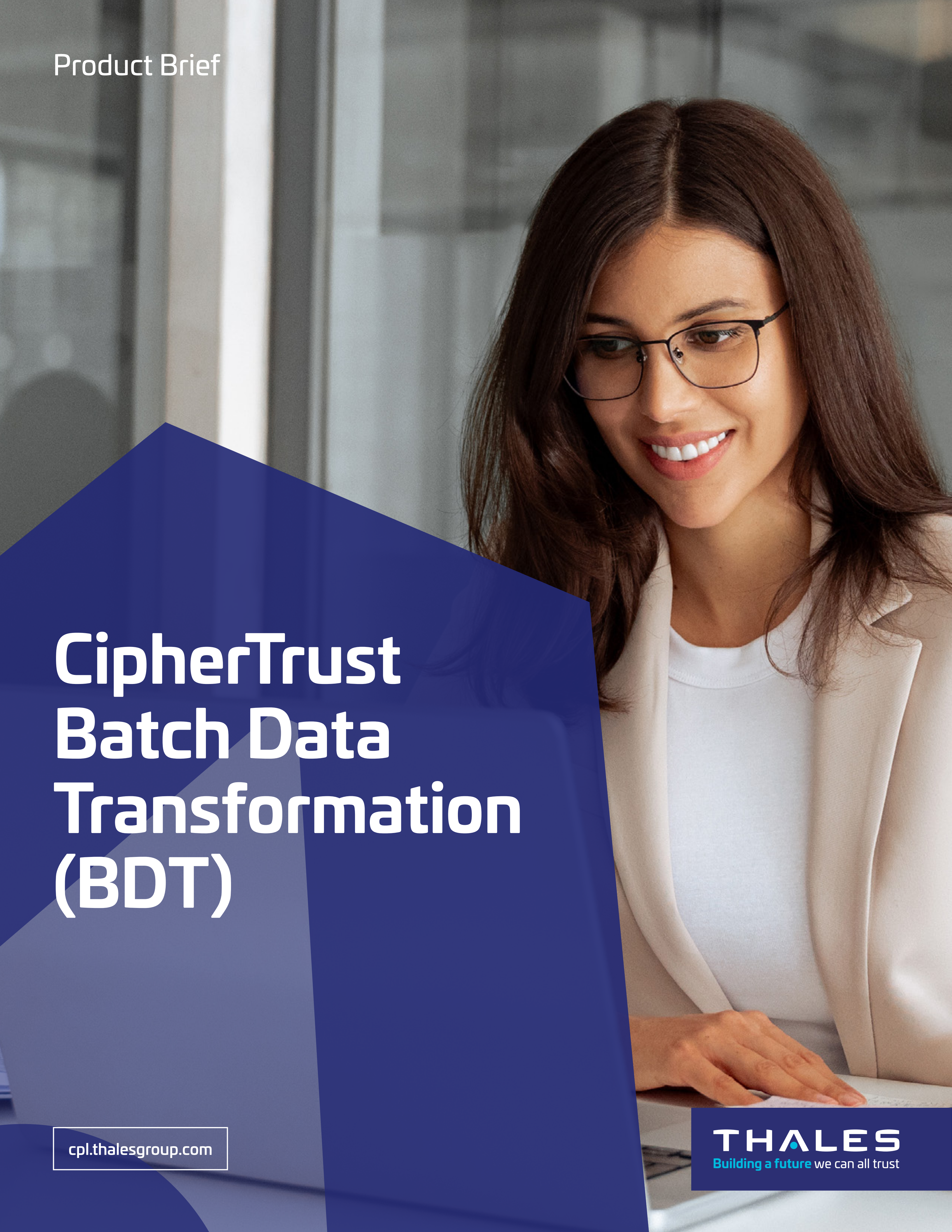
Product Brief

CipherTrust Batch Data Transformation (BDT)



cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Batch Data Transformation (BDT) is a bulk transformation tool that is used offline to protect/re-protect data inside your data store. BDT can be part of an ongoing extract and transform operation. BDT may also be the primary means of doing annual key rotations on existing data, and part of the process to securely move production data into QA and staging for test purposes while tokenizing it for protection.

