Introduction to Cloud Security - Overview

Tracy Wallace

Azure Architect*
Azure Security Engineer*

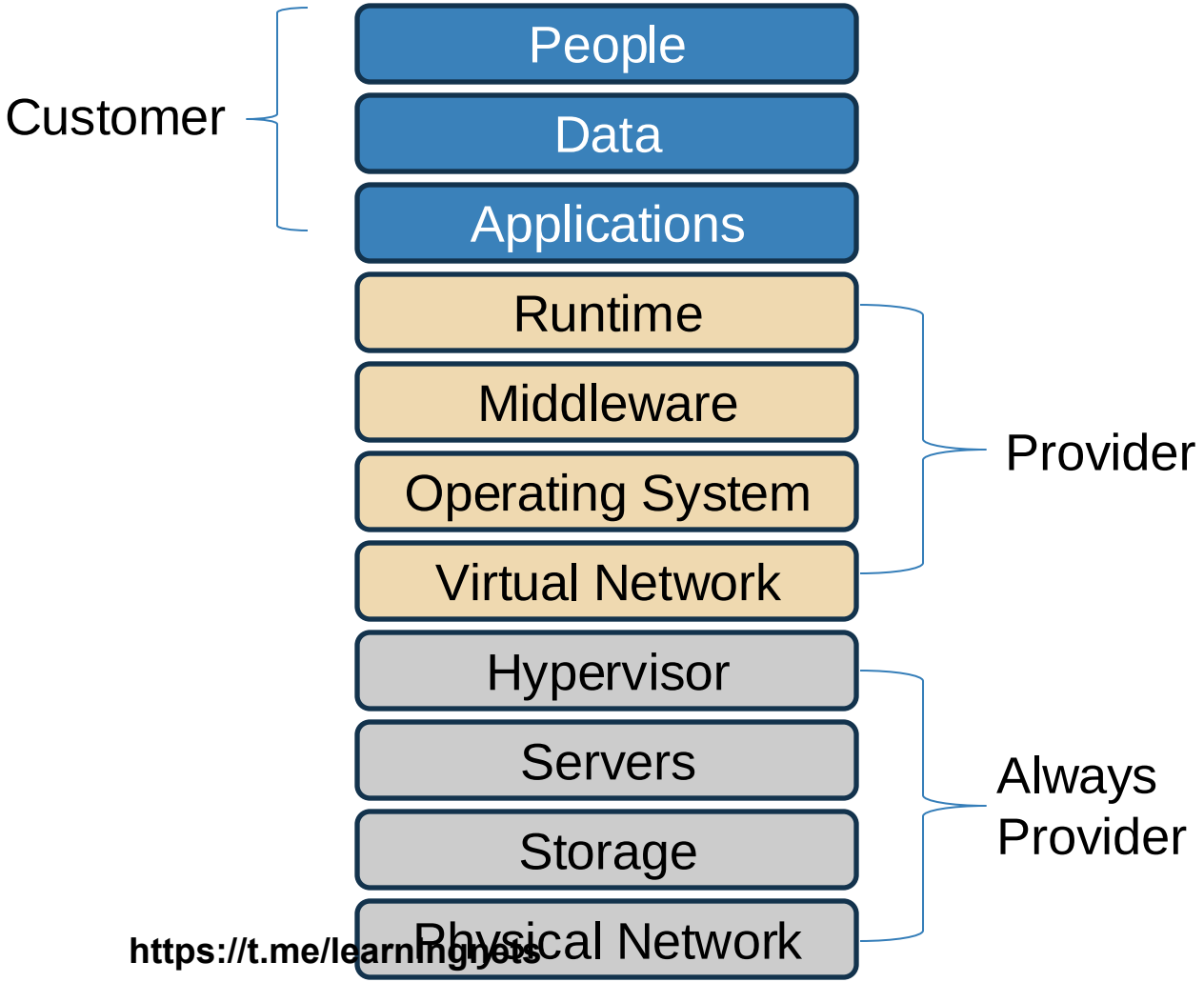
Key Concepts

- Cloud Introduction
- Cloud Workloads

MAJOR TOPICS

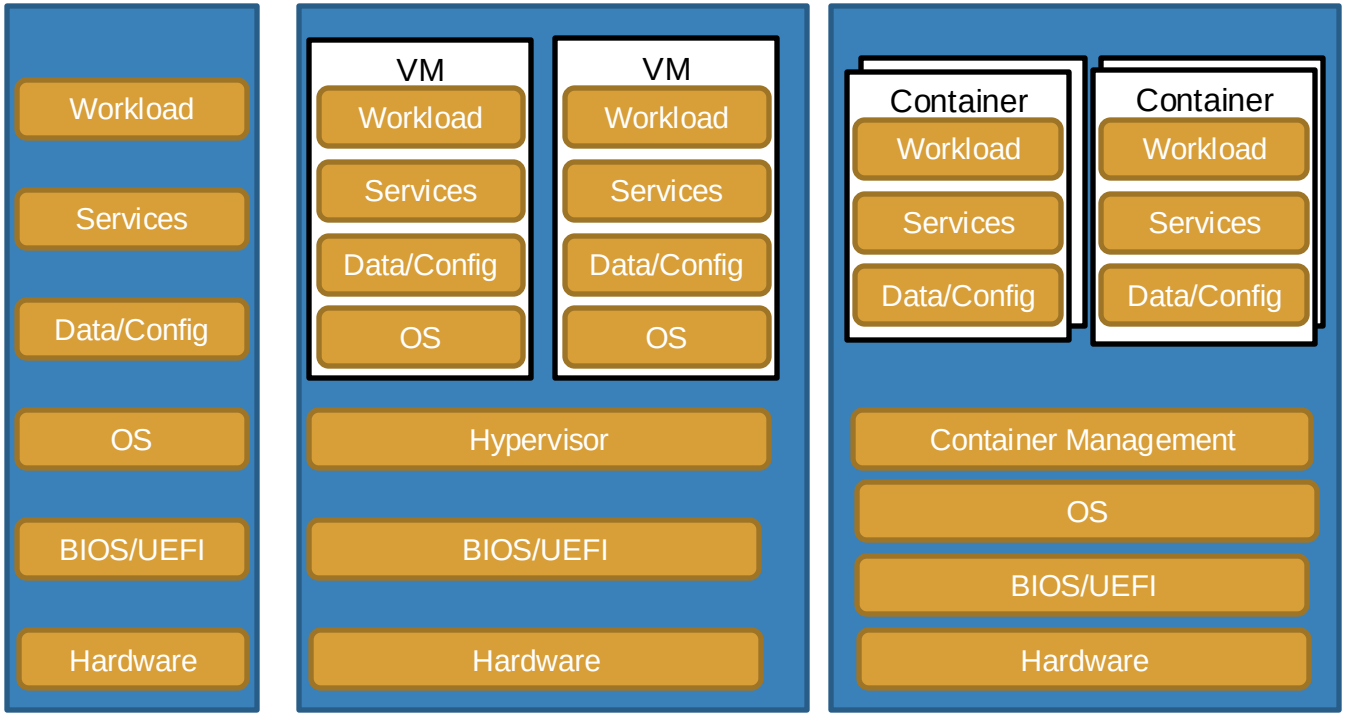
- Cloud Concepts
- Cloud Security
- Cloud Compute
- Cloud Workload Security

PaaS Shared Responsibility



Containers

- Physical Hosting
- Virtualization
- Containers



LEARNING OUTCOMES

+ Understand the fundamental concepts of cloud computing, including the definition and characteristics.
+ Describe the various cloud deployment models: Public, Private, Hybrid, and Community.
+ Define the shared responsibility model in cloud computing.
+ Understand the integration of DevOps practices with cloud technologies.
+ Identify the key security requirements for cloud deployments.
+ Recognize common cloud security threats.

PREREQUISITES

+ **Understand cyber security fundamentals**

Let’s Go

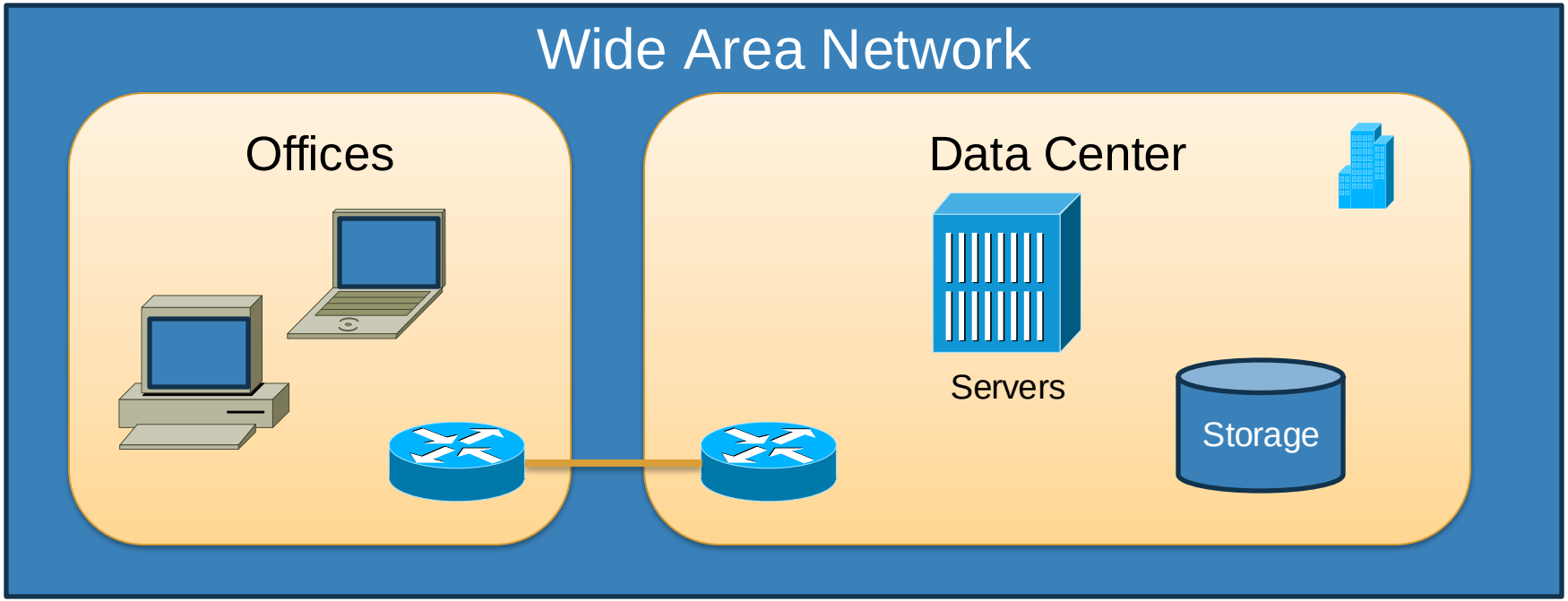
Cloud Basics

What Is Cloud?

