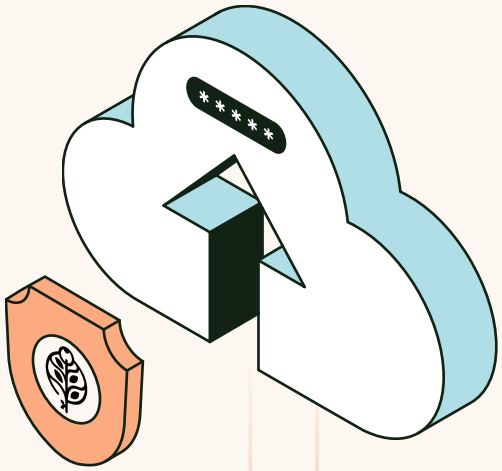

Vaultree and Google BigQuery:

Pioneering Secure Data Analysis in the Cloud

Data is the cornerstone of strategic decision-making. Therefore, the security of this data is imperative, especially as organisations around the world continue to migrate increasingly to cloud environments.

In 2023, the number of organisations using the cloud for operational purposes reached 94%, with 92% of businesses having a multi-cloud strategy in place or in the works - Zippia Cloud Adoption Study

As a trusted Google Cloud Platform (GCP) partner, Vaultree's groundbreaking Fully Homomorphic Encryption (FHE) & Data-In-Use Encryption technology is revolutionising cloud security, already demonstrating significant enhancements through its integration with Google CloudSQL and AlloyDB. These successful collaborations have established new standards for trust and security within cloud environments, underscoring Vaultree's solution's effectiveness and reliability.

Building on this momentum and responding to the increasing need for advanced data protection in cloud-based analytics, Vaultree is excited to extend this innovation to BigQuery. This integration makes BigQuery, in conjunction with Vaultree, the first to offer an always-encrypted Personally Identifiable Information

(PII) Data Warehouse, ensuring encryption across all data lifecycle stages: at rest, in transit, and now uniquely, in use. This advancement means customers can fully utilise their data without ever needing to decrypt it, marking a pivotal moment in secure data analysis.

"Vaultree gives our customers the peace of mind they need when it comes to security and overcoming the fear of giving up control of their data." Jobin George - Data and Analytics Solutions Architect at Google

The Current State of Cloud Security

As with any technology primed to modernise legacy systems, cloud computing has faced a large degree of scepticism, with a recent report finding that "94% of organisations surveyed were moderate to extremely concerned about cloud security." This hesitancy is warranted as the cloud security landscape continues to evolve and adapt to new threats and advances in technology. Some key trends in this space include:

1. The Rise Of Hybrid And Multi-Cloud Environments

Organisations are increasingly adopting hybrid and multi-cloud strategies to leverage the benefits of different cloud providers. However, managing security across multiple platforms and environments poses a significant challenge. This approach may also result in data integration, compliance and complexity issues.

2. Increased Sophistication Of Cyberattacks

Cloud environments are quickly becoming prime targets for cyberattacks. Organisations must stay up-to-date on the latest threats and trends to continually improve or fill gaps within their current security infrastructure.

3. A Growing Need For Data Privacy And Compliance

Data privacy and compliance regulations are becoming increasingly stringent, requiring organisations to ensure that their cloud environments adhere to them. This can be a complex and time-consuming process that necessitates careful planning and implementation, especially when operating in multiple jurisdictions.

4. Cloud Hesitancy

Cloud hesitancy remains a significant concern among organisations, primarily due to security worries and the conventional practice of processing plain text data in modern data warehouses, leaving sensitive information vulnerable.

Vaultree and BigQuery: A Synergistic Partnership

What is BigQuery?

Google BigQuery is a fully managed, serverless data warehouse that enables scalable, cost-effective, and fast analysis of big data. It is designed to process vast amounts of data in seconds to minutes, providing insights through SQL queries.

BigQuery's serverless architecture allows users to focus on analysing data to find meaningful insights using familiar SQL and does not require any infrastructure management. Its capabilities are integral for businesses looking to leverage powerful analytics to drive decision-making, optimise operations, and predict trends.

