

# Cloud Concepts, Architecture and Design for CCSP®

---

## CLOUD CONCEPTS AND ARCHITECTURE



**Kevin Henry**

CISM CISSP CCSP

[kevin@kmhenrymanagement.com](mailto:kevin@kmhenrymanagement.com)



# CCSP Certification Examination

Domains	Weights
1. Cloud Concepts, Architecture and Design	17%
2. Cloud Data Security	20%
3. Cloud Platform and Infrastructure Security	17%
4. Cloud Application Security	17%
5. Cloud Security Operations	16%
6. Legal, Risk and Compliance	13%



# Cloud Concepts, Architecture, and Design

## Agenda



**Cloud Concepts and Architecture**

**Principles of Secure Cloud Computing**

**Evaluating Cloud Providers**



# Cloud Concepts and Architecture

---



# Understanding the Cloud



Historical



Future



# Cloud Computing (ISO/IEC)

Paradigm for enabling network access to a shared and elastic pool of shareable physical or virtual resources with self-provisioning and administration on-demand



# Cloud Computing (NIST)



Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

# The Problems with Definitions



It is important to understand, however, that the term "cloud computing" encompasses a variety of systems and technologies as well as service and deployment models, and business models. A number of claims that are sometimes made about cloud computing, e.g., that it "scales," or that it converts capital expenses to operational expenses, are only true for some kinds of cloud systems.

# Cloud Deployment Models

---



# NIST Cloud Deployment Model

This cloud model is composed of five essential characteristics, three service models, and four deployment models.

**NIST SP800-145**



# Essential Characteristics of the Cloud



**On-demand self-service**

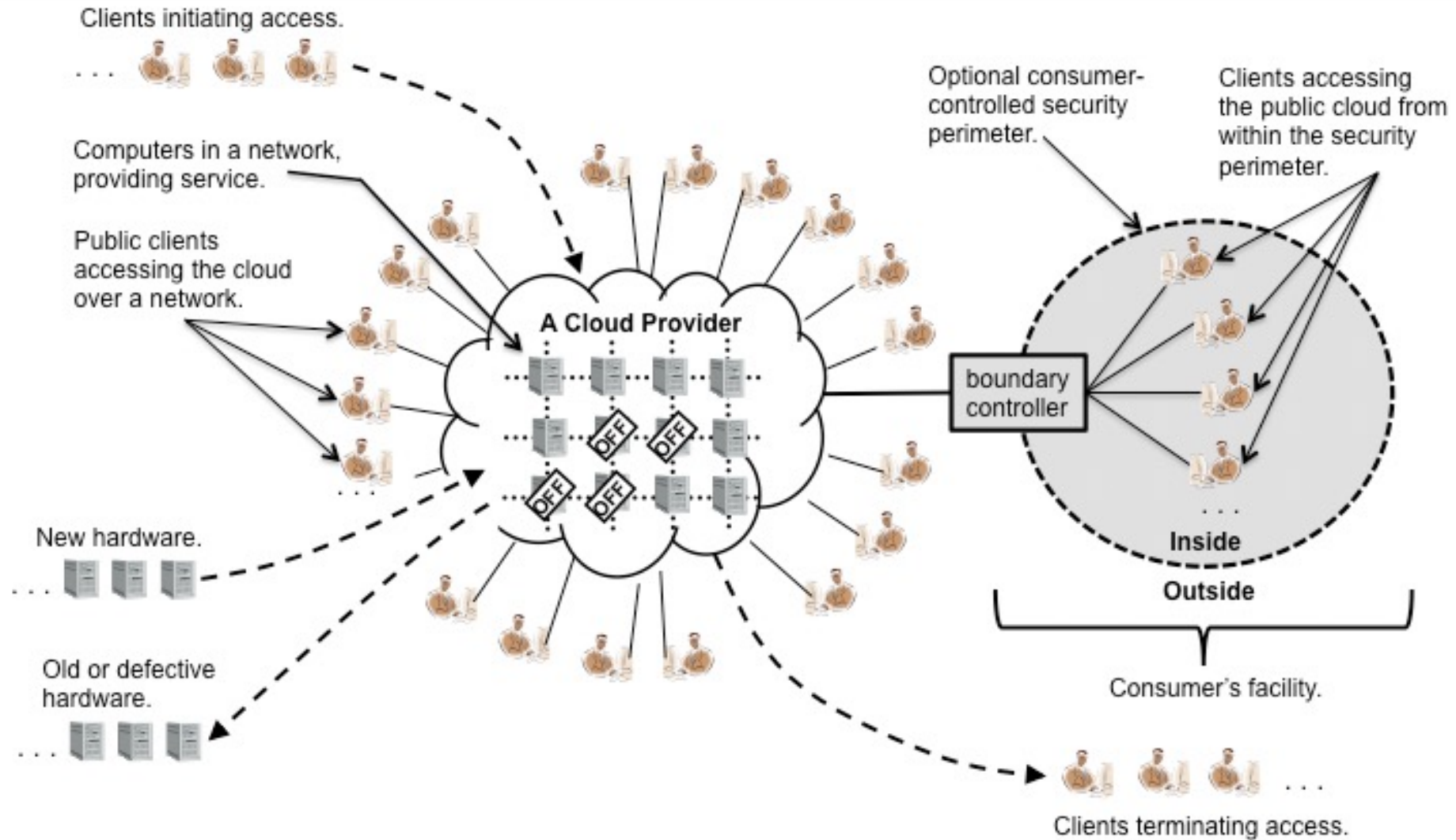
**Broad network access**

**Resource pooling**

**Rapid elasticity**

**Measured service**

# Public Cloud



# Service Models



Cloud Software as a  
Service (SaaS)



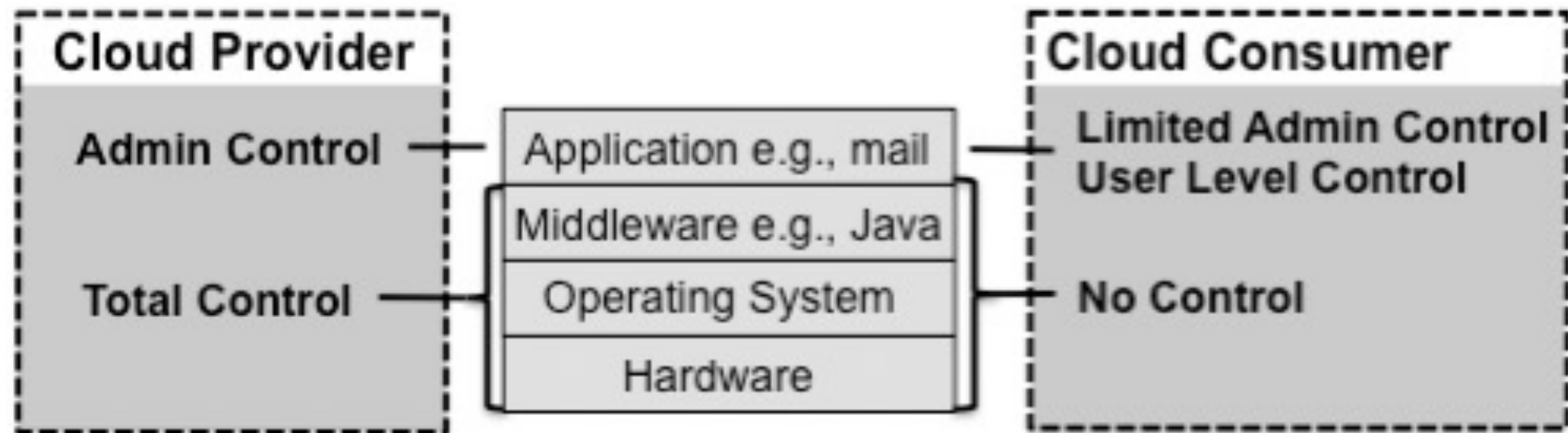
Cloud Platform as a  
Service (PaaS)



Cloud Infrastructure as  
a Service (IaaS)



