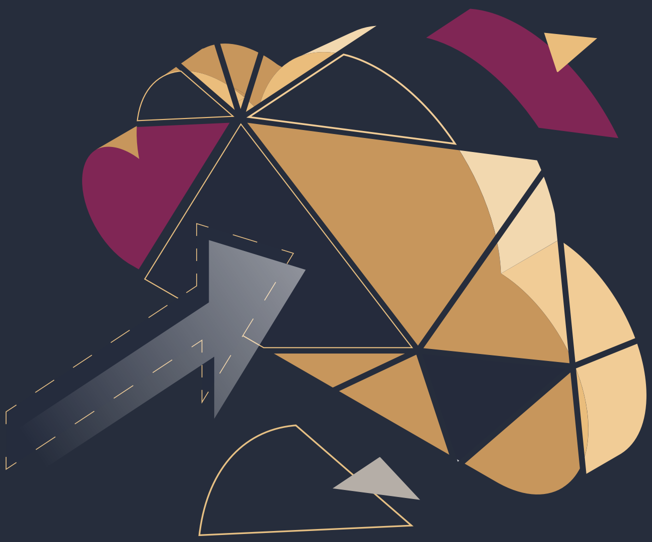
UNBOUND

(MATH OVER MATTER)

CONTROLLING YOUR DATA AND KEYS IN GOOGLE CLOUD WITH CLOUD EKM

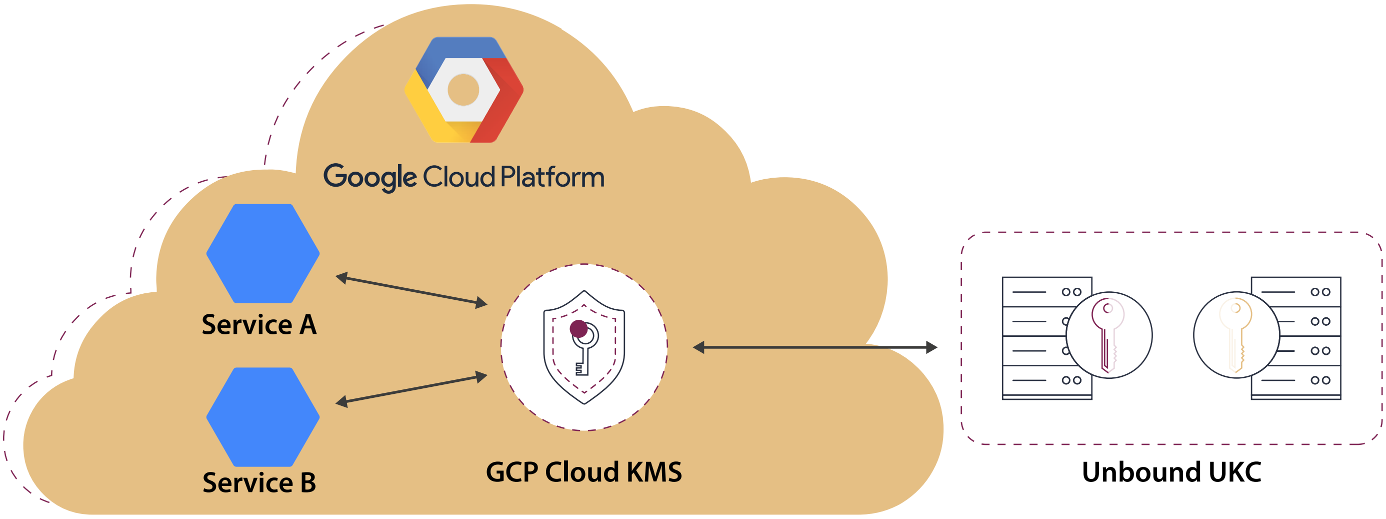
Solution Brief



Unbound Tech and Google Cloud

Unbound Tech has partnered with Google Cloud Platform, integrating with the Google Cloud External Key Management (Cloud EKM) product, to allow Google Cloud users to control their data by having full control of their encryption keys. Currently in Beta, Cloud EKM is part of Google's existing Cloud Key Management Service (Cloud KMS), which enables users to manage cryptographic keys for cloud services in the same manner they would on-premise.

With Cloud EKM, it is now possible to use cryptographic keys outside of Google Cloud Platform to protect data at rest for customers using Google's Cloud Key Management Service (KMS). Unbound Key Control (UKC), the first and only software-based virtual HSM solution that is FIPS-140-2 Level 2 certified by NIST, leverages secure multiparty computation (MPC) to protect cryptographic keys by ensuring they never exist in complete form throughout their lifecycle. Through the integration of these two products, Google Cloud customers now have unprecedented levels of security and control over cryptographic keys while maintaining access to critical data sets.



UKC serves as a pure-software virtual HSM, combining HSM-level security with the flexibility and agility of software. UKC eliminates the vulnerability of cryptographic keys as a single point of failure by ensuring that they never exist in complete form at any point in their lifecycle – not even when generated, while in use or while at rest – rather, keys exist as multiple random shares distributed among segregated machines.

