ENCRYPTION CONSULTING

Big Query Protector

Introduction to Encryption Consulting's Big Query Protector for Google Cloud Platform.

What is BigQuery Protector?

BigQuery Protector provides a way to access and store data into the database while keeping the database encrypted. The tool provides the option to decrypt the data while extracting infromation from the database, or encrypting data while inserting into the database.

BigQuery Protector is made on Google Cloud Platform and thus provides the ability to use the Big Query Data Analytics Platform even though the data remains encrypted on the SQL database hosted on cloud. The encrypted database adds a layer of security that, in case of a data breach, prevents attackers from getting plaintext data due to the databases encryption. Also, Big Query Protector enhances data privacy enabling the option to perform analytics on encrypted data.

Use Cases : BigQuery Protector

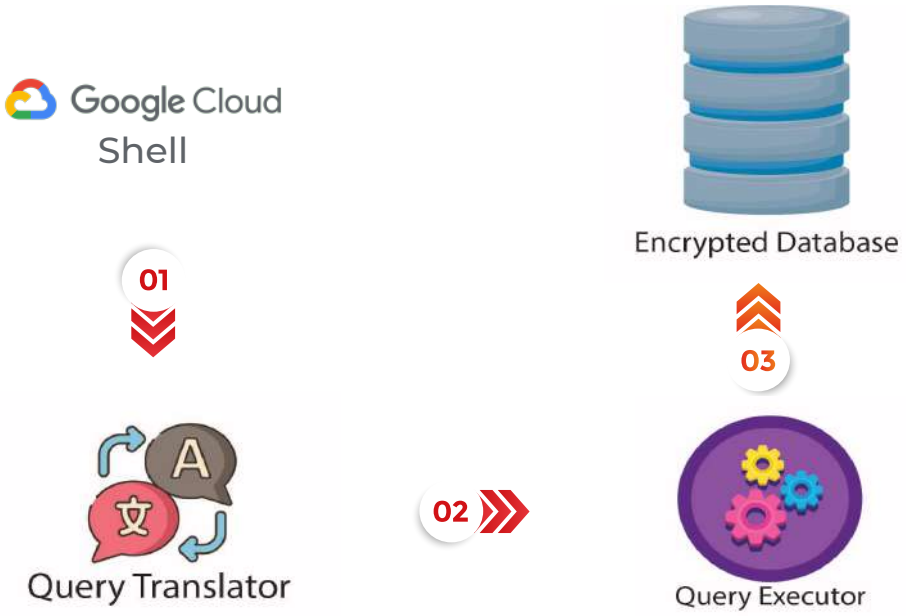
BigQuery Protector can be used for multiple reasons:

- Keep database encrypted while having the option to query the database and perform other data analytics operations on the encrypted database. Format Preserving Encryption is used when inserting new data which protects any sensitive data in the database, while still allowing the data to be queried through BigQuery.
- Big Query Protector can be deployed as containerized service or as a library embedded with other services, which provides a way to access the encrypted data on the fly without compromising performance or security.

BigQuery Protector can be used in various applications and deployed in multiple ways, such as:

- Standalone: BigQuery Protector can be deployed directly on GCP project
- Containerized: BigQuery Protector can be deployed in a container in Kubernetes
- Library: BigQuery Protector can be embedded with other services such as a executable

How BigQuery Protector works?



Working with Google Cloud Platform's BigQuery service, BigQuery Protector ensures that data stored within a GCP database can be inserted and queried in an encrypted state.
After the initial setup, where the project has several services enabled, BigQuery Protector is ready to be used.

01 We would first need to log into Google Cloud Platform and use Cloud Shell to be able to use BigQuery Protector. BigQuery Protector takes queries directly from the shell itself and pass it on to the Query Translator.

02 The accepted Query from the shell is translated to a true BigQuery query using the translator and then is passed onto the BigQuery. BigQuery would then execute the given query on Google Cloud Platform.

03 The Query would be responsible for extracting or inserting data onto the database. The database would be encrypted, and Format Preserving Encryption is used when inserting new data which protects any sensitive data in the database. Values in the table can be searched for by either their encrypted or unencrypted value, and will be displayed as the encrypted value by default.

About Encryption Consulting

Encryption Consulting is a customer-focused cyber-consulting firm providing an array of services in all aspects of Encryption. Our areas of expertise include Public Key Infrastructure, enterprise key management, cloud key management, code-signing, 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.