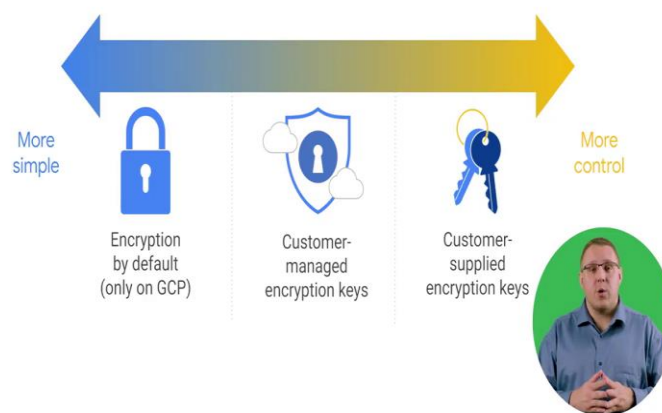


**Google Cloud Computing Foundation Course**  
**Seth Vargo**  
**Google Cloud**

**Lecture-46**  
**Explore encryption options**

**(Refer Slide Time: 00:05)**

Encryption options

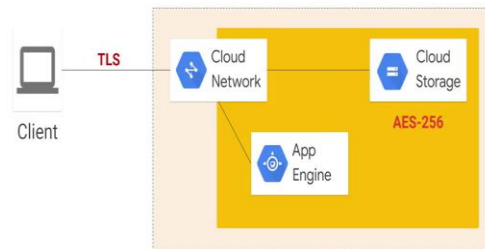


You will now explore the options that Google cloud offers for encrypting your data. There are several encryption options available on Google cloud. These range from simple but with limited to control to greater control and flexibility but with more complexity. The simplest option is GCP default encryption, followed by customer managed encryption keys or CMEK and then the option that provides the most control our customers supplied encryption keys or CSEK.

A fourth option is to encrypt the data locally before you store it in the cloud this is often called client-side encryption.

**(Refer Slide Time: 00:39)**

## Server-side encryption




By default GCP will encrypt data in transit and at rest. Data in transit is encrypted via TLS and data is encrypted at rest with an AES 256-bit key the encryption automatically happens.

**(Refer Slide Time: 00:54)**

### Customer-managed encryption keys (CMEK)

- Manage keys in a cloud-hosted solution
- Encrypt and decrypt via API
- Automated and at-will key rotation
- Symmetric and asymmetric key support



Cloud KMS


With customer managed encryption keys or CMEK you manage your own encryption keys that protect data on Google Cloud. Google clouds key management service or cloud KMS automates and simplifies the generation and management of encryption keys. The keys are managed by you the customer but the keys never leave Google Cloud. Cloud KMS supports encryption, decryption, signing and verifying of data.

It supports both symmetric and asymmetric cryptographic keys and a variety of popular algorithms. Cloud KMS allows you to both rotate keys manually and to automate the rotation of keys on a time-based interval. Cloud KMS also supports both symmetric and asymmetric keys for encryption and signing.

**(Refer Slide Time: 01:45)**

### Customer-supplied encryption keys (CSEK)

- ✓ Use your own AES-256 encryption keys with GCP services.
- ✓ Store the keys locally and provide them as part of GCP API calls.
- ✓ GCP uses the key in-memory and discards it immediately after use.



Customer supplied encryption keys or CSEK give you more control over your keys but with greater management complexity. With CSEK you use your own AES 256-bit encryption keys you are responsible for generating these keys. You are also responsible for storing these keys and providing them as part of your GCP API calls. Google Cloud will use the provided key to encrypt the data before persisting it. And we guarantee that the key only ever exists in memory and is immediately discarded after use.

**(Refer Slide Time: 02:19)**

## Customer-supplied encryption keys (CSEK)

- ✓ Use your own AES-256 encryption keys with GCP services.
- ✓ Store the keys locally and provide them as part of GCP API calls.
- ✓ GCP uses the key in-memory and discards it immediately after use.



Persistent disks such as those backing virtual machines can be encrypted with customer supplied encryption keys. With customer supplied encryption keys for persistent disks the data is encrypted before it leaves your virtual machine. But even without CSEK or CMEK your persistent disks are still encrypted with Google's default encryption. When a persistent disk is deleted the keys are discarded rendering the data irrecoverable by traditional means.

**(Refer Slide Time: 02:48)**

## Other persistent disk encryption options



For even more control over persistent disk encryption you can create your own persistent disks and redundantly encrypt them.

**(Refer Slide Time: 02:58)**

Other encryption options



Client-side encryption



And finally client-side encryption is always an option with client-side encryption you encrypt data before sending it to Google Cloud. Neither the unencrypted data nor the decryption keys ever leave your local device.