# SaaS Architecture and Control



# Deployment Models



Private Cloud



Community  
Cloud



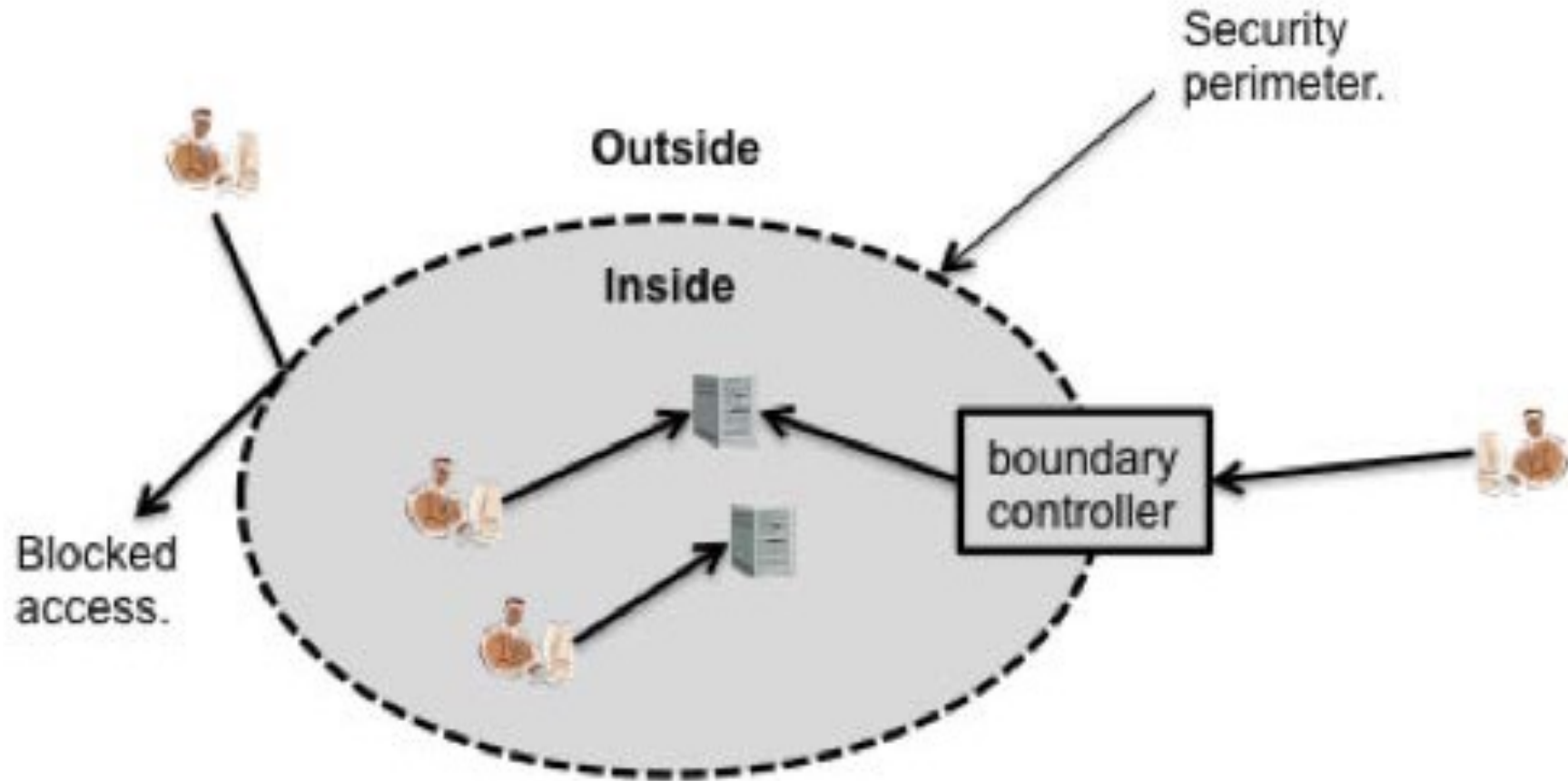
Public Cloud



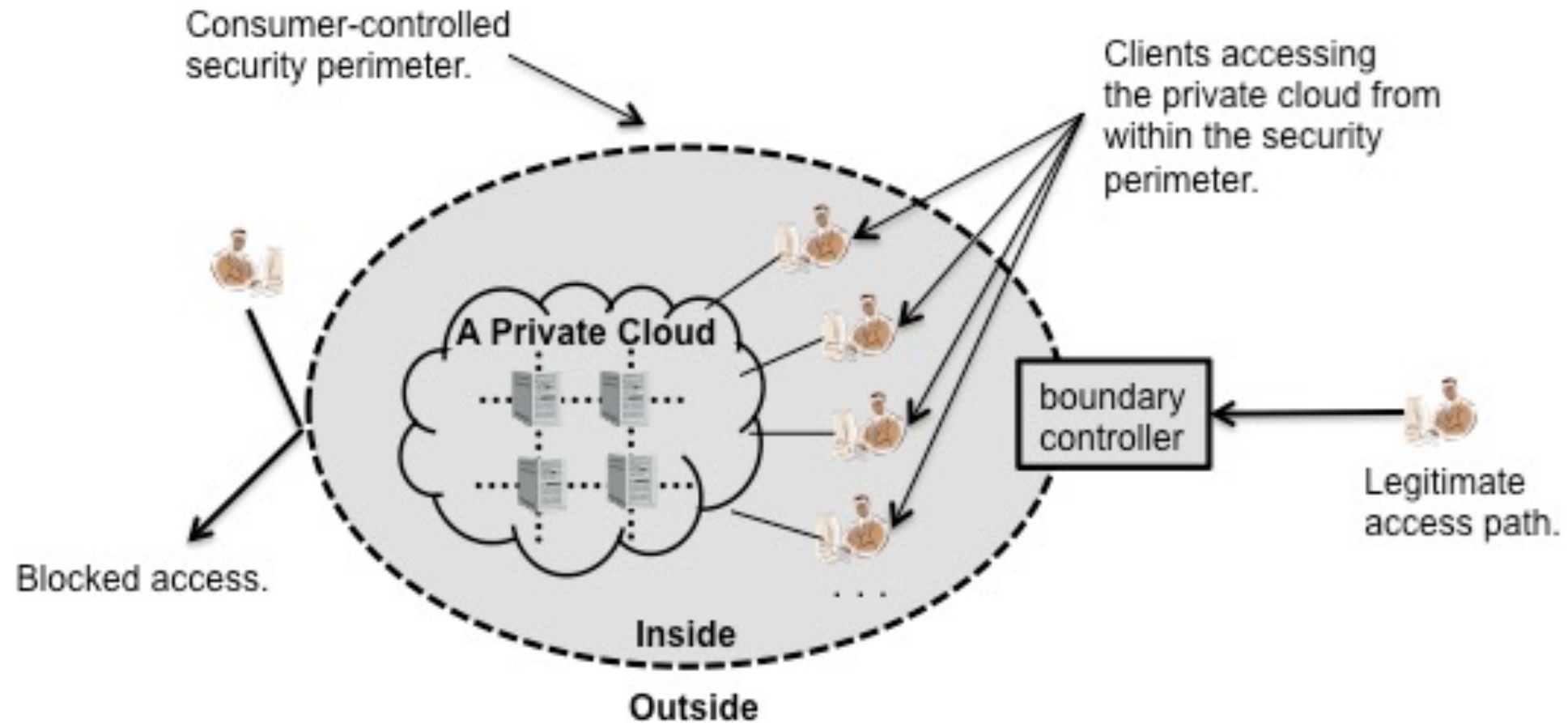
Hybrid Cloud



# The Security Perimeter



# On-site Private Cloud



# Cloud Roles Overview



## Cloud consumer or customer

- Note that many parts of this course have the perspective of the cloud consumer, not the cloud service provider

## Client or User

## Cloud provider

## Carrier



# Key Points Review



The term Cloud Computing may be used in many ways – and is based on the way that cloud providers define their services and that cloud customers use those services.

