opentext™ | Cybersecurity

Case Study

# Large Financial Services Company

**Voltage SecureData successfully protects confidential data wherever it flows while expanding analytics capabilities for deeper business insights.**

## Introducing Data-Centric Protection in an AWS Environment

Over the last couple of years, data protection has grown in importance, as data privacy regulations have tightened and technology has evolved. In response, this financial services company launched a corporate data protection program to protect restricted or confidential data in a consistent manner across the enterprise. Although data at rest was fully encrypted, data in transit was a different matter. In addition, it was felt that a columnar database model would provide more flexible data analytics opportunities. This led the team to the implementation of Vertica, on which its enterprise data warehouse is now based. A further data lake is based on Amazon S3, as part of an Amazon Web Services (AWS) cloud implementation.

The company's Director of Data Engineering explains further: "We have long been committed to AWS, and Vertica is deployed on top of Amazon EC2, leveraging Amazon S3 for data archiving and storage. We needed a data protection solution that would be compatible with this environment. Our challenge is to maintain referential data integrity while improving the ability to query data and perform sophisticated analytics. Exploring the market led us to Voltage SecureData. With its OpenText heritage, this solution has great native out-of-the-box capabilities to support our Vertica data processing. It also has a host of flexible libraries we can leverage, and an amazing track record in other financial services organizations."

> "Voltage SecureData reassures our business stakeholders and our customers that their data remains protected, no matter how it is leveraged within the company."
>
> **Director of Data Engineering**
> Large Financial Services Company

## Voltage SecureData FPE and UDFs Key in Providing End-to-End Data Protection

After a series of proof of concepts, the Voltage by OpenText™ implementation was underway, focusing on protecting the data that flows from thousands of data sources into the Vertica data warehouse and the S3 data lake for processing and analytics purposes. Amazon EMR is a managed cluster platform that simplifies running big data frameworks on AWS. As part of this infrastructure, Apache Airflow manages the workflow within AWS, with Jenkins as an orchestration tool, deployed on EC2. The company maximized scalability by introducing on-demand clusters to spin up specifically for Voltage SecureData by OpenText™ encryption.

### At a Glance

**Industry**

Financial Services

**Location**

USA

**Challenge**

Maintain referential data integrity to allow full movement for processing and analytics purposes while taking advantage of AWS cloud capabilities

**Products and Services**

Voltage SecureData

**Success Highlights**

- Flexible data-centric protection provides many expansion opportunities
- Full data privacy regulation compliance
- Native out-of-the-box Vertica support
- FPE capability improves productivity with reduced rework and ETL updates
- Data scientists provide deeper analytics insights

> **“Exploring the market led us to Voltage SecureData. With its OpenText heritage, this solution has great native, out-of-the-box capabilities to support our Vertica data processing. It also has a host of flexible libraries we can leverage, and an amazing track record in other financial services organizations.”**
>
> **Director of Data Engineering**
> Large Financial Services Company

**Connect with Us**
www.opentext.com

With almost 800 terabytes of data between OpenText™ Vertica™ and the S3 data lake, and over 5.5 trillion fields of encrypted data, this is a sizeable operation. When a data file comes through, Voltage automatically extracts relevant data fields and types to encrypt the data before loading it in Vertica so that it is encrypted from the source. It will continue its processing and analytics journey in an encrypted state for full protection. Leveraging Voltage SecureData’s User Defined Functions (UDFs) and SimpleAPI, sensitive data is protected using Format Preserving Encryption (FPE), either in the S3 data lake or in Vertica, depending on the source. No schema changes are required as the data format is preserved, enabling it to be queried by other applications and systems with persistent protection throughout its journey. Voltage SecureData can easily decrypt data to make the necessary transformations before loading the encrypted results back to a worktable. UDFs are also leveraged to empower database administrators to allow consumers clear access to data to perform certain types of business processing or reporting.

## Full Regulation Compliance, Improved Productivity, and Deeper Data Analytics

“We also use Voltage SecureData in our Master Data Management (MDM) tool to encrypt and decrypt data on the fly,” says the Director of Data Engineering. “This is where OpenText’s flexible pricing model comes into play and sets us up for strategic expansion. We subscribe to a per-event model, and this allows us to extend the Voltage capabilities to many different databases, in addition to Vertica.”

The new model of data-centric protection with Voltage provides the highest data security level and ensures full adherence to data privacy compliance standards. At the same time, it is flexible enough to modify data models and data standards, and apply new policies and best practices. “Voltage SecureData reassures our business stakeholders and our customers that their data remains protected, no matter how it is leveraged within the company,” says the Director of Data Engineering. “As we are now able to perform complex operations on encrypted data, we have noticed a reduction in the amount of rework and Extract, Transform, Load (ETL) updates we process. The solution allows us to share more datasets, and Voltage’s FPE capability makes it a faster and more compute-resource efficient process.”

He concludes: “With Voltage SecureData, we have increased the data volumes that we share with our data scientists for analytics and insight, to include restricted or confidential data that they previously weren’t authorized to access. The Voltage team clearly wanted to help us succeed and develop a solution that will stand the test of time. We see many opportunities for further use cases and the flexible licensing structure will pave the way for these.”

**opentext™ | Cybersecurity**

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.