Symantec

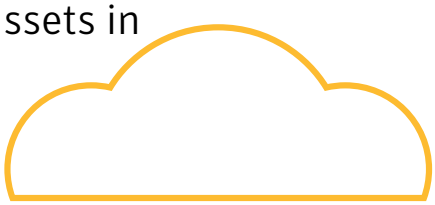
Now Who Protects What?

Do you understand public cloud shared responsibility concepts well enough to stay out of the cloud failure trap? Take our brief quiz and find out.

		Choose One
01	Your public cloud provider allows you to block IPs and ports. Is your personally identifiable information (PII) and other sensitive information adequately protected?	YES // NO
02	You're on an Infrastructure-as-a-Service (IaaS) platform. The cloud provider is going to take care of keeping the OS security patches up-to-date. Right?	YES // NO
03	You've just started using containers. In that case, should you manage the security for the host or application?	YES // NO
04	Your credentials to your cloud provider have been compromised. Is your cloud provider responsible for detecting suspicious activity within your accounts and for resolving this situation?	YES // NO
05	You're storing sensitive data in the cloud and just discovered that some of it is publicly accessible. Is the cloud provider responsible for notifying you?	YES // NO
06	You use the default settings provided by your cloud provider. That means your cloud environment is securely configured, right?	YES // NO
07	One of your users has been making a number of changes to the security settings for your infrastructure in the public cloud. Both the frequency of requests and the types of changes are unusual. Who is responsible for investigating this behavior?	ACCOUNT OWNER // CLOUD PROVIDER

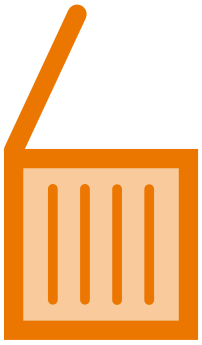
SHARED RESPONSIBILITY QUIZ LEARNINGS

Q1: **NO.** The cloud provider only provides security for access to the cloud environment. You are still responsible for protecting assets in that environment.

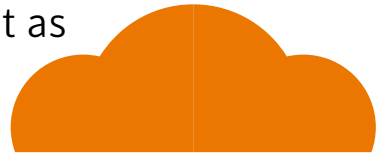


Q2: **NO.** OS patches and other application controls are the responsibility of the customer/account owner.

Q3: **YES.** Depending on the service, you may still be responsible for the host and you always want security for the application regardless of using containers.



Q4: **NO.** Your cloud provider is only responsible for protecting the platform and not your account. Your organization is most likely responsible. Securing and monitoring your control plane is just as important as protecting the rest of your infrastructure.



Q5: **NO.** Your cloud provider may give you tools to secure your data, but it's ultimately up to the account owner to take action.

Q6: **NO.** Don't assume the default configurations are adequate/ appropriate. You are responsible for actively checking and managing your cloud resource configurations.

Q7: **The Account Owner.** Although the cloud provide can monitor account changes, only you know if these changes were authorized or not.

Learn More: go.symantec.com/cwp