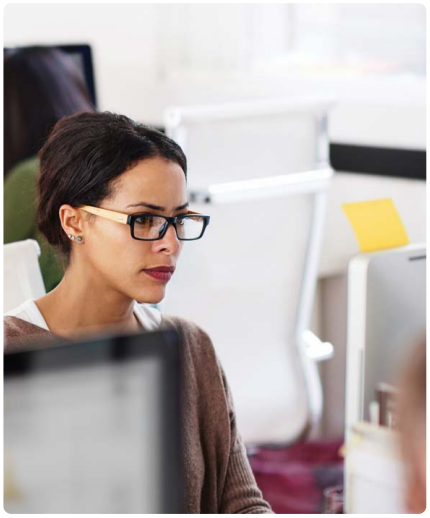
Large International Financial Services Organization

Within just 8 weeks Voltage and SDM deliver secure data exchange between mainframe and Azure for regulation compliance and data analytics.



PSD2 Compliance Complicates Data Management

Like all European banks, this large organization works within the new open banking era. Open banking makes bank information available to third parties throughout the European Economic Area. It aims to optimize banking and give customers greater control over their financial data, which they can freely share with third parties by giving their specific consent. In turn, banks will be able to offer customers new, more personalized services. To secure open banking, all European banks must comply with the Payment Services Directive 2 (PSD2). This increases the security of online payments and makes banking more competitive, which benefits customers. It also gives customers the chance to control who has access to their accounts and how they can access them.

Exchanging financial data securely is a challenge faced by all banks, as the Data Security Engineer for this particular organization explains: "Being a large bank, we hold over 20TB of account data, much of it very sensitive. This is stored on a mainframe environment, hosted in our various data centers. We tried to publish all the data required by PSD2 from the mainframe but there just was no effective and secure way to share this data in a sustainable manner."

He continues: "When people think of a mainframe, they assume very robust data security. This is true, but to comply with regulations and new ways of working, we must transport the data securely, which is an issue in a closed mainframe environment. In partnership with Microsoft we decided on an Azure cloud approach with daily replication from our data center. Although Azure offers some security features, we felt this was not sufficient for sensitive data in transit, or in use in the cloud for data analytics, so together with Microsoft and our consultancy partner Accenture we looked for a solution."

"Voltage and SDM were implemented in just eight weeks and we saw the benefits straightaway. Micro Focus has a unique and innovative cybersecurity solution that enabled us to seamlessly replicate our sensitive data into an Azure cloud environment, ready to be leveraged and analyzed as required."

SENIOR PROGRAM MANAGING ARCHITECT
Large international financial services organization

At a Glance

Industry

Finance

Location

Spain

Challenge

Securely unlock mainframe-based data to comply with open banking industry regulations and enable more flexible reporting and data analytics

Products and Services

- Micro Focus Voltage SecureData Enterprise
- Micro Focus Structured Data Manager

Critical Success Factors

- Vastly enhanced reporting and data analytics capabilities
- Seamless cloud integration with robust encryption algorithms
- Fully compliant with PSD2, PCI, and GDPR regulations
- Short 8-week implementation timeframe

"The combination of Voltage and SDM means data can be safely decrypted on-the-fly which is very helpful in our scenario. This flexibility makes it much easier to create reports and perform analytics, enabling data-driven decision making which is vital for our organization's future success."

SENIOR PROGRAM MANAGING ARCHITECT
Large international financial services organization

Contact us at **CyberRes.com**
Like what you read? Share it.

Voltage Robust Encryption and Azure Cloud Integration

With the explosion of data and the regulatory pressures such as the General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standard (PCI DSS) and PSD2, companies must enforce solid policies and procedures across the full information lifecycle. Micro Focus Voltage SecureData Enterprise secures sensitive data wherever it flows: on-premises, in the cloud, and in big data analytics platforms. Accenture and Microsoft liked the robust data protection deployed by Voltage with its SecureData integrations for Azure capabilities. The team felt Voltage would be a great addition to the bank's architecture and in a joint agreement between Micro Focus and Microsoft, the solution was implemented.

"We particularly like the Voltage encryption and pseudonymization capability," says the Senior Program Managing Architect. "With other solutions you can encrypt the data in transit, but you can't easily reverse this. This is not helpful when you need the data for analytics purposes as we do. Voltage's pseudonymization means that personally identifiable information fields are replaced by one or more artificial identifiers, or pseudonyms, for a securely reversible, two-way data transformation."

Voltage + SDM = a Winning Team

To manage its high data volumes with solid processes and analytics without compromising performance, the team chose Micro Focus Structured Data Manager (SDM). This enables organizations to secure data according to the latest compliance and protection requirements, including GDPR, PCI DSS, and PSD2. SDM integrates with Voltage SecureData to automatically encrypt sensitive data in place or in the archive using Format-Preserving Encryption (FPE). FPE makes it possible to integrate data-level encryption into legacy business applications. This is the key to success, as otherwise the organization's data analysts would need to develop custom-made queries and algorithms and manual processes.

Voltage and SDM manage a nightly incremental data replication from the mainframe into Azure Big Data as the organization's data lake. Azure Databricks executes any necessary data transformation, i.e., building a full name from first and last name fields, after which the data is then stored in the organization's Azure SQL Database. Third party providers can then consume this data through cloud API connectors, maintaining full data security.

The use of SDM can be expanded to identify sensitive data that the organization may not be aware of. By scanning all the data available, SDM can discover, analyze, and classify the data. Agreed upon algorithms can then either protect this data through the Voltage encryption process or recommend it for archiving or deletion if the data is redundant. This automated process has the potential to realize significant cost savings, and further risk reduction through defensible data deletion. The organization is interested in exploring this soon.

Full Analytics and Reporting Flexibility in Just 8 Weeks

"The integration of Voltage and SDM means data can be safely decrypted on-the-fly which is very helpful in our scenario," says the Senior Program Managing Architect. "This flexibility makes it much easier to securely create reports and perform analytics in cloud services, enabling data-driven decision making which is vital for our organization's future success."

He concludes: "Voltage and SDM were implemented in just eight weeks and we saw the benefits straightaway. Micro Focus has a unique and innovative cybersecurity solution that enabled us to seamlessly replicate our sensitive data into an Azure cloud environment, ready to be securely used and analyzed as required."