OTAVA

DATA SHEET

FILE INTEGRITY MONITORING

Quickly catch unexpected file and folder changes

Let's face it... there are files and folders on your systems that require protection from unintended modification in order to ensure a secure environment as well as compliance with many regulatory bodies. Otava File Integrity Monitoring (FIM) provides valuable insight into your technical environment and offers an additional layer of data security. Otava FIM is a service that can monitor any changes made to your files, regardless of circumstance.

FIM is customizable and simple to manage - Choose which folders and files you want to monitor and Otava manages the security management console and FIM notification process.

You're a perfect fit for Otava File Integrity Management if...

- Your business desires greater control and protection of data, seeks a better method to identify the source of system or human errors, and needs a way to identify the source should a breach or attack occur.
- Are looking for a zero-CAPEX, fully managed cloud recovery target Your business is required to monitor change detection for PCI-DSS compliance.
- Your business is required to protect ePHI under HIPAA privacy rules.
- Your business requires reporting control under SOX accountability requirements.
- Your business must protect data according to articles of GDPR regulations.

Why Otava File Integrity Monitoring?

Compliant, Secure, High Availability, Managed Service

Otava offers File Integrity Monitoring to detect unauthorized file system modifications in accordance with PCI DSS requirements. It is also a recommended service to assure data and record integrity for many other compliance and regulatory bodies.

Given the dynamic nature of Information Technology, changes to files and file attributes are both frequent and necessary. However, some changes may impact file or configuration integrity - by accident, misuse, or malicious intent. These changes can compromise security or even indicate a breach.

Otava's FIM solution, based on OSSEC from Trend Micro, helps ensure that files on your network are both secure and compliant. The service monitors and evaluates file/system changes and records alerts when suspicious, or unplanned activity is detected.

Otava's FIM service automatically and periodically compares current files and systems to a known-safe baseline and provides summaries to administrators of any changes.

How is FIM Configured?

A Simple, Dependable Software Solution

An agent, or software is installed on a server. Direct logging is sent to the security management console (managed by Otava - Software OSSEC configured by the client). Anomaly alerts are summarized and provided to administrators at a regularly scheduled interval.

Modify Rules to Match Requirements

An agent, or software is installed on a server. Direct logging is sent to the security management console (managed by Otava - Software OSSEC configured by the client). Anomaly alerts are summarized and provided to administrators at a regularly scheduled interval.

Compliance Reporting

Otava reports changes to files on a weekly basis for compliance. Clients have the ability to change the frequency of this reporting.

How File Integrity Monitoring Works

Otava's File Integrity Monitoring and Compliance

PCI DSS

FIM is required in order to meet PCI DSS compliance. PCI requirement 10.5 requires companies to secure audit trails so they cannot be altered, and requirement 11 requires regular testing of systems and processes. Specifically, the use of FIM relates to sub requirements 10.5.5 and 11.5.5.

HIPAA

FIM is recommended as an added level of security and to help met HIPAA requirements for protection of ePHI data from improper alteration or destruction and to corroborate the same. FIM can help meet these standards by tracking files and user activity within a system. Specifically HIPAA standards §164.312(b) §164.312(c)(1) and §164.312.(c)(2) are pertinent to the use of FIM.

GDPR

Applies to the protection of personal data for EU residents. Specifically, the use of FIM applies to articles 25, 32 and 59.

FISMA

Regulations for federal data security standards. Specifically, the use of FIM applies to NIST 800-171 and NIST 800-53 regarding the integrity and risk management for government data.

SOX

Sarbanes-Oxley, US Law intended to protect investors from fraudulent corporate accounting practices. Section 404 speaks to "internal control over financial reporting" for which FIM is a useful tool.

PCI-DSS | **HIPAA** | **GDPR** | **FISMA** | **SOX/COBIT**

Otava File Integrity Management Benefits:

- FIM provides additional security with alerts to track change management, including registry changes
- FIM provides notifications and alerts that can help the client remediate the situation
- FIM is customizable to monitor specific folders and files.
- FIM is managed by Otava. (Leave the heavy-lifing to us!)

OTAVA

OTAVA provides secure, compliant hybrid cloud solutions for service providers, channel partners and enterprise clients. By actively aggregating best-of-breed cloud companies and investing in people, tools, and processes, Otava's global footprint continues to expand. The company provides its customers with a clear path to transformation through its highly effective solutions and broad portfolio of hybrid cloud, data protection, disaster recovery, security and colocation services, all championed by its exceptional support team. Learn more at www.otava.com.

READY FOR IMPROVED COMPLIANCE & ADDED SERCURITY OF FIM?

Talk to a specialist now.

OTAVA.com (877) 740-5028 solutions@otava.com