Google Discussions

Exam Professional Cloud Security Engineer All Questions

View all questions & answers for the Professional Cloud Security Engineer exam

Go to Exam

EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 318 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 318
Topic #: 1
[All Professional Cloud Security Engineer Questions]

Your organization must store highly sensitive data within Google Cloud. You need to design a solution that provides the strongest level of security and control. What should you do?

A. Use Cloud Storage with customer-supplied encryption keys (CSEK), VPC Service Controls for network isolation, and Cloud DLP for data inspection.

B. Use Cloud Storage with customer-managed encryption keys (CMEK), Cloud DLP for data classification, and Secret Manager for storing API access tokens.

C. Use Cloud Storage with client-side encryption, Cloud KMS for key management, and Cloud HSM for cryptographic operations.

D. Use Cloud Storage with server-side encryption, BigQuery with column-level encryption, and IAM roles for access control.

Show Suggested Answer

by abdelrahman89 at *Oct. 25, 2024, 1:59 a.m.*

Comments

Type your comment...

Submit

YourFriendlyNeighborhoodSpider 4 months, 1 week ago

Selected Answer: B

HSM is only for regulatory purpose and Client-side encryption won't provide highest security. Do not for a second think it's C, when you have B as an option.
Why Option B is Correct?
Cloud Storage with CMEK:
CMEK (Customer-Managed Encryption Keys) allows you to manage your own encryption keys, providing you with full control over your data encryption at rest.
It ensures that Google Cloud can store and process your data, but the encryption keys remain under your control, enhancing security.

Cloud DLP (Data Loss Prevention):
Cloud DLP helps you inspect, classify, and redact sensitive data, such as personally identifiable information (PII), before it's stored or processed. This is crucial for compliance and risk management.

Secret Manager:
Secret Manager is a service for securely storing API keys, passwords, certificates, and other sensitive data.
By using Secret Manager, you ensure that access tokens and secrets are encrypted and controlled with IAM access policies, further increasing the security posture.

upvoted 1 times

KLei 7 months, 1 week ago

Selected Answer: C

A more suitable option would involve using Cloud HSMs in conjunction with other strong security measures such as CMEKs and Cloud DLP.

upvoted 1 times

MoAk 8 months ago

Selected Answer: C

Highly Secure etc = HSM

upvoted 1 times

vamgcp 8 months ago

Selected Answer: C

Client-Side Encryption: Encrypting data before it leaves your control ensures that even if someone gains access to your Cloud Storage bucket, they cannot decrypt the data without the encryption keys. This provides an extra layer of protection against unauthorized access or data breaches.
Cloud KMS: Cloud KMS provides a secure and managed service for generating and storing your encryption keys.1 You can control key access with granular IAM permissions and audit all key operations.
Cloud HSM: Cloud HSM takes key security to the next level by using dedicated, tamper-resistant hardware security modules (HSMs) to generate and protect your keys. This offers the highest level of protection against key compromise.

upvoted 2 times

abdelrahman89 9 months, 1 week ago

Selected Answer: C

Answer C

upvoted 2 times