

What is the key difference between traditional virtualization and cloud?

Hypervisors

Commercial virtualization software

Orchestration

Abstraction

Which of the following is **not** a key potential benefit of cloud computing:

Agility

Resiliency

Compliance

Economics

What business benefit(s) was Amazon attempting realize when they created their internal cloud computing program? Select all that apply.

Faster time deploy developer resources

Build a world-class public cloud computing platform

Better match real-time capacity fluctuating demand

Beat Microsoft

Resource pools permanently assign resources ta user.

True

False

Cloud computing supports scaling up of required resources, but not scaling down.

True

False

**Which of the following appear in both the NIST and ISO/IEC cloud computing definitions?
Check all**

Services scaling out and scaling in quickly are an example of which essential characteristic of cloud.

Resource Pooling

On-Demand Self Service

Rapid Elasticity

Measured Service

Broad Network Access

Which of the following is not an emergent property of resource pooling?

Governance

Isolation

Segmentation

Broad Network Access

Which service model would a cloud database be considered?

Storage as a Service

Platform as a Service

Software as a Service

Infrastructure as a Service

Software as a Service is always built on top of Platform as a Service which is always built on Infrastructure as a Service.

True

False

Which of the following is most likely to be considered IaaS:

OA container registry

OA cloud message queue

The cloud's management console

OA virtual machine

In laas , individual virtual machines use which kind of storage?

VSTOR-based hardware

OA database platform

The local hard drives on the servers

Virtual volumes from a storage pool

Platform as a Service abstracts application platforms and platform components from underlying resources, and can be built on top of

IaaS.

True

False

Which of the following is not required to be considered SaaS?

Underlying physical hardware

Customer management of the underlying resources

The essential characteristics

A complete application

If an organization uses a Community Cloud Deployment Model, some portion of the physical infrastructure MUST be on-premises with one of the community members.

True

False

If an organization employs the technique of cloud bursting, which cloud deployment model are they utilizing?

Proprietary

Multi-Tenancy

PaaS

Hybrid

Which element of the logical model describes the cloud management plane?

Infostructure

Infrastructure

Applistructure

Metastructure

In which service model does the cloud consumer have the least amount of control over security?

Infrastructure as a Service

Platform as a Service

Security as a Service

Software as a Service

In which cloud service model is the cloud consumer responsible for ensuring that the hypervisor is not vulnerable to attack?

Software as a Service

Infrastructure as a Service

Platform as a Service

None of the above

When should you define the security controls when building a cloud deployment?

Before determining the service and deployment models

Before selecting the provider

After identifying control gaps

After identifying requirements

Cloud infrastructure security does not include the virtualization components:

False

True

Which of the following resource pools is not associated with IaaS:

Storage

Network

Middleware

Compute

Which of the following are typically in the underlying infrastructure of a cloud? (click all that apply)

Database

Message queue

API server

Hypervisors

Identity service

Why is hardening infrastructure components so important?

Clouds are sometimes based on common components that may contain vulnerabilities.

All security is important

Infrastructure components are most likely to be exposed to cloud consumers

This prevents the cloud provider from accessing cloud consumer data

Which of the following physical networks is used for Internet to instance traffic?

Storage

Management

Virtual

Service

Why should cloud providers use multiple underlying physical networks? (select all that apply)

Cost management

Resiliency

Better performance

Better isolation

Which virtual network technology is best suited for cloud?

SDN

VLAN

Token Ring

V-flow

Virtual networks:

Are more flexible, but more difficult to secure

Take fewer resources

Substitute for physical networks

May include inherent security capabilities

Which is a defining characteristic of Software Defined Networks

Uses OpenFlow

Decouples the control plane from the underlying physical network

Leverages packet tagging

Autoscaling for resiliency

Which SDN security capability often replaces the need for a physical or virtual appliance?

Default deny

Lack of support for packet sniffing

Security groups

Integrated isolation

The most effective way for an attacker to compromise a security group is to compromise the host/virtual machine and then modify the rules.

True

False

Which of the following is the most effective security barrier to contain blast radius?

