CASE STUDY

IBM i File Integrity Monitoring with FileScope

Asian Insurance Provider *Anonymized | Confidential*

Client Profile

Industry	Insurance
Region	Asia-Pacific
Environment	IBM i — 4 LPARs supporting policy administration, claims processing, customer management, financial systems, and regulatory reporting
Security Scope	File Integrity Monitoring (FIM), Sensitive Data Protection, Compliance Monitoring, and Change Detection
Assessment Type	Cybersecurity Risk Reduction & Regulatory Compliance Initiative

The Challenge

The insurance provider relied on IBM i systems to manage highly sensitive customers, policyholders, claims, and financial information. As regulatory requirements and cybersecurity threats continued to evolve, the organization recognized the need for greater visibility into changes affecting critical files, directories, and sensitive data repositories.

Limited Visibility into File and Data Changes

Security and compliance teams lacked a centralized mechanism to monitor modifications occurring within critical IBM i file systems. Concerns included:

- Unauthorized modifications to sensitive business data
- Difficulty identifying who changed critical files and when
- Limited visibility into file creation, deletion, and modification activities
- Challenges detecting suspicious or unexpected changes
- Increased investigation time during security incidents

The organization required continuous monitoring capabilities to detect and report file-level changes affecting business-critical information.

Growing Regulatory and Compliance Requirements

Insurance regulators and internal auditors required stronger controls around data integrity and monitoring. Compliance challenges included:

- Demonstrating accountability for sensitive file changes
- Maintaining audit trails for critical business information
- Detecting unauthorized access or modifications
- Supporting internal investigations and compliance reviews
- Reducing the risk of data tampering or accidental changes

The institution needed a solution capable of continuously monitoring critical files and generating actionable alerts when unauthorized activity occurred.

Solution Deployed

Raz-Lee deployed the following iSecurity modules across the IBM i environment:

iSecurity FileScope

Implemented continuous File Integrity Monitoring (FIM) for critical IBM i files, directories, and sensitive data repositories.

Capabilities included:

- Real-time monitoring of file creation, modification, deletion, and rename activities
- Detection of unauthorized changes to critical business files
- User-level accountability for file-related activities
- Automated alerts for suspicious or unexpected modifications
- Centralized reporting and audit trail generation
- Monitoring of sensitive data locations and business-critical directories
- Support for compliance and regulatory reporting requirements

The implementation provided security teams with immediate visibility into changes affecting critical information assets across the IBM i environment.

Results

- Improved visibility into file and data integrity across critical insurance systems
- Faster detection of unauthorized or suspicious file modifications
- Strengthened controls protecting policyholder and claims information
- Enhanced audit readiness and compliance reporting capabilities
- Reduced investigation time during security and compliance reviews
- Increased accountability for file-related activities
- Improved monitoring of sensitive business information
- Deployment completed without disruption to daily insurance operations

The organization significantly improved its ability to protect critical information assets while strengthening compliance and operational security controls.

Key QSA Feedback

> *"Protecting the integrity of policyholder and claims information is a fundamental requirement for our business. FileScope provided the visibility and control we needed to identify unauthorized changes immediately, support regulatory compliance efforts, and strengthen confidence in the integrity of our IBM i environment."*

— Information Security Manager (paraphrased)