MICRO FOCUS

Case Study

Security

# Leading Provider of Business Processing Services

Voltage delivers data-centric security to streamline fraud detection and prevention without exposing sensitive data.

## Applying Fraud Analytics to Data while Complying with Regulations

In a world where fraud moves fast and across all channels, modern fraudsters can exploit banking silos. This organization's powerful fraud fighting platform empowers organizations to stand united against fraud, harnessing the strength of advanced analytics applied to cross-bank data, and benefiting from dedicated product, fraud intelligence, and data science resources.

To make this a reality, the team faced several challenges, as explained by the Senior Program Managing Architect: "We needed to adhere to strict data protection rules such as SOX and PCI, while still allowing our data scientists to work on the data, including Personally Identifiable Information (PII) and credit card details. And how could we test on production data? Disk encryption is a basic requirement for regulation compliance, but that doesn't solve the issue of applying analytics to exposed data. Data masking was another option, but this is a one-way transformation and you cannot replicate insights with masking."

The existing infrastructure was another major consideration. The team did not want to support an isolated system; any new solution had to fit seamlessly into the existing landscape, consisting of a fully virtualized environment, leveraging Hadoop and Hortonworks to process the high data volumes flowing into the system from its member banks.

**"Before Voltage, our product managers could not access the data at all. Now that they can, they are using the data to review volumes and emerging trends to be ahead of the game with new offerings. Our data scientists apply AI machine learning to the data to drive insights into fraud detection and prevention, without exposing any sensitive data."**

**SENIOR PROGRAM MANAGING ARCHITECT**
Leading business processing organization

## Voltage Data-Centric Security Model—Data Stays Encrypted

The Senior Program Managing Architect researched the market thoroughly for the latest trends in data security: "Pure data masking tools did not support the regulations we need to comply with. However, when I learnt about Micro Focus Voltage, my interest was piqued straight away. With Voltage Format-Preserving Encryption (FPE), the data stays encrypted end-to-end throughout the process. That, right there, would massively increase my data security."

## At a Glance

- **Industry**
  Software and Technology
- **Location**
  Canada
- **Challenge**
  Enable wider access to sensitive data for analytics and testing purposes, by introducing a data-centric security model
- **Products and Services**
  Micro Focus Voltage SecureData Enterprise
- **Critical Success Factors**
  + Mature data protection practice
  + Secure advanced analytics provide insights into fraud detection and prevention without exposing sensitive data
  + Secure data testing environment
  + Improved disaster recovery and high availability
  + Successful partnership with Micro Focus Professional Services

> **"Voltage is the one-stop shop for all our data security use cases. It complies with all current data privacy regulations, integrates superbly into our environment, and has matured our data protection approach and processes."**
>
> **SENIOR PROGRAM MANAGING ARCHITECT**
> Leading business processing organization

Contact us at:
**www.microfocus.com**

Like what you read? Share it.

Voltage embeds protection in the data itself, and this data-centric security model keeps the data usable for analytics and business processes. System analysts and QA engineers can do their jobs in a safe environment, with data flowing in its protected form without breaking applications or databases. As an added bonus, Voltage is designed to integrate seamlessly with all leading big data platforms, including those in use at this organization.

Micro Focus Professional Services supported the implementation: "We wanted support and hands-on Voltage training, specific to our environment and use cases," says the Senior Program Managing Architect. "Working with the Micro Focus Professional Services consultants was the best experience I have had in the industry! They supported us all the way from start to finish, ensuring our use cases worked within the Voltage environment and were integrated into our wider infrastructure. We were up and running within just three months, which really speaks to the maturity of the Professional Services engagement."

Voltage now sits on top of Hadoop and Hortonworks, ensuring mature data protection. Nothing is ever stored in the clear, and all data is housed decentralized on local Hadoop instances. Product managers can log onto a user-friendly tool to view data activity, without seeing any sensitive data, such as PII and credit card information, as this is permanently encrypted. The Senior Program Managing Architect values the ease of access he can give users: "Before Voltage, our product managers could not access the data at all. Now that they can, they are using the data to review volumes and emerging trends to be ahead of the game with new offerings. Our data scientists apply AI machine learning to the data to drive insights into fraud detection and prevention, without exposing any sensitive data."

He adds: "with Voltage FPE we can match and search on the encrypted data. We really appreciate the mature integration with our existing access control, monitoring, and authentication and authorization environments, which eases compliance, audits, and privilege management."

Voltage has enabled a secure data testing environment in which all direct and secondary identifiers have been removed so that the Quality Assurance team can work directly on the data. The Voltage motto of 'encrypt once and decrypt rarely, or only when needed' works perfectly, as the Senior Program Managing Architect illustrates: "We try not to decrypt at all. If we need to, Voltage allows us to decrypt the bare minimum, such as one field or a row, in memory only, never at disk level or during processing."

## Controlled TCO in a Transparent Security Model

The importance of data security sits at the very center of this organization's success. Voltage, with its Stateless Key Management, supports load balancing between two data centers to provide reliable disaster recovery and high system availability. Maintaining keys and a key vault in a traditional approach to encryption would have reduced data protection.

The Senior Program Managing Architect comments: "Voltage is the one-stop shop for all our data security use cases. It complies with all current data privacy regulations, integrates superbly into our environment, and has matured our data protection approach and processes. The one-framework approach helps us control total cost of ownership (TCO) in a fully transparent security model."

He concludes: "Working with Micro Focus, and the Professional Services team in particular, has been a great experience. Leveraging Voltage, we can now satisfy all relevant security and governance policies; crucial for our success in the financial services industry."