Cloud account/project/subscription

Virtual subnet (with or without ACLs)

Virtual network

Security group

How does a virtual network affect network visibility?

An SDN can provide more visibility than a physical network

Virtual machines on the same physical host don't use the physical network

Virtual networks block packet capture for better isolation

Virtual networks always encrypt traffic and break packet capturing

Place the following network security tools in the preferred order in most cloud deployments, from 1 (most preferred) to 4



Place the following network security tools in the preferred order in most cloud deployments, from 1 (most preferred) to 4.

1 Inherent cloud controls

2 Host security agents

3 Virtual appliance

4 Physical appliance

What is the purpose of a bastion network/transit VPC?

To better support multiple virtual networks and accounts in hybrid scenarios

To better lock down a hybrid cloud

To create a cloud DMZ

To improve internal routing and IP address space availability

Which of the following is primarily a responsibility of the cloud provider?

Configuring security groups

Securing the underlying virtualization technology**

Correct configuration in the management plane

Designing subnets, virtual networks, and ACLs

Of the following, which is the most important use case for the Software Defined Perimeter?

To secure hybrid networks

To encrypt SDN traffic

For federated network identity

To improve and secure remote access

Which of the following are cloud workloads? Select all that apply:

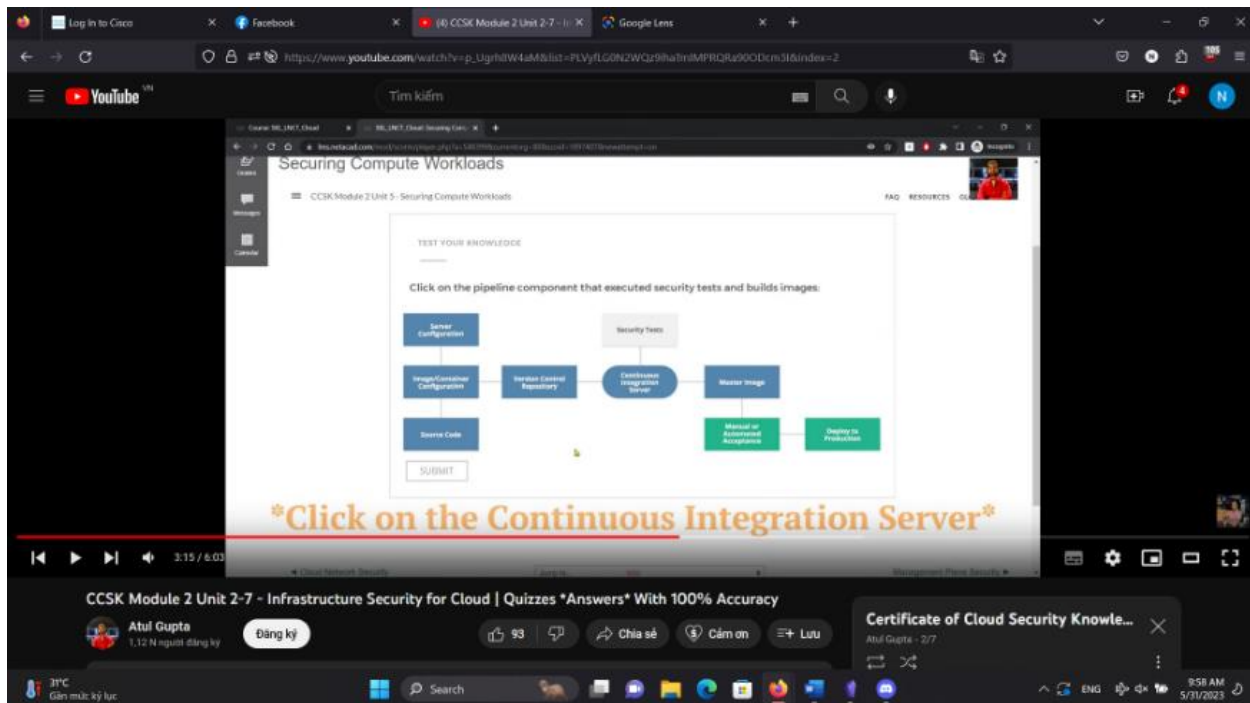
Host servers

Containers

Virtual machines

Serverless/Function as a Service

Click on the pipeline component that executed security tests and builds images:



Which of the following most controls when applied to cloud impacts traditional workload security deployments?

