Written by Marco Attard
12 January 2017

Google adds the Key Management Service (KMS) to its Cloud Platform-- a means for enterprises to create, use, rotate and destroy AES-256 standard encryption keys on the cloud.

Cloud KMS is an alternative to the on-premise management of keys. As such it is ideal for customers moving more workloads on the cloud, and is an update on a more basic version of KMS for users wanting to supply own encryption keys.

"With Cloud KMS, you can manage symmetric encryption keys in a cloud-hosted solution, whether they're used to protect data stored in [Google Cloud Platform] or another environment," a company blog post announcing the service adds.

The service is directly integrated with Google Cloud Identity Access Management and Cloud Audit logging service, meaning organisations have more control over keys. It can store and manage millions of keys on the cloud, and users can set automatic key rotation at regular intervals and limit the scope of data accessible with a single key version, minimising exposure in case of security breach.

Cloud KMS is initially available in beta form in around 50 countries, with pricing based on the number of keys stored and frequency of keys used.

Go Google Cloud Key Management Service