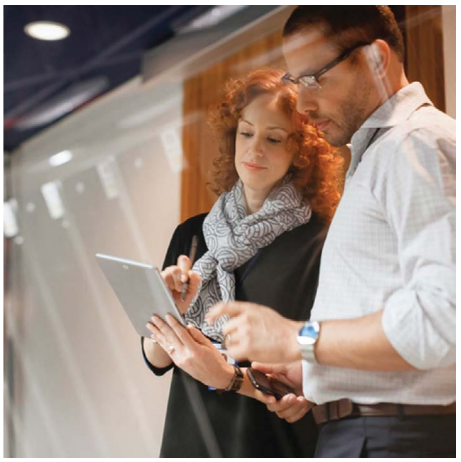
MICRO FOCUS

Case Study

Security

European Insurance Company

Innovative data-centric security strategy uses Micro Focus® Voltage SecureData to address privacy concerns about the use of personal data.



Overview

Insurance companies can gain valuable business insights by analyzing the data they store about their customers. But the legal risks of using this data improperly are increasing. For one European insurer, which prefers to remain anonymous, this meant complying with national data privacy regulations and Europe's General Data Protection Regulation (GDPR), due to come into effect in May 2018. The company used Micro Focus Voltage SecureData Enterprise to address these risks, allowing employees to more confidently analyze customer data to uncover revenue opportunities.

Challenge

The GDPR is expected to further restrict the use of customer information when it comes into effect in 2018. It and other privacy laws require that companies storing personally identifiable information (PII) about customers—such as their names and birth dates—only do so for specific purposes.

"This is really smart and highly sophisticated technology. We looked at other vendors and none offered this."

BUSINESS INTELLIGENCE MANAGER
European Insurance Company

This could cause legal risks for organizations using data warehouse and business intelligence tools. These tools generally store as much data as possible for a long period of time and don't clearly define a specific purpose for doing so until the data is presented in a report. To comply with privacy regulations while using these tools, organizations must have very high protection of PII.

"The insurance industry is one of those faced with particularly far-reaching GDPR implications," explains the European insurer's Business Intelligence Manager. The consequences of breaching the GDPR also include financial penalties, and losing customers' trust.

Common encryption techniques such as AESCBC (Advanced Encryption Standard-Cipher Block Chaining) convert information such as birth dates into a long string of numbers, letters, and symbols, known as hashes. Because the data would no longer be stored in its original format, a developer would have had to modify the existing database structure and any programs that processed the encrypted data—a very time-consuming task with a high risk of compromising data quality and reliability of the system.

Another problem with using common encryption methods was that employees would have

At a Glance

- **Industry**
  Financial Services
- **Challenge**
  Address compliance with data privacy laws while controlling costs.
- **Products and Services**
  Voltage SecureData Enterprise
- **Results**
  + Saves developers years of work, including extracting, transforming, and loading database content
  + Protects customers' personal information and privacy
  + Addresses compliance with data privacy laws
  + Reduces costs of data security integration

to spend time managing encryption keys. And the encryption solution had to work with the insurer's data integration software, Informatica PowerCenter. This is used to extract data from various sources, transform it, and load it into a new system, such as a data warehouse.

Solution

To address these challenges, the insurer turned to Micro Focus and its Voltage SecureData (SD) platform. This data-centric security platform protects data by ensuring that it stays encrypted in motion, as it moves through an organization's systems. It employs several techniques that make this encryption process much easier for companies to integrate and deploy.

One of Voltage SecureData Enterprise's advantages is its use of format-preserving encryption (FPE). Instead of converting information such as credit card numbers, dates of birth, and email addresses into a long string of characters, it encrypts the information while retaining its original format.

For example, the software might encrypt the birth date "07/07/1973" by turning it into "04/03/2585" though it doesn't change numeric values to alphanumeric hashes. This requires much less integration work because the encrypted information is in a format the insurer's data warehouse system was designed for.

FPE also preserves the meaning, logic, and value of data, such as the relationships in date ranges. These factors are often critical to business analytics.

"This is really smart and highly sophisticated technology. We looked at other vendors and none offered this. We were relieved when we finally ran across SecureData and its FPE framework," the Business Intelligence Manager says.