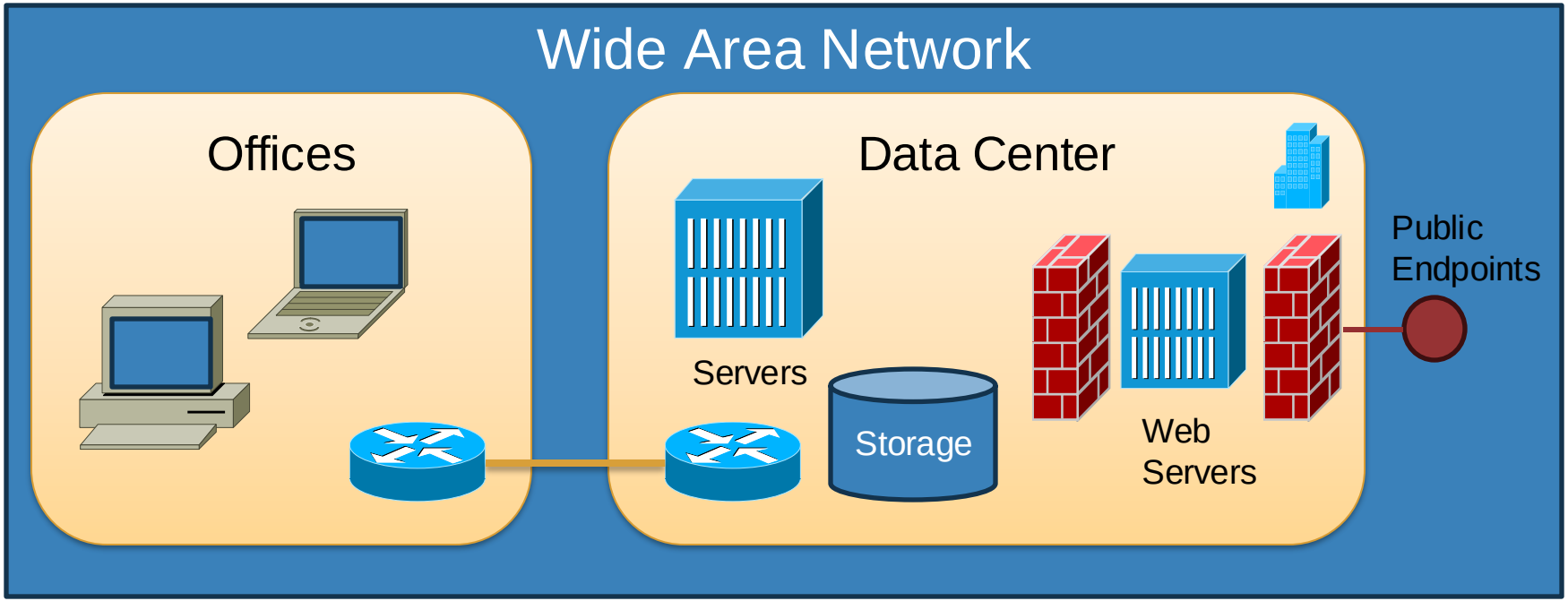
There is No Cloud

There is just someone else's servers

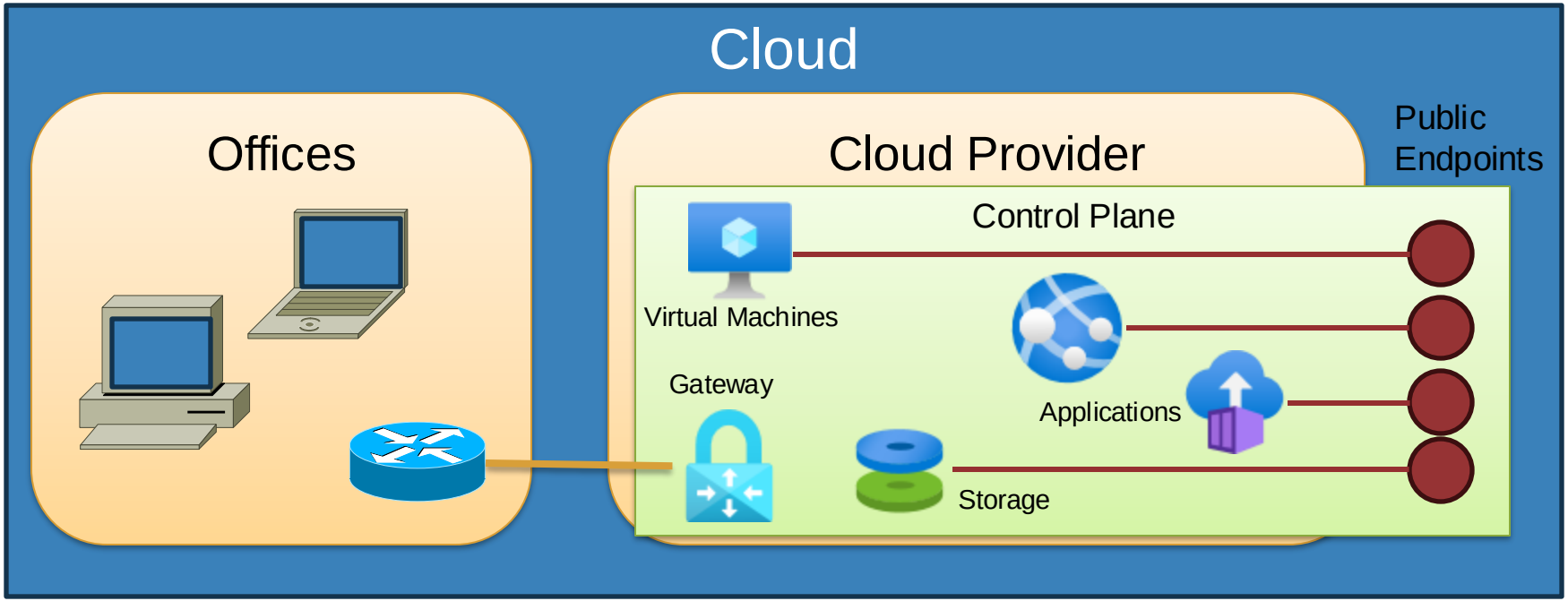
What is the Cloud?



What is the Cloud?



What is the Cloud?



Cloud Advantages

- Distributed storage
- Scalability
- Resource pooling
- Access from any location
- Measured service
- Automated management

NIST SP 800-145 “The NIST Definition of Cloud Computing”