Hypervisors

Serverless

Low resiliency

Security groups

High volatility/rates of change

How can immutable workloads improve security?

They eliminate error-prone manual management

They scale for DDOS

They better meet performance requirements

They better support use of traditional security tools

Select the cloud workload security option that can most improve overall security and reduce attack surface:

Select cloud aware host security agents

Use immutable as much as possible

Store logs external to instances

Leverage existing/traditional vulnerability assessment tools

Which of the following is primarily a cloud consumer workload security responsibility?

Underlying infrastructure security

Hypervisor security

Volatile memory security

Monitoring and logging

Why is management plane security so critical?

Compromise of the management plane potentially compromises all cloud assets

REST APIs are inherently insecure.

It is the primary integration point for hybrid cloud.

It is the best way for cloud consumers to protect themselves from hostile cloud provider employees.

Select the best option for authenticating to a cloud API

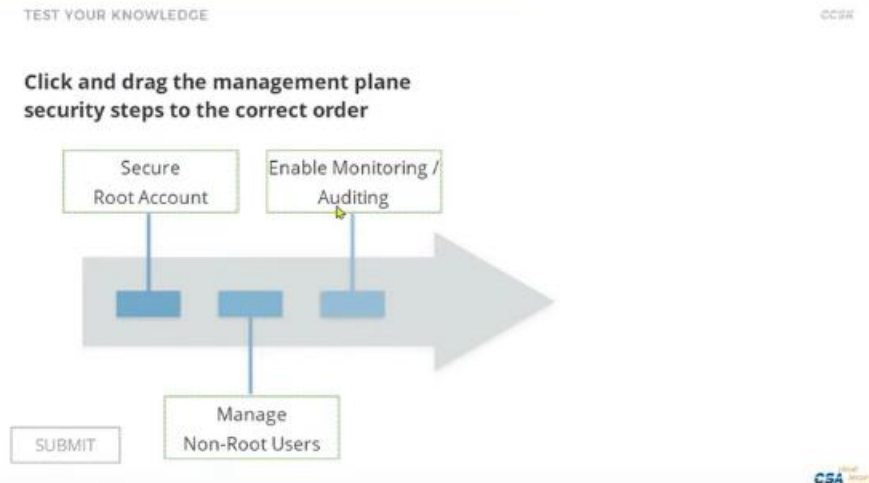
HTTP request signing

Username/password

Biometrics

TLS-MA

Click and drag the management plane security steps to the correct order



Multi factor authentication is the single most important management plane security control.

True

False

Identify one drawback to managing users in the management plane:

Insufficient MFA support

The reliance on RBAC

High variability between cloud providers

Lack of SSO support

What is the role of a service administrator?

To administer cloud platform/management plane users.

To isolate application security

To administer a limited set of cloud services

They are the core administrators for a cloud account

Select the best option for management plane monitoring, when it is available:

Inherent cloud auditing, since it captures the most activity

Inherent cloud auditing, since that offloads responsibility to the cloud provider

Proxy-based auditing, since it eliminates the need to trust the cloud provider

Proxy-based auditing, since it captures more activity

What is the single most important rule for cloud BC/DR?

Use object storage for backups

Snapshot regularly

Use multiple cloud providers

Architect for failure

Which is not a key aspect of cloud BC/DR?

