine FIM as a vigilant librarian, armed with magical glasses that spot even the tiniest book circulating in your digital bookshelf. In simple terms, FIM is an IT security process that allows analysts to monitor the tampering of files and maintain their integrity. FIM ensures your files are on their best behavior by standing guard and protecting your digital realm from the chaos of unauthorized modifications and covert file capers. Welcome to the show, where FIM takes center stage.

FIM's customizable dashboards shine a spotlight onto tampered files and unauthorized users. This provides your team with consolidated file and user data, charts and graphs for visualization, and more. It's a visual feast for security managers everywhere.

What challenges does FIM resolve?

Every organization has critical assets and sensitive information in their digital environment. With thousands of files, manual management and tracking can be excruciating. This is where FIM comes in.

FIM solves the critical problem of ensuring the integrity and security of an organization's digital assets. It addresses unauthorized or unexpected changes to files within a computer system or network. There is a huge array of use cases for this feature that range from detecting ransomware and insider threats to preventing data exfiltration and more.

How does it work?

FIM works by deploying agents on individual or multiple machines. The agent initiates the modification of Active Directory policies and system access control lists (SACLs) to gather data from specific file locations and get access to Windows security logs.

FIM in ManageEngine Log360 Cloud employs an in-house correlation engine that reads individual Windows events (e.g., Event IDs 4656, 4664, 4659) and correlates them to identify modifications and accesses to files and folders.

FIM use cases

Let's now go over three use cases where FIM will make an impact for your business.

1. The protection of crucial files

Did you know that attackers frequently use files as their cyberattack vectors? Although operating systems, applications, and software differ greatly throughout platforms, files are used by almost all contemporary computers, making it a convenient choice. Similarly, a lot of the data that people and companies today use are stored in files.

How FIM helps

When it comes to sensitive or business-critical files, FIM is an invaluable tool for identifying and responding to changes in file access and permissions.

- FIM can provide real-time alerts when there are changes to file access permissions. This enables security teams to respond quickly to any changes that may impact the security of sensitive files.
- User actions, such as modifications to file permissions, are monitored by FIM. This enables organizations to keep an eye on who is modifying the access controls so security teams can look into any suspicious or unauthorized actions.

Continual monitoring enables organizations to identify and prevent unauthorized access, data tampering, or malicious activities. By detecting and responding to security incidents in real time, FIM helps enterprises minimize the downtime and disruptions.

2. Malware detection

Did you know that in 2022, there were 5.5 billion malware attacks worldwide? These attacks use a file or code that is usually distributed via a network and is designed to infect, explore, or steal. This gives attackers the ability to obtain confidential information, send fake emails from your email account, and gradually slow down your computer. This is why it's crucial to monitor your files and folders.

How FIM helps

Malware frequently tries to modify or alter important system files, so FIM detects unauthorized changes, including file modifications and creations. Any abnormal spike in file changes triggers immediate alerts based on customizable alert criteria. These alerts make it possible for your team of security analysts to respond quickly to possible malware infections, investigate the issue, and mitigate the threat as soon as possible.

Since FIM helps in promptly identifying and addressing malware, you can safeguard private information and lower the chance of data breaches. Additionally, you can implement appropriate corrective measures to lessen the malware's effects and stop further damage. With FIM, your business can save major expenses related to incident response, remediation, and potential legal liability resulting from data breaches.

3. Compliance management

FIM ensures the security and integrity of important files and configurations, making it an asset for fulfilling compliance requirements. By adopting a proactive approach toward cybersecurity and data protection, organizations can use FIM solutions to demonstrate compliance with industry-specific requirements and standards.

FIM assists enterprises in adhering to these regulatory standards through constant monitoring and detection of any unauthorized changes or access to critical files and directories. Organizations can maintain the dependability and trustworthiness of their data—which is essential for compliance—by quickly recognizing and resolving integrity issues.

How FIM helps achieve compliance

- Organizations that process credit card payments must use FIM in accordance with the PCI DSS. FIM monitors and detects changes to system files and configurations that may have an impact on security, which helps safeguard cardholder data.
- The GDPR highlights the significance of privacy and data protection. By preventing unauthorized file accesses and modifications to sensitive data, FIM supports GDPR compliance by assisting in maintaining the integrity of files holding personal data.
- Healthcare organizations are legally bound to protect sensitive patient information. By guaranteeing the integrity of files relating to patient health and databases, FIM assists healthcare organizations in meeting HIPAA data security regulations.

A FIM tool should assist organizations with out-of-the-box, compliance-ready templates for all file operations. This will help organizations save several work hours spent on manually auditing, documenting, and managing file creation, deletions, or modification events.