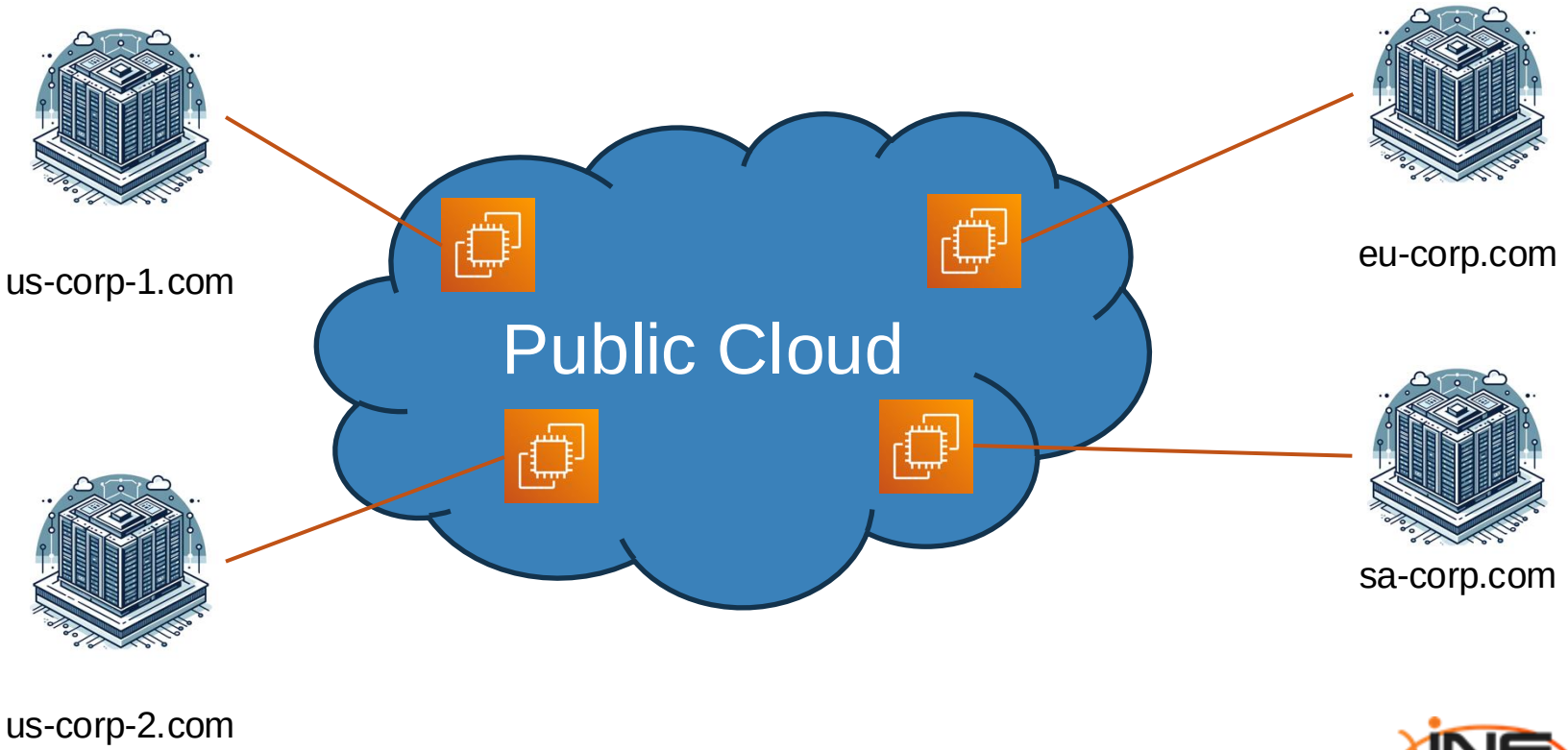
- On-demand self service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

Cloud Computing Models

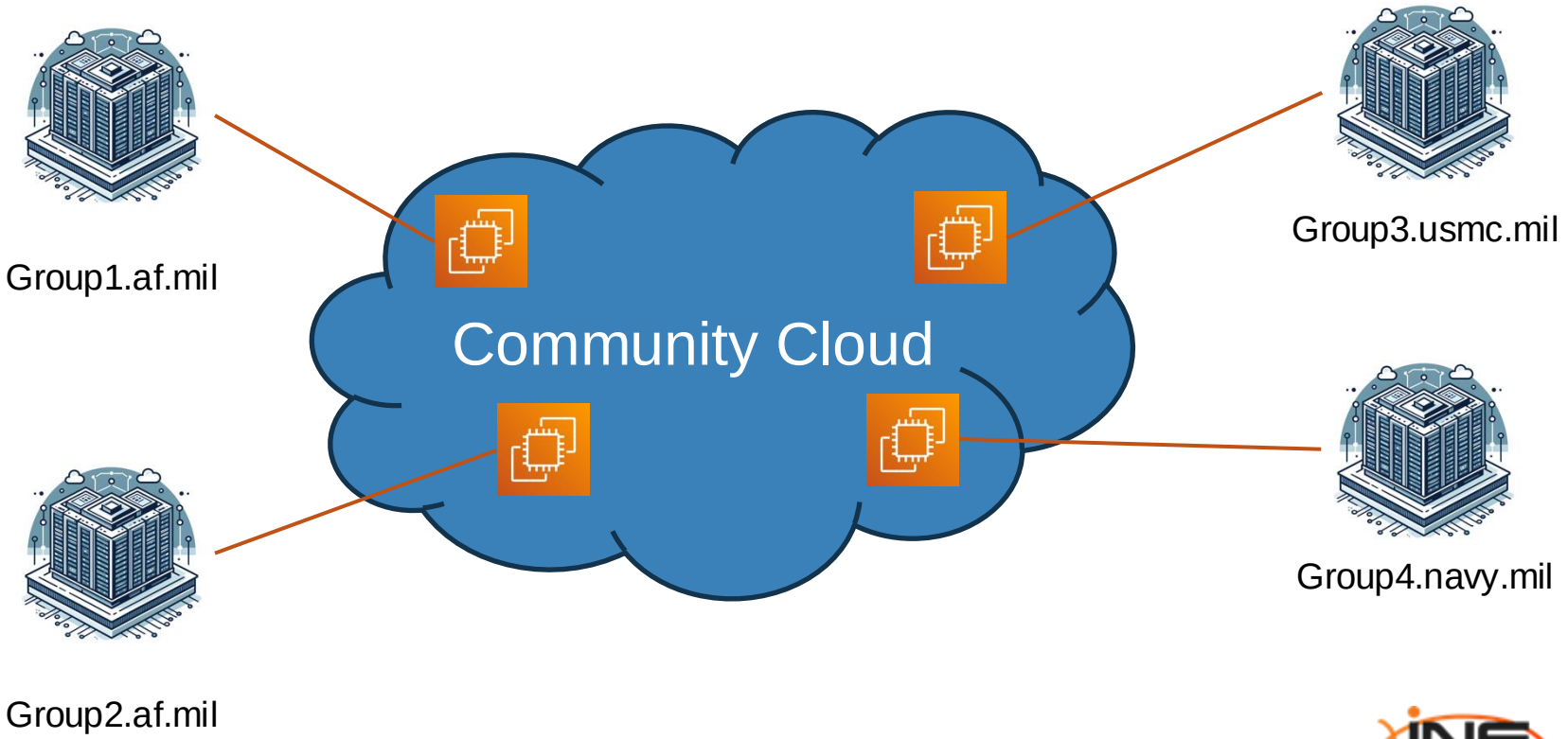
Topics:

