PowerTech
your security expert

SECURITY REVIEW

File Integrity Monitoring

Secure sensitive data against unauthorized changes

OVERVIEW

Users have access to corporate data through more avenues than ever. Protecting unauthorized access to all of them is crucial—not to mention a requirement of eminent security standards like the Payment Card Industry Data Security Standards (PCI DSS).

Fortunately, **file integrity monitoring** (FIM) prevents unauthorized configuration and data changes from going unnoticed. The right combination of FIM methods and solutions can keep your critical and sensitive data secure.

BASELINE VS. REAL-TIME MONITORING

There are two main ways to monitor file integrity. Baseline validation is effective for determining if a configuration file has been altered from its desired state. Taking a copy—typically after any authorized change—establishes the baseline against which future copies are checked for discrepancies. This, however, does not identify the source and timing of the event causing the discrepancy.

Real-time monitoring records these discrepancies and even records an event if a file is returned to its desired state before the next validation. It also sends notification of noncompliance more quickly than periodic baseline validation. But because it monitors in real time, it can affect performance.

Depending on the file and data, the best approach is to combine these methods. In any case, both require someone to review the file changes to determine whether or not they were authorized.

FIM ON IBM i

IBM i manages much of its server operations through system values. This differs from some operating systems, which rely on files for their configuration. Instead of scouring for configuration changes to individual files, the IBM i OS allows security officers to watch auditing facility records for system value changes.

The Compare Physical File Member command, triggers, and journaling give IBM i users the ability to monitor changes to database files, which typically hold an application's configuration and data. While these facilities are part of a successful FIM infrastructure, they aren't designed for that purpose, and each have shortcomings when used alone.

POWERTECH FIM SOLUTIONS

PowerTech has designed a portfolio of solutions that leverage and extend the core features of IBM i. Many provide specific benefits to an organization embarking on a FIM initiative.

The PowerTech Group, Inc.
www.powertech.com

TEL USA: 253.872.7788
TOLL FREE: 800.915.7700

DataThread

Real-time file monitoring of unauthorized activities—including field-level changes made through low-level utilities—combine with real-time email alerts, e-signatures, and powerful filtering to virtually eliminate false positives and ensure no change passes unnoticed. **DataThread**™ also sends an instant notification when highly sensitive data is viewed.

Compliance Monitor

A highly scalable compliance and audit reporting solution, **Compliance Monitor**™ provides visibility to hundreds of IBM i configuration settings. Forensic reports over event-based audit journal entries are complemented by its impressive baseline validation functions for system values.

Network Security

Permissive object-level authority renders IBM i audit controls useless when access originates from client applications like FTP, ODBC, and remote command. Much like an internal firewall, **Network Security**™ provides auditing and access control for non-traditional interfaces.

Interact

With visibility to IBM i audit entries—as well as to requests logged by Network Security—**Interact**™ facilitates real-time notification to an enterprise syslog sever or messaging solution. The source filtering capabilities of Interact ensure that only important events are escalated.

CONCLUSION

Timely reaction to unauthorized changes can mean the difference between an attempted breach and an actual breach. Combining IBM i features with PowerTech solutions makes it viable to monitor and alert on unusual activity—even if your configuration suffers from overly powerful users or open public access.

Are you considering a FIM initiative? The following process can help you implement smoothly:

- Determine if FIM is mandated
- Identify and locate sensitive data
- Identify critical configuration values
- Implement PowerTech solutions to monitor and report on non-compliance

GET THE WHITE PAPER

Learn more about how PowerTech can simplify your FIM initiative. Find more information and download the white paper at **www.powertech.com/fim**.

About the PowerTech Group, Inc.

Because Power Systems servers are used to host particularly sensitive corporate data, every organization needs to practice proactive compliance security. As an IBM Advanced Business Partner with over 1000 customers worldwide, PowerTech understands corporate vulnerability and the risks associated with data privacy and access control.

Visit www.powertech.com to find white papers, case studies, and product demonstrations. Or, call 800-915-7700 (USA) or 253-872-7788 to speak to a Security Advisor.

IBM Business Partner