Product Brief

CipherTrust Database Protection (CDP)

cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Database Protection (CDP) is a performant option to encrypt sensitive column-level data inside a database – quickly, transparently and without changing applications.

CDP supports compliance with online key rotation and delivers column-level data encryption in databases at near-native DB speed, with no re-testing cycles when ciphers change or keys are rotated, and with no changes to most application code. CDP delivers granular access controls with the option for unique keys for each column to protect sensitive data across on-prem, hybrid and multi-cloud environments.

Gain column-level data protection with either AES or FPE encryption with data masking without needing to know anything about cryptography. No Developer involvement required.

Encrypting column-level data is known to be such painstaking work that many organizations delay updating their encryption – sometimes for years. The pain occurs when you want consistently high performance regardless of the cloud or data lake you are using, when developers are involved, when you don't want to change your application code or when you use a hyperscaler solution in a multi-cloud environment.

To make the encryption easier, we developed CDP to protect structured data in performance-intensive environments while preserving format and usability for joins and analytics. Transparency for database applications is achieved using auto-generated database views and triggers created and deployed during solution design and deployment. For highest performance, Encryption can occur on the database server. If it is more important to you that keys never leave the secure enclave, Encryption can occur in CipherTrust Manager. Implement your choice with a simple configuration change.

Another CDP strength is the ability to rotate encryption keys without application downtime or application rewrite. Data protection best practices require the alteration of the encryption key used to protect data over time. This is frequently referred to as "key rotation" or "data re-key" and is commonly executed every year or two for all encrypted data. CDP provides AES encryption with live key rotation capabilities to eliminate rotation outages and eliminate the manual effort to rotate keys.

You can let us do the work of encrypting your database and managing your encryption keys so that you don't have to do the work of recovering from a data breach.

A security solution is effective only if it both reduces business risks and meets organizational goals. By focusing on specific database columns, CipherTrust Database Protection encrypts and decrypts data efficiently, in a fraction of the time required for an entire database — and Format Preserving Encryption (FPE) enables data analytics on encrypted data.

CDP features comprehensive logging and auditing capabilities to enable organizations to track access to encrypted data and keys and integrate them with a SIEM, if desired. As a result, you can effectively address internal policies and all relevant regulatory mandates, including encrypting personally identifiable information (PII) and other sensitive, confidential data to comply with privacy mandates such as, Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA).

Benefits

Developers Focus on Development

- No changes to business applications
- Transparent encryption through auto-generated database views and triggers
- No need to manage cryptography inside code

Security Experts Manage Security

- Centralized key and policy management in CipherTrust Manager (FIPS 140-2 up to Level 3) with built-in key rotation and data re-keying to lower ongoing costs
- Granular access controls to enforce separation of duties
- Keys and data remain isolated from DBAs

Continuous Compliance

- Meets regulatory mandates including PCI DSS, HIPAA, and GDPR
- Comprehensive logging and auditing to track access to encrypted data and keys—supports SIEM integrations
- Reduced audit complexity due to targeted encryption for regulated fields

Crypto Agility

CDP supports crypto agility for data protection due to:

- Live key rotation for protected data
- Separation of duties
- Centrally-managed policies for fast updates

Cloud-Ready and Cloud-Scale

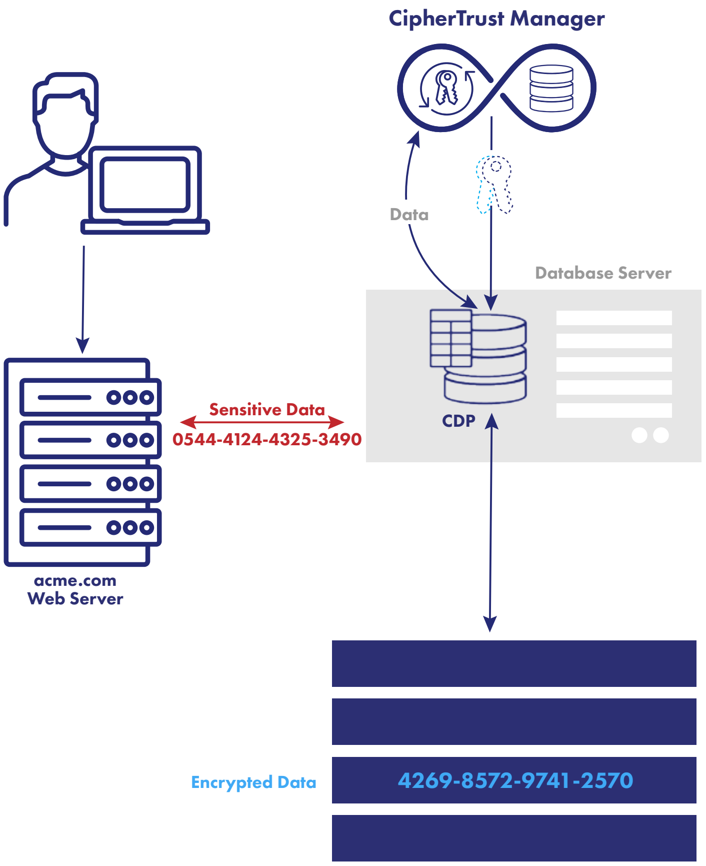
CDP enables efficient resource management across multiple instances to protect sensitive column-level data across on-prem, hybrid and multi-cloud environments. CDP architecture supports automation for rapid deployment.

Architectural Overview

CipherTrust Data Protection encrypts and decrypts specific database columns without requiring application changes. It can run:

- Locally on the database server for maximum performance
- Within CipherTrust Manager to ensure encryption keys never leave the secure enclave

CDP Encrypt/Decrypt and Key Management



Operational Flow

Data can be sent to CDP either from a user or a database. In the user scenario, sensitive data passes from the user, through the web server, to CDP. In the database scenario, sensitive data is passed from a database to CDP.

To perform encrypt/decrypt operations, CDP authenticates to CipherTrust Manager using credentials stored encrypted on CDP. The transformed data is returned through the application server to the user or used to perform a database update.

To Encrypt/Decrypt locally on the database server, an Encryption key is exported from CipherTrust Manager to CDP and remains in CDP memory only for the duration of a database session.

To Encrypt/Decrypt remotely on CipherTrust Manager, the Encryption key remains within CipherTrust Manager, and CDP sends the sensitive data to CipherTrust Manager for encryption/decryption. CipherTrust Manager returns the transformed data to CDP which sends the transformed data to the database.

Technical Specifications

Supported Databases

- Oracle
- Microsoft SQL Server
- IBM DB2
- Teradata Database

Supported Platforms

- Microsoft Windows
- Linux
- Solaris
- HP-UX
- AIX

Encryption Algorithms

- AES, FF3, RSA, ECC

About Thales

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