Leading Technology Provider

Voltage SecureData partners with AWS to flexibly and scalably support data-centric protection in hybrid environment.

Ensuring Safe Payments in a Hybrid Environment

When this leading provider of technology solutions for the finance sector made a major acquisition, it created a best-in-class company to serve financial institutions and businesses worldwide. Its main aim is to streamline the checkout experience and online payments processing, so customers can easily and safely pay how they want, resulting in fewer abandoned carts and a lot more sales. The company's senior technology engineer explains why security and data integrity are imperative to the organization's success: "We process billions of transactions each year, managing very sensitive information such as credit card information and personal identifiable information (PII). We sometimes say there are two types of companies in the world: those who have been breached, and those who don't know they have been breached. We already relied on Voltage SecureData Payments to protect our payments data on a global scale. The acquisition made our environment more complex, with applications residing in physical datacenters, as well as hosted in AWS cloud Infrastructure as a Service (IaaS)."

> "Even in our new hybrid environment, Voltage gives us the flexibility and scalability we need to take our AWS cloud transformation initiatives to the next level with data protection and privacy by default."
>
> **Senior Technology Engineer**
> Leading Technology Provider

Although the company operates a 'cloud first' strategy, it is also universally accepted that not all applications suit a cloud environment and this hybrid model is likely to continue well into the future. Voltage's ability to move existing protected data between on-premises and cloud applications is unprecedented. As an example: data can be encrypted on-premises and moved to a cloud application where it can be decrypted easily and without risk, creating much-needed data resilience. Voltage SecureData Payments by OpenText is used to provide a worldwide tokenization service for merchants to tokenize and detokenize primary account numbers (PANs) using REST calls. It also provides encryption of PII customer data, using either REST calls or API integration, with Voltage SecureData File Processor (SDFP) by OpenText for bulk

At a Glance

Industry

Finance

Location

USA

Challenge

Protect payment data, both at rest and in transit, across 80+ applications in a hybrid on-premises and AWS environment

Products and Services

Voltage SecureData Payments

Success Highlights

- Effective and flexible data protection in hybrid environment
- Great integration with AWS
- Full data privacy regulation compliance, reducing audit scope and costs
- 80 applications leverage data-centric security

> “Because Voltage SecureData persistently protects data, both at rest and in transit, with industry-leading, format-preserving, stateless tokenization and encryption, we are PCI compliant, reducing our audit scope and costs.”
>
> **Senior Technology Engineer**
> Leading Technology Provider

Connect with Us
www.opentext.com

file encryption and decryption. Over 80 key applications now benefit from Voltage data-centric security, with a target to migrate all applications containing sensitive data to Voltage by 2024.

Voltage + AWS = a Winning Team

“As we operate in one of the most heavily regulated industries in the world, our compliance with global data privacy regulations is of paramount importance to us,” says the company’s senior technology engineer. “Because Voltage SecureData persistently protects data, both at rest and in transit, with industry-leading, format-preserving, stateless tokenization and encryption, we are PCI compliant, reducing our audit scope and costs. As we serve global audiences, we also need to be GDPR compliant, and Voltage provides the pseudonymization and anonymization required for this.”

Voltage operates a stateless architecture that enables unlimited growth, eliminating the need to synchronize data between datacenters and databases while guaranteeing high performance. Before Voltage was deployed, data residing on AWS was stored in clear form due to the lack of proper encryption and key management solutions. This clearly posed a security risk.

Deploying Voltage SecureData appliances on AWS in different regions and availability zones helps protect sensitive data locally on AWS. Data entered by business users and engineers moves protected via Voltage through a variety of AWS services, such as AWS Kinesis, AWS IoT, and AWS SQS into the AWS cloud environment, consisting of AWS S3, AWS EMR as a managed big data service, AWS Redshift for data warehousing, and AWS Elasticsearch, a popular open source search and analytics engine. EC2 is used for compute, AWS S3 for file storage, and R53 for DNS routing, while Amazon CloudFormation supports infrastructure automation.

Leveraging Voltage throughout, the data can then be decrypted and routed to BI users and data scientists via AWS Glue. AWS Glue is a serverless data integration service that makes it easy to discover, prepare, and combine data for analytics, machine learning, and application development. To process data at the scale required, the team leverages AWS Lambda for real-time data processing from Amazon S3-stored data.

Flexible and Scalable Data-Centric Security

The company’s senior technology engineer concludes: “We are grateful for the decision we made years ago to entrust our data protection to Voltage as it is clear it’s stood the test of time. Even in our new hybrid environment, Voltage gives us the flexibility and scalability we need to take our AWS cloud transformation initiatives to the next level with data protection and privacy by default. We value our partnerships with CyberRes (now OpenText Cybersecurity) and AWS, and are pleased to see ongoing engineering work to ensure that Voltage integrates with AWS offerings.”

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.