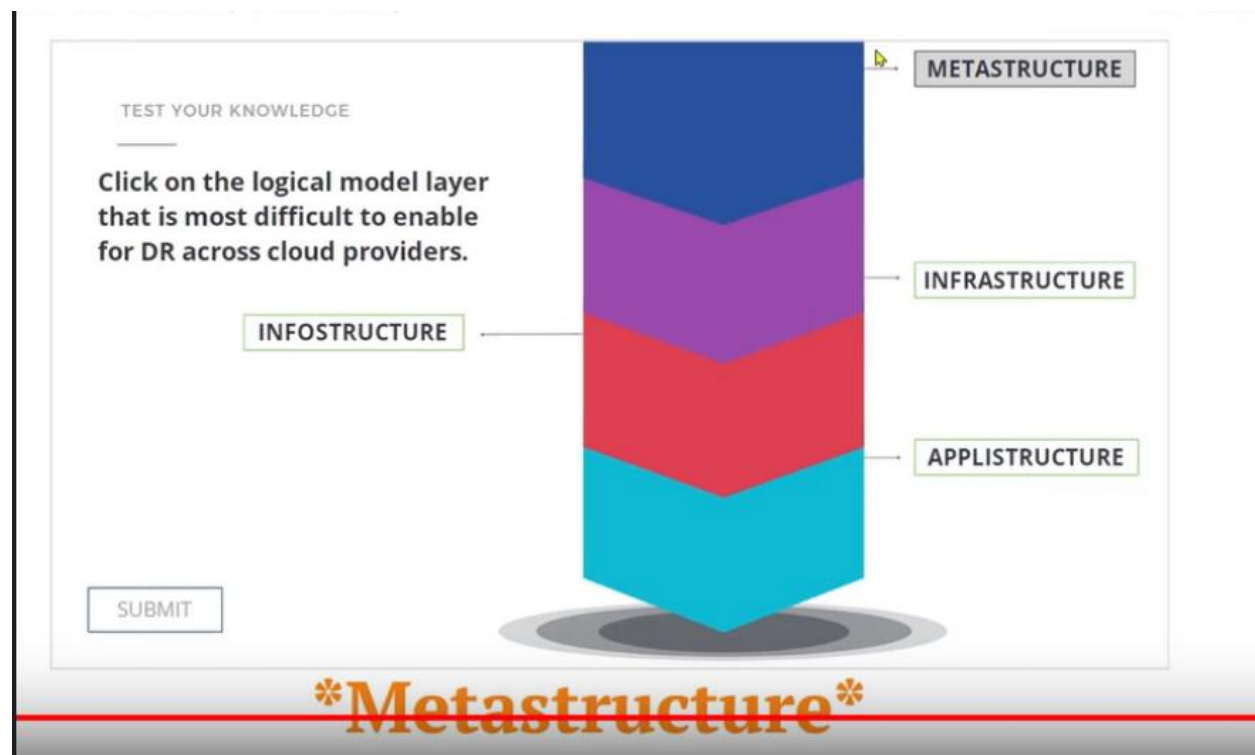
Continuity within the provider/platform

Hypervisor resiliency

Portability

Preparing for provider outages

Click on the logical model layer that is most difficult to enable for DR across cloud providers.



Select a technique to manage continuity within the cloud provider.

Data portability

Multi-cloud provider plans

Hybrid cloud backup

Cross-location/region design

Select the governance tool that is most affected by the transition to cloud computing:

Mission statement

Compliance reporting

Board of director reporting

Chart of accounts

In terms of cloud computing and security... what is the primary governance role of a contract?

Regulatory requirements

Defines how you extend internal controls to the cloud provider

Cost management

To define the data custodian

Does the shared responsibilities model define the contract or the contract define the shared responsibilities model?

The shared responsibilities model defines the contract

The contract defines the shared responsibilities model

What is the responsibility of information risk management?

Align risk management to the tolerance of the data owner

O Manage overall risk to the organization

Determine the overall risk of cloud providers

Eliminate all risks to information assets

Your risk assessment effort should be equal for all information assets

True

False

In which service model does the cloud consumer have to rely most on what is in the contract and documented to enforce and manage security?

PaaS

Hybrid

IaaS

SaaS

Under which conditions is managing risk similar for public and private cloud?

No conditions; public cloud is always riskier

The risk profiles are always the same

When your private cloud is third party hosted and managed

When using a major public cloud provider

What is critical when evaluating a cloud service within your risk management program?