- Types of Cloud
- Cloud Compute Models

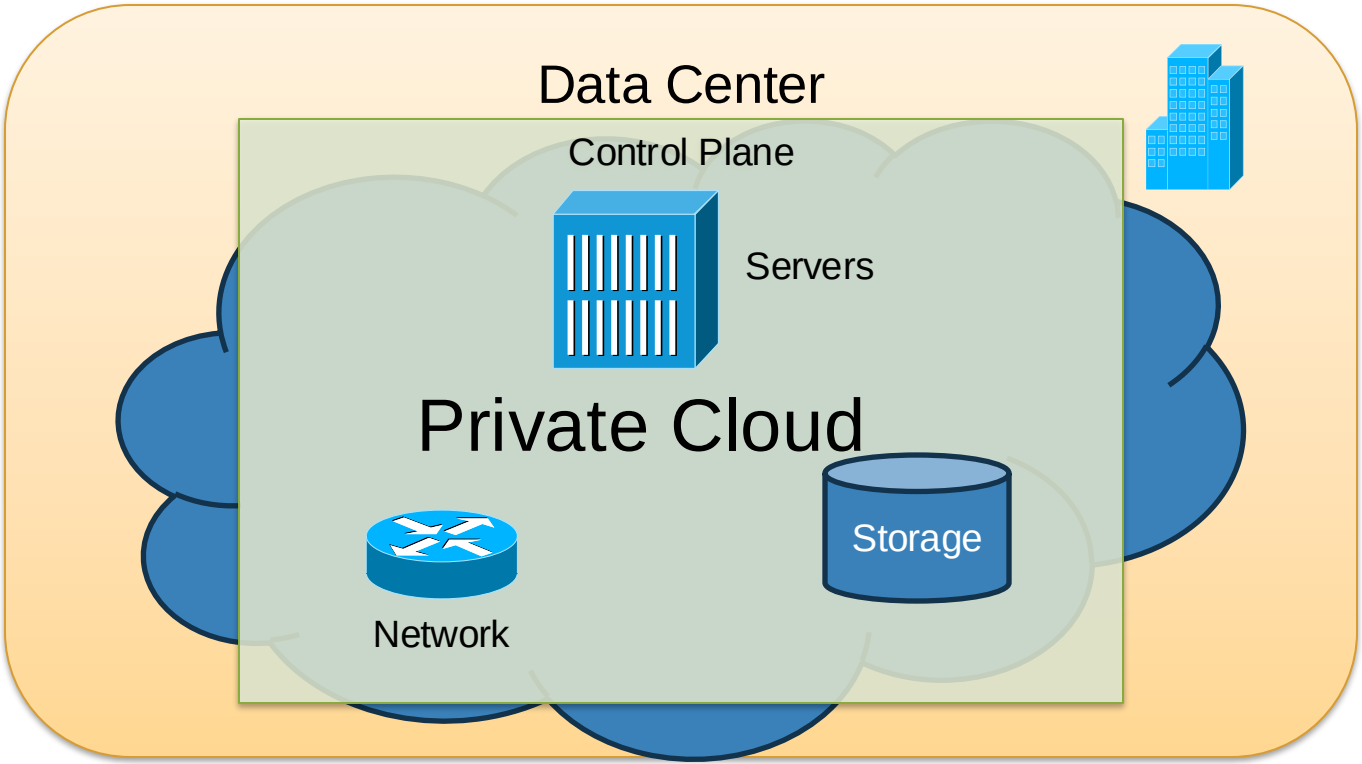
Types of Cloud



Types of Cloud

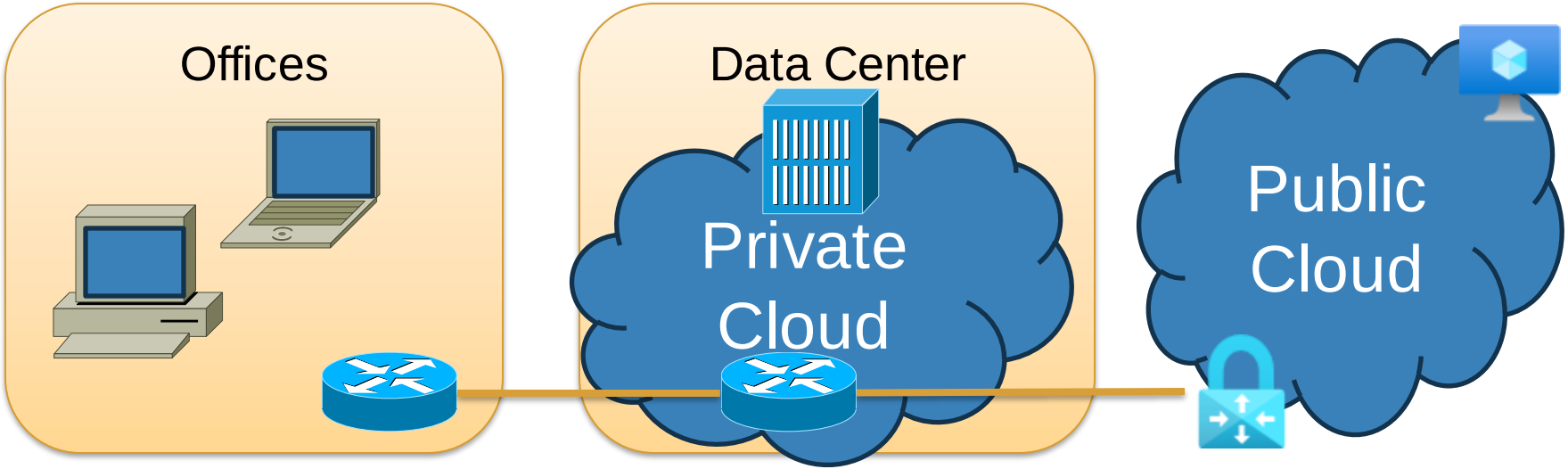


Types of Cloud

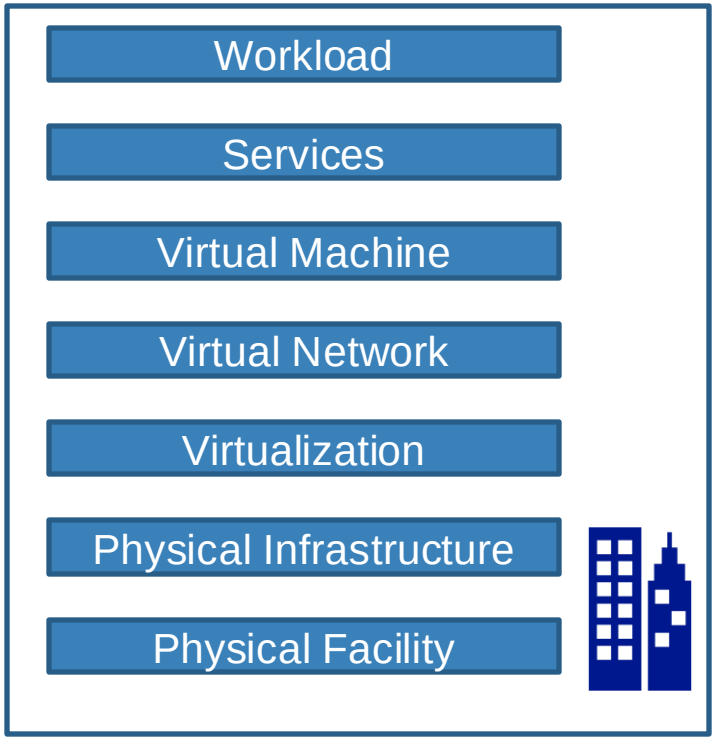


Types of Cloud

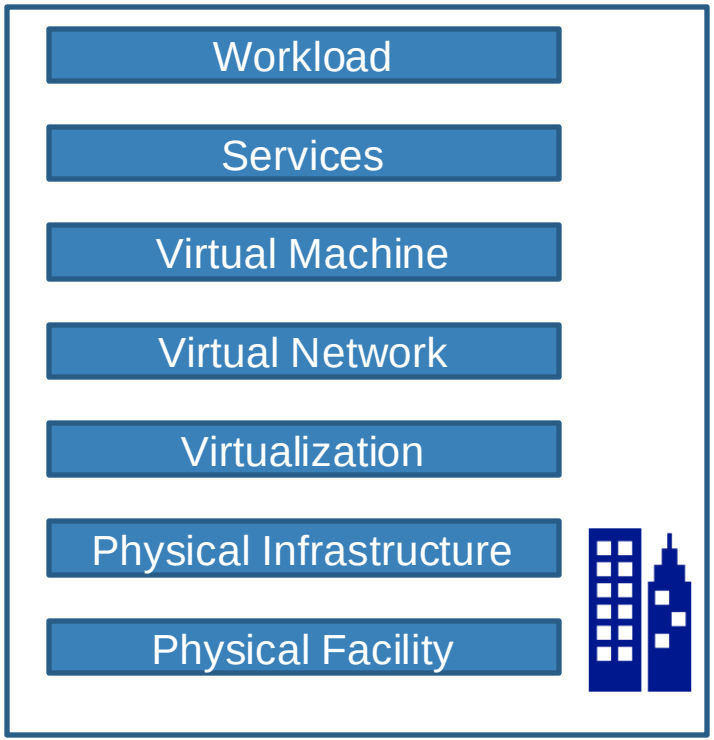
Hybrid Cloud

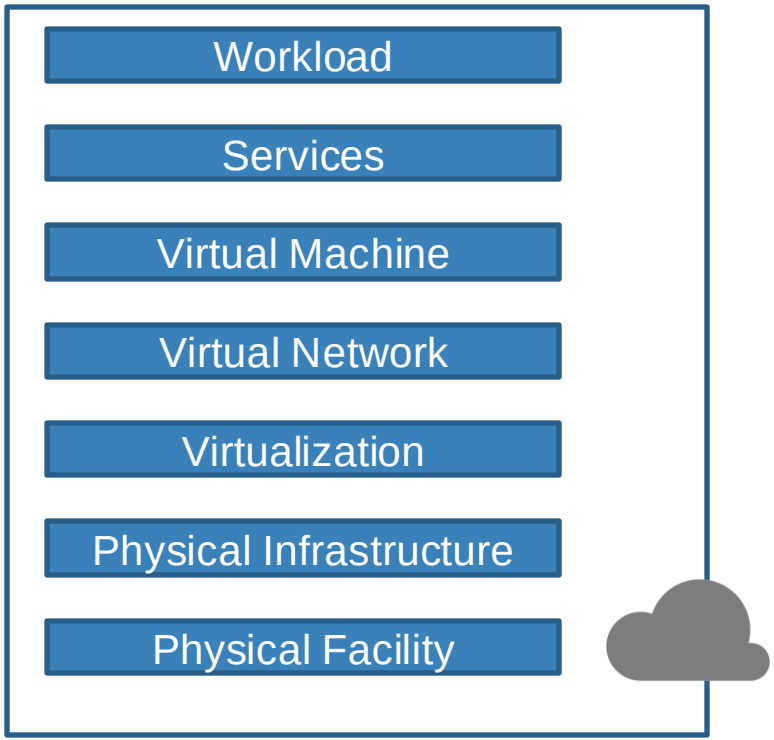


Cloud Architecture

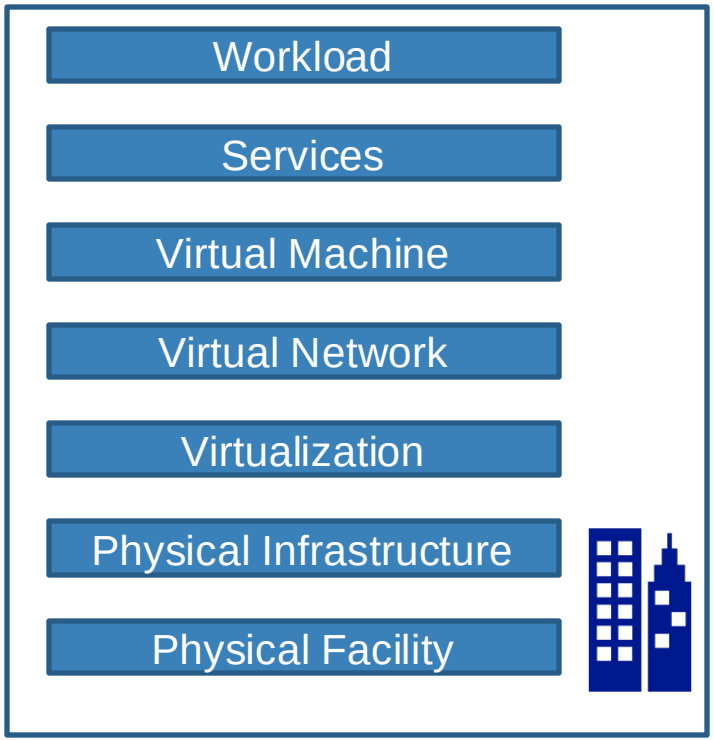


