CASE STUDY

IBM i DB-Gate Securing Cross-Platform Database Integration

Latin American Software Factory *Anonymized | Confidential*

Client Profile

Industry	Software Development & Technology Services
Region	Latin America
Environment	IBM i integrated with Oracle, SQL Server, PostgreSQL, MySQL, BI platforms, customer portals, and third-party applications
Security Scope	Cross-Platform Database Access Control and Data Governance
Assessment Type	Data Integration Security & Customer Compliance Initiative

The Challenge

The software factory developed and maintained business applications that relied on IBM i as a central repository of operational and customer data. As the organization expanded its services, increasing amounts of DB2 for i data were being exchanged with Oracle, SQL Server, PostgreSQL, MySQL, cloud applications, and business intelligence platforms.

Growing Database Integration Requirements

Multiple applications and external platforms required direct access to IBM i data for reporting, analytics, customer portals, API services, and data synchronization. This included:

- DB2 data being accessed from multiple external database platforms
- Difficulty controlling which users and applications could access sensitive information
- Increased risk of unauthorized data extraction
- Limited visibility into cross-platform database access activity
- Need to maintain security without disrupting integrations

The IT team required a solution capable of protecting DB2 data while allowing legitimate business integrations to continue operating normally.

Customer Data Protection and Compliance

Many customers require assurance that sensitive information stored on IBM i remained protected even when accessed through external systems. Key concerns included:

- Exposure of customer records through reporting and integration tools
- Access to sensitive tables by non-authorized applications
- Lack of granular controls over integrated database environments
- Compliance requirements related to data access governance
- Increasing audit requests from enterprise customers

The organization needed stronger controls at the IBM i database level, regardless of which platform initiated the connection.

Solution Deployed

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

iSecurity DB-Gate

Implemented centralized database access control for DB2 on IBM i, securing access originating from IBM i applications as well as external platforms.

Capabilities included:

- Granular control over access to DB2 files, tables, and fields
- Protection of sensitive information regardless of access method
- Security enforcement for Oracle, SQL Server, PostgreSQL, MySQL, ODBC, JDBC, and reporting tool connections
- Restriction of access based on users, groups, applications, and jobs
- Monitoring and logging of database access attempts
- Enforcement of corporate data governance policies
- Centralized administration of database security rules

The implementation allowed the company to continue expanding its integration ecosystem while maintaining strict control over sensitive IBM i data.

Results

- Secured DB2 data accessed from Oracle and other external database platforms
- Improved governance across integrated application environments
- Reduced risk of unauthorized data extraction and exposure
- Strengthened protection of customer and proprietary information
- Enhanced visibility into cross-platform database activity
- Simplified compliance audits and customer security assessments
- Maintained seamless operation of existing integrations and business processes
- Deployment completed without application modifications

The organization successfully established a security layer protecting IBM i data across its entire integration architecture, ensuring that business growth and connectivity did not compromise data security.

Key QSA Feedback

> *"Our IBM i environment had become a central data source for numerous applications and database platforms. DB-Gate allowed us to maintain complete control over sensitive DB2 information, regardless of whether access originated from Oracle, SQL Server, reporting tools, or external applications. This significantly improved both security and compliance across our integration landscape."*

— Chief Technology Officer (paraphrased)