Ensuring the provider's security program supports your existing on-premise tools

Accounting for the context of the information assets involved

Minimizing regional harm

Eliminating all outsourcing risk

How can you manage risk if you can't negotiate a contract with the cloud provider?

Use compensating controls and your own risk mitigation mechanisms

Always choose a different provider

Obtain cyberinsurance

Accept all potential risks

Audits are only used to meet government regulatory requirements.

True

False

Cloud changes compliance. Select the statement that is incorrect:

There may be a greater reliance on third party audits

The cloud provider is ultimately responsible for their customer's compliance

There are large variations between the compliance capabilities of different cloud providers

Metastructure/management may span jurisdictions even if data is localized

Which is *not* a source of compliance obligations?

Contracts

Internal Audits

Legislation

Industry Standards

Compliance inheritance means that an application built on top of a cloud provider's service that is compliant with a regulation/standard is always guaranteed to be compliant.

True

False

The Cloud Security Alliance Security Guidance provides:

Legal Guidance

Information you should discuss with your attorneys.

Legal Recommendation

Legal Advice

The Australian Privacy Act of 1988 can apply to Australian customers, even if the cloud service provider is based elsewhere:

True

False

What is the purpose of a data localization law?

To require that data about the country's citizens be stored in the country

To require service providers to register with the country's data protection commission

To require company to hire only local workers

To require that all business documents be in the country's official language

Which of the following is correct?:

GDPR Stands for "Government Data Privacy Rule".

GDPR Establishes fines of \$1,000 per credit card number compromised

GDPR prohibits the transfer of personal data outside the EU or EEA to a country that does not offer a similar privacy rights

GDPR requires that EU member state's national laws impose network requirements on operators of essential services

The Federal Government in the United States does not directly address issues of data privacy, but instead leave it up to the states to create laws that address privacy concerns:

True

False

If a business is located outside the European Union it does not have to comply with the privacy laws of the European Union

True

False

In the United States, only entities that collect or process financial data or health data must comply with privacy or security laws

True

False

Which of the following is a standard?

APPI
COPPA
PCI DSS
GDPR

When selecting a cloud provider, if a provider won't negotiate a contract:

Always choose another provider

Read the contract carefully, and consult with your advisors, to evaluate the terms and understand the potential risks.

Always trust the provider

Contracts are not enforceable in cloud due to the wide range of jurisdictions

Cloud consumers are ultimately responsible for understanding the legal implications of using a particular cloud provider and service.

True

False

A contract with a cloud service provider can fulfill all of the following except one

Clarify what happens when the service is terminated

Clarify whether metadata can be reused for secondary purposes

Clarify the price for the service

Define the minimum security measures taken by the cloud provider

Prevent a breach of security

If you own the data, it is still possible for your CSP to own the metadata:

True

False

Why do cloud providers typically limit their customers' ability to directly assess and inspect their facilities and services?

They are worried customers will find vulnerabilities and they will lose business

Cost management

On-site inspections can be a security risk, and remote assessments are hard to distinguish from real attacks

Do deter paying out bug bounties

Audit scopes for any given standard, like an SSAE16 are always consistent.

True

False

Select all the following sources that are considered artifacts of compliance

Activity reports

System configuration details

Log files

Change management details

Should you assess or review the audits of a cloud provider more or less frequently than traditional outsourcers?

More

Less

Which CSA tool maps cloud security control specifications to architectural relevance?

STARWatch

Cloud Controls Matrix

The Security, Trust and Assurance Registry (STAR)

Consensus Assessment Initiative Questionnaire

You are a cloud provider and struggling to respond to a large amount of highly variable customer RFP requests for security controls documentation. Which CSA document could you instead complete and send to customers:

Cloud Controls Matrix

STARWatch

The Security, Trust and Assurance Registry (STAR)

Consensus Assessment Initiative Questionnaire

Where can cloud providers publish their CAIQ and other security/compliance documents to help cloud prospects and customers assess the provider's current security posture?

The Security, Trust and Assurance Registry (STAR)

The AWS marketplace

The United States Federal Register of Cloud Providers

Google

Which CSA tool allows you to quickly search a providers assessment for controls that map to regulations you care about and see the responses to those controls?

