COMFORTE DATA PROTECTION FOR GOOGLE CLOUD AND BIG QUERY

BRING YOUR OWN ENCRYPTION TO GOOGLE CLOUD

SOLUTION AT A GLANCE

- Bring Your Own Encryption (BYOE) protection for Google Cloud, hybrid environments, and multi-cloud setups
- Consistent data-centric security for complex environments
- Granular data access controls
- De-identification of data for cloud-based analytics through advanced tokenization or format-preserving encryption (FPE)
- Cloud-native integration for rapid implementation
- Seamlessly integrate with Google BigQuery

INTRODUCTION

Operating in the cloud carries inherent risks related to security and privacy. To address these concerns, comforte's Data Protection for Google Cloud provides a comprehensive solution that integrates seamlessly with BigQuery, ensuring strong safeguarding of sensitive data. This approach not only enables organisations to meet regulatory obligations, but also allows for the data to remain accessible for essential business processes, applications, and analytics.

WHY ADDITONAL DATA PROTECTION

For some organizations Google's built-in security features will meet their requirements, as the native encryption in BigQuery provides robust security measures for data at rest and in transit.

Google Cloud Platform (GCP) encrypts customer content stored at rest, by default without any action required from the customer. This is possible if the data is stored on GCP not elsewhere. To move data outside of Google's environment, e.g. to another cloud service provider or data analytics tools, it may be necessary to re-identify the data before applying a new protection method.

For organizations operating in highly regulated industries, additional security measures are often mandated by regulators. Here, an additional layer of data-centric security may be required.

COMFORTE DATA PROTECTION FOR GOOGLE BIG QUERY: HOW IT WORKS

Comforte Data Protection for Google Cloud and BigQuery pseudonymizes sensitive data (PII, PHI, PCI) using tokenization or FPE on a field level, the data element is completely replaced by a token in the database. The token itself preserves compatibility and usability for analytics tools but doesn't expose any sensitive information. This allows for use of BigQuery or any BI tool without the need to change the SQL syntax.

Furthermore, tokens do not require a lot of computational resources to process, allowing for high performance and low latency. Although tokens can be converted back to their original value if required for business purposes, since the data store and protection engine are strictly separated, this method helps achieve compliance with privacy and data protection regulations and immensely reduces risks related with data breaches, because tokenized data has no value for potential misuse.

YOUR OWN DATA PROTECTION FOR GOOGLE CLOUD

In the BYOE concept, the customer of a public cloud has the freedom to use their preferred encryption and protection technologies, regardless of the specific offerings provided by the public cloud provider. This allows the customer to have exclusive control over the generation of all protection secrets, such as encryption keys or tokenization secrets. As a result, only protected data is ever stored in the public cloud.

Comforte goes beyond the built-in capabilities of cloud-based data stores by offering comprehensive end-to-end data protection for hybrid and multi-cloud environments. It provides the data-centric ability to secure data before storing it in the cloud and ensures continuous protection throughout its movement and processing by applications and users.

The de-identifying techniques include data masking, format-preserving hashing, tokenization, and format-preserving encryption (FPE). They enable the process of pseudonymization or complete anonymization of data. Anonymization eliminates sensitive information, rendering the data unsuitable for advanced analytics. On the other hand, pseudonymization methods such as tokenization or FPE retain data usability for analytics purposes and ensure data integrity.

This data-centric approach can simplify security management in complex environments, allowing confident self-service access, movement between cloud services or usage in analytics tools without compromising privacy and security.

BENEFITS

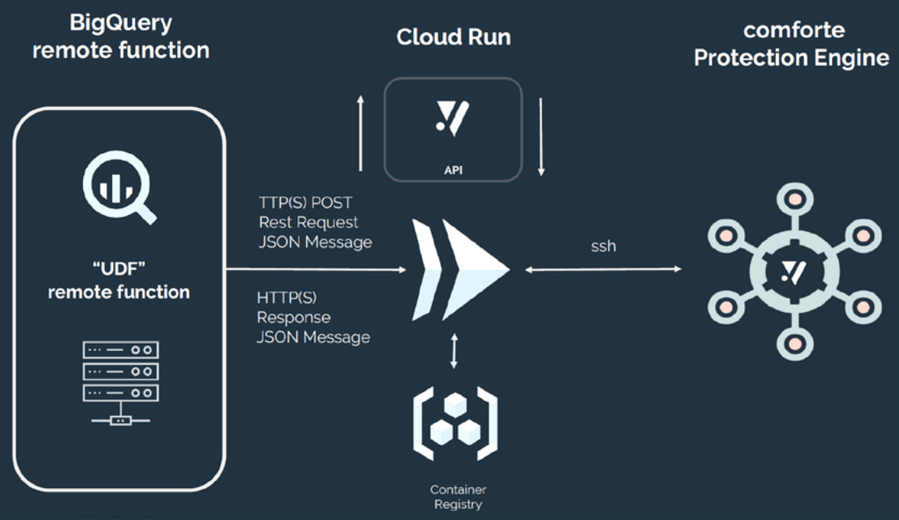
- **Enhanced security for cloud-based analytics** - Preserve privacy and protect the data
- **Bring Your Own Encryption (BYOE) to the cloud** - Maintain control and increase flexibility for multi-cloud setups
- **Cloud-native integration** - Rapid implementation for data protection from the earliest opportunity
- **Run analytics on protected data sets** - Enable secure usage of sensitive data
- **Protect privacy and achieve compliance** - Pseudonymized data is fully compliant with privacy regulations

IMPLEMENTATION OPTIONS

1. **Preemptive data protection before data reaches BigQuery:** comforte provides a suite of transparent integrators and APIs that enable data protection measures at the earliest stages of the data lifecycle. This means that sensitive data can be shielded at different stages during its ingestion into BigQuery. Protecting sensitive data prior to ingestion into the cloud i.e. before it even touches Google storage, ensures that no sensitive information is stored on the cloud, mitigating potential risks associated with cloud storage.

2. **Remote function from within BigQuery:** Use Cloud Functions and Cloud Run by leveraging APIs to safeguard sensitive data already residing within BigQuery. Role-based access controls enable granular management of data access. Data analysts, for example, can retrieve data in its original form, while other users are limited to viewing protected data only.

   [see the diagram below]



Contact us to start a discussion