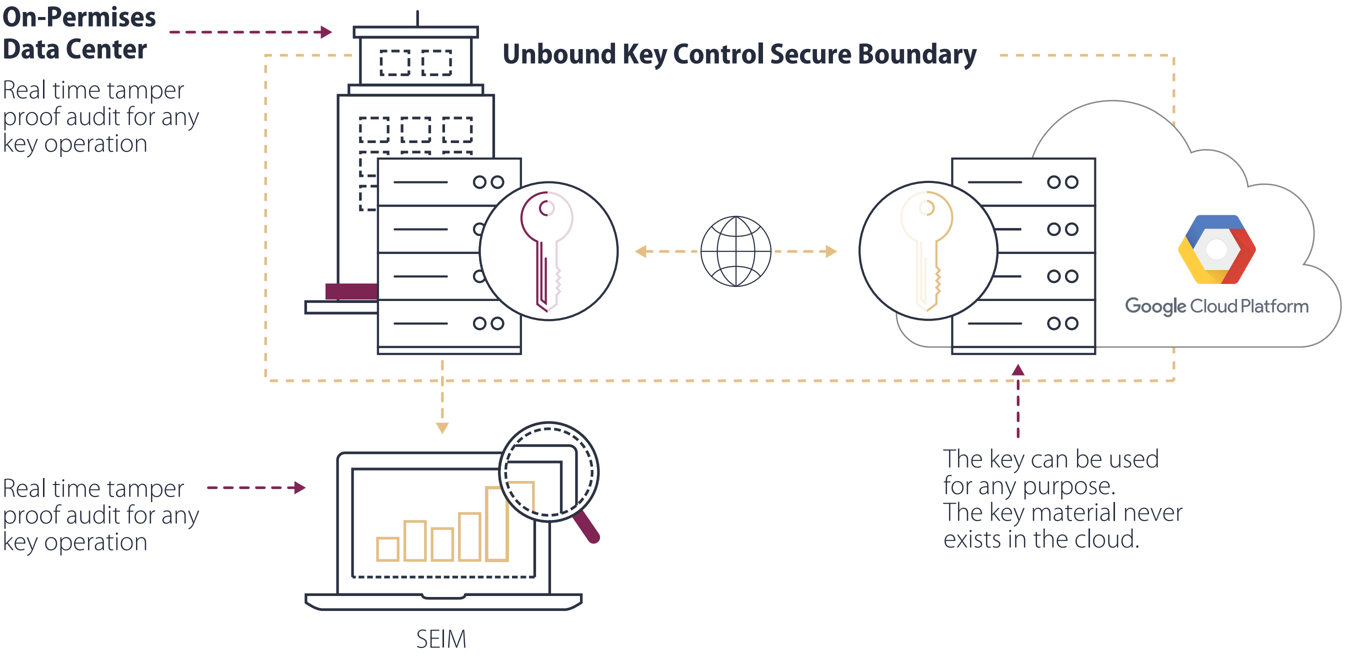
With UKC, highly security-minded Google Cloud customers gain the assurance they need to confidently operate in the cloud along with easy deployment that doesn't require dedicated hardware. Unbound UKC gives organizations control over their data in the cloud by allowing full control over their most sensitive cryptographic keys from their own environment (via on-premises or cloud instances), rather than relying on a third party, such as a SaaS vendor, to protect these keys.

Control Your Own Key (CYOK) in Google Cloud

CYOK is a unique architecture enabled by Unbound's core MPC technology that allows to split the key into two random shares stored separately and never united. The customer can deploy the UKC across on-premises, private cloud and public cloud, and while keeping at least one key share under his full control, it is guaranteed that the keys can never be compromised at any event, even by rogue adversary in the cloud or a subpoena.

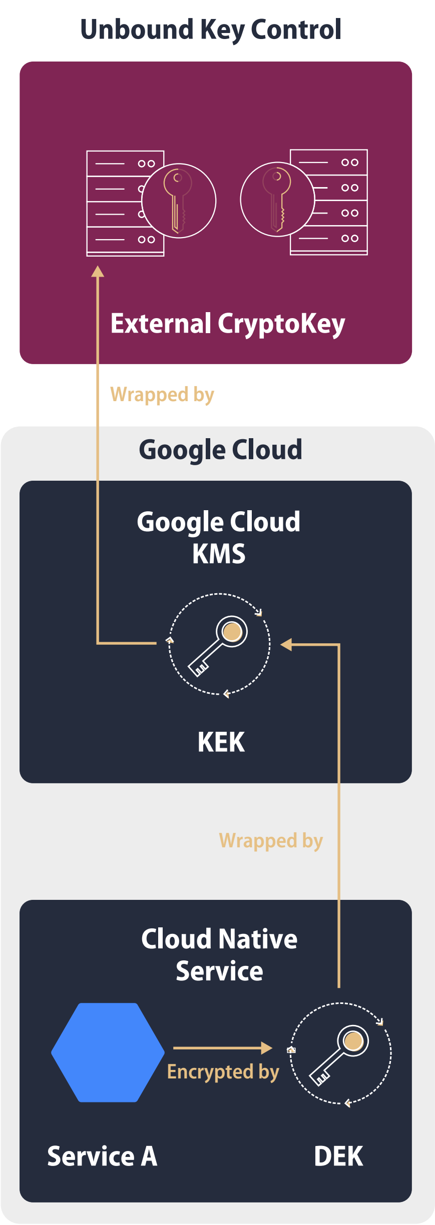
The diagram below shows a sample architecture, in which keys are split between one UKC node[1] held by the customer on-premises, and another node in a Google Cloud customer-controlled instance. The customer has ultimate control of the keys, and it is guaranteed it is guaranteed that the key cannot be obtained/compromised without compromising the customer's infrastructure. A subpoena will have to be directed at the customer (and not any other entity such as a CSP or a SaaS provider) in order to obtain any key material and the data that it protects. Google Cloud KMS (Key Management Service) can use the cryptographic keys in UKC via integration of the two products.

