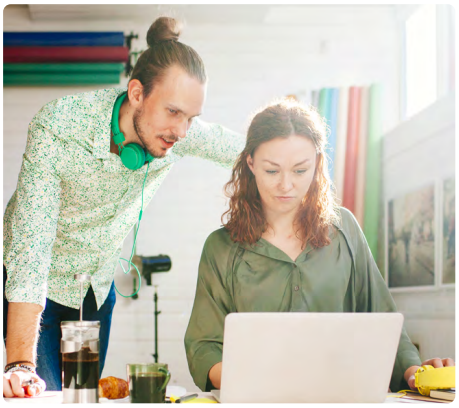
opentext™ | Cybersecurity

Case Study

Multi-National Retail Organization

Voltage SecureData Enterprise supports digital transformation by providing comprehensive data security to 7+ million cloud-hosted customer records.



Data-Centric Security vs Siloed Approach

With a global presence of over 12,000 physical stores, the organization is also extremely focused on digital transformation with a successful multi-channel approach.

In a classic IT model, organizations manage their security in a layered or siloed approach. Sensitive data flows between applications, the network layer, databases, file systems, and data center storage systems. Although the data is secured at each of these levels, there are inevitable security gaps between the different layers, as data moves around the infrastructure. A project manager for the organization's CISO office, explains the issue: "Although within the layers all data was encrypted, if a privileged user account is compromised this could still cause a data leak. We used SFTP for data flow protection, but the exchanged file contained plain text data which is risky too since it is stored between the different steps from the source to the destination. Our layer approach was also expensive, as each layer needed its own security solution with its own expertise, making resourcing complex. With an enterprise-wide move towards the cloud, leveraging Azure and Google Cloud, we needed the peace-of-mind of comprehensive data security. We felt transforming our security model to a data-centric approach would solve these issues."

"On average, we on-board a new application into Voltage every other week. We encrypt data by default so that it is only ever exposed when really required. This gives us a much better risk and compliance position."

Project Manager
CISO office
Major Retailer

Voltage: 'Privacy by Default'

Unlike point solutions that require system-based security integration, data-centric security enables trusted data to move between untrusted environments. It allows full data security as data moves from storage to in-flight to in use within applications, remaining entirely usable in encrypted form. After evaluating several market options, the organization moved forward with Voltage SecureData Enterprise by OpenText™, to drive business value through secure data.

Making 'privacy by default' central to the organization's security architecture means that data stays fully encrypted from the moment it enters the system. The data format and integrity, including validation rules, are respected through the use of Voltage's Format-Preserving Encryption (FPE) by OpenText™. Standard encryption can lead to data bloatage, where more fields are used in the encrypted format than in the original. This can result in system performance issues,

At a Glance

Industry

Retail

Location

Global

Challenge

Support customer's digital transformation while enabling them to focus on their core business and reduce hardware and maintenance investment

Products and Services

Voltage SecureData Enterprise

Critical Success Factors

- 7+ million customer records comprehensively protected
- Google Cloud and Azure cloud deployment
- Improved team collaboration and shared data knowledge
- Accelerated time-to-market to respond to changing business requirements
- Enhanced risk and governance position

“Working with Micro Focus (now part of OpenText™), we have enhanced collaboration between security, development, operations, and project teams as they share data knowledge they require for their particular task in the product lifecycle.”

Project Manager
CISO office
Major Retailer

Connect with Us
www.opentext.com

and unnecessary maintenance and support overhead. Leveraging Voltage FPE, partial or full fields are encrypted but the fields remain the same size and format. The project manager comments on the importance of this: “We have over seven million cloud-hosted customer records, each one containing up to 10 encrypted fields. [Voltage] FPE supports virtually any data type in any format and no database schema updates are required to preserve usability and referential integrity for data processes and applications. We can have field-specific decryption, for instance to decrypt just the fields required for sending emails during a marketing campaign.”

Fast Time to Market While Fully GDPR-Compliant

Traditionally, decryption key administration is complex and costly. An organization needs to maintain a key database, as well as the corresponding hardware, software, and IT processes required to protect the database continuously. There is typically also a need to replicate or backup keys from site to site. Not so with Voltage Stateless Key Management by OpenText™. This securely derives keys on-the-fly as required by an application, once that application and its users have been properly authenticated and authorized against a centrally managed policy. The keys don’t need to be stored as they are just generated when required, making life easier from an operations and disaster recovery perspective.

Fast time to market is everything, and service delivery improvement is a key success factor for the organization. The project manager recalls a recent scenario where having ‘security by design’ at the heart of the IT architecture proved invaluable: “Our marketing department came up with a great idea to engage our loyalty card holders through a collaboration with an innovative gaming company. We would gain valuable extra intelligence on our customers, while they could have some fun. Normally, we would need to fully understand how an application works and how it manages sensitive data, including data flows. However, the Voltage basis we have in place makes it easy for us to integrate 3rd party applications really quickly, often from start-up companies who are very agile, but may not have data security at their forefront. Because we keep control of the data access we can speed up the global process, while complying fully with GDPR and other relevant data privacy regulations. We accelerate our business, but in a fully secure manner.”

Big Data and Data Lake Protection

All data is captured in a Hadoop data lake where it stays encrypted. Consuming applications retrieve data from it and if it needs to be decrypted, Voltage manages the authorization through the key identifier stored in each data object. Google Big Query is used by the data science and business intelligence teams to process data correlation which drives data-driven decision making. Business analysts enjoy working with Voltage as it is clear the data is protected through its end-to-end lifecycle, while integrating with a broad range of environments, clients, and platforms.

Accelerated Application On-Boarding and Improved Team Collaboration

As part of its organization, a banking and finance division stores sensitive financial customer data. Applying the Voltage data-centric security principles at a central level means that the company saves time and money on individual Privacy Impact Assessments (PIAs), as the auditing authorities already have full visibility into the data security processes.

The project manager can see clear benefits: “As a result of implementing Voltage in a data-centric security model, we are more agile and can respond much faster to ever-changing business requirements. On average, we on-board a new application into Voltage every other week. We encrypt data by default so that it is only ever exposed when really required. This gives us a much better risk and compliance position.”

He concludes: “Working with Micro Focus (now part of OpenText™), we have enhanced collaboration between security, development, operations, and project teams as they share data knowledge they require for their particular task in the product lifecycle. We now feel very confident in our brand image: ‘all your data is encrypted—Your data is safe with us!’”

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.

768-000015-003 | O | 10/23 | © 2023 Open Text