cpl.thalesgroup.com

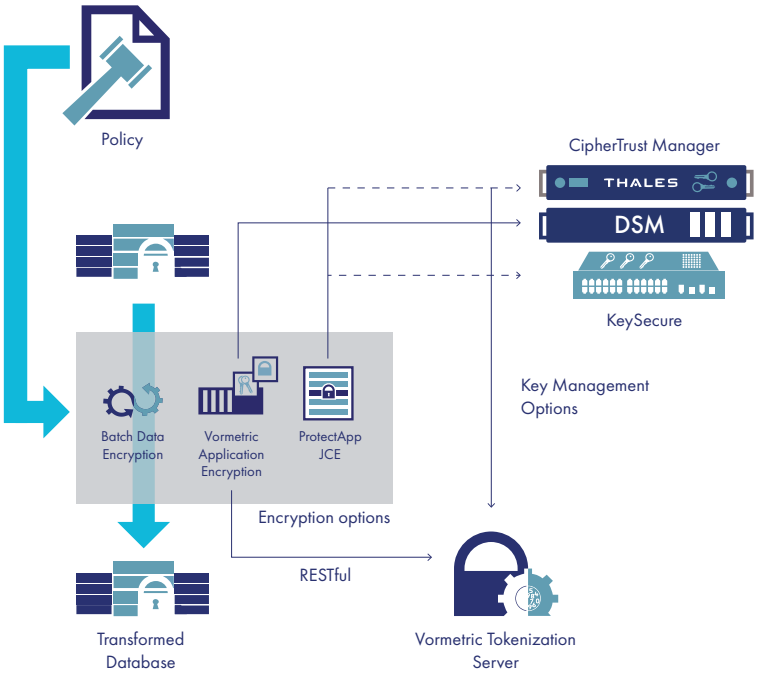
Vormetric Batch Data Transformation

The relentless march of data breaches is matched by other more positive trends: rapid digital transformation initiatives drive new data uses and places data in new locations, coupled with smarter and more detailed data protection requirements from industry and government regulatory bodies.

Emerging data warehouses and big data on premises and in the cloud enable faster analysis and decision-making. Modern DevOps methods require local copies of production databases at scale to ensure performance and scalability of rapidly-evolving applications. Outsourced data scrubbing and analysis enhances efficiency while lowering costs. In all of these use cases, regulations like the EU GDPR, the California Consumer Privacy Act, and many others, make it imperative to protect personally-identifiable information (PII). When present, Primary Account Numbers (PAN) and payment fields must be protected to comply with Payment Card Industry Data Security Standards (PCI-DSS).

Modern use cases can be leveraged with comprehensive data protection with Vormetric Batch Data Transformation from Thales. Batch Data Transformation is a high-speed data protection tool offering both encryption and tokenization. It operates in conjunction with Thales CipherTrust Manager, Thales ProtectApp, Vormetric Application Encryption and Vormetric Tokenization to facilitate the encryption or tokenization of high volumes of sensitive records without lengthy maintenance windows and downtime.

You can also tokenize or mask sensitive columns in production databases and in copies of databases before they are shared with third-party developers and big data environments. No changes to applications, network systems or storage architectures are necessary.



Overview

Vormetric Batch Data Transformation can either encrypt or tokenize data on a per-column basis. Tokenization and encryption may be used concurrently on different database columns. Vormetric Batch Data Transformation is commonly used for a wide range of static data masking use cases:

- Masking sensitive data before or loading into a data warehouse or data lake
- Initial encryption or tokenization of existing data in production databases prior to deployment of applications that encrypt or tokenize new data
- Enable third-party data analysis and clean-up without exposing sensitive or private information
- Enable data science or data analysis team members to utilize accurately represented data without exposure of sensitive content
- Fast and efficient re-keying of existing encrypted data

Batch Data Transformation leverages external services for tokenization and encryption.

- Tokenization is provided by the Vormetric Tokenization Server
- Encryption is provided by either
  - Vormetric Application Encryption or
  - Thales ProtectApp
- The encryption providers each depend on a key source. In the case of Vormetric Application Encryption, the key source is the Vormetric Data Security Manager. For ProtectApp there are two possible key sources: Thales CipherTrust Manager or Thales KeySecure

Batch Data Transformation encrypts all passwords for its services.

Flexible Encryption Modes

For encryption purposes either Vormetric Application Encryption or Thales ProtectApp is installed on the same server as Batch Data Transformation. Both of the encryption solutions has these "operating modes"

- They can cache encryption keys provided by their key sources and perform encryption on the Batch Data Transformation server.
- They can forward encryption operations to the key source. This mode is available for the highest security transformation environments where there is a requirement to retain the key in the key source.

Tokenization Key Source Options

The Vormetric Tokenization Server offers multiple options for its key source for both random and format-preserving tokenization. They are

- Thales CipherTrust Manager
- Vormetric Data Security Manager
- Thales KeySecure

Data transformation options

On a field-by-field level, Batch Data Transformation permits data protection with

- Format-Preserving Encryption (FF1, FF1) with ASCII and Unicode character set options
- AES-CBC, AES-CTR, 3DES
- Random Tokenization

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> cpl.thalesgroup.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: apacsales.cpl@thalesgroup.com
Europe, Middle East, Africa – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com