CASE STUDY

IBM i Anti-Ransomware & Antivirus Protection

Insurance Company *Anonymized | Confidential*

Client Profile

Industry	Insurance
Region	Americas
Environment	IBM i — 2 LPARs supporting policy management and claims processing
Security Scope	Ransomware Prevention & Malware Protection
Assessment Type	Internal Security Review & Cybersecurity Hardening Initiative

The Challenge

The client's IBM i environment hosted critical insurance operations and sensitive customer information, making it a strategic target for ransomware and malware attacks.Following several ransomware incidents affecting organizations within the insurance sector, the company identified major security concerns within its IBM i infrastructure.

Ransomware Protection

The organization lacked a dedicated IBM i-native solution capable of:

- Detecting abnormal file encryption activity
- Identifying mass file modifications in real time
- Alerting administrators before operational impact occurred stopping suspicious jobs or users

The security team required immediate visibility into malicious behavior targeting production libraries and shared business data.

Malware & Virus Detection

The existing security posture did not include native antivirus protection for IBM i integrated file systems (IFS) and exchanged files.

The company required:

- Continuous malware scanning
- Detection of infected files entering the environment
- Protection against malicious uploads and file transfers
- Reduced risk of malware propagation across interconnected systems

Operational Requirements

The organization needed a solution that:

- Could be deployed rapidly without application changes and Operated natively on IBM i
- Minimized performance impact on production workloads
- Integrated with existing security monitoring processes

Solution Deployed

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

iSecurity Anti-Ransomware (AR)

Implemented real-time ransomware detection and automated response capabilities for IBM i.

- Continuous monitoring of file activity and encryption behavior
- Detection of abnormal file modifications and mass encryption patterns
- Automatic response actions to stop suspicious processes and users
- Immediate alerting for security administrators
- Protection for production libraries and critical business data

The implementation enabled the organization to identify ransomware-related activity before operational disruption could occur.

---

iSecurity Antivirus (AV)

Implemented native malware and virus protection for IBM i environments.

- Real-time antivirus scanning for files within the IFS
- Detection and quarantine of infected files
- Protection against malicious file transfers and uploads
- Scheduled on-demand scanning processes and signature updates

The solution helped secure file exchanges between IBM i and external systems while reducing malware exposure risks.

Results

- Improved protection against ransomware attacks targeting IBM i workloads
- Real-time visibility into suspicious encryption and file activity
- Reduced risk of malware propagation through transferred files
- Faster incident response through automated detection and alerting
- Deployment completed with no application modifications required
- Minimal impact on IBM i system performance and business operations
- The organization significantly strengthened its IBM i cybersecurity posture while maintaining operational stability for critical insurance services.

Key QSA Feedback

> *“Ransomware became one of our highest security concerns. Raz-Lee provided a native IBM i solution capable of detecting suspicious activity immediately while also protecting our environment against malware threats. The deployment was fast, efficient, and integrated smoothly into our existing operations.”*

— IT Security Manager (paraphrased)