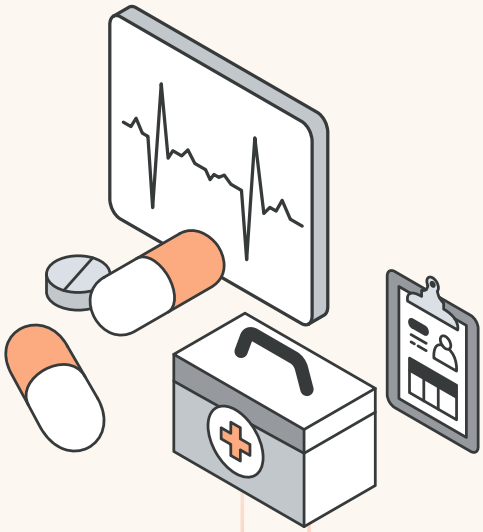

Vaultree and Google BigQuery:

Revolutionising Healthcare Data Analysis

In healthcare, sensitive patient data meets the forefront of technological advancement. The partnership between Vaultree and Google BigQuery emerges as a beacon of innovation and security. This groundbreaking integration utilises Vaultree's proprietary Data-In-Use encryption technology, coupled with Google BigQuery's robust, scalable analytics capabilities, offering a solution that is both secure and efficient.

As healthcare organisations increasingly migrate to cloud environments to leverage big data analytics for improved patient outcomes and operational efficiencies, the paramount importance of data security and compliance with stringent regulations cannot be overstated. Vaultree's integration with BigQuery is not merely a technological advancement; it is a commitment to transforming the healthcare industry's approach to data analysis, ensuring that sensitive information remains encrypted and secure, even during processing. This collaboration sets a new standard for data security in the cloud, enabling healthcare providers to harness the power of their data without compromise.

The Current State of Cloud Security in Healthcare

The healthcare sector's adoption of cloud technologies for data storage and analysis has heightened concerns around data security and patient privacy.

1. Hybrid And Multi-Cloud Strategies

There is an increasing trend amongst healthcare organisations to adopt hybrid and multi-cloud environments 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 Rate And Sophistication Of Cyberattacks

The exponential growth of healthcare data has made organisations vulnerable to advanced ransomware and cyber attacks, with cloud breaches through phishing and ransomware becoming increasingly prevalent. Such attacks have led to 95% of organisations becoming moderately to extremely concerned about cloud adoption(1). This underscores the need for comprehensive security measures that protect against threats not only from external actors but also from internal vulnerabilities.

3. Unauthorised Access

Unauthorised access to cloud resources poses a significant threat, with attackers exploiting vulnerabilities like excessively permissive access, poorly protected passwords, encryption keys, and admin credentials. Such poor access control leads to endangered intellectual property safety and undermines potential secure collaboration efforts.

4. Regulatory Compliance Challenges

Healthcare providers must navigate complex regulatory frameworks like HIPAA and GDPR while managing data across multiple jurisdictions when utilising cloud services, adding layers of complexity to ensure compliance and data privacy

Vaultree and BigQuery: A Synergistic Partnership

Vaultree's integration with Google BigQuery marks a pivotal advancement in secure cloud computing for the healthcare industry. This partnership synergises Vaultree's groundbreaking Data-In-Use Encryption technology with BigQuery's robust, scalable, and cost-effective data analysis capabilities. The collaboration is designed to address the unique challenges faced by healthcare organisations, ensuring the highest levels of data security and privacy without compromising on analytical power or operational efficiency.

Transforming Cloud Security with Vaultree's Data-In-Use Encryption

Vaultree’s technology ensures data remains encrypted even during processing, unlike traditional encryption methods that secure data only at rest or in transit. This continuous encryption is crucial for healthcare data, often including sensitive patient information. By integrating this technology with BigQuery, healthcare organisations can securely move their data analytics to the cloud, significantly enhancing data security in cloud environments.

Streamlining Healthcare Data Analytics

BigQuery's serverless, fully managed data warehouse allows for scalable and fast analysis of big data, providing insights through SQL queries. Integrating with Vaultree’s technology enables healthcare organisations to analyse encrypted patient data within BigQuery. This means they can leverage the cloud's computational power for data-driven decisions without exposing sensitive information, thus streamlining analytics processes while maintaining data security.

Enhancing Compliance

The combination of Vaultree’s encryption capabilities with BigQuery's infrastructure ensures that healthcare organisations can meet stringent data privacy and compliance regulations, such as GDPR and HIPAA. In fact, under HIPAA, organisations shown to protect PHI with advanced encryption, such asVaultree’s solution, need not report a breach as data remains encrypted at all times. This ability to perform computations on encrypted data simplifies compliance with regulations.

Data Sovereignty and Veractiy in the Cloud

Vaultree's Data-In-Use technology offers selective encryption down to the column and table level, allowing healthcare providers to safeguard sensitive patient data precisely and efficiently.

Moreover, Vaultree enhances data veracity through comprehensive audit logs, meticulously recording all data access and processing activities. This capability is critical for maintaining a transparent and traceable data handling process, allowing organisations to monitor, verify, and report data usage and access, crucial for regulatory compliance and operational integrity. Additionally, Vaultree's granular access controls further bolster data sovereignty by enabling precise management of who can access or process data, ensuring that only authorised personnel can interact with sensitive information.

Facilitating Secure Collaboration and Innovation

Through Vaultree’s recently launched product, Vaultree Encrypted Data Sharing (VEDS), secure collaboration is revolutionised for the healthcare sector, allowing organisations to share and analyse encrypted cloud-based datasets. This synergy enables healthcare entities to securely collaborate on research and data analysis without compromising data security or patient privacy. By facilitating the secure analysis of encrypted data, VEDS empowers healthcare professionals to leverage shared insights and advance medical research while ensuring compliance with privacy regulations. The combination of VEDS and BigQuery sets a new standard in healthcare data management, merging powerful analytics with unmatched data protection.

A New Standard in Healthcare Data Management

Vaultree's Data-In-Use Encryption and BigQuery together set a new benchmark in secure, efficient, and compliant healthcare data management. This partnership demonstrates how advanced encryption can be integrated with cloud-based data warehousing solutions to offer a comprehensive data management solution. It enables healthcare organisations to harness the power of cloud computing for analytics without sacrificing security or compliance.

Conclusion

Vaultree's integration with Google BigQuery represents a transformative leap forward for the healthcare industry, bridging the gap between the need for robust data security and the demand for advanced data analytics. This partnership not only enhances the security and privacy of sensitive healthcare data but also empowers healthcare organisations to confidently leverage cloud technology for data-driven insights. Vaultree's technology, in synergy with BigQuery's analytics capabilities, ensures that healthcare data remains encrypted, secure, and compliant, even during complex analyses.

Discover how Vaultree's collaboration with Google can elevate your organisation's data management capabilities. Contact us today to explore our partnership's transformative potential for your operations.

Contact Information

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

Solutions Team
solutions@vaultree.com