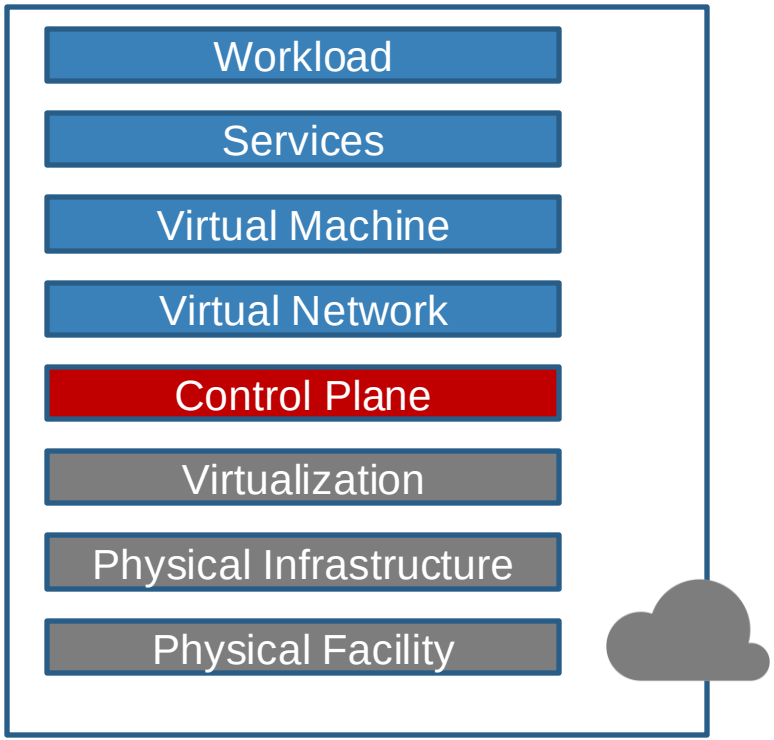
Cloud Architecture



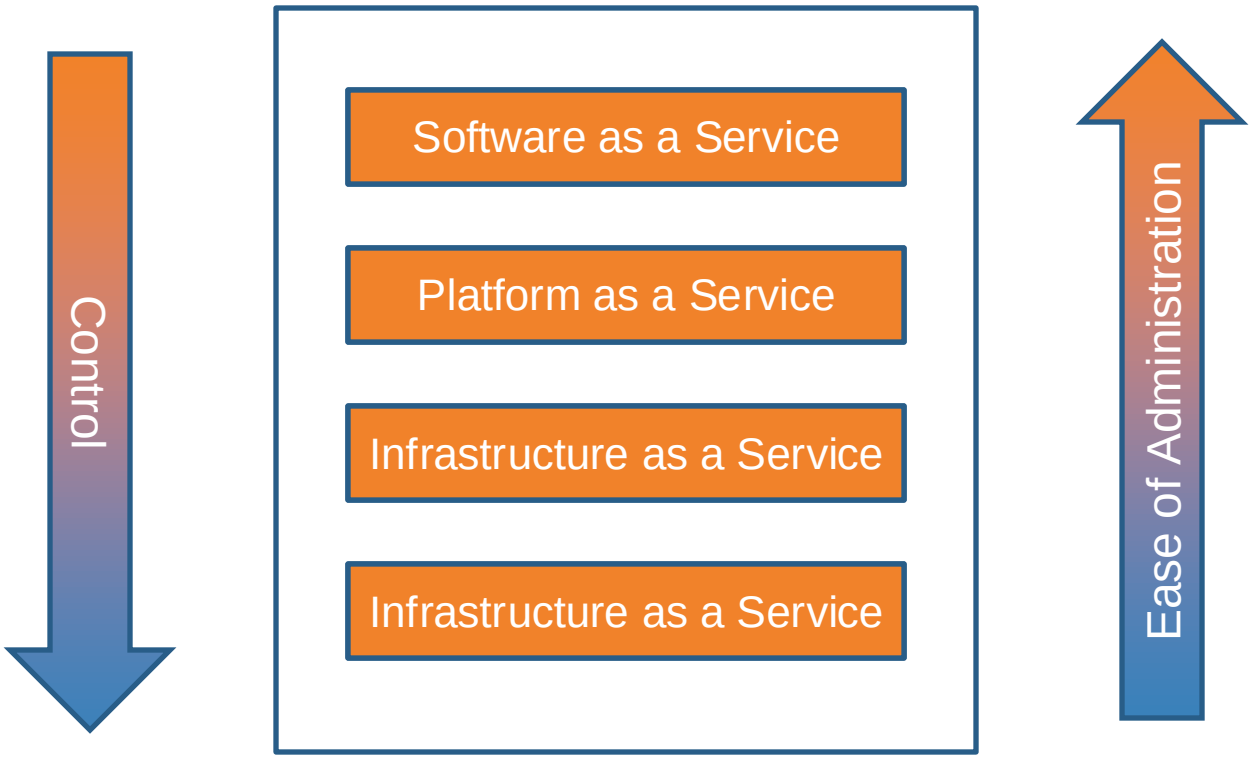


Cloud Architecture





Types of Cloud Services



Shared Responsibility Model

Topics:

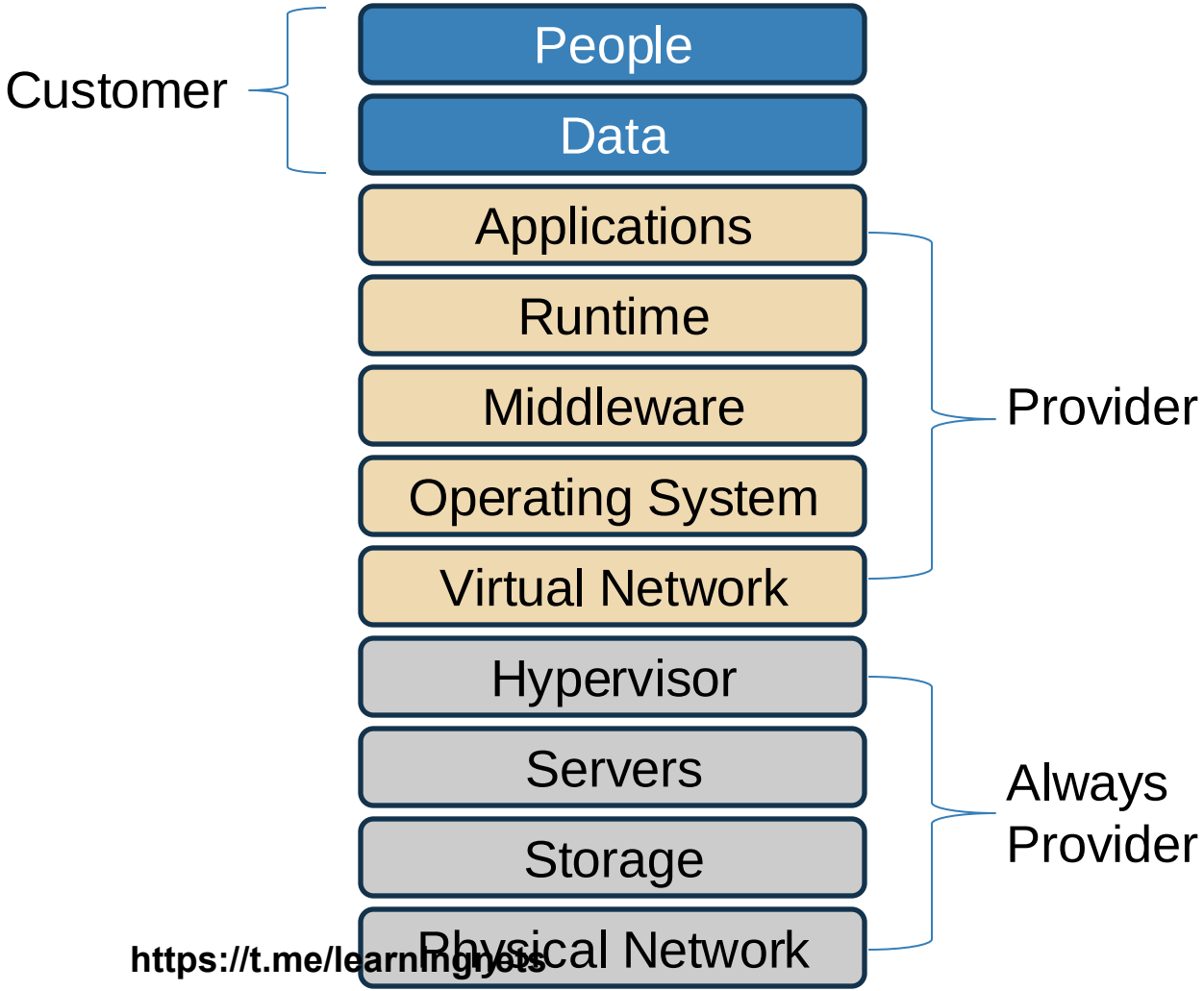
- Shared Responsibility Model
- Shared Responsibility for SaaS
- Shared Responsibility for PaaS
- Shared Responsibility for IaaS

