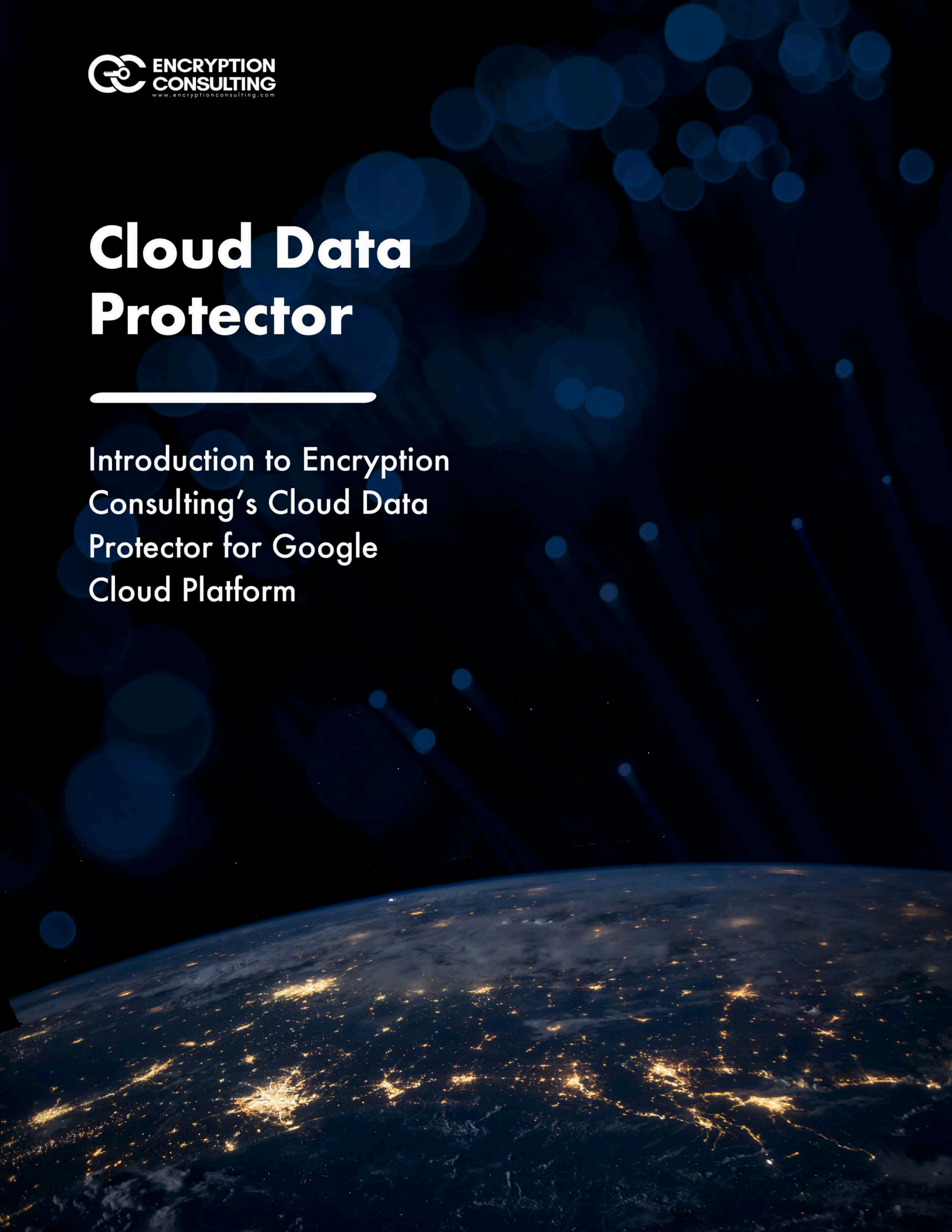
ENCRYPTION CONSULTING
www.encryptionconsulting.com

Cloud Data Protector

Introduction to Encryption Consulting's Cloud Data Protector for Google Cloud Platform



What is Cloud Data Protector (CDP)?

A secure transition of structured/unstructured data from on-premises to Google Cloud Platform while the data is protected via Format Preserving Encryption (FPE) or has been masked. Cloud Data Protector hides all sensitive information to maintain compliance while the migration takes place.

The data would also preserve its format and referential integrity; hence a 16 digit card number would have the same format after encryption. FPE would allow all systems to remain functional, even post-migration.

Cloud Data Protector works with Google Cloud Platform (GCP), which stores encryption keys used for FPE. GCP ensures the whole process is at least FIPS 140-2 Level 1 compliant, while Level 3 compliance can be reached with CloudHSM or keys with Hardware Level Protection.

