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 104 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 104

Topic #: 1

[All Professional Cloud Security Engineer Questions]

You are a security engineer at a finance company. Your organization plans to store data on Google Cloud, but your leadership team is worried about the security of their highly sensitive data. Specifically, your company is concerned about internal Google employees' ability to access your company's data on Google Cloud.

What solution should you propose?

A. Use customer-managed encryption keys.

B. Use Google's Identity and Access Management (IAM) service to manage access controls on Google Cloud.

C. Enable Admin activity logs to monitor access to resources.

D. Enable Access Transparency logs with Access Approval requests for Google employees.

Show Suggested Answer

by jitu028 at *Oct. 3, 2022, 11:30 a.m.*

Comments

Type your comment...

Submit

⊟ Sammydp202020 Highly Voted 👍 1 year, 5 months ago

Selected Answer: D

D

https://cloud.google.com/access-transparency
https://cloud.google.com/cloud-provider-access-management/access-transparency/docs/overview

upvoted 5 times

zellck Highly Voted 1 year, 9 months ago

Selected Answer: D

D is the answer

upvoted 5 times

Xoxoo Most Recent 10 months, 2 weeks ago

Selected Answer: D

To address your organization’s concerns about the security of highly sensitive data stored on Google Cloud, you can propose the following solution:

D. Enable Access Transparency logs with Access Approval requests for Google employees. This solution provides an additional layer of control and visibility over your cloud provider by enabling you to monitor and audit the actions taken by Google personnel when accessing your content. Access Transparency logs capture the actions performed by Google Cloud administrators, allowing you to maintain an audit trail and verify cloud provider access. Access Approval requests allow you to approve or dismiss requests for access by Google employees working to support your service. By combining these features, you can gain greater oversight and control over your sensitive data on Google Cloud.

Please note that this is a high-level recommendation, and it is important to evaluate your specific requirements and consult the official Google Cloud documentation for detailed implementation guidance.

upvoted 3 times

passex 1 year, 7 months ago

Answer D - but, for "highly sensitive data" CMEK seems to be reasonable option but much easiest way is to use Transparency Logs

upvoted 1 times

PATILDXB 1 year, 7 months ago

B is the correct answer. IAM Privileges provide fine grain controls based on the users function

upvoted 1 times

Littleivy 1 year, 8 months ago

Selected Answer: A

Use customer-managed key to encrypt data by yourself

upvoted 2 times

Littleivy 1 year, 8 months ago

D should be the answer on second thought

upvoted 2 times

AzureDP900 1 year, 8 months ago

D is correct

upvoted 3 times

jitu028 1 year, 9 months ago

Answer is D

https://cloud.google.com/access-transparency
Access approval
Explicitly approve access to your data or configurations on Google Cloud. Access Approval requests, when combined with Access Transparency logs, can be used to audit an end-to-end chain from support ticket to access request to approval, to eventual access.

upvoted 4 times

Platform

- Home
- Examtopics PRO
- All Exams
- Training Courses