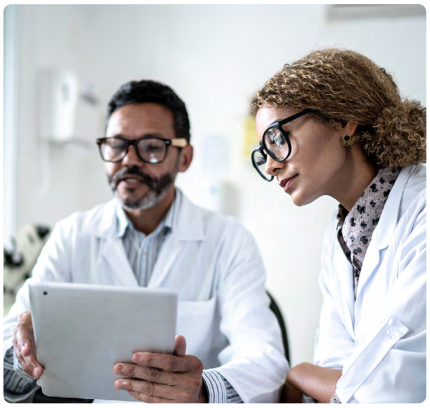
opentext™ | Cybersecurity

Case Study

Large Healthcare Insurance Organization



Voltage SecureData reduces costs and risk while safely enabling data monetization from big data cloud analytics platforms to SaaS web analytics.

Securing Customer Data in Analytics Platforms

As a major U.S. healthcare and health solutions company, and a provider of health insurance pharmacy benefits, this enterprise holds very sensitive data for its customers. Their IT organization is an early adopter of advanced technologies to support business initiatives, while also putting customer data security and privacy in the forefront of requirements for all their projects.

The data security story with Voltage SecureData began years ago with the introduction of data analytics technology and a Hadoop data lake to help drive insights and innovations for their customer offerings. They quickly saw then that hosting sensitive personal and health care data in a data lake, however, posed major security challenges. Anyone with access to the data lake had access to all data in the data lake. The limited number of data scientists couldn't keep up with the analytics needs of the business. The company needed a way to protect the data while allowing it to be accessed by developers, marketers, and other functions to accelerate insights and get value from the technology investment.

> "We found [Voltage] SecureData to be a cost-effective and flexible solution in securing our sensitive customer data compared with cloud-specific solutions that don't meet our need for end-to-end data privacy and protection."
>
> **Director of Enterprise Digital Initiatives**
> Healthcare and Insurance Organization

The Director of Enterprise Digital Initiatives noted: "The data in our data lake was too vulnerable to misuse to expose for analytics purposes to the wide audience we had in mind. We had to limit access to just a handful of data scientists, which defeated our purpose in making data analytics widely available in the organization so that we can drive data-driven decision-making across the board."

The organization had some previous relevant experience with the Voltage by OpenText portfolio and understood the benefits of stateless key management. Voltage stateless key management eliminates operational complexities of data encryption, and the automated on-demand key generation can be infinitely scaled with no additional overhead. A proof-of-concept showed the business owner that Voltage SecureData by OpenText could address the data protection needs and scale required for big data analytics. Voltage SecureData was successfully deployed and enabled secure use of data in its protected form for analytics—the team even opened the data lake to its developer community for an internal 'hackathon' to encourage innovative thinking and product ideas.

At a Glance

Industry

Healthcare Insurance

Location

USA

Challenge

Cost-effectively protect sensitive customer data from breach while leveraging the power of secure cloud and web analytics to support data-driven decision making

Products and Services

Voltage SecureData Enterprise
Voltage SecureData Sentry

Success Highlights

- Secure analytics on sensitive data, in cloud data warehouse (CDW) and SaaS platforms
- Enterprise-wide coverage of databases, applications, analytics platforms, and cloud workloads
- Full control with format-preserving encryption (FPE) for protected data portability across hybrid IT
- Integration flexibility with SecureData APIs, database UDFs, and Sentry JDBC and HTTPS interception
- Data protection in Adobe Analytics SaaS with substantial cost savings vs. point solutions

“With Voltage solutions, we can take full advantage of the benefits of cloud analytics platforms, including SaaS-based web analytics, prevent exposure of sensitive customer data, and realize substantial cost savings in the process.”

Director of Enterprise Digital Initiatives
Healthcare and Insurance Organization

Connect with Us
www.opentext.com

Voltage SecureData can easily be used with virtually any system, ranging from decades-old custom applications to the latest enterprise programs. The IT team has since that time extended Voltage data protection to many systems, including mainframe and Relational Database Management Systems (RDBMS), and over 150 applications across their distributed IT environment.

Securing Web Analytics Data Proves a Challenge

With the pharmacy benefits side of its business, a lot of customer interaction takes place on its website and so the team introduced a SaaS web analytics platform for more advanced data analytics to help streamline the customer experience. However, the Director of Enterprise Digital Initiatives noted: “Our web analytics provider does not have the security controls we require by law when we share our customers’ sensitive data. We had a data encryption solution in place, but it was not format-preserving and, as all analytics platforms are sensitive to data type and format, it was causing issues. We also discovered that deploying this solution against our large volume of web analytics data was very expensive, and so we looked for alternatives.”

Full Format-Preserving End-to-End Data Security with SecureData Sentry

Voltage SecureData Sentry by OpenText is a data protection and privacy broker that deploys easily into any existing infrastructure. Sentry extends the SecureData platform with data interception and protection capabilities while leveraging the same format-preserving technologies and key management features as other SecureData clients. SecureData Sentry protects data fields flowing to or from the SaaS-based web analytics solution, while preserving their original format, a key differentiator between SecureData Sentry and the previous solution. SecureData Sentry resides between the health insurance customer-facing website and the web analytics platform to encrypt sensitive data tags before they reach the SaaS analytics platform. It enables secure data analytics while the organization retains authority over their own data encryption for full control of their sensitive customer data, end-to-end, throughout its lifecycle. Sentry is also used to intercept data via JDBC, and provides an alternate approach to protecting business data in application databases. The solution prevents exposure of sensitive customer data and fits in well with the existing data security ecosystem.

Improved Analytics Value from Sensitive Data, Reduced Risk, and Substantial Cost Savings

By using Voltage SecureData and Voltage SecureData Sentry as the standard for enterprise data protection, both on-premises and in the cloud, the organization gains infinitely more value from its data, regardless of where it resides. The team recognized that Voltage SecureData can offer data protection for many enterprise platforms and use cases thanks to its broad range of systems support and flexible integration capabilities. Since data no longer stays in one application or database or repository, the method of protecting data at the data level means the data stays protected wherever it goes.

The next step could include Google BigQuery, a fully managed, serverless data warehouse that enables scalable analysis over petabytes of data. SecureData’s new capabilities for cloud functions-as-a-service (FaaS) allow it to easily support Google BigQuery and other cloud data warehouses.

The Director of Enterprise Digital Initiatives concludes: “We found [Voltage] SecureData to be a cost-effective and flexible solution in securing our sensitive customer data compared with cloud-specific solutions that don’t meet our need for end-to-end data privacy and protection. With Voltage solutions, we can take full advantage of the benefits of cloud analytics platforms, including SaaS-based web analytics, prevent exposure of sensitive customer data, and realize substantial cost savings in the process.”

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.

768-000086-003 | O | 11/23 |