Use Cases : Cloud Data Protector

Cloud Data Protector can be used for multiple reasons:

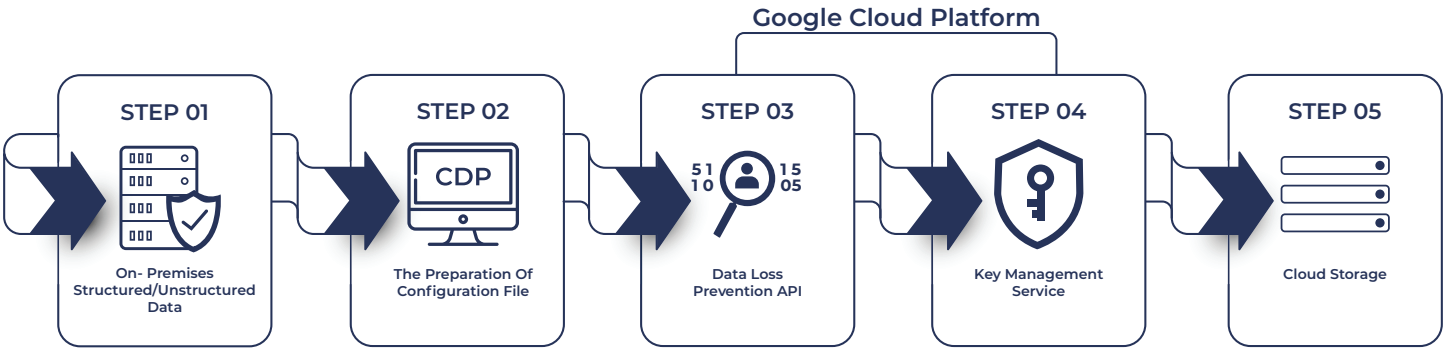
- It securely migrates data from on-premises to the cloud. Data can be encrypted using FPE or masked
- Cloud Data Protector can also help customers achieve compliance with PCI-DSS, HIPAA/HITECH, GDPR, CCPA, NYDFS along with other regulations.

Being open-source, Cloud Data Protector has different use cases, such as:

- CDP can be normally be used as intended. For that, a configuration file needs to be prepared, passed onto the utility, which will then initiate the task. The preparation of the configuration file would need some attention and planning.
- CDP can be used with scheduled tasks or cron jobs, which will prepare files overnight for bulk secure migration.
- For bulk migrations, CDP can be combined with a script that will handle the de-identification process of all the data involved.

> ***"It securely migrates 100 % DATA from on-premises to the cloud. Data can be encrypted using FPE OR MASKED"***

How Cloud Data Protector works?



After the initial setup, where Google Cloud Platform needs to be set up and enabling a few of the services, the Cloud Data Protector is ready to be used.

01. The data that needs to be protected first needs to be prepared. The structured/unstructured data would be passed to Cloud Data Protector.

02. A configuration file will be prepared, consisting of the path to the data, keys that need to be used , data that needs to be encrypted or masked, and the method they would undergo. Methods include FPE, masking, and more. The preparation of configuration file does require attention and planning. We discussed this in detail in our documentation.

03. After the CDP is launched with proper configuration file, CDP first connects DLP API and implements the methods that need to be done per column.

04. If the process requires FPE, the DLP API will contact Google Cloud Plaform's KMS, where the keys are stored. FPE would require a key from KMS or CloudHSM, and another key that will be generated on the user's end.
The key generated would be saved in a file named wrapped_keys.json with sufficient information. Users can use the file with other utilities under Cloud Data Lake Protection.

05. Finally, after the whole process, the user can safely transfer the data to cloud storage on the Google Cloud Platform.

About Us

Encryption Consulting LLC is a customer-focused cyber security consulting firm providing an array of services in all aspects of data protection.
Our areas of expertise include Public Key Infrastructure, enterprise key management, cloud key management, codesigning, hardware security modules, transparent data encryption, element level format preserving encryption, homomorphic encryption, and tokenization.

Our Expertise

Our knowledge and experience put experts on your team to deploy the industry's best, proven encryption technologies. Our people and services enable organizations to successfully achieve their data security goals in Confidentiality, Integrity, and Availability.

Our solutions will secure your sensitive data throughout its entire lifecycle.

The Problem We Solve

Our specialty is delivering Assessments, Strategies, and Implementations for organizations who either lack the specialized resources or who simply value having a trusted advisor to assist them to upgrade their data security posture.

At Encryption Consulting, we have created a custom framework based on NIST 800-57, NIST 800-53 standards, FIPS and industry best practices to accelerate our client's data protection projects.

See it in action

Encryption Consulting LLC is a customer-focused cyber securtiy consulting firm providing an array of services in all aspects of data protection.

Contact Us

encryptionconsulting.com

facebook.com/encryptionconsulting

linkedin.com/company/encryptionconsulting

twitter.com/encryptioncons