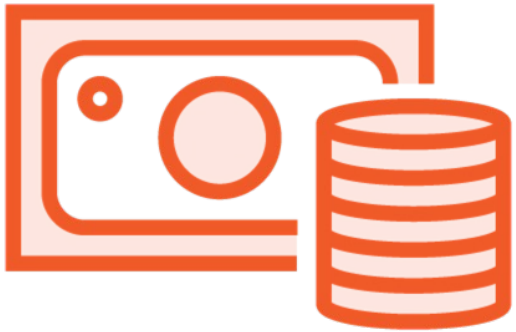


# Why Choose Cloud Computing?

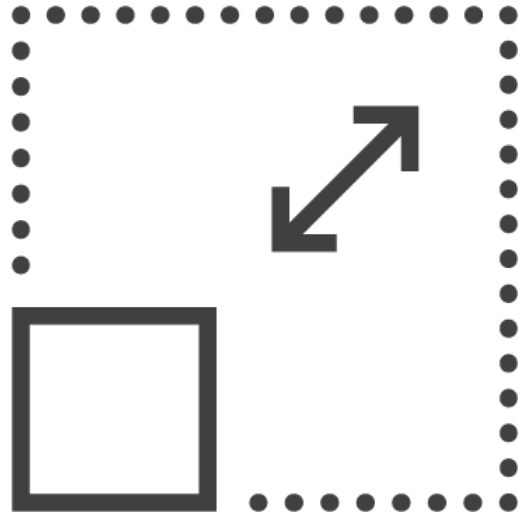
---



# Benefits of Cloud Computing



Capital cost  
control



Flexibility

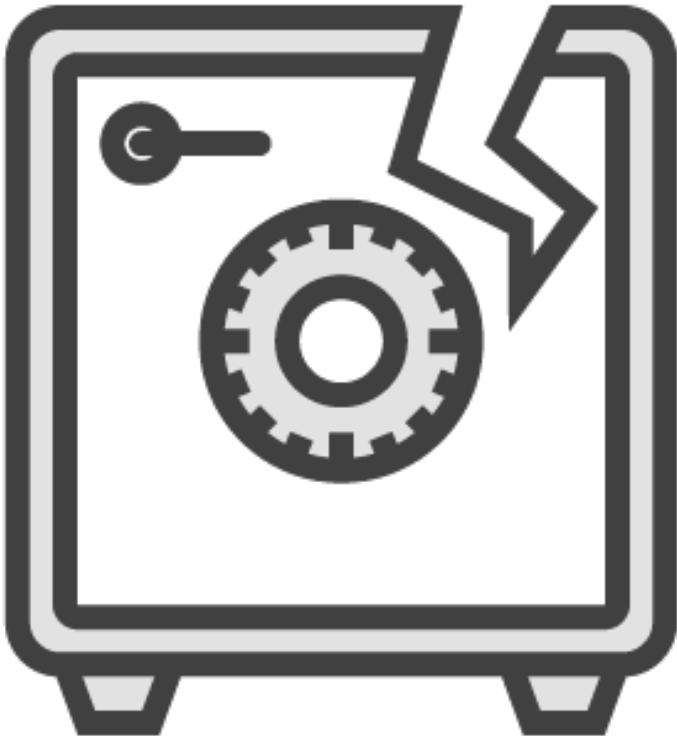


Access to skilled  
staff



Environmental  
impact

# Is the Cloud (More) Secure?



## **Tough question:**

- It depends
  - Maturity of the organization
  - Maturity of the Cloud Service Provider
    - Services stipulated in contract

# Laws and Regulations



**Placing data on the cloud requires consideration of applicable laws and regulations**



# The Business Case

**The Cloud is not the ideal solution for every business or for some types of services:**



**Real-time sensors**



**Highly sensitive data**

**This course will examine this in more detail later**



# Migrating to the Cloud



## Considerations before choosing to migrate to the cloud:

- The type of business
- Legal requirements – uptime, reporting
- Options available
  - Delivery models
  - Cost

# Understanding the Business



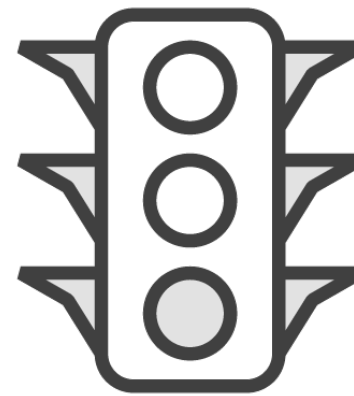
Type



Location



Customers



Network  
requirements  
Traffic volumes



Storage and  
processing  
needs



# Building the Cloud

---



# Building the Cloud



**The Cloud is based on many components working together:**

- Software
  - Applications
  - APIs, Drivers and Utilities
  - Operating Systems
  - Hypervisors
  - DBMS
- Hardware
  - Compute
  - Storage
- Networks

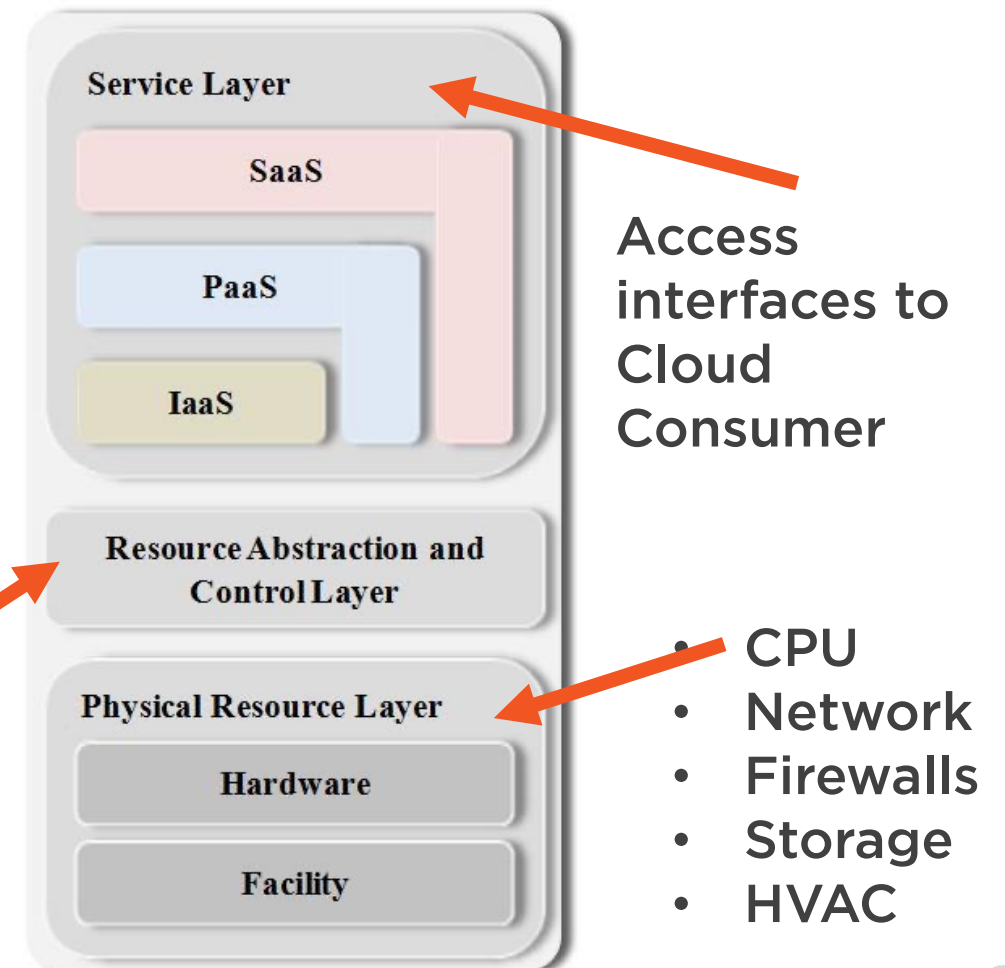


# Service Orchestration

Arrangement, coordination and management of system components.

