cpl.thalesgroup.com

THALES

CipherTrust Batch Data Transformation

Secure Static Data Masking

Static Data Masking

Static Data Masking refers to the process of transforming selected data in various data stores to unreadable or unusable forms, typically order to utilize data sets while preventing misuse of sensitive data.

CipherTrust Batch Data Transformation offers high-performance static data masking with centralized encryption key management as part of the CipherTrust Data Security Platform. It leverages the power of CipherTrust Application Data Protection and CipherTrust Tokenization to protect vast quantities of data quickly. It also can be used a a high-performance encryption or tokenization solution for compliance.

The breadth of use cases for static data masking is surprisingly large. These first four begin with "masking sensitive data":

1. Prior to third-party data sharing
2. In databases shared with development, QA, R&D, or data science/analytics teams
3. Before adding a data set to a data lake or big data environment
4. In advance of starting big data extract, transform and load (ETL) operations

Batch Data Transformation has many other use cases beyond Static Data Masking. Here are a couple of examples:

- Preparing a database for tokenization or encryption deployment
- Rekeying data in a database following a new key version or key rotation

Key Advantages

Secure, cost-effective static data masking

Not every static data masking solution is secure. With Batch Data Transformation, you can depend on the security of centralized key management provided by CipherTrust Manager, which can provide up to FIPS 140-2 Level 3 key security. Meanwhile, every investment in the Data Security Platform makes it more valuable to you.

Accelerate Transformation of Existing Sensitive Data

Following deployment and execution of CipherTrust Data Discovery and Classification, you can protect sensitive information in database columns quickly and efficiently using either encryption or tokenization with minimal disruption, effort and cost.

Enable database sharing with reduced risk

Static data masking enables you to remove sensitive information before sharing with third-party developers and big data environments while maintaining data integrity and still supporting mission-critical testing and analytical activities.

Static Data Masking where you need it

Batch Data Transformation and its data protection tools are all software and completely cloud friendly. You can mask data on premises and use it in the cloud, mask data in the cloud and use it there, or secure data in one cloud and use it in another.

The CipherTrust Data Security Platform provides a wide range of data protection capabilities from on-premises to cloud, enabling secure digital transformations.

Batch Data Transformation Key Features

Efficient and Flexible Encryption

Large volumes of data are encrypted quickly with Batch Data Transformation in conjunction with CipherTrust Application Data Protection installed on the same server. Policy files define encryption options including standard AES encryption or format preserving encryption, while identifying the database columns to be protected and the number of records in each batch. Data filtering enables creation of customized destination record subsets.

Batch Data Transformation offers a choice in encryption "operating modes":

- Encryption keys provided by CipherTrust Manager are cached on the Batch Data Transformation server where encryption occurs
- Encryption operations can occur on CipherTrust Manager. This mode is available for the highest security transformation environments where there is a requirement to retain the key in the key source

Flexible Tokenization

An alternative to encryption in Batch Data Transformation is tokenization. Batch Data Transformation can utilize the CipherTrust Tokenization Server to tokenize select database columns. Detokenization is supported so that applications can access the clear data again when required, or, irreversible tokenization can ensure that third parties never gain access to original sensitive data.

Flexible Conversion Between Data Stores

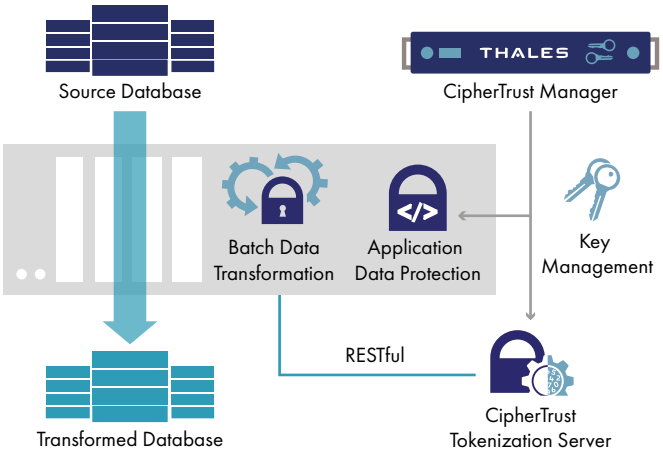
CipherTrust Batch Data Transformation can protect data while it is moving, for example, from a database to various flat file formats or in reverse. CipherTrust Batch Data Transformation supports:

- Flat-file (CSV) to flat-file
- Flat-file to Database
- Database to flat-file
- Database to Database

Supported databases include

- Oracle
- Microsoft SQL Server
- Oracle MySQL
- IBM DB2
- SAP HANA

Transformation from a source database is read-only, so production databases may be used transparently.



CipherTrust Data Security Platform

CipherTrust Tokenization is part of the CipherTrust Data Security Platform, which unifies data discovery, classification, data protection, and unprecedented granular access controls, all with centralized key management. This simplifies data security operations, accelerates time to compliance, secures cloud migrations and reduces risk across your business. You can rely on Thales CipherTrust Data Security Platform to help you discover, protect and control your organization's sensitive data

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.