CCM

CAIQ

STAR

STARWatch

The CSA Cloud Controls Matrix v3.0.1 maps control specifications to FedRAMP High Impact Level.

True

False

The CSA Cloud Controls Matrix v3.0.1 contains how many control specifications?

57

16

133

295

All cloud data is eventually stored on a physical device, like a hard drive.

True

False

Which of the following cloud data storage types can be described as "a database for files":

Object storage

Database storage

Volume storage

Platform storag

Why dwe use data dispersion in cloud computing?

Timprove resiliency by eliminating the need for physical drives

Timprove security by obviating the need for encryption

Time prove resiliency in case of individual drive failure

Timprove security by reducing the chances a complete file can be stolen

Which security tool can help detect sensitive data migrating the cloud?

Data security proxies (DSP)

Firewalls

Data Loss Prevention (DLP)

IPS

Which of the available CASB modes is most cloud-native but often not supported by smaller, especially SaaS, providers:

O API

Inline (cloud)

Inline (local)

Cloud-integrated

Which is the preferred model of protecting data migrating the cloud:

Encryption proxies, because they are the most efficient

Encrypting network connections, since you can't trust file encryption

Encrypting files, since you can't trust network encryption

All are equally effective

How does cloud complicate access controls as compared traditional data storage?

There is difference; they are not more complicated

Cloud storage may offer more options, such as sharing privileges or access the data's metadata

Cloud access controls are less reliable

All providers must support the same access controls, which makes building the cloud more Complex

In a Cloud Computing Environment, what is always your most significant security control?

Encryption controls.

Access controls

Provider-specific controls

Management controls

Select the 3 components of an encryption system.

Protocol

Encryption engine

Key

Data

In "externally managed" encryption, which is the key component that should be kept externally time prove security:

Key management

Data

Encryption Engine

Application code

Instance managed encryption is:

Your preferred option for volume encryption

An example of what not do

Which of the following options encrypts data before you transfer it object storage:

Externally managed encryption

Application encryption

Server-side encryption

Client-side encryption

Select all *potential* options for encrypting data in PaaS, if they are supported by the platform:

Database

Application-level (in your own code)

Provider-integrated

Volume storage

When using provider managed encryption, you are always sharing the same keys with other tenants.

True

False

Proxy-encryption requires you break any existing secure connection your cloud provider:

True

False

In the diagram below, what area shows the greatest reduction in attack surface?

Network attack paths

The cloud provider

The data center

Application logic attacks

For cloud, where is DLP often best integrated?

Secure Web Gateway

NGFW

The cloud virtual network/VPC

CASB

What is the primary goal of data masking?

Stop hackers

Generate test data that still resembles production data

Hide production data from employees

Turn test data back into production data

Logs of some events in a cloud environment may not be available to you depending on your choice of cloud provider.

False

True

Which is the most inherently secure key management option, but it may not be viable or even needed depending on your project requirements and platform/provider support:

Virtual Appliance

Third-Party Service

Cloud Provider Service

HSM/Appliance

The considered Bring Your Own Key (BYOK) the provider must not be able to ever see or manage your keys:

False

True

Which key management option should you select if you are dealing with highly sensitive data that you don't want your provider potentially access under any circumstances:

Virtual appliance

BYOK

3rd party key management service

HSM/hybrid

Which option allows you to use an existing build for key management without replicating everything in the cloud?

Third-party Service

Hybrid

Virtual Appliance

HSM/Appliance

How should the data security lifecycle be used?

create granular documentation for all sensitive data in the cloud.

create granular documentation for all data, sensitive or not, in the cloud.

replace existing data security architectures.

As a lightweight tool better understand data flow and potential vs. desired data usage.

Why do we map locations and access?

know when force users use a VPN

replace data flow diagrams

understand where data flows, in what phases, and how it might be accessed (e.g. devices)

find the security boundary between internal and external

What is the primary objective of mapping functions, actors, and locations?

list all potential security controls

Replace data flow diagrams

determine what's possible vs. what should be allowed

document information risk

What we use reduce what is possible what should be allowed within the context of the lifecycle?

