Product Brief

CipherTrust RESTful Data Protection

cpl.thalesgroup.com

THALES

Building a future we can all trust

THALES
Building a future we can all trust

Prospects tell us traditional encryption solutions require their Developers (Devs) to handle fire drills when ciphers, parameters or keys need to change—taking Devs away from revenue-generating projects for a minimum of two months each and every time an update is needed for ciphers, parameters or keys.

Their Devs get pulled into projects that are a minimum of two calendar months, where the Devs are required to become cryptographers and change source code for every corresponding piece of sensitive data in every database column multiplied by every service protecting data. As a result, organizations typically delay their data protection updates for two years, resulting in a weakened security posture, increases in failed audits and more security breaches.

To reduce Dev involvement and remove the need to become cryptographers, we abstracted away the cryptography with simplified APIs and centrally-managed policies, delivering CipherTrust RESTful Data Protection (CRDP) — a centrally-managed policy-based solution that limits a Dev's involvement to the initial coding.

Devs insert Protect and Reveal method calls that reference the centrally-managed policies, and do not need to learn or apply cryptography.

Data Security Admins manage the policies, entering ciphers, keys and parameters. The admins update data protection by making a selection from a dropdown menu.

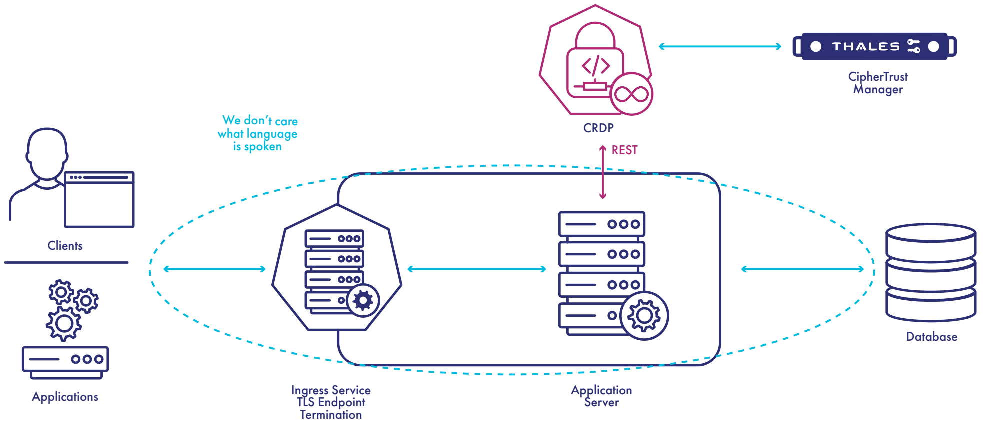
Vulnerability gaps are reduced from months to less than a minute due to centrally-managed policies with no changes to source code required, so no Dev involvement required

.Benefits

- Devs increase their capacity by using a simplified API to write the initial code—inserting Protect and Reveal method calls, they do not have to learn, apply and test cryptography
- Devs do not have to be involved in updating security within their code when ciphers, parameters or keys need to be changed
- Human error decreases due to fewer changes to source code for the initial setup, no changes to source code for updates, and subject matter experts managing the data protection
- Vulnerability gaps for sensitive data can be closed in minutes after discovery – instead of requiring months or years of Dev and testing time
- Data Security Admins can perform updates without taking Devs off of other projects
- Separation of Duties aligns with compliance regulations
- 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
- Visibility on a single pane of glass showing where protection is deployed
- Organizations can re-allocate the freed-up Devs to revenue-generating projects
- Sensitive data can be stored and/or processed in any CSP or on premises
- Configured on CipherTrust Manager (CM) through REST API or GUI. REST API enables automation through Scripts and Orchestrators
- License management and capacity planning through CM

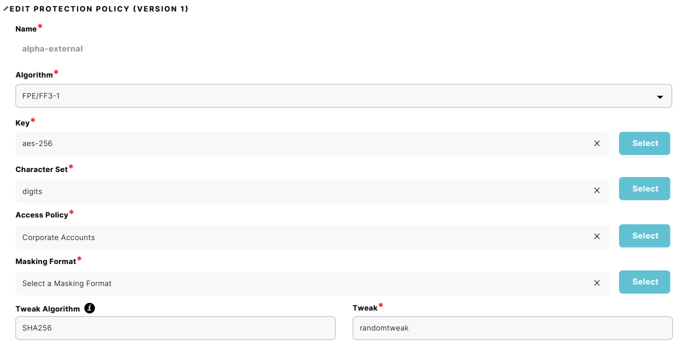
Architectural Overview

CRDP is deployed close to your application/service and can be scaled up to provide high availability and performance.



Protection Methods

We enable the Data Security Admin to define a protection policy selecting from an ever-growing list of NIST-sanctioned algorithms.



EDIT PROTECTION POLICY (VERSION 1)

Name*: alpha-external

Algorithm*: FPE/FF3-1

Key*: aes-256

Character Set*: digits

Access Policy*: Corporate Accounts

Masking Format*: Select a Masking Format

Tweak Algorithm: SHA256

Tweak*: randomtweak

Creating a Protection Policy

Cloud-Ready and Cloud-Scale

CRDP is deployed as a container and is fully compatible with orchestration systems such as Helm, Ansible, Terraform, OpenToFu and PowerShell, and can take advantage of Kubernetes horizontal scaling. CRDP can also be deployed as a standalone container for legacy production deployments in addition to being used in development and testing use cases.

Thales Application-Layer Protection

CRDP is one of several application-layer data protection offerings from Thales. CipherTrust Data Protection Gateway (DPG) offers transparent data protection to any RESTful web service or microservice leveraging REST APIs. CipherTrust Application Data Protection (CADP) offers data protection to developers as a simple-to-integrate library. CipherTrust Database Protection (CDP) offers transparent, column-level data protection for a wide range of databases. CipherTrust Batch Data Transformation (BDT) offers high-performance encryption, tokenization and data masking for databases and structured files.

CipherTrust Data Security Platform

CRDP is part of the CipherTrust Data Security Platform (CDSP), which unifies data discovery, classification and data protection with unprecedented granular access controls and centralized key management. Protecting your sensitive data with CDSP accelerates 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 and control your organization's sensitive data, wherever the data resides.

ESG Statement

The Thales CipherTrust RESTful Data Protection (CRDP) containerized solution makes a smaller carbon footprint than a full server solution or virtual appliance, because CRDP makes the orchestrator aware of when resources change and resources should be scaled up or down, in alignment with Thales' ESG (environmental, social, and governance) commitment to a greener, safer world.

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.