Intro to Cloud Security

Show Split View | Cloud Details | Awards | Help

Learn fundamental concepts regarding securing a cloud environment.

Chart | Scoreboard | Discuss | Writeups | More

Difficulty: Easy

Active Machine Information

Loading... *Loading...* *Loading...* *Loading...*

17%

Task 1 Introduction

Task 2 Architectural Concepts of Cloud

Characteristics of Cloud

A few years back, no one could even imagine that organisations would place their data and operations on a geographically miles away platform that unknown people would manage. However, cloud computing is becoming so popular that organisations of every type and size use it for different purposes, such as storing data, taking backups, disaster recovery and Business Continuity Operations (BCO). It is becoming popular due to the following characteristics:

- **Scalability**: In cloud computing, organisations only buy resources at a time. Instead, they buy upon the need. Also, resources can be scaled up or down as per business needs and requirements.
- **Simplicity**: Renowned cloud service providers believe in simple design & interface. Usually, the customer only needs to buy and use the cloud services with little configuration.
- **Cost Effective**: Cloud computing allows us to pay for our services. The cost is reduced as a third party provides infrastructure and does not need to be purchased at once.
- **Enhance Automation**: Cloud computing services require limited human administration, so companies can focus more on their goals without worrying about managing and maintaining systems.

Models of Cloud Computing

The following three cloud computing models are based on what the cloud provider offers and the needs of customers/organisations.

Infrastructure as a Service (IaaS)

In IaaS, infrastructure is provided by cloud providers. The customer has complete control of operating systems, services and applications.

- Cloud Provider's Responsibility: Maintaining and providing data centres with racks, machines, cables, and utilities.
- Customer's Responsibility: In this case, the customer manages logical resources like software and operating system.

Platform as a Service (PaaS)

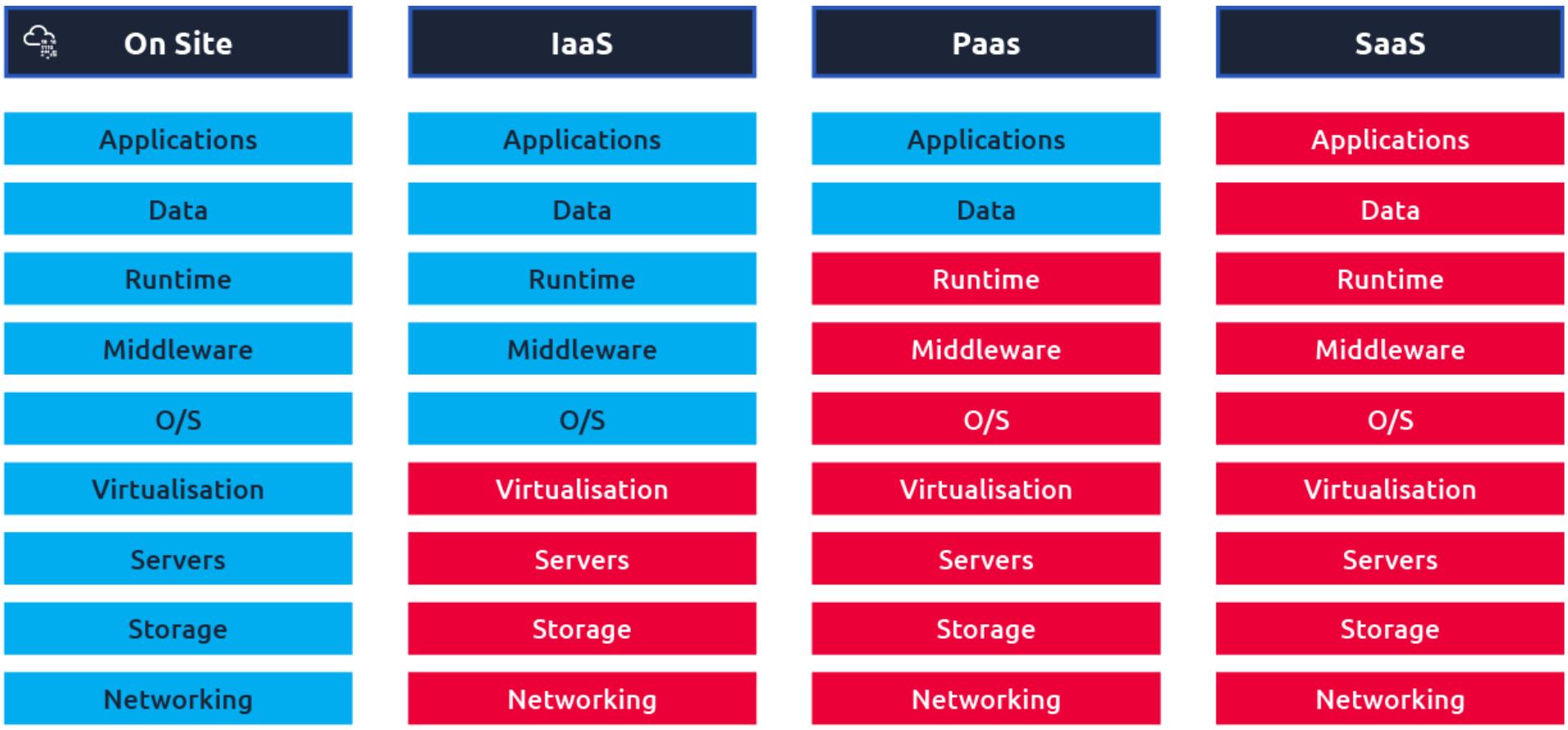
It contains all services offered in IaaS with the addition of an operating system (the user manages that in IaaS).