Gain transparent field-level encryption, tokenization, data generalization, data masking or redaction without needing to know anything about cryptography. Developers do not need to be involved. All DevOps needs to do is deploy BDT in communication with the source it is going to protect. The source can be either a database or a file. Your Data Security Admin will handle all data protection including creation of policies for rapid data transformation.

You keep months of Developer time, and Security gains the ability to close vulnerability gaps efficiently.

To sustain your compliance and your capacity per sprint, we removed Developer (Dev) involvement from data transformation.

Data multiplies, but team members don't. So that you can focus on more exciting projects, you need an automated process to prepare an existing database to transform data from clear text to protected text, re-encrypt data to the most current key using version metadata, and move data to Data Lakes or Data Warehouses.

Organizations tell us traditional encryption, tokenization, data generalization, data masking and redaction solutions require their Devs to handle fire drills when ciphers, keys or parameters need to change—taking Devs away from roadmap and/or innovative topics for a minimum of two months each and every time an update is needed for ciphers, keys or parameters.

Their Devs get pulled into projects that are a minimum of two calendar months because the Devs have to change source code, and DBAs/Devs have to migrate current data to the new ciphers/keys/parameters. After all changes are submitted, all of the code must be tested and re-tested until it passes all tests. The Devs are required to become cryptographers and change source code for every individual piece of sensitive data in every database column multiplied by every service protecting data. As a result, organizations report that they typically dedicate resources to revenue generating projects and delay their data protection updates for two years, resulting in a weakened security posture, increases in failed audits and more security breaches.

CipherTrust Batch Data Transformation (BDT) removes the need to learn cryptography and automates batch data transformation to encrypt/decrypt, tokenize/detokenize, or re-key large volumes of data quickly. BDT empowers you to perform data transformation on your schedule of choice with no Developer involvement.

DBAs or Data Security Admins configure BDT's policies and initiate data transformation. Using BDT removes the need to write and maintain scripts to read data from source, protect data and then move the transformed data to target systems.

BDT reduces your workload with centrally-managed policies that 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.

Since transformation from a source database is read-only, BDT uses production databases transparently.

Data Security Admins manage the policies, entering ciphers, keys or parameters. They update data protection in real time, making a selection from a dropdown menu in the GUI or by REST API. Vulnerability gaps are reduced from months to less than a minute.

Since there are no changes to code, no Dev or Test involvement is required to update ciphers/keys/parameters.

Benefits

Increase Developer Capacity

- Devs are not involved in data transformation. Instead of managing security workflows, automation allows developers to focus on higher-value tasks, such as delivering business logic and innovation
- Human error decreases due to no changes to source code for the initial setup or for updates
- Dev and Test are not involved so vulnerability gaps for sensitive data can be closed in minutes after discovery

Security Experts Manage Security

- Data Security Admins configure protection policies and BDT jobs, identifying which columns of sensitive data need to be Protected/Revealed with which policy and the target column or data source for the transformed data
- Data Security Admins can initiate jobs and view job status using the CM GUI or REST APIs
- Data Security Admins can define centrally-managed access policies describing how people see data, including static data masking and redaction
- Data Security Admins can leverage crypto agility to change ciphers, parameters and keys in real time without taking Devs off of other projects

- Visibility on a single pane of glass shows where protection is deployed

Continuous Compliance

- Compliance teams can easily demonstrate compliance without involving Devs – the audit will be more complete, accurate and faster. Includes tracking of all data access for easy integration with SIEM tools
- Separation of Duties aligns with compliance regulations

Ease of use

- Deploy centrally and scale automatically using containers
- Automate batch transformations and control the schedule
- Flexible data extraction/ingestion

Crypto Agility

BDT supports crypto agility for data protection due to the convergence of three design elements:

- Centrally-managed Protection and Access Policies
- No changes to code, ever
- Separation of duties

Crypto agility enables Data Security Admins to change ciphers, keys and parameters in real time.

High Speed Transformation

Flexible Conversion Between Data Stores

BDT can protect data while it is moving, for example, from a database to a comma-separated values (CSV) file or in reverse. BDT supports:

- File to File
- File to Database
- Database to File
- Database to Database

Supports:

- Databases (Oracle, Microsoft SQL Server, IBM Db2, MySQL, SAP Hana)
- CSV files
- Fixed Length files

Views and Triggers can be built to associate the UDFs to Inserts or Queries automatically.