The Voltage SecureData solution also streamlines the management of encryption keys. It uses stateless key management to create keys on the fly, rather than storing them in a key database. This reduces costs by removing the need to protect and maintain a key database.

The insurer worked with a Micro Focus partner to understand the technology required to answer these challenges, as well as implement the solution. Working together, the two companies set up Voltage SecureData within Informatica PowerCenter in less than a week. The solution was implemented and tested to make sure that all encryption transformations worked correctly with the data warehouse's processes for extracting, transforming, and loading data. Once that work is complete, the insurer plans to start encrypting PII in all its data environments regularly. It expects to start doing this at the beginning of 2018.

Results

Addresses Compliance

The insurer expects to be in a strong position for compliance with data privacy laws once Voltage SecureData starts being used to encrypt personal information about customers. "We haven't had any GDPR audits yet, but we are confident that following this strategy will enable our compliance when it comes to data security and privacy," says the Business Intelligence Manager.

Rather than storing names, birth dates, and other information in the data warehouse in clear text, Voltage SecureData will use FPE to de-identify the data. Informatica PowerCenter processes call Voltage SecureData to encrypt any PII as it is loaded into the first persistent layer of the data warehouse. The data remains encrypted in the data warehouse until it is presented to a data warehouse user.

Data warehouse users will only see a customer's PII when they are authorized to do so under the company's security policy and when they make a legitimate query—a central requirement of data privacy laws.

Reduces the Cost of Data Security

The company cannot calculate how much money will have been saved until the project is completed. However, the company's Business Intelligence Manager says Voltage SecureData has "definitely" saved "years of time and effort."

Costs also have been reduced by avoiding extensive database development work. "All of the solutions we considered before looking at Voltage SecureData would have required a tremendous effort to adapt our existing database structures, ETL (extract, transform, and load) processes, front-end data warehouse models, and reports," says the Business Intelligence Manager.

This extra work would have brought the developers' other activities to a halt, he says. "We couldn't see another way to address all relevant data privacy requirements with another technology without bringing other development work to a standstill, probably for years."

By contrast, the insurer has integrated Voltage SecureData in phases to reduce disruption. "The encryption functionality is kind of sleeping until we have finished the whole implementation," the Business Intelligence Manager says. Once all the pieces are in place, developers will only need to set a few parameters to switch on the data-centric encryption. "Taking into account that thousands of attributes in our data warehouse system containing PII need to be encrypted, there wouldn't have been another option to implement data protection without a data hazard.

> "…we are confident that following this strategy will enable our compliance when it comes to data security and privacy."
>
> **BUSINESS INTELLIGENCE MANAGER**
> European Insurance Company

Contact us at:
www.microfocus.com

Like what you read? Share it.

"The flexibility of the Voltage SD framework allowed us to find a way to implement it in silent mode. This avoided disruption and confusion for our developers and testers, which may have occurred if they had seen both encrypted and unencrypted PII during the long implementation phase," he says. "Of course, there will still be a phase where we have to freeze our system to be able to initially encrypt all PII in all environments. But we are talking about a time period of several days or weeks, rather than months or even years."

Voltage SecureData has several other capabilities that save developers time, in addition to its FPE capability. For example, developers can use a simple Java application programming interface (API) to integrate Voltage SecureData with Informatica PowerCenter.

"It required only a little effort by a few people in our team to develop a handful of highly reusable components. Our data protection framework is very small, but spread widely, and it is both easy to understand and easy to maintain," the manager says.

The company's developers don't need deep knowledge about the encryption process either. A single developer acts as the company's Voltage SecureData expert, and their work ensures that the encryption process remains automatic, reducing technical tasks for other developers. Micro Focus' partner provides technical knowledge and manpower, enabling the insurer's data warehouse team to focus on business-related tasks.

Allows Use Of Data Analytics

The insurer can more confidently use data analytics to uncover revenue opportunities now that the Micro Focus solution is in place.

The company is increasingly relying on these insights about insurance customers, to optimize service and marketing offerings.

While Voltage SecureData does not directly provide customer insights, it secures the data so that employees can access and analyze it. The PII that wasn't integrated into the data warehouse system previously, because it was not sufficiently protected, can now be loaded and stored in the data warehouse while being protected by encryption.

As a result, Voltage SD enables the company to responsibly obtain, store, use, and extract value from data.