How Log360 Cloud can help

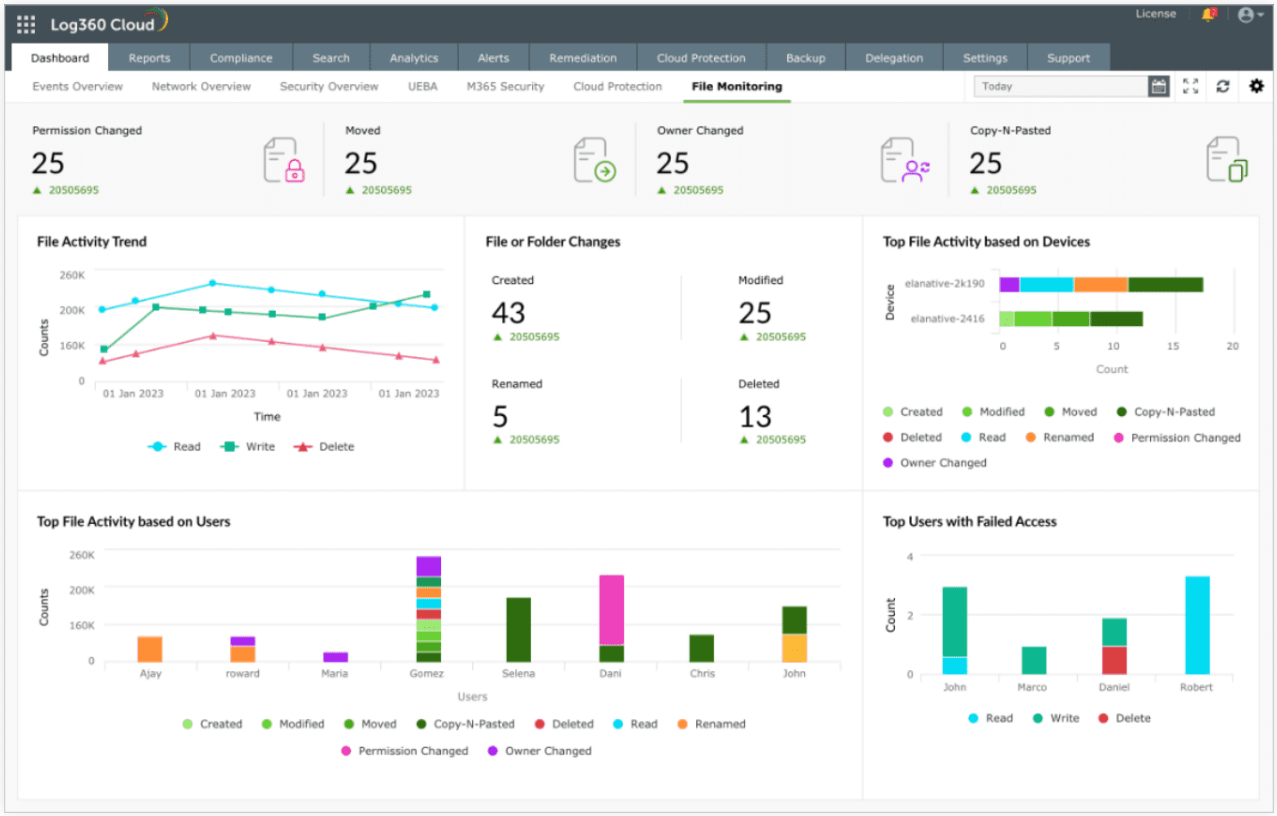
Log360 Cloud is ManageEngine's cloud-based SIEM solution that provides comprehensive visibility and security management across both on-premises and cloud environments in a single platform.

Manage the details of what needs to be monitored

You can configure individual devices and also create templates with Log360 Cloud to indicate the locations of files and folders that need to be monitored for multiple devices. This feature can help reduce redundancy and increase efficiency. Filters are another tool you can use to include or exclude files, folders, and subfolders for monitoring.

Track real-time changes to files and folders

You can access dashboards and reports on all creations, deletions, modifications, owner changes, and permission changes made to files and folders using Log360 Cloud. It also tracks all unsuccessful file access attempts. This feature has multiple benefits for your security team such as early detection of potential threats, including IT sabotage, ransomware, malware, and more. This can reduce your team's mean time to detect and respond.



Track any modifications made to a file or folder's permissions

Attackers can potentially bypass all security alerts related to unauthorized accesses by first changing permissions to sensitive files and folders before gaining access to your data. Log360 Cloud monitors all the permission changes in files and folders.

Receive instant alerts to changes in files and folders

Configure alerts to receive real-time email or SMS updates. The system keeps track of unsuccessful change attempts and can notify your security team when a failed access threshold is exceeded.

Correlate events to ensure file integrity

With Log360 Cloud's correlation rules, users can specify a sequence of events that can indicate an anomaly or a security loophole. Get a deeper understanding of the incident by correlating the events occurring within your network, which may have been overlooked while examining the situation at the individual level.

Why wait? Try FIM in Log360 Cloud today

Files hold vital information needed for every organization's everyday operations, including collaboration, interaction, compliance, and decision-making processes. Effective file management and security are essential in today's digital world if an organization is to maintain its competitiveness, productivity, and reputation. The first step in creating a secure environment is recognizing changes in the surroundings in real time. Log360 Cloud allows you to monitor the integrity of important files and folders for your organization, keeping you safe against file-based threats, protecting sensitive data, and ensuring compliance.

About Log360 Cloud

ManageEngine Log360 Cloud, a unified cloud SIEM solution with integrated CASB capabilities, helps enterprises secure their network from cyberattacks. With its security analytics, threat intelligence, and incident management capabilities, Log360 Cloud helps security analysts spot, prioritize, and resolve threats in both on-premises and cloud environments. The solution is highly scalable and helps drive down infrastructure and storage costs. For more information about Log360 Cloud, visit www.manageengine.com/cloud-siem/.

Sign up: Access your free trial account

Get a personalized demo