ManageEngine
Log360

USE CASE

Using Log360 to monitor integrity of files and folders

Using Log360 to monitor integrity of files and folders

Malicious insiders and external hackers are always on the lookout for ways to sabotage your business. Tampering with critical files can aid attackers in activities such as accessing confidential data, crashing a business operations server, and even creating backdoors for future attacks. They could then cover their tracks by deleting logs. This is why monitoring critical activities on files and folders is essential for ensuring data security, and maintaining the integrity of the sensitive data stored in them. However, files and folders are subject to changes every day. The challenge is recognizing legitimate changes performed for regular operational purposes, compared to malicious changes that pose security risks. How do you distinguish between the two and ensure the integrity of your organization's critical files?

How Log360 can help

File Integrity Monitoring (FIM) is a security process that tracks changes to the operating system, database, application software, log files, and many other files and folders. ManageEngine Log360 is an easy-to-use SIEM solution that provides a dedicated FIM module to help you maintain the integrity of your data by protecting your critical files against illicit access and tampering.

Exercise granular control over what needs to be monitored

Log360 lets you create templates to specify the file and folder locations that need to be monitored. You can also use filters to include or exclude files, folders, and subfolders for monitoring. These templates can be applied to as many devices as required.

Monitor file and folder changes in real time

Ensure that your data and critical configuration files are safe by monitoring executable files, folders, system configuration files, content files, zipped files and folders, and more. Log360 provides you with security analytics dashboards and reports on every access creation, deletion, modification and permission changes made to files and folders. You can also configure alerts for real time notifications through email or SMS. The solution tracks failed attempts to make changes, and can alert security teams when the number of failed access or change attempts crosses a threshold.

Monitor permission changes made to files and folders

Even when strict controls for data access are implemented, malicious actors might succeed in enacting a data breach. They could first modify permissions to sensitive files and folders and then access the data, thus escaping all illicit access security alarms. Log360 monitors all the permission changes made to files and folders. The solution also provides prebuilt alerts to notify you of changes made to file and folder permissions.

Meet compliance requirements with ease

Most regulatory mandates, such as the PCI-DSS, FISMA, HIPAA and GDPR, require you to implement strong FIM techniques to safeguard sensitive data from illegitimate access and modifications. To demonstrate compliance, you need exhaustive reports that list all the changes made to the files and folders that store critical data. Log360 provides those reports out-of-the-box, and even lets you create custom reports to simplify your compliance audits.

Detect data exfiltration in real time

Log360 features a powerful correlation engine that provides several prebuilt rules such as suspicious file access, external file removal, failed file access attempts, and more. These rules help detect data exfiltration attempts by both malicious insiders and external hackers. For instance, one of the predefined correlation rules, Suspicious file access, is triggered only when a number of failed access attempts precede a file modification.

Mitigate quickly with the incident management system

Log360 comes with an end-to-end incident management system that has a built-in ticketing module which helps assign tickets to security admins, track their status, and ensure accountability in the incident resolution process. This system also includes an automatic remediation framework that can associate workflow profiles with correlation rules. These workflow profiles can be executed automatically when a correlation alert is triggered to remediate the incident.

Ensure the integrity of your organization's critical files and folders with ManageEngine Log360.

Supported file systems and platforms

Log360 provides extensive out-of-the-box FIM support for a wide range of devices, such as Windows file servers, failover clusters, Linux file servers, EMC servers, and NetApp filers.

Gartner's Peer Insights Voice of the Customer 2023 is out!

ManageEngine named a Customers' Choice for SIEM

Check out why

Latest Gartner Magic Quadrant for SIEM is out!

ManageEngine recognized in Gartner's Magic Quadrant for Security Information and Event Management, 2024.

Get the report

Log360, a comprehensive SIEM solution, helps detect, investigate, and mitigate security threats and cyberattacks. With its intuitive security dashboard, log correlation, threat intelligence, advanced threat analytics, machine learning-based user and entity behavior analytics, and end-to-end incident management capabilities, the solution helps companies enhance and maintain their cybersecurity posture, detect intruders, and pre-empt attacks. Automate incident resolution with Log360's workflow and incident management console. Secure data residing in physical and cloud platforms with advanced security monitoring. Comply with the regulatory mandates with Log360's audit-ready report templates.

For more information about Log360, visit our website.

ManageEngine Log360

$ Get Quote

⤓ Download