Product Brief

CipherTrust Data Protection Gateway

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

CipherTrust Data Protection Gateway (DPG) is a gateway that protects data in requests and responses to RESTful web services or microservices with no change to code, ever. Protects data In Use, In Transit and At Rest.

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 DPG in front of the service it is going to protect. Your Data Security Admin will handle all data protection — no matter how many times:

- **NIST declares a cipher to be at risk**
- **Keys need to be rotated**
- **Parameters need to be updated**

You keep months of Developer time and Security gains the ability to close vulnerability gaps in less than a minute.

Just as you use different keys for different columns in your database, you use different ciphers for different types of data. Learning and applying the rules of cryptography is time-consuming and you have more exciting projects to work on.

Organizations tell us traditional encryption, tokenization, data generalization, data masking and redaction solutions require their Developers (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 of the 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.

To sustain your compliance and your capacity per sprint, we removed Dev involvement and their need to become cryptographers.

Data Security Admins make the association between the field and the policy and 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, ever, no Dev, DBA or Test involvement is required for the updated ciphers/keys/parameters.

Benefits

Developers Focus on Development

- Devs are not involved in updating security within their code when ciphers, keys or parameters need to be changed
- Human error is removed due to no changes to source code for the initial setup, no changes to source code for updates, and subject matter experts managing the data protection

Security Experts Manage Security

- Data Security Admins can perform initial setup and updates without taking Devs off of other projects
- Data Security Admins can define access policies describing how people see data, including data masking and redaction
- Vulnerability gaps for sensitive data can be closed in minutes after discovery – instead of requiring months or years of Dev and testing time
- Configured on CipherTrust Manager (CM) through REST API or GUI
- 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

Crypto Agility

DPG 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

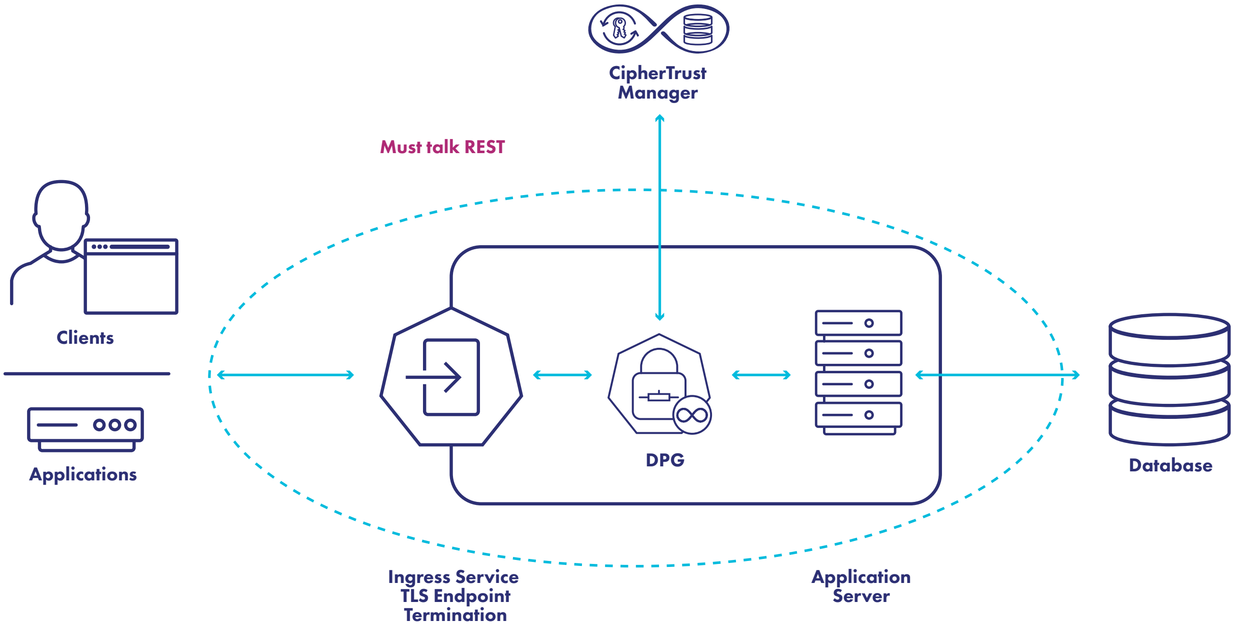
Crypto agility enables Data Security Admins to change ciphers, keys and parameters in real time.

Cloud-Ready and Cloud-Scale

DPG enables efficient resource management across multiple instances. DPG 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. DPG can also be deployed as a standalone container for legacy production deployments in addition to being used in development and testing use cases.

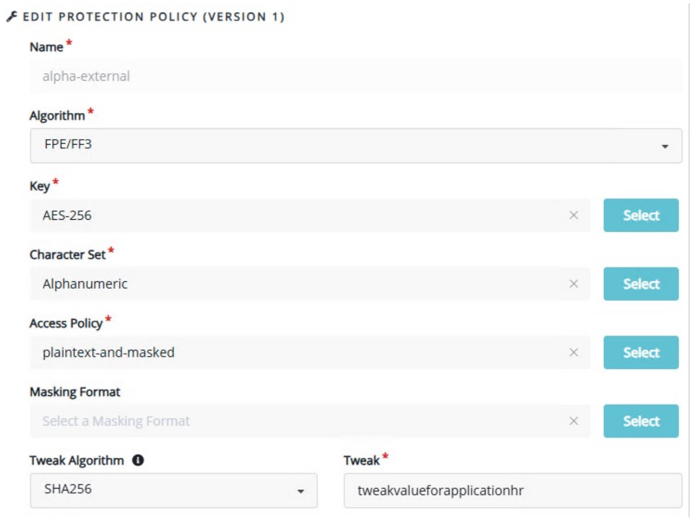
Architectural Overview

DPG 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 by selecting from an ever-growing list of NIST-sanctioned algorithms.


EDIT PROTECTION POLICY (VERSION 1)

Name *
alpha-external

Algorithm *
FPE/FF3

Key *
AES-256 × Select

Character Set *
Alphanumeric × Select

Access Policy *
plaintext-and-masked × Select

Masking Format
Select a Masking Format × Select

Tweak Algorithm
SHA256

Tweak *
tweakvalueforapplicationhr

The Access Policies can be automated for onboarding/offboarding.

Thales Field-Level Data Protection

DPG is one of several centrally-managed Thales data protection offerings. CipherTrust RESTful Data Protection (CRDP) is a RESTful service that offers field-level data protection. CipherTrust Application Data Protection (CADP) offers field-level 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 and tokenization for databases and structured files.

All centrally-managed Connectors support Static Data Masking, Dynamic Data Masking and Redaction.

CipherTrust Data Security Platform

DPG 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 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 and control your organization's sensitive data, wherever the data resides.

ESG Statement

The Thales CipherTrust Data Protection Gateway (DPG) containerized solution makes a smaller carbon footprint than a full server solution or virtual appliance, because DPG is a sidecar to your application and makes the orchestrator aware of when resource needs 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

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