CASE STUDY

IBM i Command Protection & Administrative Control

Latin American Insurance Group *Anonymized | Confidential*

Client Profile

Industry	Latin American Insurance Group
Region	Latin America
Environment	IBM i — 4 LPARs supporting policy administration, claims processing, customer management, financial operations, and regulatory reporting
Security Scope	Command Protection, Privileged Access Control, Administrative Security, and Compliance Monitoring
Assessment Type	Internal Security Hardening & Privileged User Risk Reduction Initiative

The Challenge

The insurance group relied on IBM i to support mission-critical business operations involving policyholder information, claims data, financial transactions, and regulatory reporting. As the number of administrators, operators, and third-party support personnel increased, the organization identified growing risks associated with unrestricted command-line access.

Excessive Privileged Access

Users with elevated authorities had access to powerful IBM i commands capable of modifying system configurations, accessing sensitive data, and affecting business operations. Concerns included:

- Unauthorized execution of sensitive commands
- Excessive privileges granted to operational personnel
- Risk of accidental system modifications
- Potential misuse of administrative authorities
- Limited control over powerful native IBM i commands

The organization required tighter control over command execution without impacting on the productivity of authorized administrators.

Compliance and Audit Requirements

Internal auditors and regulatory reviewers requested stronger controls governing privileged user activities. Challenges included:

- Demonstrating control over administrative functions
- Reducing risks associated with privileged users
- Enforcing separation of duties
- Limiting access to critical system functions
- Strengthening accountability for command execution

The organization sought a solution capable of controlling, restricting, and monitoring command usage across the IBM i environment.

Solution Deployed

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

iSecurity Command

Implemented advanced command protection and administrative control capabilities for IBM i.

Capabilities included:

- Restriction of access to sensitive IBM i commands
- User and group-based command authorization policies
- Prevention of unauthorized command execution
- Granular control over administrative activities
- Enforcement of separation-of-duties requirements
- Centralized management of command permissions
- Detailed auditing of command access attempts

The implementation allowed the organization to maintain operational flexibility while significantly reducing risks associated with privileged access.

Results

- Reduced exposure to unauthorized administrative activities
- Improved control over powerful IBM i system commands
- Strengthened separation of duties across IT operations
- Reduced risk of accidental or intentional system modifications
- Enhanced compliance with internal governance requirements
- Improved accountability for privileged user actions
- Increased visibility into command execution activities
- Deployment completed without disruption to insurance operations

The organization significantly improved its control over administrative access while strengthening security governance across its IBM i environment.

Key QSA Feedback

> *"Administrative privileges are necessary for managing our IBM i systems, but unrestricted command access creates unnecessary risk. iSecurity Command allowed us to enforce precise controls over sensitive commands, strengthen compliance efforts, and significantly reduce our exposure to privileged-user threats without affecting operational efficiency."*

— IT Security Manager (paraphrased)