Diagram 1 shows BDT deployed as a docker container. BDT can be scaled up to provide high availability and performance.

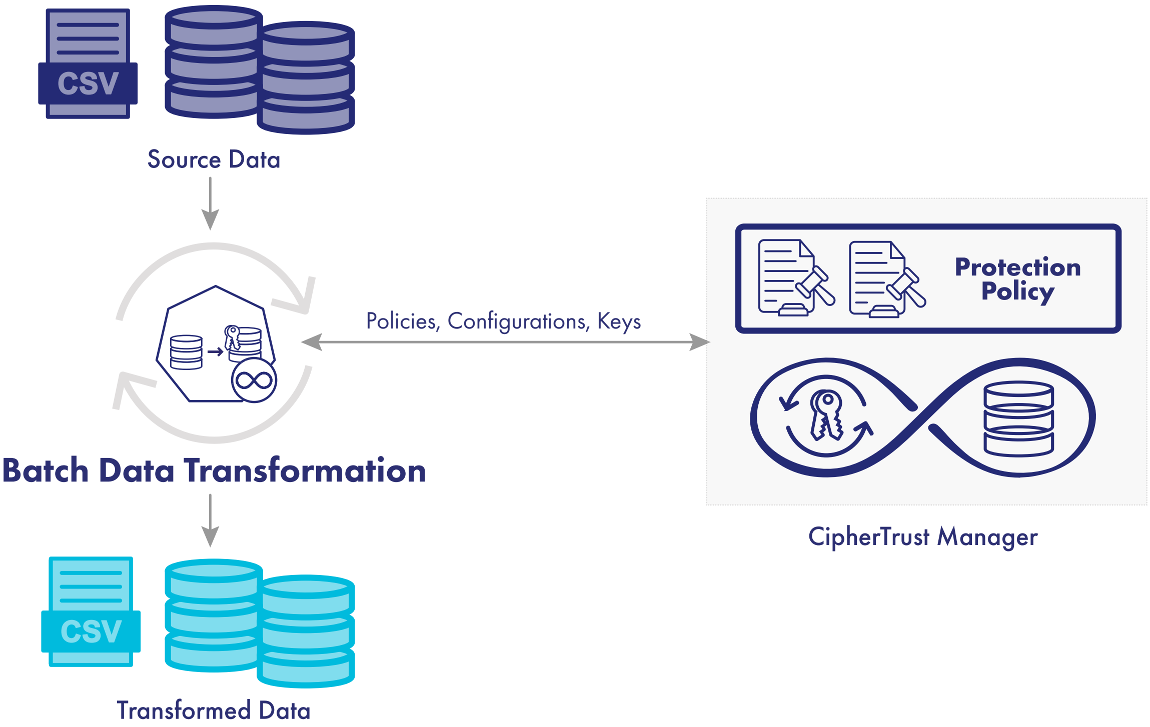
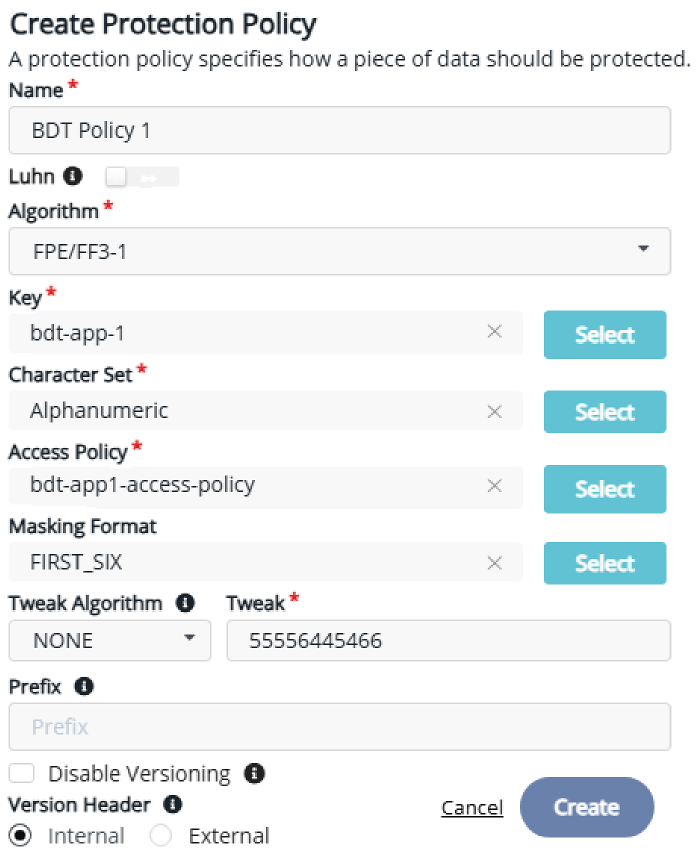


