Case Study

Major Insurance Provider Uses CipherTrust Tokenization to Protect Customer Privacy

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

A leading provider of property and casualty insurance services in North America and Europe used digitalization to dramatically improve the efficiency, availability, and customer satisfaction of and with its services. However, that also entailed capturing and storing gigabytes of personal and financial customer information.

As a financial institution, the company was subject to multiple industry mandates and regulations requiring the protection of customer data and privacy. These included the Payment Card Industry (PCI) mandate, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), United States' National Association of Insurance Commissioners (NAIC) Data Security Law, and the European Union's General Data Protection Regulation (GDPR).

As awareness of potential data breach risks grew, the board of directors prioritized customer privacy protection and compliance with all relevant legislation in North America and Europe.

The challenge

Every month, thousands of customers shopping for insurance apply to the insurance provider online. They submit their personal and financial information in web forms for a real-time quotation, processing, and approval. The company needed a way to protect sensitive customer data from the application and approval process, to the back end quoting and billing systems, and, finally, to long term storage.

The solution

Acting as a trusted adviser, Thales helped implement security policy best practices for the protection of structured sensitive data for the financial institution.

CipherTrust Tokenization with dynamic data masking

CipherTrust Tokenization, a module of the CipherTrust Data Security Platform, provides protection for structured data in databases. This solution enables the pseudonymization of sensitive information in databases while maintaining the ability to analyze aggregated data without exposing sensitive data during analysis or in reports. RESTful APIs enable quick implementation with minimal changes to existing applications.

The client implemented CipherTrust Tokenization to protect all structured data captured from customers and stored in Oracle databases. Tokenized data was then used in back-end processes and applications, such as LDAP, maintaining customer privacy and protecting against external attack or internal threats. All customer systems were running in Kubernetes and communicating with the Tokenization server appliance.

CipherTrust Tokenization helped the customer improve compliance with regulations such as PIPEDA, NAIC and GDPR by protecting millions of customer records with minimal impact to operations or performance.

The results

Overall, the company achieved its board mandate by improving its security posture and ability to comply with industry mandates, such as PCI, and legislation, such as PIPEDA, NAIC, and GDPR, by de-identifying sensitive data with tokenization. CipherTrust Tokenization protected millions of customer records with minimal impact to operations or performance. The de-identified data protected customer privacy while maintaining the ability to work with the tokenized data for most functions.

The Ciphertrust Tokenization was quickly implemented by leveraging REST APIs and allowed the customer to configure token templates on the token server without the need to develop apps.

Results:

- Improved compliance with PCI, PIPEDA, NAIC, and GDPR
- Protected privacy of millions of customers
- Minimal impact on operations or performance
- Agile implementation with REST APIs

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us