Used by the Cloud Provider to provide services to the Cloud Consumer

Used by Service Provider to manage system components:  
Hypervisor  
Virtual machines



# Terms Used in the Cloud



**Portability**

**Vendor lock-in**

**Cloud migration**

**Cloud backup**

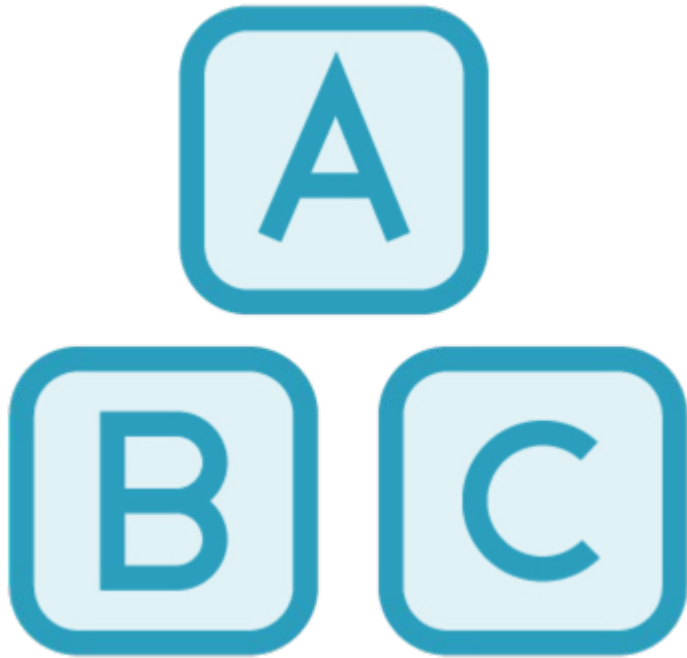
**Hypervisor**

**Virtual machines**

**Containers**



# Building Blocks of the Cloud



## Facilities

- Power, HVAC, physical access

## Hardware

## Operating systems

## Hypervisor

## Network

## APIs

## Applications

## Data

## Users



# Well-Architected Framework



**Operational excellence**

**Security**

**Reliability**

**Performance efficiency**

**Cost optimization**

**Sustainability**

<https://docs.aws.amazon.com/wellarchitected/latest/framework/welcome.html>



# Key Points Review



**In many cases, businesses are already using more cloud-based services than they are aware of.**

**Migrating more services to the Cloud is an excellent option for many organizations – but not all.**



# Cloud Computing Roles

---



# Roles and Responsibilities

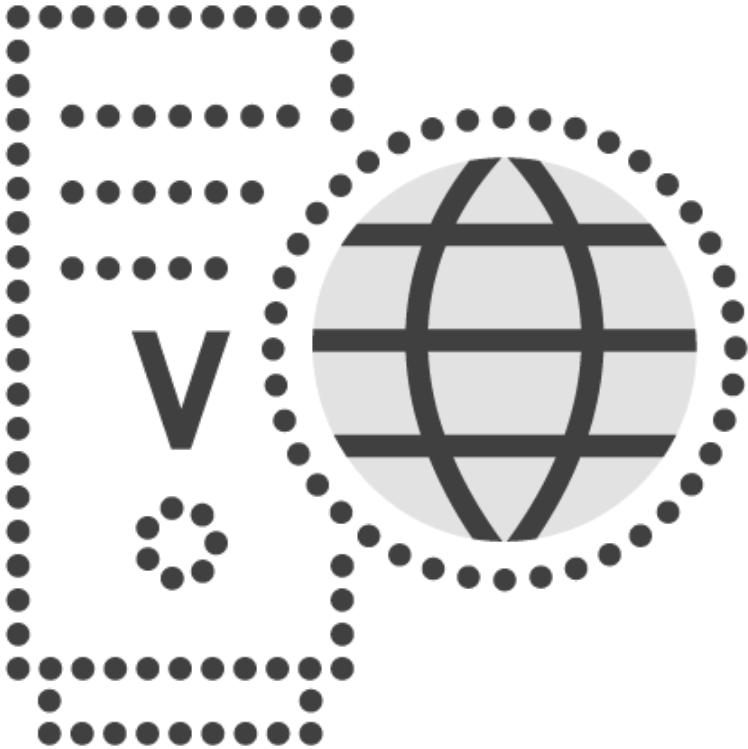


**Accountability can only be established through assigning roles to individuals**

**Each person assigned a role must:**

- Understand the requirements of the role
- Execute their tasks in a responsible manner

# Cloud-based Roles



**Roles and responsibilities become more complex when there are responsibilities shared and divided between different entities**

# Cloud Service Provider



Sells Cloud services to customers  
Various deployments and service models



Purchases and maintains:

- Equipment
- Access control
- Network
- Facilities (buildings)
- Power
- HVAC



Manages staffing



# Cloud Customer



**An individual or organization that consumes cloud services**

- May be a cloud provider as well!
  - PaaS versus SaaS
- Cloud services may be free or at a contracted price

# Cloud Carrier



**Provides network access**



**Redundancy**

- **Diverse routing**



**Bandwidth**



# Cloud Broker



**Manages relationships between cloud customers and service providers**

- Negotiate contracts
- May represent several CSPs

**Reseller – resells services of a CSP**



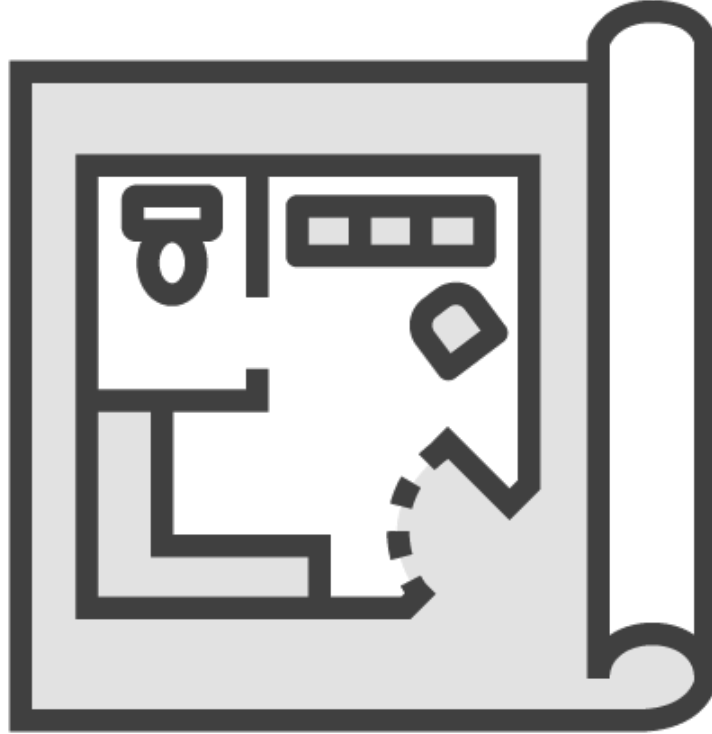
# Cloud Access Security Broker



## CASB

- Monitors cloud usage
- Allows IT to 'see' what cloud services are being used
- May manage the relationship between the cloud service provider and the cloud consumer
- May manage access controls

# Cloud Architect



**Specialist that designs cloud implementations and ensures that business requirements are met**



# Cloud Auditors and Regulators



**Provide independent assessment of cloud providers**

- STAR
- SSAE 18/20
- ISAE 3402
- FISMA

# Shared Security Responsibilities

## Responsibility Zones

Responsibility	SaaS	PaaS	IaaS	On-prem	
Data governance & rights management	Customer	Customer	Customer	Customer	Always retained by customer
Client endpoints	Customer	Customer	Customer	Customer	
Account & access management	Customer	Customer	Customer	Customer	
Identity & directory infrastructure	CSP	CSP	Customer	Customer	Varies by Service Type
Application	CSP	CSP	Customer	Customer	
Network controls	CSP	CSP	Customer	Customer	
Operating system	CSP	CSP	Customer	Customer	
Physical hosts	CSP	CSP	CSP	Customer	Transfers to Cloud Provider
Physical network	CSP	CSP	CSP	Customer	
Physical data center	CSP	CSP	CSP	Customer	
	CSP	CSP	CSP	Customer	



