Unbound CORE GCP External Key Manager

The Google Cloud External Key Management (EKM) introduces unique capabilities for securing your data. You can now have tight control over your data in Google's cloud platform, ensuring it is encrypted at rest using keys that are fully controlled by you. This holds true even for data used by Google services such as BigQuery and Cloud SQL. The Unbound CORE GCP External Key Manager allows you to leverage this unique security functionality. With Unbound CORE, you are in control of the keys to your data in the cloud. In this brief we introduce this innovative offering by Unbound.

Government Access and CLOUD Act

As government agencies worldwide make daily requests for access to customer data stored by the major cloud providers, ensuring you are in full control of your data becomes essential. There are many factors leading to this increase in government interest. For one, it is the rise in the significance of compliance and regulation in the technology space at large. In addition, new initiatives such as the Clarifying Lawful Overseas Use of Data (CLOUD) Act play a key role. These requests for data can cause conflict — the responsibility to preserve consumer privacy on the one hand, while meeting regulatory and/or public safety obligations on the other. Unbound CORE manages the keys used to encrypt your data on Google Cloud. This goes a long way to solve the privacy vs. transparency issues, as well as the many security challenges associated with holding sensitive and private data in the cloud.

About Google External Key Manager

The Google EKM enables users to secure and control use of cryptographic keys for cloud services. With EKM, it is now possible to use cryptographic keys held outside of the Google Cloud Platform, to protect data at rest stored by Google cloud. The EKM acts as an extension of Google's Key Management Service (KMS).

The Google EKM works in the following way: Google Cloud native services encrypt data with a local data encryption key (DEK). This key is in turn "wrapped" (encrypted) with a KEK (key encryption key) that is held within the Google Cloud KMS. In order to allow customers to manifest control and management over their data, the EKM allows them to wrap the KEK with an External-KEK residing within the Unbound CORE GCP External Key Manager.

The customer has exclusive control over the External-KEK, thus can audit, approve or deny any request to access customer's data in the cloud.

The Unbound CORE GCP External Key Manager Integration

With Unbound CORE, Google Cloud customers enjoy unprecedented control over their data. This data is privately and securely stored at rest, encrypted with keys exclusively controlled by the customers. This architecture is often referred to as Control Your Own Key (CYOK).

Unbound's External Key Manager for Google Cloud is unique in its approach – it secures keys in the cloud using secure multiparty computation technology. This software-based solution can be easily deployed in any cloud region, while offering excellent performance, robustness and ease of management.
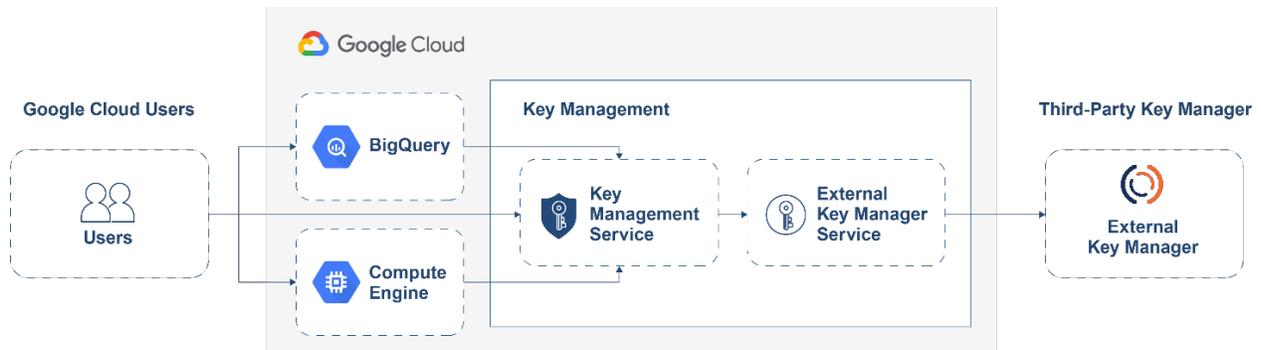
Better Together: Benefits of GCP + CORE

The Unbound CORE GCP External Key Manager enables businesses worldwide to protect and be in full control of their data on Google Cloud. Customer data stored and used by Google, including services such as BigQuery, can now be encrypted at-rest using keys that are fully controlled and owned by the customer. Google does not have access to these encryption keys – they are protected and managed solely by the enterprise customer using Unbound CORE.

The solution offers the following benefits:

- Help comply with data protection legislation and regulations, including the EU General Data Protection Regulation (GDPR).
- Regulate the key management process – by managing their own keys, enterprises can better protect their data and improve compliance.
- Maintain client data confidentiality – only the customers of the cloud service have access to their data and encryption keys, reducing the risk of breach.
- Protect against rogue administrators – minimize the risk of unauthorized data access by a service administrator who may be misusing privileges.
- Control government access to corporate data – cloud service providers periodically respond to subpoenas where they are legally compelled to provide user data to government agencies (e.g., under CLOUD Act).
- Ensure scalability and stability – CORE is easily scalable to any enterprise's needs. By integrating with GCP, the client gains the ability to bring this scalability to GCP and its associated services.
- Deploy quickly and easily – CORE is easy to deploy at multiple metro areas and availability zones, thanks to its mesh technology auto synching keys across sites.

- Utmost security and privacy – data at rest is secured using the CYOK (control your own key) approach.
- Auditing tools with multiple integrations – all operations are logged in a tamper-proof audit that can be connected to tools such as Splunk.

Summary

Unbound CORE allows security-conscious enterprises to utilize Google Cloud, enabling them to move confidential data into the cloud while maintaining the security and compliance characteristics of their on-premises infrastructure. It empowers enterprise to control their own cryptographic keys, used to secure their data in the cloud, without the need to rely on any other third party such as an additional SaaS provider to control and protect the encryption keys.

Unbound offers a proven solution that enables companies to maintain control while fully realizing the benefits of the cloud without compromising security, privacy, or compliance requirements. The integration with Google, as an external key manager, is an important step forward in ensuring more companies can protect their most precious assets.

About Unbound

Unbound Security is the global leader in cryptography and empowers enterprise customers worldwide to confidently secure, manage and authenticate all critical business transactions, information, identity, and digital assets – anywhere, anytime. Unbound Security CORE is the enterprise platform of choice for secure key management, trusted by many of the world's largest banks and Fortune 500 companies. Unbound Security is a recent recipient of the Deloitte Fast 500 award and is headquartered in New York, with research and development facilities in Tel Aviv.

unboundsecurity.com