CMEK compliance in Cloud Build

Cloud Build provides customer-managed encryption keys (CMEK) compliance (/kms/docs/cmek#cmek_compliance) by encrypting the build-time persistent disk (PD) with an ephemeral key that is generated for each build. No configuration is required. The key is uniquely generated for each build.

As soon as the build completes, the key is wiped from memory and destroyed. It is not stored anywhere, is not accessible to Google engineers or support staff, and cannot be restored. The data that was protected using such a key is permanently inaccessible.

How does the ephemeral key encryption work?

Cloud Build supports CMEK through the use of ephemeral keys, allowing it to be fully consistent and compatible with a CMEK-enabled setup.

Cloud Build does the following to ensure build-time PDs are encrypted with an ephemeral key:

1. Cloud Build mints a random 256-bit encryption key in local RAM for encrypting each built-time persistent disk.
2. Cloud Build leverages the Customer-Supplied Encryption Key (CSEK) feature of PD to use this new encryption key as a PD encryption key.
3. Immediately after starting the build, Cloud Build wipes the key it ephemerally generated for the build from local RAM. The key is never logged or written to any persistent storage and is now irretrievable.
4. When the build is completed, the persistent disk is deleted, at which point no traces of the key nor the encrypted PD data remain anywhere in Google infrastructure.

When does ephemeral key encryption not apply?

In the following scenarios, ephemeral key encryption does not apply:

- When you create or trigger a build using source mirroring (and not via GitHub app triggers), your source code is stored in Cloud Storage or Cloud Source Repositories. You have full control over the code storage location, including control over its encryption.

- When you specify your own bucket for Cloud Build build logs and supply an encrypted logs bucket, you must disable Stackdriver logging and then disable the Cloud Build log streaming option, as described in `BuildOptions` (/../cloud-build/docs/api/reference/rest/v1/projects.builds#buildoptions).
- When you trigger a build from the Cloud Build GitHub app, Cloud Build pulls your source code from GitHub, creates a storage bucket with a one-day object TTL, and deposits the code in that bucket. You have no access to or control over this bucket.
- When you reside in a geographic region affected by local restrictions on encryption, such as Brazil or India, Cloud Build cannot apply ephemeral key encryption to the PDs.

Last updated 2020-07-07 UTC.