# Key Points Review



**It is only possible to establish accountability and responsibility when roles are clearly defined.**

**This is even more important when several different organizations are involved**



# Cloud Essential Characteristics

---



# Broad Network Access

Network based connection between cloud consumer and cloud service provider



Internet  
(cloud)



Redundancy  
*Maybe?*



Capacity



Support  
many types  
of end point  
devices



# On-demand Self-Service



**Ability of cloud consumer to obtain compute, processing, storage and network services automatically without requiring interaction with cloud provider staff**

# Resource Pooling



## Multi-tenant model

- Pooled resources
  - Equipment
  - Staff
  - Network
  - Memory

## Private (off-site)

- Pooled infrastructure
- Staff

# Rapid Elasticity



**Ability of the consumer to provision and release service capabilities automatically according to demand**

- Cloud bursting
  - Private cloud onto public cloud

# Measured Service



**The cloud consumer pays for the resources consumed**

- Billing and monitoring
- Does not really apply to private cloud

# Cloud Deployments

---



# Cloud Deployment

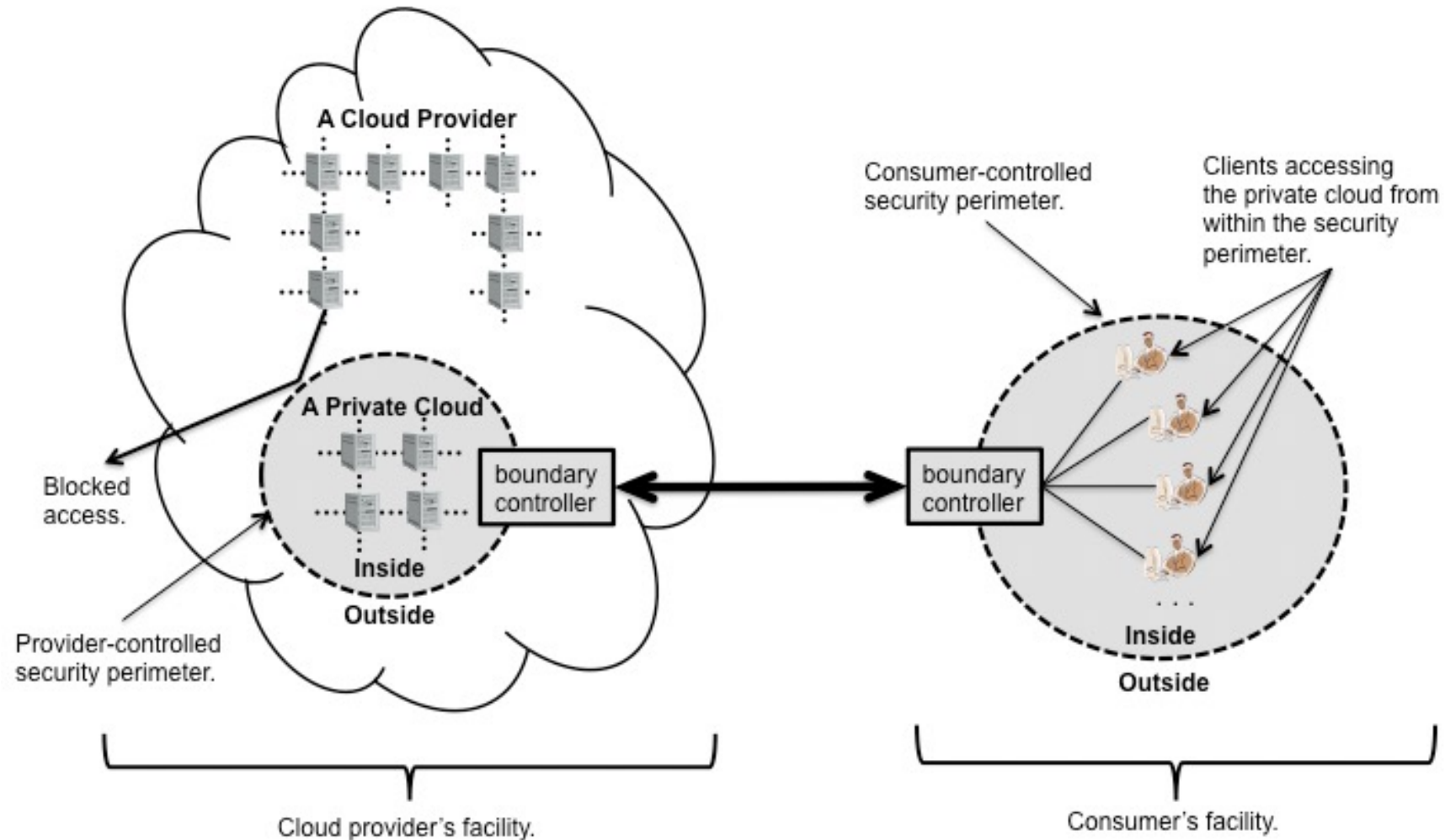


## Private Cloud

- Infrastructure provisioned for exclusive use of one organization
- May be on or off-premises
- May be owned, managed and operated by the organization or a third party (or a combination of both)



# Outsourced Private Cloud Scenarios



# Cloud Deployment



## Public Cloud

- Cloud infrastructure provisioned for open use by the general public
  - Exists on premises of the cloud provider