Shared Responsibility Model

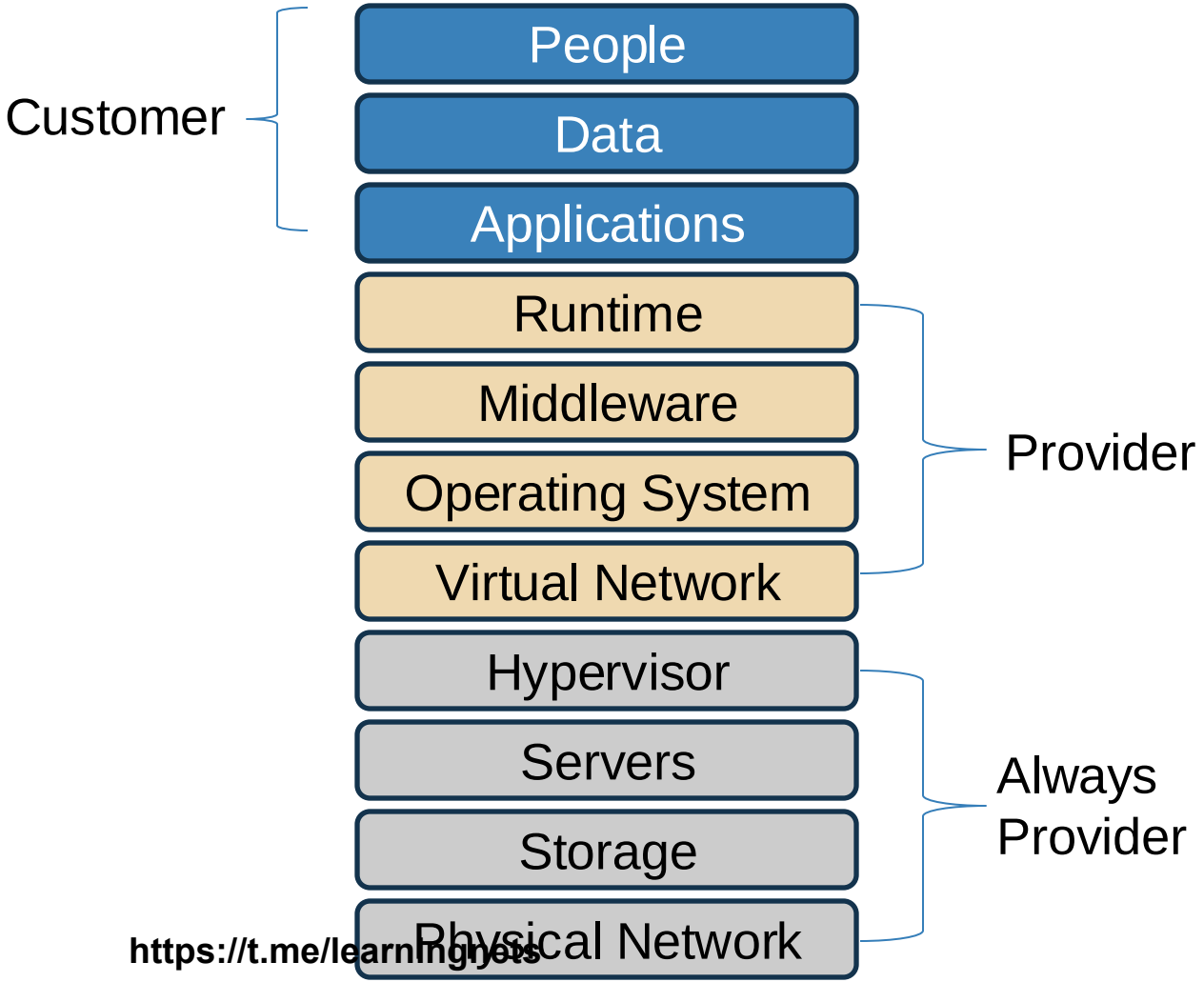
The Shared Responsibility Model is a security and compliance framework that outlines the responsibilities of cloud service providers (CSPs) and customers for securing every aspect of the cloud environment, including hardware, infrastructure, endpoints, data, configurations, settings, operating system (OS), network controls and access rights.

Source: https://www.crowdstrike.com/cybersecurity-101/cloud-security/shared-responsibility-model/

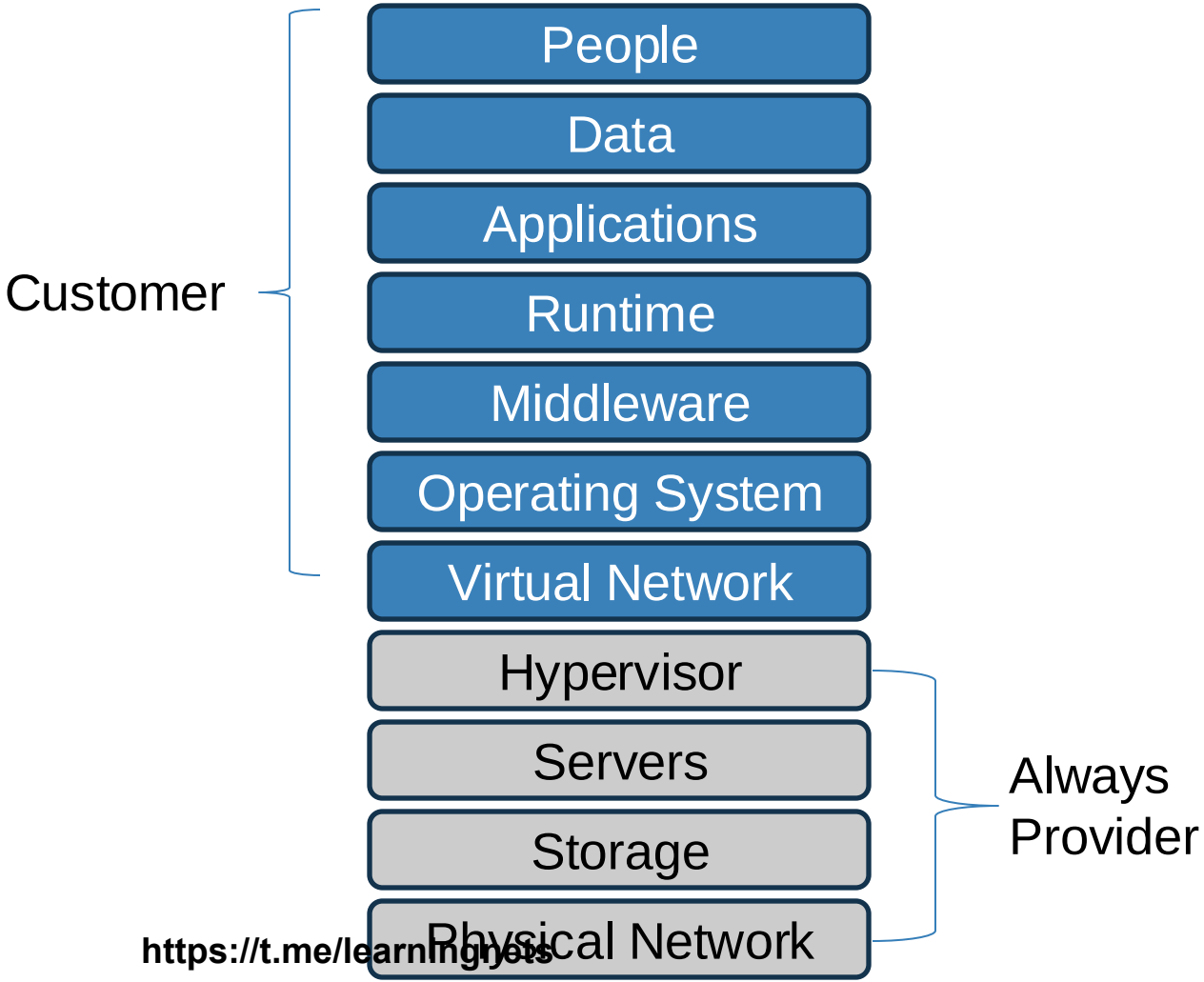
SaaS Shared Responsibility



PaaS Shared Responsibility



IaaS Shared Responsibility



Cloud Security Tools & Assessments

Topics:

- Cloud Security Tools
- Patch Management
- Cloud Penetration Testing

Cloud Security Tools

Azure

Defender 365
Microsoft Defender for Cloud
Microsoft Sentinel

AWS

AWS Guard Duty

Google Cloud

Security Command Center

All platforms have network protection and compute protection and support third party security solutions

Patch Management

Cloud Penetration Testing

Azure

- No DoS
- No access to other's resources
- No notification necessary

AWS

- No DNS
- No DoS
- No notification necessary

Google Cloud

- Abide by Acceptable Use
- Abide by Terms of Service
- No notification necessary

All platforms allow penetration testing within reasonable guidelines

DevOps & the Cloud

Topics:

- Traditional Development
- Agile Development
- What is DevOps?
- CI/CD
- DevOps & the Cloud
- DevSecOps

