

Best practices for file integrity monitoring

File integrity monitoring examines file changes for tampering of any kind, or indicators of a possible cyberattack. It's an ongoing process that requires a combination of strategic practices and comprehensive tools. Follow these file integrity monitoring best practices to detect a potential attack promptly, and minimize the chances of cyberattacks.

8 best practices for file integrity monitoring

1. Assess files to be monitored

Create a list of the files and directories that need to be monitored. This generally includes system files, configuration files, sensitive information like personally identifiable information (PII), etc. Exercise caution—auditing too many directories will only lead to alert fatigue, and make it difficult to perform root cause analysis in case of an attack.

2. Test and evaluate your strategy

Employ a virtual setup that mirrors your infrastructure to test scenarios. Review how processes and procedures work in case of unauthorized file changes. When deploying file integrity monitoring software, viewing a demo in your infrastructure will help you choose the right tools for your environment. Take time to convey to all employees the changes that will be brought about by implementing file integrity monitoring practices.

3. Monitor cloud applications

In addition to auditing file servers, control web traffic and keep track of data going in and out of the cloud. Monitor file uploads by users to services like Office 365, Dropbox, and cloud applications. Keep track of user and file activity through your cloud environment with the aid of cloud protection software. Wherever necessary, block user access to risky websites and applications.

4. Establish incident detection and response

Contextual information on every file change—including who made the change, when, and from where—is essential to verify file integrity. Set up alerts and automated responses for excessive file changes triggered by malware or insider activity. Use file change notification software to detect mass file modifications or deletions, and immediately respond to the activity by shutting down the user device.

5. Define user privileges

Document user permission guidelines, and define exceptions with respect to organizational roles. Define user accountability policies to keep user privileges in line. Detect permission inconsistencies and files with open access with a security permissions analyzer to streamline your remediation strategy.

6. Formulate an organizational policy

File integrity monitoring isn't only useful as a security auditing tool, but is mandated by PCI-DSS, HIPAA, and other regulations. PCI DSS mandates organizations to monitor changes made to critical files, particularly audit logs, system files, and configuration files.

These regulations also recommend drafting a plan detailing which tool will be run, and how frequently. Maintain periodic checks to ensure the plan is executed promptly and effectively.

7. Evaluate IT infrastructure changes

Be informed when users or user groups are added to and deleted from access lists. Update your applications with patch fixes, and endpoints with the latest software versions. Integrate file change monitoring software with your security information and event management (SIEM) tool for spontaneous threat detection. The audit data from these tools is essential for post-incident analysis, and as forensic evidence.

8. Prepare for ransomware attacks

Protection against ransomware attacks needs significant emphasis when it comes to file security. Employ a ransomware detection tool to identify sudden spikes in file renaming events, file deletion, and permission changes. Spot these characteristic symptoms straight away to prevent a full-scale attack on your network. The tool also comes in handy to immediately defend your network by isolating the infected device from your network.

Next steps

- [Free trial](#)
Set up and evaluate DataSecurity Plus's capabilities with a free, fully functional 30-day trial.
- [Interactive demo](#)
View an online instance of DataSecurity Plus (available without signing up).
- [Guided product tour](#)
Schedule a demo to have a product expert walk you through the software and answer your questions.
- [Request a quote](#)
View pricing details and request a personalized quote

About DataSecurity Plus

ManageEngine DataSecurity Plus is a unified data visibility and security platform. It audits file changes in real time, triggers instant responses to critical events, shuts down ransomware intrusions, and helps organizations comply with numerous IT regulations. It also analyzes file storage and security permissions, deletes junk files, and detects file security vulnerabilities. Users can assess the risks associated with sensitive data storage by locating and classifying files containing PII, PCI, and ePHI. It also prevents data leaks via USBs, email, printers, and web applications; monitors file integrity; and audits cloud application usage.

[\\$ Get Quote](#)[⬇ Download free trial](#)