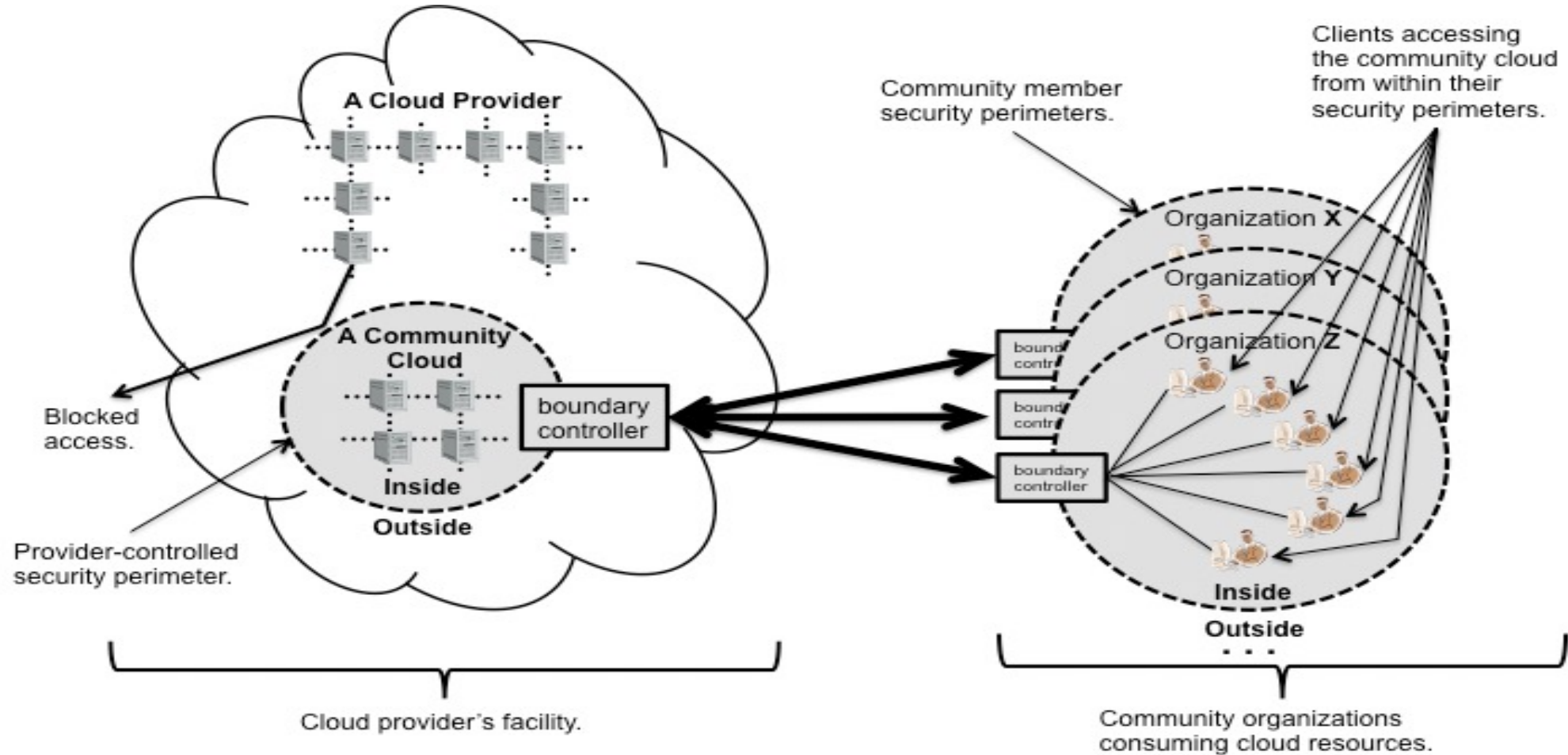
# Cloud Deployment



## Community Cloud

- Infrastructure provisioned for exclusive use by a specific community of consumers that have shared concerns (mission, security, policy, compliance)
- May be managed by one member of the community or a third party
- On or off premises

# Outsourced Community Cloud



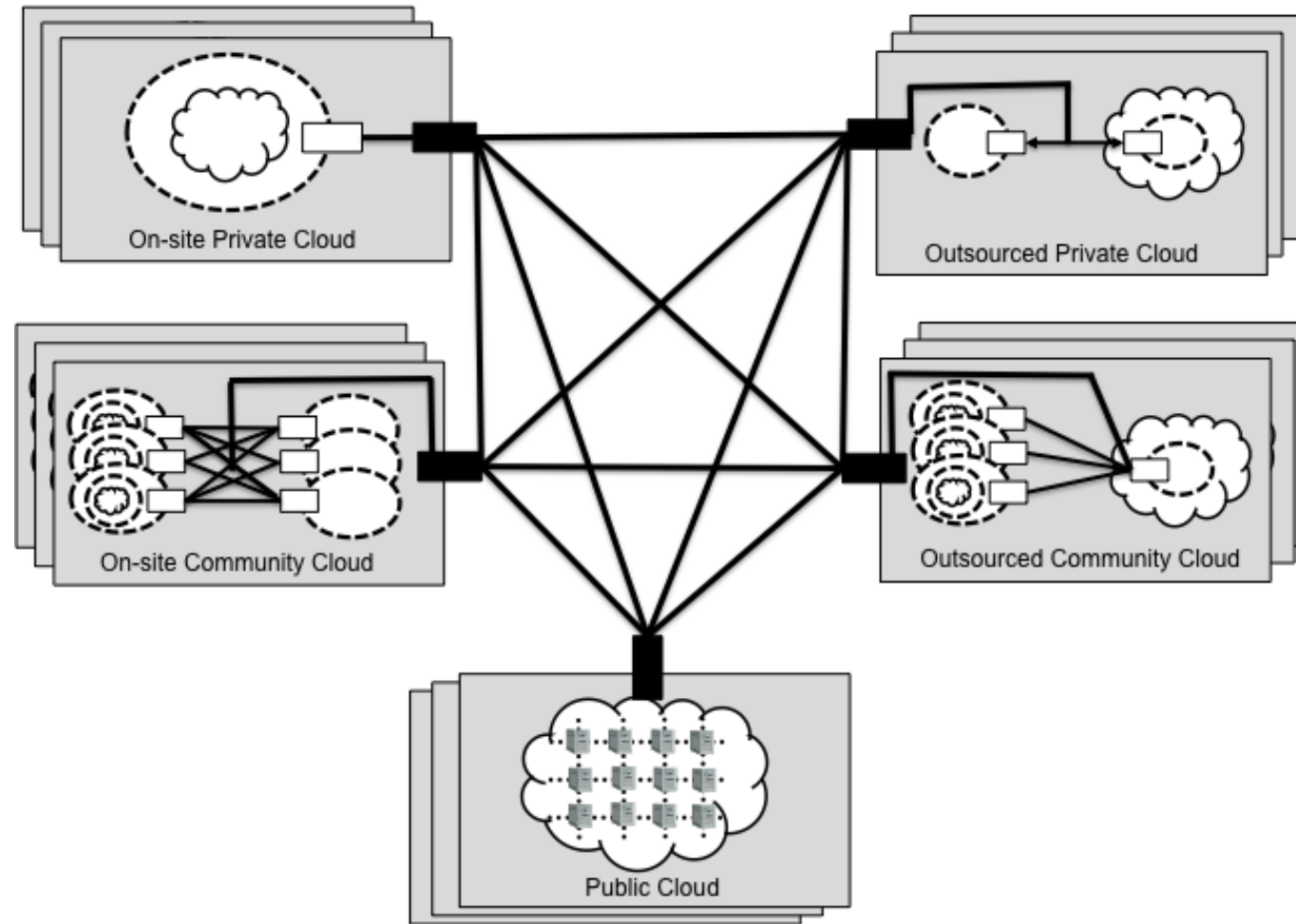
# Cloud Deployment



## Hybrid Cloud

- Composition of two or more distinct cloud infrastructures that operate as separate entities but are bound together by standardized or proprietary technology
- Enables data portability (cloud bursting)