Traditional Development

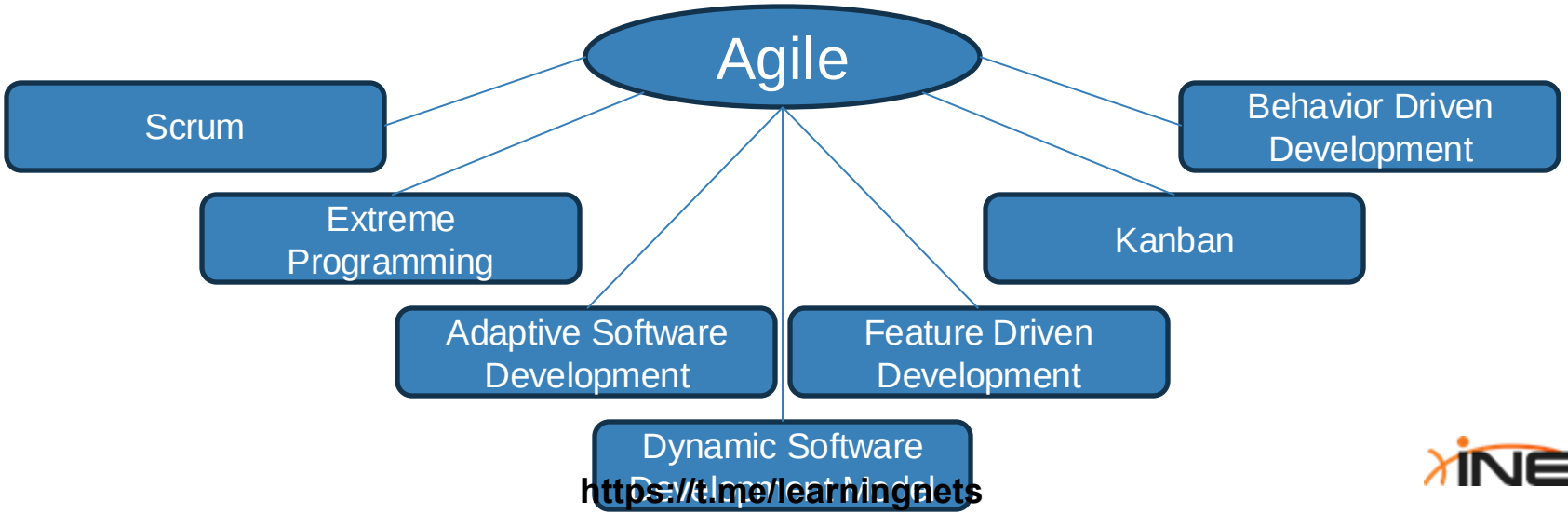
Agile Philosophy

+ Individuals and interactions over processes and tools
+ Working software over comprehensive documentation
+ Customer collaboration over contract negotiation
+ Responding to change over following a plan

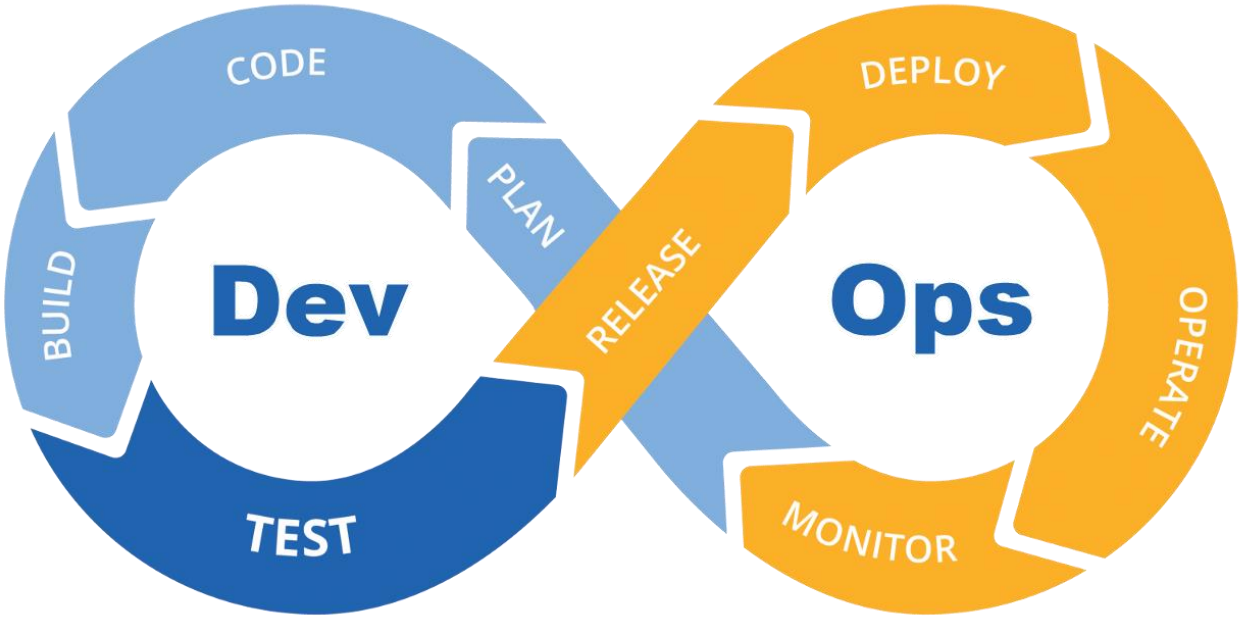
Agile manifesto, 2001
https://agilemanifesto.org/

Agile Philosophy

- Twelve principles
- Defines an overall approach, not a process
- Many processes have developed



Agile Development - DevOps



https://www.interxect.com/main/wp-content/uploads/2018/02/devops_2.png

DevOps

- Continuous Improvement
- Shared Responsibility
  - Product management
  - Software development
  - QA
  - IT operations
  - Infosec
- Automation

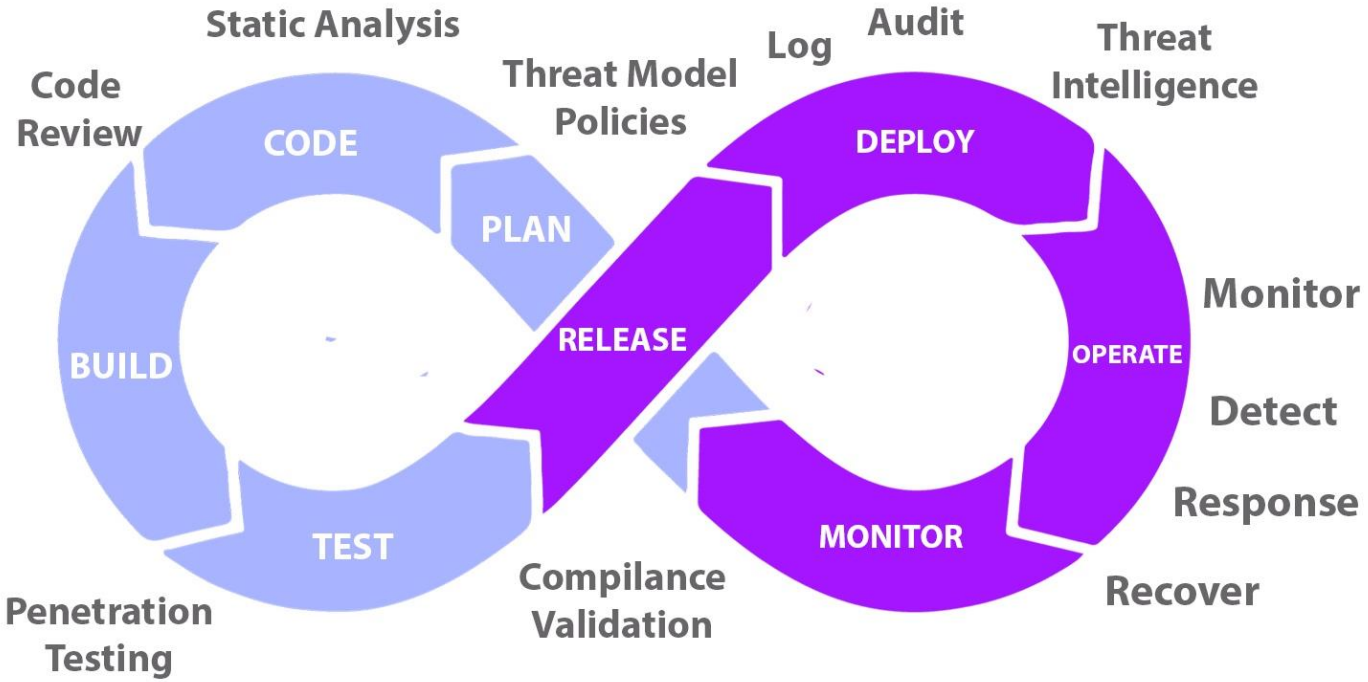
DevOps – CI/CD

+ Continuous Integration – Continuous Deployment/Delivery
+ Automated workflow
+ Vulnerability and security opportunity

DevOps & The Cloud

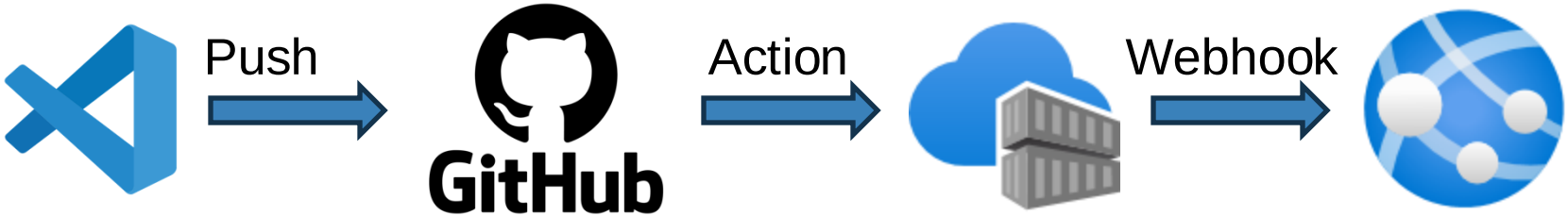
+ Deployment endpoints are often in the cloud (IaaS and PaaS)
+ DevOps processing often occurs in the cloud