Diagram 1: Extract, Transform, Load (ETL) – CipherTrust Manager handles configuration, policies and keys for BDT.

Protection Policies

We enable the Data Security Admin to define a protection policy by selecting from an ever-growing list of NIST-sanctioned algorithms. The Access Policies can be automated for onboarding/offboarding.



Create Protection Policy

A protection policy specifies how a piece of data should be protected.

Name *: BDT Policy 1

Luhn

Algorithm *: FPE/FF3-1

Key *: bdt-app-1

Character Set *: Alphanumeric

Access Policy *: bdt-app1-access-policy

Masking Format: FIRST_SIX

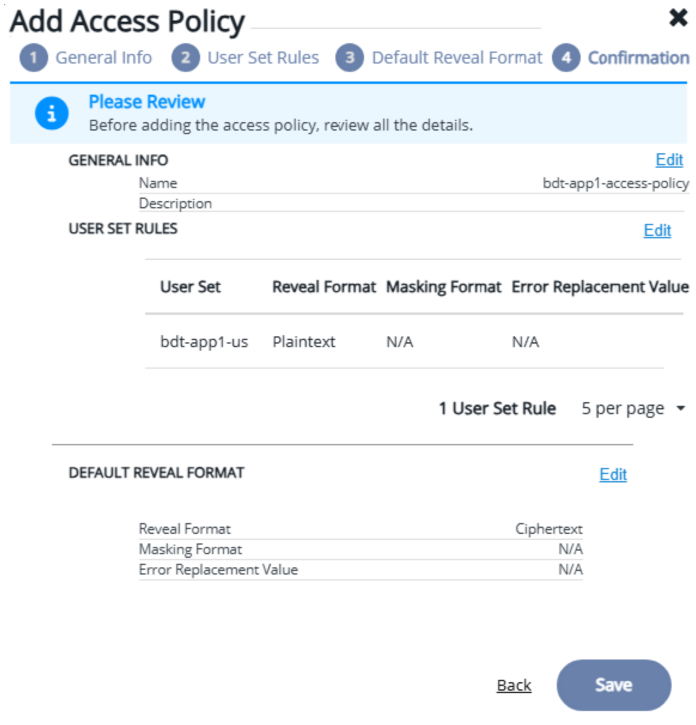
Tweak Algorithm: NONE

Tweak *: 55556445466

Prefix: Prefix

□ Disable Versioning

Version Header: ● Internal ○ External



Add Access Policy

1 General Info 2 User Set Rules 3 Default Reveal Format 4 Confirmation

Please Review
Before adding the access policy, review all the details.

GENERAL INFO

Name	bdt-app1-access-policy
Description	

USER SET RULES

User Set	Reveal Format	Masking Format	Error Replacement Value
bdt-app1-us	Plaintext	N/A	N/A

1 User Set Rule 5 per page

DEFAULT REVEAL FORMAT

Reveal Format	Ciphertext
Masking Format	N/A
Error Replacement Value	N/A

Protect Data Across Apps, APIs and Databases

BDT is one of several centrally-managed Thales data protection offerings. CipherTrust Application Data Protection SDK (CADP SDK) offers field-level data protection to developers as a simple-to-integrate library. CipherTrust RESTful Data Protection (CRDP) is a RESTful service that offers field-level data protection across cloud and on-premises applications.. CipherTrust Data Protection Gateway (DPG) is a Gateway that transparently intercepts RESTful API calls and protects data with no code changes required on the RESTful service or clients.