- Cloud Providers' Responsibility: In Platform as a Service, a cloud provider offers infrastructure and platform. Customers can choose any platform as per their needs. The service provider is responsible for managing the infrastructure and platform.
- Customer's Responsibility: Customers can install software as per their requirements.

Software as a Service (SaaS)

It includes every service that is being provided in IaaS and PaaS.

- Cloud Providers' Responsibility: In SaaS, everything is managed by the cloud provider, including infrastructure, OS and software.
- Customer Responsibility: This model is used by customers who need more technical skills in managing things. They only pay and use the services without worrying about the underlying architecture.



Cloud Deployment Models

Public Cloud

In the public cloud, as the name suggests, resources provided by cloud providers are shared among multiple customers. **Organisation A** will use resources from the same hardware that offers services to any other organisation. For example, Microsoft Azure and Amazon Web Services (AWS) are examples of public clouds. However, they also offer Virtual Private Cloud (VPC) services.

Private Cloud

In the private cloud, customers will not share the underlying resources (hardware and software) as in the public cloud, and resources are dedicated to a single customer. **Organisation A** will get a Virtual machine hosted on a system specifically dedicated to a particular customer.

Hybrid Cloud

It is a combination of a public and private cloud. For example, **Organisation A** might want to use some private cloud resources (to host confidential data of the production system) but also want some public cloud (for testing of the applications/software) so that the production system does not crash during testing.

Important Terminologies

There are some essential terminologies of cloud computing that one needs to understand. Some of the concepts are defined below:

- **Virtualisation:** Virtualisation is the primary technology used in cloud computing that allows sharing of instances of an application or resources among multiple customers or users simultaneously.
- **Compute:** Defined as the processing power customers require to run their applications and systems for data processing and carry out different tasks. In cloud computing, customers can get computing power from a combination of virtual machines hosted in the cloud environment.
- **Storage:** In cloud computing, we do not need to buy and maintain physical hard drives; instead, our data is stored in logical pools of physical storage on cloud provider premises, and we can scale up and scale down the resources as per needs.
- **Networking:** As cloud computing is a system of computers/processes that are interconnected, maintaining a high-speed network connection is very important. The cloud provider is responsible for providing network connectivity to meet customer needs without disruption.

Answer the questions below

In Infrastructure as a Service, what will be deployed by the vendor (Hardware or Software)?

hardware — Correct Answer

What is the type of cloud dedicated to a single customer called?

private — Correct Answer

Task 3 ○ Cloud Security Concepts

Task 4 ○ Cloud Security Risks Concerning Deployment Models

Task 5 ○ Security Through Access Management

Task 6 ○ Security Through Policies

Task 7 ○ Security Through Network Management

Task 8 ○ Security Through Storage Management

Task 9 ○ Cloud Security - Some Additional Concepts

Task 10 ○ Conclusion