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 309 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 309
Topic #: 1
[All Professional Cloud Security Engineer Questions]

Your development team is launching a new application. The new application has a microservices architecture on Compute Engine instances and serverless components, including Cloud Functions. This application will process financial transactions that require temporary, highly sensitive data in memory. You need to secure data in use during computations with a focus on minimizing the risk of unauthorized access to memory for this financial application. What should you do?

A. Enable Confidential VM instances for Compute Engine, and ensure that relevant Cloud Functions can leverage hardware-based memory isolation.

B. Use data masking and tokenization techniques on sensitive financial data fields throughout the application and the application's data processing workflows.

C. Use the Cloud Data Loss Prevention (Cloud DLP) API to scan and mask sensitive data before feeding the data into any compute environment.

D. Store all sensitive data during processing in Cloud Storage by using customer-managed encryption keys (CMEK), and set strict bucket-level permissions.

Show Suggested Answer

by abdelrahman89 at *Oct. 4, 2024, 10:20 p.m.*

Comments

Type your comment...

Submit

json4u 9 months, 2 weeks ago

Selected Answer: A

It's A.
Well explained in abdelrahman89's comment.

upvoted 1 times

abdelrahman89 9 months, 3 weeks ago

A - Confidential VMs: Using Confidential VMs provides a strong security boundary around the memory of the VM instances, protecting sensitive data from unauthorized access, even if the VM is compromised.
Hardware-Based Memory Isolation: Leveraging hardware-based memory isolation ensures that the data within the VM's memory is protected by hardware-enforced mechanisms, making it significantly more difficult for attackers to access.
Comprehensive Protection: This approach provides a comprehensive solution for securing data in use, as it combines both software-based (Confidential VMs) and hardware-based (memory isolation) protections.

upvoted 2 times

nah99 8 months ago

I would think A, but how do Cloud Functions leverage hardware-based memory isolation?

is this you or chatgpt speaking

upvoted 1 times