CipherTrust Database Protection (CDP) offers transparent, column- level data protection for a wide range of databases.

All centrally-managed Connectors support Static Data Masking and Redaction. CADP, CRDP and DPG additionally support Dynamic Data Masking.

BDT complements our other CipherTrust data protection solutions by automating batch data transformation processes.

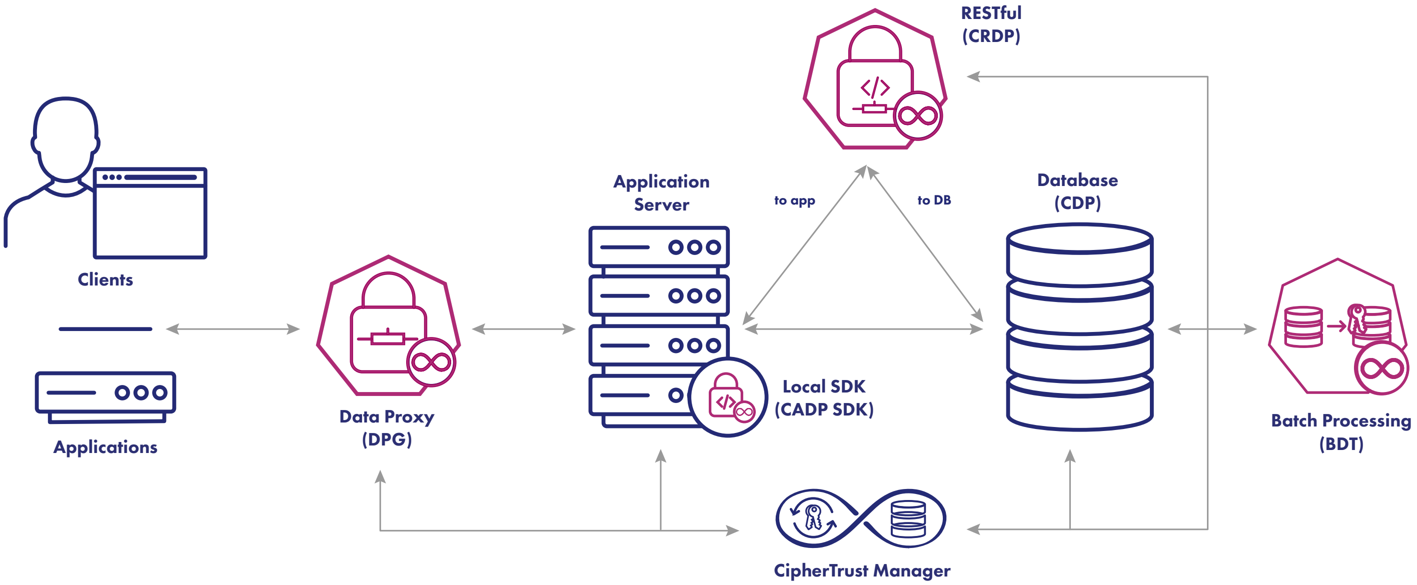


Diagram 2: BDT can be used with DPG, CADP, CRDP and CDP to transform data in files or databases and rotate keys to maintain security compliance. BDT can connect to a database or to a server. Diagram 2 shows Connection to a database.

CipherTrust Data Security Platform

BDT is part of the CipherTrust Data Security Platform (CDSP), which unifies data discovery, classification, protection and monitoring with unprecedented granular access controls and centralized key management. Protecting your sensitive data with CDSP decreases time to compliance, simplifies data security operations, secures cloud migrations and reduces risk across your business. You can rely on the Thales CipherTrust Data Security Platform to help you discover, protect, control and monitor your organization's sensitive data, wherever the data resides.

ESG Statement

The Thales CipherTrust Batch Data Transformation (BDT) containerized solution makes a smaller carbon footprint than a full server solution or virtual appliance because BDT elastically scales, in alignment with Thales' ESG (environmental, social, and governance) commitment to a greener, safer world.

About Thales

Thales is a global leader in cybersecurity, helping the most trusted companies and organizations around the world protect critical applications, sensitive data, and identities anywhere at scale. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

cpl.thalesgroup.com

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