

File Integrity Monitoring

Employing steady-state monitoring to ensure the integrity of sensitive files is more than just a security best practice. For many organizations it is a regulatory mandate as well. By combining File Integrity Monitoring with enterprise-class Log & Event Management and Endpoint Monitoring & Control, LogRhythm allows customers to simplify and strengthen their security, audit and compliance posture with a single, fully integrated solution.

User-Aware File Integrity Monitoring

LogRhythm's holistic approach allows security personnel to be notified when files are created or key files are viewed, deleted or modified, and when group ownership of files is changed. For selective monitoring, LogRhythm provides granular controls and filters that can pinpoint specific files and perform scans at desired intervals. File-level behavior can then be correlated to additional security and audit activities to build a comprehensive window into potentially harmful network activity.

With the addition of File Integrity Monitoring, LogRhythm can be used to monitor for and alert on a variety of malicious behaviors, from improper user access of confidential files to botnet related breaches and transmittal of sensitive data. The combined solution allows organizations to meet specific regulatory compliance requirements, such as Payment Card Industry Data Security Standard (PCI DSS) 11.5 and 12.9, without purchasing a separate product.

Fully integrated with Log & Event Management and Endpoint Monitoring & Control

- Addresses 35 specific mandates of PCI DSS 1.2.
- Sends contextualized alerts whenever confidential data is viewed, modified or deleted.
- Provides a complete set of forensic data for rapidly identifying the root cause of security breaches.
- Centralized, policy-based configuration and administration.

Monitors All Types of Files in Near-Real Time

- Including executables, configuration files, content files, log and audit files, web files, database files, and more.
- Granular controls ensure that each monitored file is scanned at the desired frequency.
- User activity monitoring adds relevant context to file modifications and views by identifying what users and/or processes are logged into the system.

Out-of-the-box policies are provided for common applications.

LogRhythm File Integrity Monitoring is Supported on Windows, Unix and Linux systems.

PCI DSS 11.5 mandates:

Deploy file integrity monitoring to alert personnel to unauthorized modifications of critical system or content files, and perform file comparisons at least weekly or more frequently if the process can be automated.



“PCI compliance is just a snapshot. Assuming that you are safe because you take preventative measures makes you weaker – you must take action to be a step ahead of those who are constantly looking to exploit holes in your network.”

Bernie Rominski
IT Security Officer
Regis Corporation



File Integrity Monitoring Bundle Appliances

Include Log & Event Management, Endpoint Monitoring & Control and File Integrity Monitoring



LRX1-FIM Includes licenses for 25 servers



LRX2-FIM Includes licenses for 100 servers