FIM+ for z/OS

Advanced Mainframe Threat Detection and Security Compliance

Preventing a malicious attack is a significant challenge for any mainframe security team. Typical file monitoring methods that are meant to detect changes to vital systems are often behind the ball, reporting discrepancies too late to prevent damage.

FIM+ for z/OS is a quick-response monitor for mainframe components, able to scan files on schedule or on demand, identify even minor changes within seconds, and send an alert to an existing SAF or SIEM.

FIM+ can provide immediate, conclusive evidence that the mainframe environment is unaltered. When used regularly, FIM+ can create a full audit trail to help prove compliance with today's rigorous data security standards, such as PCI DSS Version 3.2, Requirement 11.5.

A unique, trusted baseline key is generated for each file and application and stored securely in a vault. Each component can then be verified against its trusted version. Even changes made by privileged users are detected, potentially preventing an internal attack.

FIM+ keeps a sharp lookout for unauthorized or unrecognized changes to:

- Executable programs and libraries
- JCL, HTML, panels, scripts, rate tables
- Configuration and control members
- Log files such as SMF, DB2, IMS
- Other sequential files and GDGs

If a problem is found, an alert can be sent to the enterprise SIEM for delivery to the security team. If a deeper scan is warranted, the component can be examined bit by bit to determine the what and when of any discrepancy. And how about that SIEM? Is it intact? FIM+ can inspect it, too, and sound the all-clear.

FILE INTEGRITY MONITORING
for z/OS Mainframes

- Meets **PCI DSS 11.5** requirements
- Proves history of **COMPLIANCE**
- **DETECTS ATTACKS**
  external or internal
- Verifies audit results
  ON DEMAND
- **INTEGRATES** with existing
  SAF AND SIEM systems
- **PROTECTS** critical information
- **IDENTIFIES ERRORS**
  or accidental updates
- Expands **OVERSIGHT**
  and protection
- Quick install, **QUICK RESULTS**

FIM+ for z/OS complies with regulatory standards:

PCI DSS 11.5 • FISMA • NIST • HIPAA • GDPR

SDS
DO MORE WITH LESS

FIM+ for z/OS = Mainframe file integrity monitoring
PLUS application validation and on-demand audits

Active Monitoring for Mainframe Files

Although file monitoring has become standard on other platforms, the z/OS mainframe hasn't had an equivalent solution. Until now. FIM+ for z/OS actively monitors mainframe files and can work with existing security systems for full reporting and alerting.

Because FIM+ has very little overhead, a typical weekly scan can be run much more frequently—even hourly—without impacting operations. Scans can be scheduled, random, or on demand to meet the needs of any security protocol.

Breach Detection & Prevention

FIM+ for z/OS actively monitors mainframe files and applications for changes to critical components. A trusted baseline key is created for each element and stored securely in a vault. FIM+ keeps watch, comparing the current state to the stored, trusted state.

If a discrepancy is found, an alarm can be sent in real time to the enterprise SIEM so that the issue can be immediately investigated. FIM+ can also run a deep scan that analyzes the file bit by bit to determine if an incident is a potential security breach.

PCI DSS 11.5 Compliance

For any business that transmits payment card information, file integrity monitoring is a core requirement to meet the Payment Card Industry Data Security Standard. PCI DSS 11.5 requires active monitoring of mainframe files to assure file integrity. Based on comparison to trusted keys, FIM+ can conclusively prove that production files are intact. FIM+ then exceeds standard file monitoring systems by examining full application suites and providing on-demand results. Over time, FIM+ can show a history of file integrity.

Integration with Existing Security Software

FIM+ seamlessly integrates with existing SAF and SIEM systems. Even a minor alteration to scanned data triggers a change event, which can be written to syslogs or sent to the enterprise SIEM and used to send alerts. Any changes can be cross-checked with a change management tool to ensure they are authorized, which helps avoid false alarms.

Comprehensive Audit Trail

When used regularly, FIM+ creates a comprehensive audit trail to detect issues or confirm compliance. Auditors can immediately see the frequency and results of scans, including change records and exception data.

FIM+ answers questions about data integrity, exposure, and compliance, providing a long-range analysis as well as up-to-the-minute information.

About SDS

Founded in 1982, SDS supports over 25 products for z/OS, MVS, VSE, VM, AIX, Linux, and Windows. SDS has licensed more than 1,000 enterprise clients worldwide with quality mainframe software and offers award-winning technical support. Comprehensive solutions focus on security, encryption, data compression, and network monitoring. SDS has partnered with MainTegrity, Inc., to bring you FIM+ for z/OS. To learn more, please visit our web site.

Software Diversified Services • www.sdsusa.com • info@sdsusa.com • 1322 81st Ave NE, Minneapolis, MN 55432