Vaultree’s Data-In-Use Encryption in the Cloud

Vaultree's technology represents a significant advancement in data encryption. Unlike traditional encryption methods that only secure data at rest or in transit, our technology ensures data remains encrypted even when it is being processed or used. This capability is groundbreaking, especially in cloud environments where data security and privacy are paramount.

By moving into the cloud, Vaultree offers a compelling answer to concerns fueling cloud hesitancy. Check out how below.

Vaultree and BigQuery: Securing the Future of Cloud Computing

By collaborating with Vaultree, GCP positions itself at the forefront of secure cloud computing and analysis, granting customers peace of mind.

Product Overview

Vaultree's Data-In-Use Encryption SDK integrates seamlessly with BigQuery, functioning as a set of loadable functions and a driver that facilitates the encryption of data at rest, in transit, and, importantly, in use. Utilising proprietary, searchable encryption for text data and Fully Homomorphic Encryption (FHE) for numerical data, alongside any cypher of choice for encryption at rest, this solution enables constant data encryption. Its standout feature is the ability to keep data encrypted during processing, requiring decryption only when results need to be interpreted by humans.

Technical Advantages

Vaultree's Data-in-Use Encryption differentiates itself from other FHE technologies in its performance. Operations on Vaultree-encrypted data are typically only 10-15% slower than their plaintext counterparts, marking a substantial improvement over traditional column-level encryption methods and other implementations of FHE. This efficiency is achieved through Vaultree's proprietary encryption algorithms, tailored for high-performance cloud environments.

Security and Compliance

By ensuring that data remains encrypted at all times, Vaultree's solution significantly enhances security and mitigates the impact of potential data breaches. In the event of unauthorised access, the retrieved encrypted data (ciphertext) remains unusable. The at-all-time encryption approach simplifies compliance with stringent data protection regulations like GDPR and HIPAA, as sensitive information is never exposed in plaintext.

Example Use Cases

The integration of Vaultree's Data-In-Use technology with BigQuery opens a myriad of possibilities across various sectors, particularly for enterprises handling sensitive information.

Healthcare Sector

Use Case: Patient Data Analytics

Vaultree's Data-In-Use encryption protects sensitive patient data, including medical records, allowing healthcare providers to securely analyse this information in BigQuery to enhance treatment outcomes and efficiency. By maintaining HIPAA compliance and patient confidentiality, this use case boosts trust in digital healthcare and supports the development of sophisticated, data-driven care models.

Financial Services

Use Case: Fraud Detection And Analysis

Vaultree's Data-In-Use facilitates the encrypted analysis of vast transactional data in BigQuery, aiding financial institutions in secure fraud detection without compromising customer information. This approach minimises financial fraud losses and bolsters consumer trust in digital banking, enhancing the financial system's security and integrity.

Research and Development

Use Case: Secure Collaborative Research

Vaultree's technology allows for the secure processing and analysis of encrypted research data in BigQuery, safeguarding intellectual property and participant privacy in collaborative projects. This fosters a secure research ecosystem, driving faster innovation and knowledge discovery without risking data integrity or confidentiality.

About Vaultree

Vaultree, a leader in secure data operations, has pioneered the world's first Data-In-Use Encryption solution capable of real-world application, transforming the approach to sensitive data protection and access.

Vaultree's innovative solution enables enterprise organisations to securely process, search, and compute on structured and unstructured encrypted data, enabling AI and ML applications. Vaultree eliminates traditional data in-use encryption challenges with performance, speed, and scale, making it the ideal solution for data-intensive industries.

Vaultree's technology provides persistent encryption, even during a leak. Additionally, under GDPR provisions (Under Article 34, section 3(1) of GDPR), companies are not required to disclose a breach if the data is encrypted. With Vaultree, your data is never stored in plaintext, so even if you experience a breach, your reputation remains protected.

Integrating Vaultree into existing database technologies is seamless, requiring no technology or platform changes. Google and data-driven companies worldwide trust Vaultree to safeguard sensitive data. Vaultree keeps your data always encrypted, always accessible, and always secure - fueling growth and innovation - while mitigating cybersecurity risks.

Contact Information

For further information, troubleshooting and signposting through Vaultree, please contact:

Solutions Team
solutions@vaultree.com