Architecture



[1] The UKC system is comprised from one or more pairs of standard servers that are installed and managed by the customer, forming UKC cluster. Each of these pairs is comprised of two nodes, named an Entry Point and a Partner. Together, they form the secure boundary of the UKC.

Control All Keys in the Key Hierarchy



The Cloud EKM works in the following way: Google Cloud native service encrypts its data with a local DEK (data encryption key). This key is in turn wrapped with the KEK (key encryption key) that is located within the Google Cloud KMS. In order to allow customers to manifest control and management over their data and encryption keys within Google Cloud, Google Cloud allows to wrap the KEK with an External CryptoKey residing within the UKC, external to Google Cloud. In this topology, only the customer can control the External CryptoKey, and enable the Google Cloud KMS to use it in order to preform cryptographic operations on the relevant native services. The below figure depicts the key hierarchy of the keys.

Joint Capabilities & Features

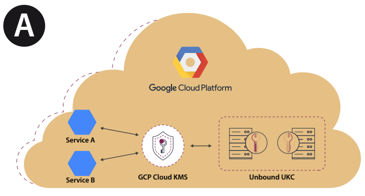
The technology integration provides a variety of benefits for Google Cloud customers, including the ability to:

- **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 unintended breaches.
- **Protect against rogue administrators:** Eliminate the possibility 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 (i.e. under CLOUD Act).

Deployment Options

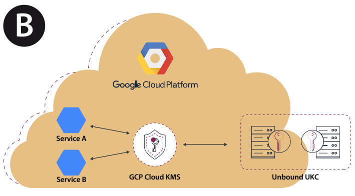
The following figure depicts the various deployment options of UKC as Cloud EKM.

A



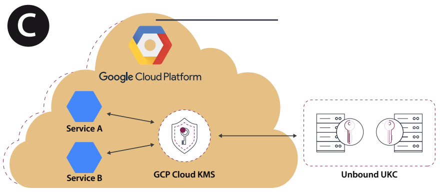
Both UKC nodes are located in GCP

B



One UKC node is located in GCP, while the other on-prem

C



Both UKC nodes are located on-prem

Summary

As more and more companies move vast amounts of data to the cloud, there is a strong desire to maintain greater control over cryptographic keys without compromising the usability or access to critical applications or services in the cloud.

Unbound's multiparty computation-based key management solution 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 by controlling their own cryptographic keys, 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 Cloud EKM is an important step forward in ensuring more companies are able to protect their most precious assets.

UNBOUND

Unbound Tech equips companies with the first pure-software solution that protects secrets such as cryptographic keys, credentials or other private data by ensuring they never exist anywhere in complete form. The Unbound Distributed Trust Platform stands as a new foundation for trust using secure multiparty computation to ensure secrets are always split into multiple shares and thereby eliminate any single point of compromise. Adopted by Fortune 500 companies, Unbound's elastic and agile platform protects secrets on untrusted infrastructure and removes existing dependence on dedicated security hardware, delivering a novel approach to security and privacy designed for the digital era. Serving as an engine for uninhibited growth, it allows enterprises to gain new levels of control over their secrets on any cloud, server or endpoint, and opens new possibilities for digital innovation.
Founded in 2014, Unbound has been recognized with numerous industry awards and named in multiple Gartner Hype Cycle Reports. Visit www.unboundtech.com.

Google Cloud Platform

Google Cloud is widely recognized as a global leader in delivering a secure, open, intelligent, and transformative enterprise cloud platform. Our technology is built on Google's private network and is the product of nearly 20 years of innovation in security, network architecture, collaboration, artificial intelligence, and open source software. We offer a simply engineered set of tools and unparalleled technology across Google Cloud Platform and G Suite that help bring people, insights, and ideas together. Customers across more than 150 countries trust Google Cloud to modernize their computing environment for today's digital world.

Control Your Own Keys while using Google Cloud Platform

Click Here for a Free Consultation

Follow Us