Google Discussions



## EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 79 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 79
Topic #: 1
[All Professional Cloud Security Engineer Questions]

An organization's security and risk management teams are concerned about where their responsibility lies for certain production workloads they are running in
Google Cloud and where Google's responsibility lies. They are mostly running workloads using Google Cloud's platform-as-a-Service (PaaS) offerings, including
App Engine primarily.
Which area in the technology stack should they focus on as their primary responsibility when using App Engine?

A. Configuring and monitoring VPC Flow Logs

B. Defending against XSS and SQLi attacks

C. Managing the latest updates and security patches for the Guest OS

D. Encrypting all stored data

Show Suggested Answer

by [deleted] at *Sept. 7, 2022, 7:14 a.m.*

### Comments

Type your comment...

Submit

**Random_Mane** Highly Voted 2 years, 10 months ago

Selected Answer: B

B. in PaaS the customer is responsible for web app security, deployment, usage, access policy, and content.
https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate

upvoted 7 times

**BPzen** Most Recent 8 months ago

Selected Answer: B

Why B. Defending against XSS and SQLi attacks is Correct:
Application-Layer Security:

When using PaaS offerings, developers are responsible for writing secure application code. This includes preventing application vulnerabilities like XSS, SQL injection, and insecure input validation.

upvoted 1 times

**madcloud32** 1 year, 4 months ago

Selected Answer: B

B is correct. Defense of App Engine and Application Security.

upvoted 1 times

**gcpengineer** 2 years, 2 months ago

Selected Answer: B

B is the ans.

upvoted 2 times

**AzureDP900** 2 years, 8 months ago

B is correct

upvoted 2 times

**AwesomeGCP** 2 years, 9 months ago

Selected Answer: B

B. Defending against XSS and SQLi attacks
Data at rest is encrypted by default by Google. So D is wrong. Should be B.

upvoted 4 times

**koko2314** 2 years, 10 months ago

Answer should be D. For SAAS solutions web based attacks are managed by Google. We just need to take care of the data as per the link below.

upvoted 1 times

**desertlotus1211** 1 year, 11 months ago

read the question again... it's not D

upvoted 1 times

**GHOST1985** 2 years, 10 months ago

Selected Answer: D

Answer is D

upvoted 1 times

**GHOST1985** 2 years, 9 months ago

In PaaS, we're responsible for more controls than in IaaS, including network controls. You share responsibility with us for application-level controls and IAM management. You remain responsible for your data security and client protection.
https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate#defined_by_workloads

upvoted 2 times

**gcpengineer** 2 years, 2 months ago

IaaS need more controls thn PaaS

upvoted 1 times

**tifo16** 2 years, 7 months ago

Data at rest is encrypted by default by Google. So D is wrong. As mentioned by your link it Should be B.

upvoted 1 times

**[Removed]** 2 years, 10 months ago

Selected Answer: B

B it is.

upvoted 3 times