



File Integrity Monitoring (FIM) with Log Manager™

File Integrity Monitoring

Regulations such as PCI DSS 2.0 (10.5.5, 11.5), Sarbanes-Oxley 404, HIPAA, the ISO 27000 standards and the EU Data Protection Directive require File Integrity Monitoring (FIM) to prove compliance. FIM solutions typically detect changes to specific files being monitored, compare current “signature” (checksum) to the previously known signature, and sample checksums periodically any errors or discrepancies.

Unfortunately, FIM can be very costly and a challenging control to manage. In order to simplify and automate these requirements, Alert Logic provides customers the ability to receive FIM alerts and reports by integrating Alert Logic Log Manager’s console with leading FIM solutions.

FIM Use Cases

Scenario 1: Addresses PCI Compliance Standards

- PCI 10.5.5: Use file integrity monitoring or change detection software on logs
- PCI 11.5: Deploy integrity monitoring tools to alert personnel to unauthorized modification of critical system files

Scenario 2: Increased Security Through File-Level Monitoring

- Detect file changes and access related to malware and other exploits
- Set alerts to notify access to a specific device or process
- Verify that no unauthorized machines are communicating with a sensitive environment

Scenario 3: IT Operations Tool to Track File Updates/Changes

- Track unauthorized changes to network devices, such as firewalls and routers
- Report successful software updates to applications
- Set alerts for critical system warnings: disc failures, memory over-utilization, loss of connectivity

Products and Services

Third-Party FIM Solutions Support

Parsing support available for the following platforms:

- Windows
- IIS
- Unix
- Cloudmark
- Tripwire
- MONIT
- MS SQL
- CLIC

Custom parsers available upon request.

OSSEC FIM Solution

OSSEC is an open-source Host Intrusion Detection System (HIDS) that also performs the FIM function to track file changes within an IT environment. This solution provides a “free” alternative for customers who do not want to invest in a dedicated third-party FIM solution.

In support of the OSSEC solution, Alert Logic provides installation and setup instructions, base OSSEC.conf files, parsers, saved views, and basic support for customers.

Agent-Based Platform Support:

- AIX 5.2, 5.3
- BSD (Open, Free and Net)
- Linux (RHEL, Ubuntu, Slackware, Debian, etc.)
- Mac OSX 10.x
- Solaris 2.7, 2.8, 2.9, 10
- VMWare ESX 3.0, 3.5
- Windows 2000, XP, 2003, Vista, 2008

Agentless Platform Support:

- CheckPoint firewall
- Cisco ASA, IOS routers, PIX, FWSM
- Juniper netscreen
- Sonic firewall

Standard Saved Views in Log Manager:

- File created
- File deleted
- Root kit check
- Checksum changed