# Hybrid Cloud



# Cloud Service Models

---



# Cloud Service Models



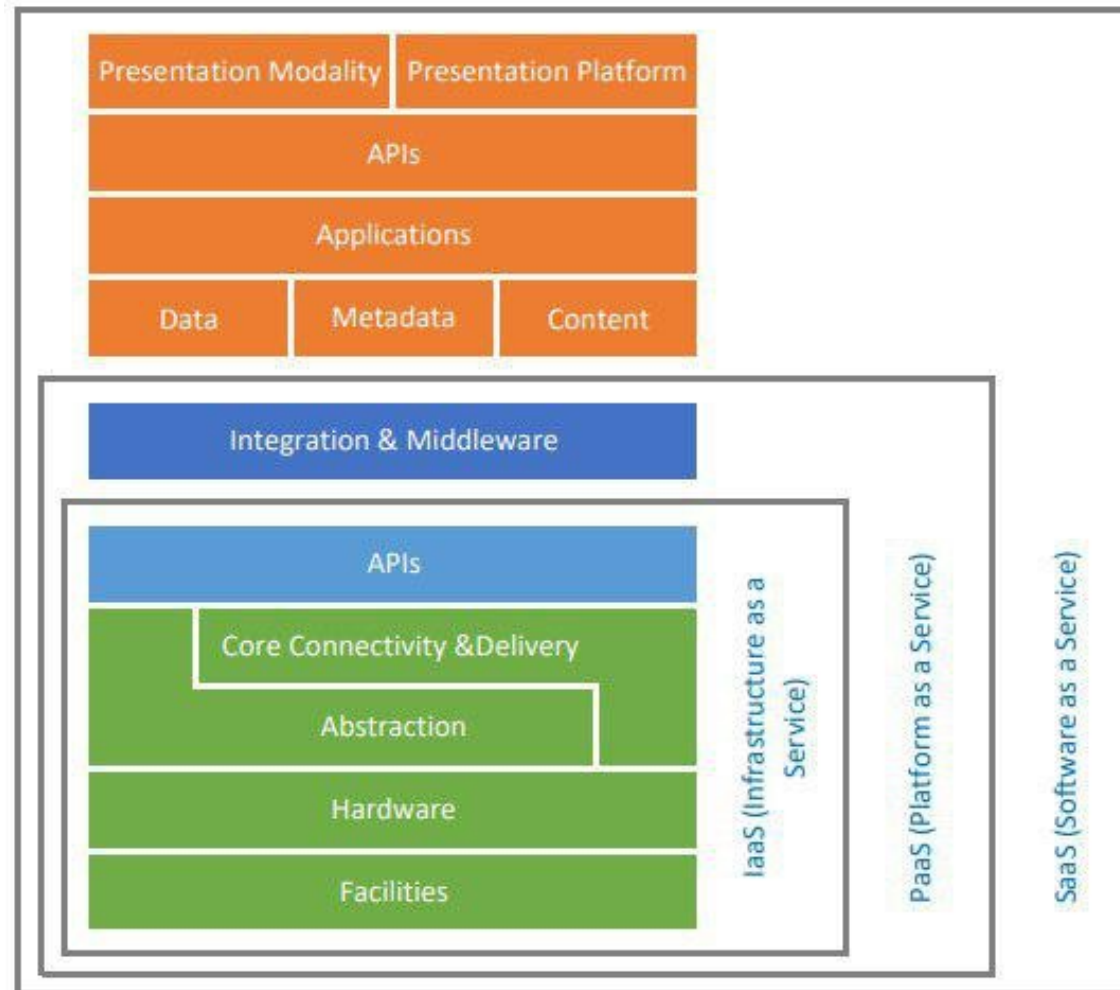
## Software-as-a-Service

The consumer uses applications provided on and running on the CSPs cloud infrastructure. The CSP manages the application. The consumer accesses the application through a thin client (browser) or Application Program Interface (API).

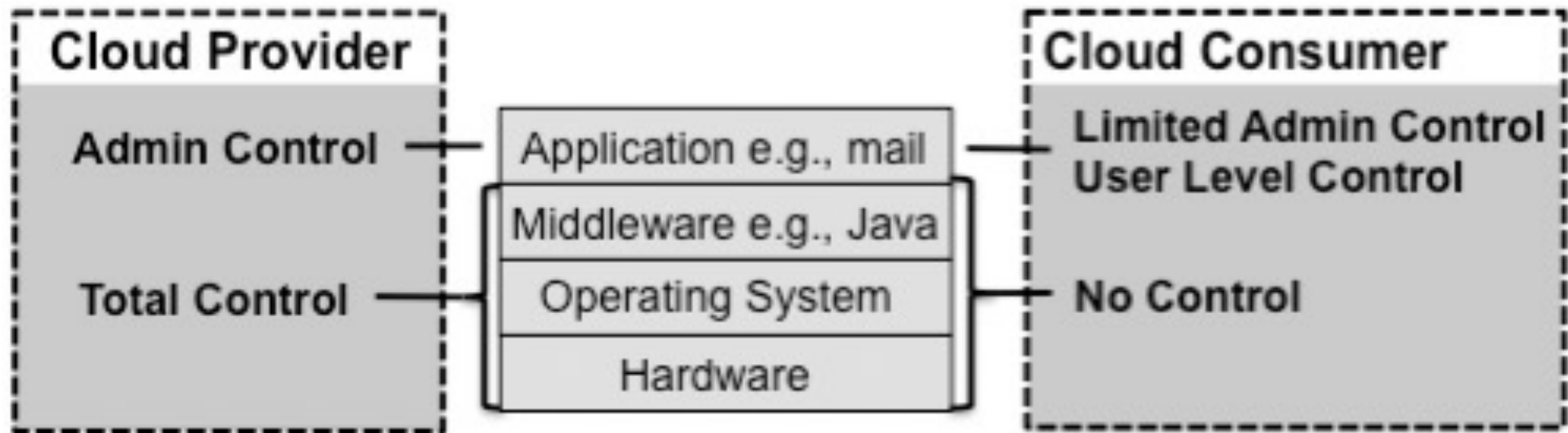
The consumer may manage access for their users.