Entitlement matrix

CASB or DLP

Key management

Security controls

When moving to cloud, what now becomes within the scope of application security unlike with traditional infrastructure?

Management Plane

SAST

Source code

Architecture

STRIDE is a common thread modeling framework. Which of the four categories does a cloud provider typically take more responsibility to manage:

Information disclosure

Spoofing

Denial of service

Privilege escalation

What is one example of a control that can reduce the potential of spoofing:

Encryption

Authentication

Audit logging

Authorization

Specific testing techniques are tightly aligned and should only be performed during their designated phase in the secure software development process:

True

False

Which kind of test should be added to static analysis for cloud deployments?

Regression tests

API resiliency

Code completion

Scanning for stored cloud credentials

Which kind of testing will most likely require permission from your cloud provider before performing?

Vulnerability assessment

Security unit tests

SAST

Composition analysis

Which vulnerability analysis option will always comply with the terms of service of the cloud provider, but may require paying close attention to network architecture:

Penetration testing

Traditional network-based

Host based

Deployment pipeline testing

While there are many definitions of DevOps, one technology/process is typically considered to be central to any DevOps program. Which technology is that?

Continuous integration

Configuration management

Composition management

Static analysis

Identify the core security benefit of immutable:

It fully isolates operations from production environments

It fully isolates developers from production environment

All security updates are automatically applied

There are no manual changes, so everything is consistent and administrative access can be disabled.

Which of the following are security benefits of DevOps?

Greater Standardization

Automated Testing

Improved Security Operations

Improved Auditing

Which of the following is not a new concern of secure operations for applications in the cloud?

WAF limitations/differences

The cloud configuration

SAST

The management plane

Which of the following is an inherent architectural security advantage of cloud?

The management plane

Segregation

Containers

12 factor applications

How can serverless improve security?

Through automation

Some attack surface is the responsibility of the cloud provider in the shared responsibilities model

Better visibility due to the management plane

Serverless actually reduces security

Many of the new architectural options for cloud offer security benefits over what is possible in traditional infrastructure:

True

False

What could an email address be considered?

Entity

Identifier

Identity

Authorization

What is the technical definition of authentication?

Allowing a user to perform an action

The process of confirming an identity

Providing a user access to a resource

The process of validating an entity

What is the defining characteristic of federated identity?

It's supports government identity management

It allows a user to manage multiple identities for a single system

It can manage an identity within a given application

It inserts an identity across different systems or organizations

Which of the following is a discrete type that will have an identity? Examples include users and organizations.

Persona

Attributes

Entity

Role

What is the biggest difference between IAM in cloud and in traditional environments?

IAM Must span at least two organizational boundaries

Cloud is more secure

They use different standards

Cloud is less secure

Which IAM standard is best suited for enterprises federating with cloud providers?

SAML

XACML

Kerberos

OATH

Which of the following is one of the 3 most common identity standards in cloud environments?

SCIM

OATH

Kerberos

XACML

In a hub and spoke model, which technology mediates between directory servers/identity providers and the service providers/relying parties:

Federated identity brokers

Attribute services

CASB

Directory servers

Which of the following IAM security incidents is more likely in cloud versus traditional infrastructure and requires a dedicated incident response focus?

Account takeover

Account abuse

Privilege escalation

Pass the hash

Multifactor authentication is absolutely mandatory for cloud computing due to the higher potential for remote account takeovers.

True

False

Checking to see if a user authenticated with MFA from a corporate IP address to authorize an action is an example of?

Multifactor authorization

Authentication

Role-based access controls

Attribute based access controls

What is an entitlement matrix used for?

To document authorizations

To communicate security controls to a cloud provider

To map the directory servers to the appropriate cloud provider

To translate physical security controls to cloud controls

Why are elasticity and infrastructure templating critical IaaS security capabilities?

They improve scalability

They optimize performance

These are operational capabilities, not security capabilities

They enable immutable deployments.

