PRODUCT OVERVIEW

File Integrity Monitoring

LogRhythm
The Security Intelligence Company

You need to protect critical files. Whether you're dealing with malware-related file changes, improper access of confidential files, or theft of sensitive data, you need a way to continuously monitor all of your organisation's files. Even more importantly, you need a way to instantly know when a file's integrity has been compromised. LogRhythm's fully integrated File Integrity Monitoring (FIM) solution will strengthen your security and streamline compliance.

Continuously monitor files

With FIM, you will be notified when files are created or key files are viewed, deleted, modified, or when group ownership is changed. You can selectively monitor with 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.

Correlate file-level behaviour to enhance security and audit activities. Easily pivot from a file access or change to a specific user, then view a full timeline of user activity, containing both FIM and other activity information.

With LogRhythm's policy-based FIM, you can assign multiple policies to the same endpoint, reducing ongoing management overhead 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 are combined. FIM multi-policy support simplifies management, ensuring that FIM policies are assigned to the appropriate assets and that changes to those policies are centrally managed and propagated across the environment.

In addition, FIM can detect changes to systems outside of authorised change control windows. LogRhythm detects these changes by monitoring production servers for changes that occur outside normal operating windows or changes that don't precede an authorised change request.

With the addition of FIM and the data it generates, LogRhythm can monitor for and alert on a variety of malicious behaviours, from improper user access of confidential files to botnet-related breaches and transmittal of sensitive data.

Monitors all types of files

- Extend monitoring to executables, configuration files, content files, log and audit files, web files, point-of-sale systems, and more
- Scan monitored files at the desired frequency with granular controls
- Review specific details about which user viewed, modified, or deleted what files—all in real time

Easy to deploy

- Pre-configured file policies are provided for common operating systems
- Simplified policy administration with the ability to assign multiple FIM policies to the same host
- Supported on Windows, Linux, and UNIX systems
- Available for deployment on both desktops and servers

Why File Integrity Monitoring?

- Easily address over 80 different control requirements of PCI DSS and many core HIPAA requirements
- Alert and report using pre-configured FIM policies
- Streamline compliance objectives to allow increased focus on critical security priorities

"We use LogRhythm extensively to meet PCI and SOX compliance. It is also used on a day-to-day security and monitoring basis."

– Network Administrator, Large Enterprise Retail Company

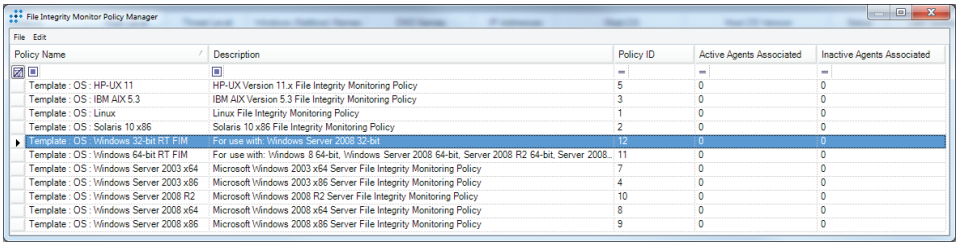

Fig. 1 The LogRhythm FIM Policy Manager lets you create and manage FIM policies specific to a host type, operating system, or application. Templates are provided so you can quickly and easily implement FIM.

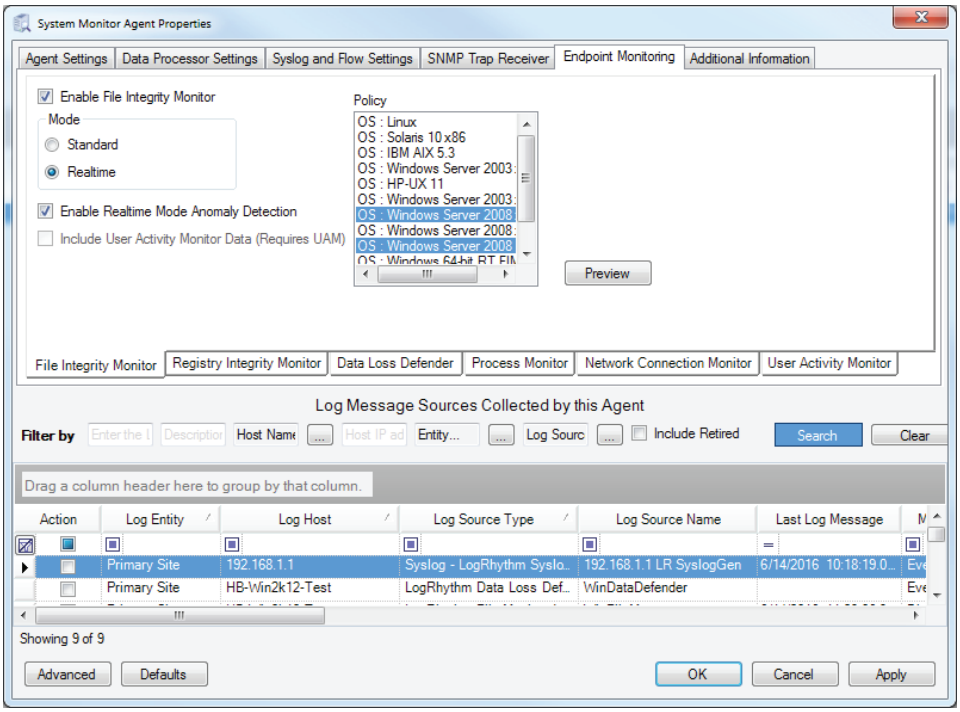

Fig. 2 The LogRhythm System Monitor Agent Properties allows you to easily assign one or more policies to the same target host. Any overlapping policies assigned to the same host are automatically mitigated.

Comply, secure, and optimise

- Automate and simplify compliance with pre-configured rules and reports
- 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
- Rapidly identify the root cause of security breaches with a complete set of forensic data
- Receive contextualised alerts whenever confidential data is viewed, modified or deleted
- Centralised, policy-based configuration and administration

Meet compliance mandates

LogRhythm helps you address compliance mandates that focus on data classification and protection by providing pre-configured compliance automation modules that address many of the most common regulatory frameworks, such as PCI-DSS and HIPAA.

PCI-DSS 11.5

Deploy file integrity monitoring software to alert personnel to unauthorised modification of critical system files, configuration files or content files. Configure the software to perform critical file comparisons at least weekly.

LogRhythm's unified solution

FIM is an embedded capability of the LogRhythm System Monitor—a lightweight agent that also provides activity and process monitoring. System Monitor is integrated with the LogRhythm Security Intelligence Platform to combine real-time endpoint monitoring with big data analytics for detecting advanced attacks and insider threats. With this unified solution you can:

- Save time on management, reporting, and monitoring
- Lower your total cost of ownership
- Gain pervasive visibility of file activity across your organisation