PRODUCT OVERVIEW

# 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 FIM with fully integrated SIEM, Log Management, Machine Analytics and Host and Network Forensics, LogRhythm allows customers to simplify and strengthen their security, audit and compliance posture with a single, fully integrated solution.

**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.

## 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 either perform scans at desired intervals or operate in real-time mode for continuous protection. File-level behavior can then be correlated to additional security and audit activities to build a comprehensive window into potentially harmful network activity.

LogRhythm's policy-based FIM allows multiple policies to be assigned to the same endpoint, reducing ongoing management as policies are updated. For example, individual policies can be created for Linux Operating System files and directories, Web Application Servers, and DNS Servers. When the Web Application Servers and DNS Servers are running on a Linux Host, all three FIM policies will be combined. FIM multi-policy support simplifies management, ensuring that FIM policies are assigned to the appropriate assets and that changes to those policies are propagated across the environment.

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 80 different control requirements of PCI DSS
- 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

- Monitoring can be extended to executables, configuration files, content files, log and audit files, web files, point-of-sale systems, and more.
- Granular controls ensure that each monitored file is scanned at the desired frequency.
- Real-time FIM provides specific details about which user viewed, modified, or deleted what files.

## Ease of Deployment

- Out-of-the-box file policies are provided for common applications
- Supported on Windows, Unix and Linux systems
- Can be deployed on both desktops and servers
- Simplified policy support with the ability to assign multiple FIM policies to the same host