protegrity

arge Bank Secures Sensitive Customer Records cross nternational orders

INTERNATIONAL BANK

KEY HIGHLIGHTS

INDUSTRY:

- Banking & Financial Services

CHALLENGE:

- Protect personally identifiable information (PII) of customers across multiple systems to the satisfaction of EU Cross Border Data Security requirements

SOLUTION:

- Deployed Protegrity Vaultless Tokenization locally to de-identify new and existing PII at source banking entities (before transfer to HQ), and on the Teradata EDW at HQ

BENEFITS:

- End-to-end, fine-grained PII de-identification across all geographically distributed bank entities and HQ

- Met all EU Cross Border Data Security requirements, including country-specific data access restrictions

BUSINESS PROBLEM

In order to streamline operations and improve analytical capabilities, a major international bank performed a consolidation of all European operational data from various European bank entities to their Teradata enterprise data warehouse (EDW) at their headquarters in Italy.

This meant protecting Personally Identifiable Information (PII), including names, addresses, phone, email, policy and account numbers, to the satisfaction and compliance with EU Cross Border Data Protection Laws.

Among these laws, Datenschutzgesetz 2000 - DSG 2000 in Austria, and Bundesdatenschutzgesetz in Germany required that access to Austrian and German customer data at HQ be restricted to only users in each respective country.

CHALLENGES

The primary challenge was to consistently secure the large amount and wide variety of PII end-to-end from the geographically distributed bank entities, back to HQ, where it would be consolidated. Existing data within all systems would also require protection.

In order to assure consistent security and auditing across all entities, the bank also desired a solution which could be distributed to each entity, but controlled centrally.

The second challenge was to adapt security to be compatible with multiple data types from a variety of systems, including SAS, Mainframe, and ERP.

And finally, all of this needed to be achieved with very high throughput, to ensure maximum reliability and data integrity.

SOLUTION

Tokenization was selected to protect the PII, due to its high performance and transparency, in addition to its benefits in Cross Border situations.

Rather than encryption, which uses a cipher/key system reliant on a mathematical algorithm, tokenization replaces sensitive data with random data of the same type and length. Because there is no mathematical relationship to the original data, tokenized data is considered replaced or removed.

The bank implemented Protegrity Vaultless Tokenization (PVT) services locally, to de-identify new and existing PII at source banking entities before transfer to HQ. PVT ensured both compliance with EU Cross Border Data Security laws, and complete business analysis capabilities in the Teradata enterprise data warehouse at HQ. PVT was delivered via clusters of multiple servers to maximize throughput with bulk tokenization.

Along with PVT, centralized policy-based access controls were implemented with integration of both LDAP and Active Directory. This restricted access to reidentified data to authorized users, including country-specific requirements for Austria and Germany.

BENEFITS

The bank was able to secure all new and existing personally identifiable information across all business entities.

Utilizing Protegrity Vaultless Tokenization, along with Protegrity's centralized policy, key management, auditing, and reporting suite (Enterprise Security Administrator), the bank achieved end-to-end data security with complete, fine-grained de-identification of sensitive data.

The flexibility of the solution provided a means to protect the wide variety of data types necessary across multiple environments, while maintaining maximum throughput, reliability and data integrity.

The unique architecture of Protegrity Vaultless Tokenization technology provides all of the benefits of tokenization - random data replacement, preserved data type and length, exposed business intelligence - without the drawbacks and limitations of traditional tokenization. No ever-growing token lookup tables and no replication, which can seriously affect performance, and most importantly, no stored sensitive data.

Protegrity's centralized policy, key management, auditing, and reporting allows the retailer to centrally manage the security of sensitive data regardless of where it goes. This includes control over information associated with persons from Austria and Germany - the security team at HQ can prevent users from accessing sensitive information associated with persons from each respective country.

Unified controls provide increased security, simplified compliance, and superior oversight, along with the added protection of a built-in separation of duties.