# SaaS



# SaaS Control



# Cloud Service Models

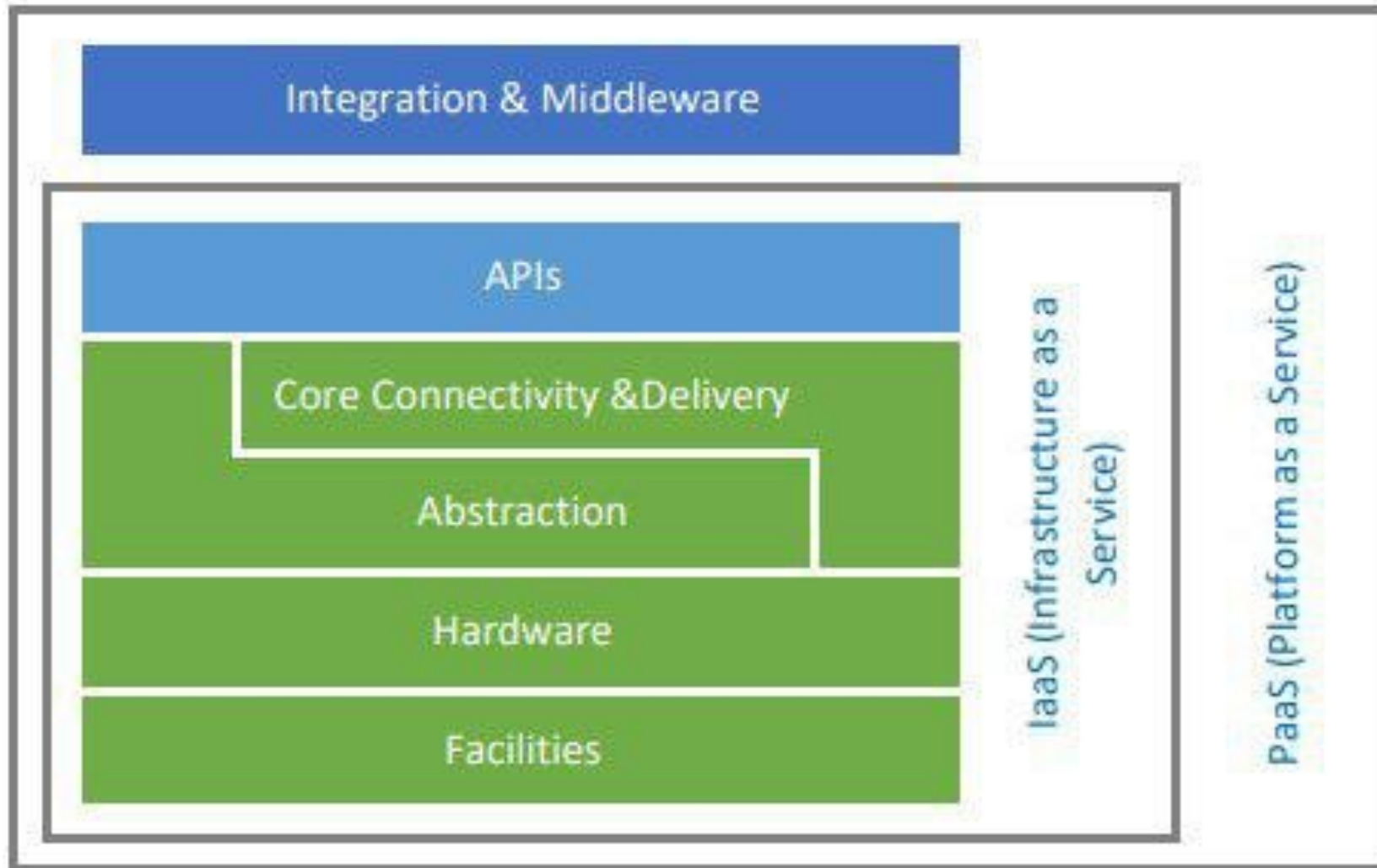


## Platform-as-a-Service

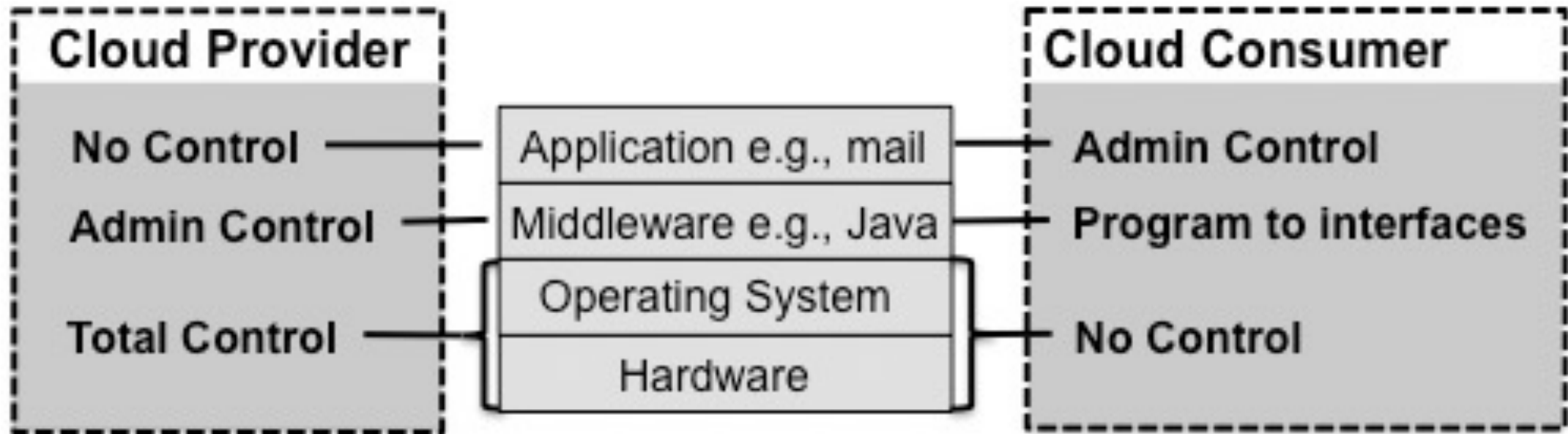
The consumer can deploy consumer-created or acquired applications on the CSPs cloud infrastructure. The CSP provides libraries, services, tools and languages.

The CSP manages the underlying infrastructure – the consumer manages their application

# PaaS



# Roles and Responsibilities



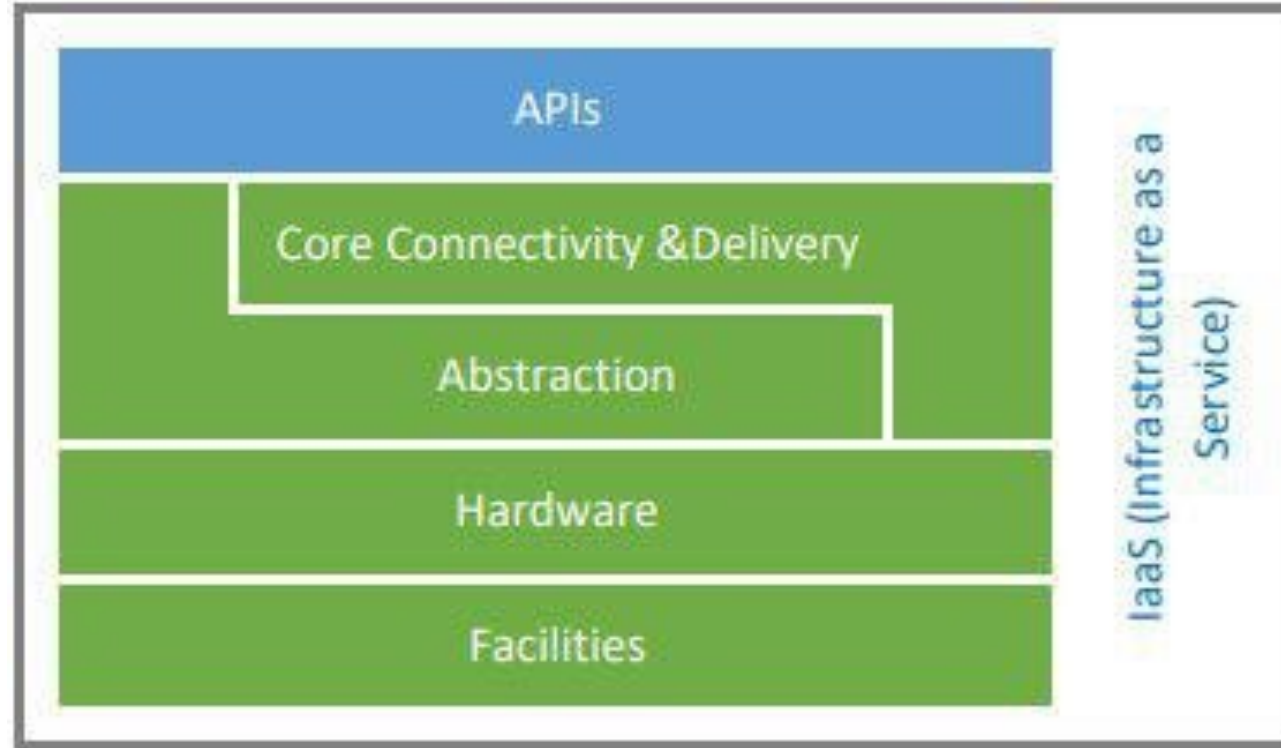
# Cloud Service Models



## Infrastructure-as-a-Service

The CSP provides the underlying infrastructure but the consumer manages operating systems, storage, applications and perhaps even some network components,

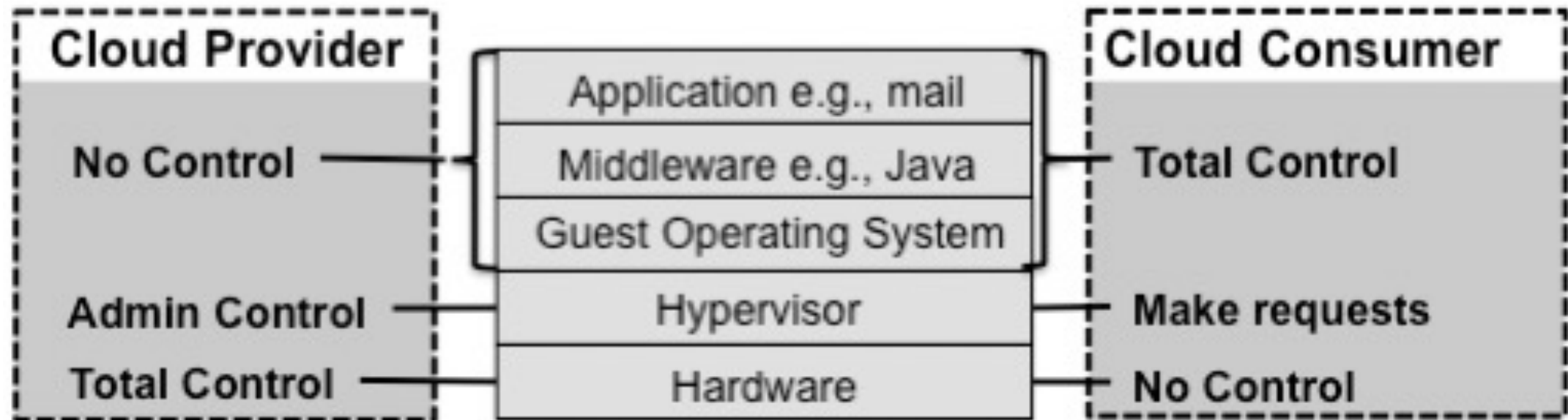
# IaaS



CSA v4



# Roles and Responsibilities



# Other Considerations for the Cloud

---



# Cloud Shared Considerations



**Interoperability**

**Portability**

- Reversibility

**Governance**

**Availability**

- Resilience

**Security**

- Privacy

**Auditability**

# Related Technologies



**Many computationally intensive tasks, and tasks that requires large storage and data analysis have benefited from the cloud:**

- Grid computing
- Blockchain
- Artificial Intelligence (AI)
- Machine learning

# Cloud-enabled Systems



Edge computing

IoT (Internet of Things)



# Cloud Services



DevSecOps  
Quantum computing



# Summary



This module examined the core principles of cloud architecture and service models.

Upon these various alternative models the consumer can deploy cloud-based systems to address their business needs.

