Fortanix | Google Cloud

Fortanix External Key Control and Management for Google Cloud Platform (GCP)

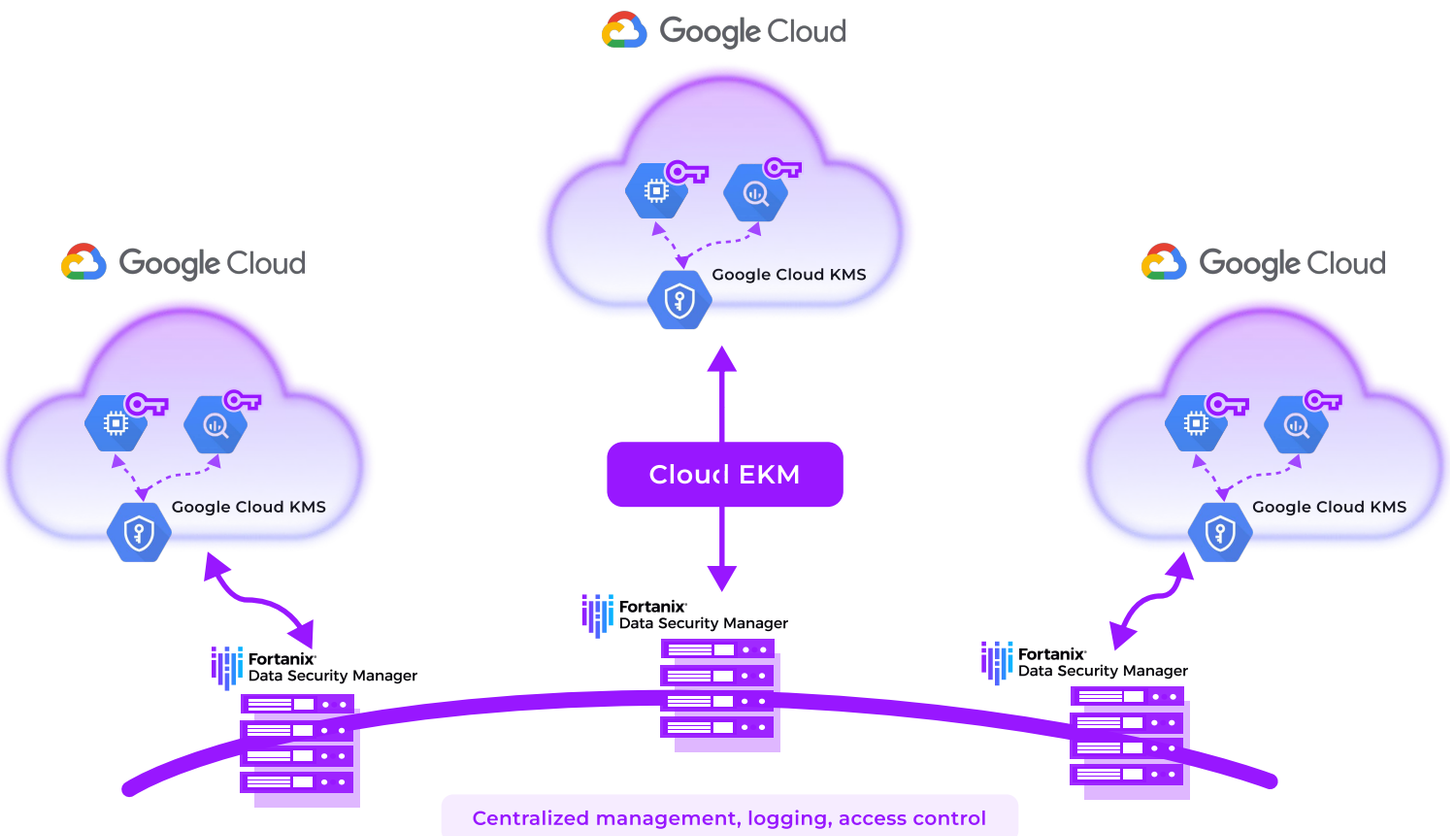
Fortanix External Key Manager generates and stores encryption keys outside of Google Cloud (GCP) and within customer datacenters.

Overview

Most organizations are looking to move their data and workloads into the public cloud. But they are held back because of compliance reasons or regulatory reasons and they are not comfortable with the cloud holding onto their keys. Organizations need greater control and security over their cloud keys.

Fortanix integrates with Google Cloud Platform's External Key Manager service to enable organizations to move the data to the cloud and get the same level of security for keys that they're used to in their own on-prem environments. Protect your BigQuery and other cloud native services data by doing server-side encryption.

Keys for the encryption are never stored at GCP. They are always under your control, away from the cloud. At a click of a button, in real time, enable and disable access to your data from specific instances and locations.



info@fortanix.com | 3910 Freedom Circle Suite 104, Santa Clara, CA 95054, United States

Key Benefits

Complete Control of Keys

Fortanix allows customers to stop decryption of data-at-rest with a kill switch and the key material never leaves the Fortanix Key Management Service. Customer gets complete control of how to authorize the use of the Google Cloud's External Key Manager keys.

Meet Compliance Requirements

Fortanix offers a FIPS 140-2 Level 3 certified Fortanix Runtime Encryption® Appliance, to store cloud keys on-premises enabling financial services, healthcare, and other regulated industries to meet their compliance requirements.

Unified Data Protection Platform

Fortanix delivers HSM, Key Management, Encryption and Tokenization for your hybrid and cloud native apps, all from a single integrated solution.

Simplified and Centralized Encryption

Fortanix with Google Cloud's External Key Manager provides a single, simple, and centralized encryption platform that accelerates moving applications to public cloud, while also providing a single set of cryptographic services to on-premises, hybrid, and cloud workloads.

Key Features

External Key Management

Encrypt data in the google cloud using encryption keys stored outside the cloud. Enforce access to data at rest for BigQuery and Compute Engine.

Control Full Key Lifecycle

Maintain full control and visibility into key creation, location, and distribution of cloud keys.

Secure Data in Use

Runtime Encryption® Technology plugin uses Intel® SGX Secure Enclave technology to protect data always.

FIPS 140-2 Level 3 Certified

Store and protect encryption keys on-premises with FIPS 140-2 Level 3 certified HSMs

Distributed and Scalable Architecture

Distributed architecture allows for key replication and scales depending on chang- ing requirements of the organization.

How Does Google Cloud's External Key Manager Work?

Services running on GCP, such as Big Query and GCE, currently can use an encryption key hosted by Google Cloud KMS or Cloud HSM to secure their data at rest. An envelope encryption scheme is followed where the data is encrypted using a local data encryption key (DEK), which in turn is encrypted using a key encryption key (KEK) in

Cloud KMS or Cloud HSM. Google allays the concerns of customers who don't want to trust the public cloud by extending the envelope encryption scheme to allow the KEK to be encrypted using an externally managed key encryption key (EKEK).