Which of the following protocols should a SaaS provider support to help extend an enterprise's existing user management security controls and is considered a critical security capability?

AuthZ

LDAP

SAML

IPv6

Why are reviewable audits important when evaluating a cloud provider?

Third party auditors provide better results than internal auditors

They will meet all regulatory and compliance standards

They fill the gaps in any cloud provider security documentation

They provide third party validation when you cannot audit a provider yourself

Frequent audits and assessments are important when looking at a cloud provider due to how rapidly they evolved their services

True

False

Select all of the following characteristics that are required for something to be considered Security as a Service:

It has a hosted web interface

It meets the NIST essential characteristics

It is built on a IaaS provider

It is a security product or service delivered as a cloud service

It is marketed as SecaaS

Which of the following is one of the more unique potential benefits of Security as a Service:

Transparency

Compliance

Customer visibility

Intelligence Sharing

Why are regulation differences a potential concern of using Security as a Service?

The cloud consumer may have regulatory obligations the SecaaS provider can't meet

SecaaS is unregulated

SecaaS is highly regulated

The cloud provider may have regulatory obligations the customer can't meet

Using SecaaS removes accountability for the client, but only for the particular security control the service addresses.

True

False

What characteristic would make a Federated Identity Broker be considered SECaaS vs. a traditional tool?

It supports SAML

It supports multiple cloud providers AND on premise directories

It brokers authentication to cloud services

It is hosted in the cloud, elastic, and you pay per user

What is a potential advantage of a web security gateway SECaaS over an on-premise tool?

Supports HTTPS

They are always less expensive

It will generally catch more malware

You can protect mobile users without requiring a VPN to the corporate network

What is required to redirect traffic to a cloud WAF?

An on-premise proxy

GRE tunneling

A VPN

DNS changes

Can a cloud-based key management service be integrated with on- premise encryption?

No

Yes

If an attacker compromises one of your virtual machines, and then uses it to attack other clients on the same cloud platform, what is the cloud provider's likely action?

The CSP will prioritize defending the rest of your deployment from the attack.


The CSP will first protect the rest of their broader clients, which may mean disrupting your deployment

The CSP will prioritize alerting you and providing information needed for you to respond to the attack.

The CSP has no responsibility in this situation per the shared responsibilities model.

Click and drag the incident response phases in the proper order.

TEST YOUR KNOWLEDGE

 Click and drag the incident response phases in the proper order.

- 1 Preparation
- 2 Detection and analysis
- 3 Containment, eradication, recovery
- 4 Post-mortem

SUBMIT

In which phase would you build a cloud "jump kit" of tools and code to speed a response?

Detection and analysis

Containment and response

Postmortem

Preparation

In which phase would you snapshot a virtual machine for forensics?

Preparation

Detection and analysis

Postmortem

Containment and response

Which of the following most helps you quickly build parallel infrastructure, so that you can rapidly restore operations while still having the compromised environment for analysis?

Snapshots

Infrastructure as code templates

PaaS

SaaS

In a postmortem what would be your highest priority to review and remediate if it was a blocker in your incident response?

Operating system vulnerabilities

Internal communications

Communications with the cloud provider

Container vulnerabilities

Which of the following is not considered a related technology?

Mobile Computing

Internet of Things

Serverless

Security as a Service

Big Data is often defined as "high volume, high velocity, and high variety". What does "high velocity" mean?

Fast raw storage speeds

Storage elasticity

Fast transfer speeds

The data changes constantly/rapidly

Why should you consider relying extensively on the isolation capabilities of cloud to defend a big data deployment?

The distributed storage is always isolated by nature

Big data platforms tend to have low inherent security

Isolation improves encryption

To meet compliance requirements

While not directly related to cloud, which IoT principle is critical for long-term security?

Data encryption

The ability to patch/update the "things" (devices)

Elasticity

Public APIs

Which of the following issues on a mobile device can actually create security risks for the cloud deployment?

Insecure wireless networks

Embedded/static/stored credentials

A malicious app

Use of an out of date operating system

Serverless, used properly, can offer more security benefits than risks.

True

False