DevSecOps



https://kodershop.com/wp-content/uploads/2023/03/DevSecOps.jpg

Demonstration



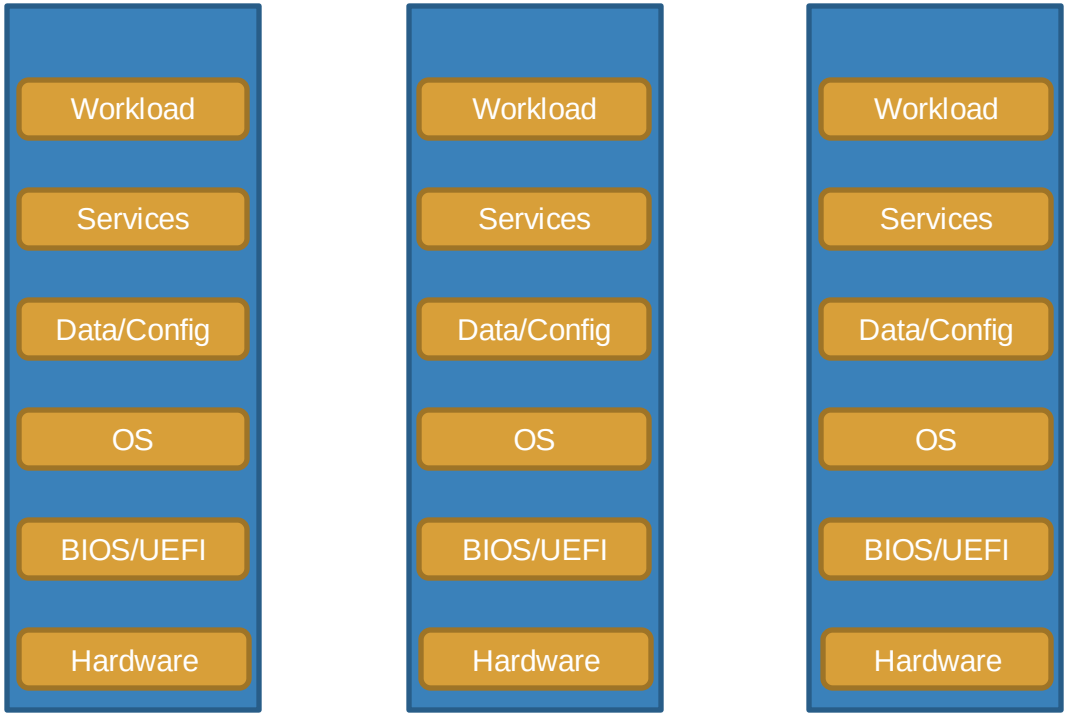
Containers

Topics:

- Containers
- Container Lifecycle
- Container Security
- Demonstration

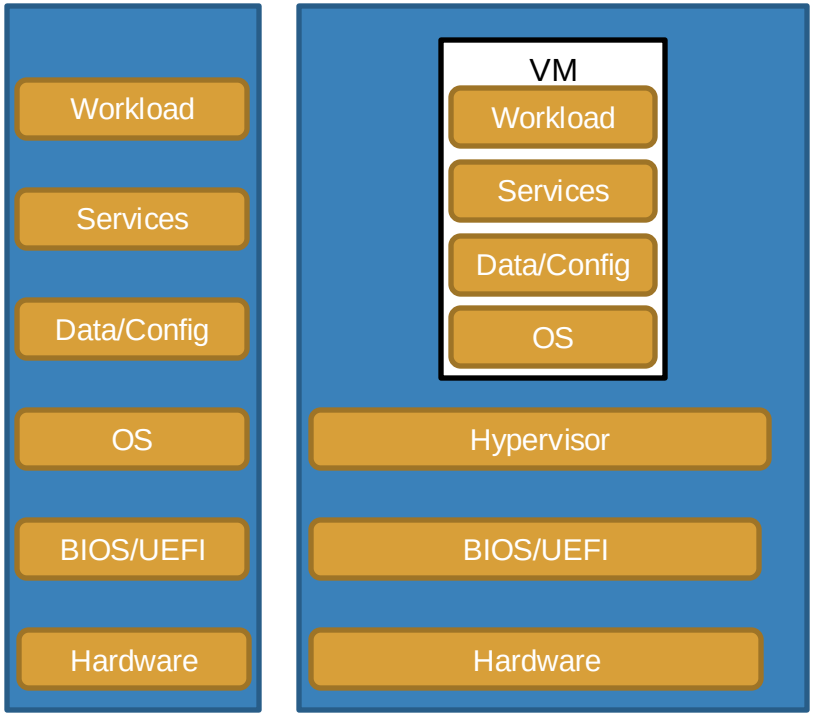
Containers

- Physical Hosting
- Virtualization
- Containers



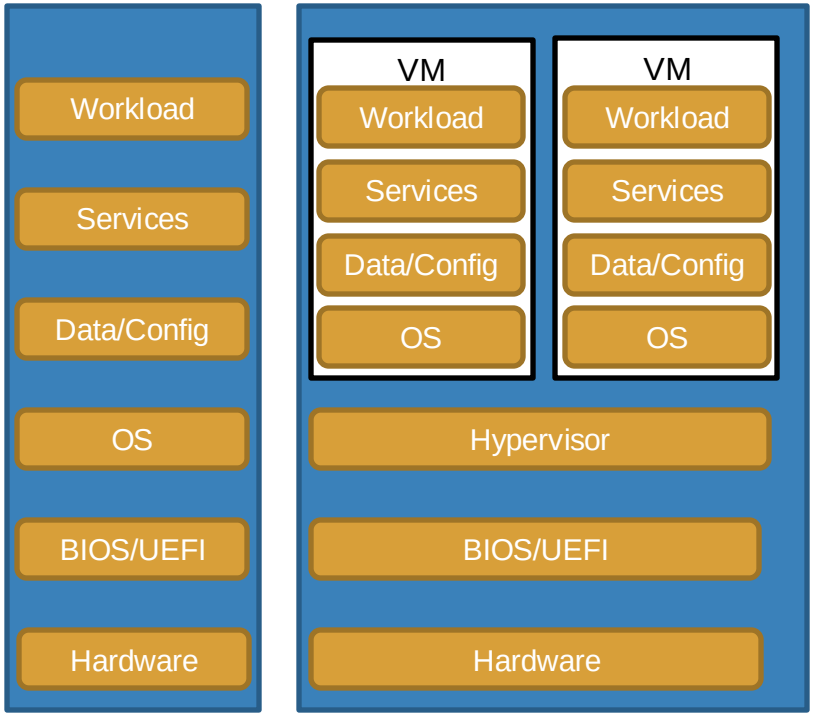
Containers

- Physical Hosting
- Virtualization
- Containers



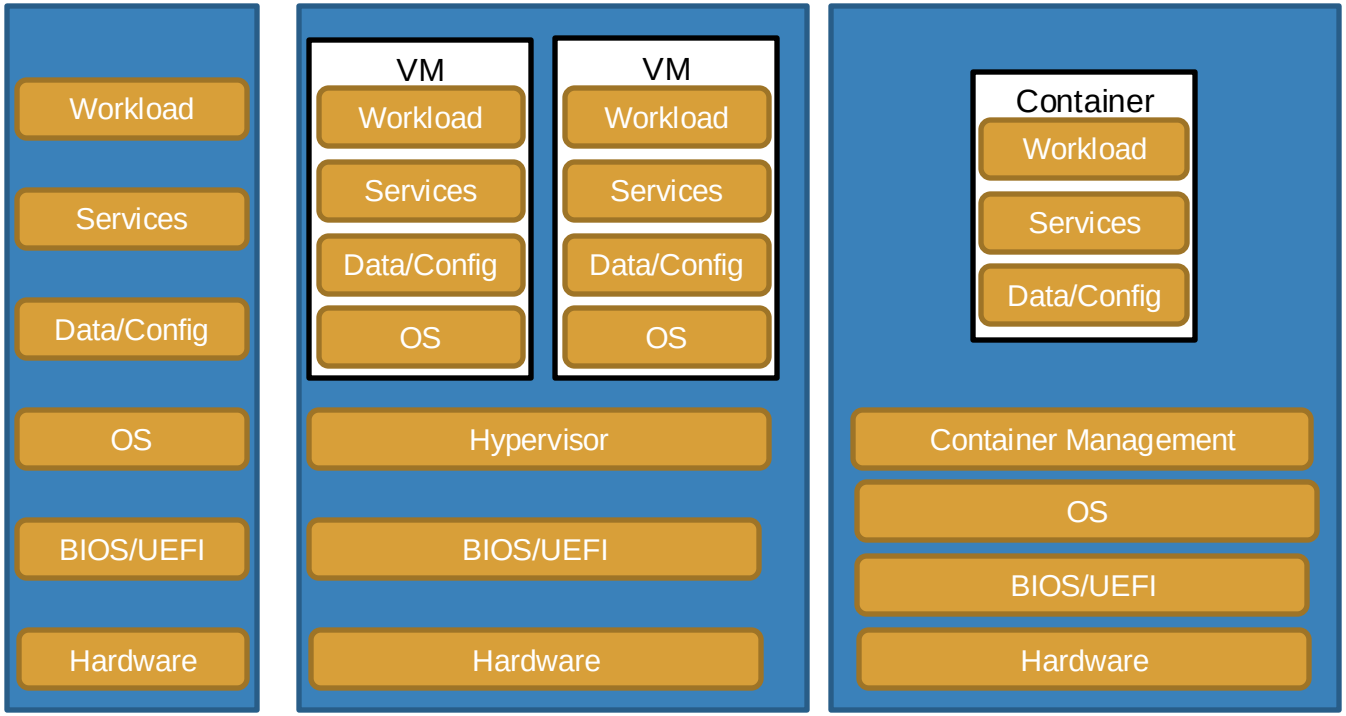
Containers

- Physical Hosting
- Virtualization
- Containers



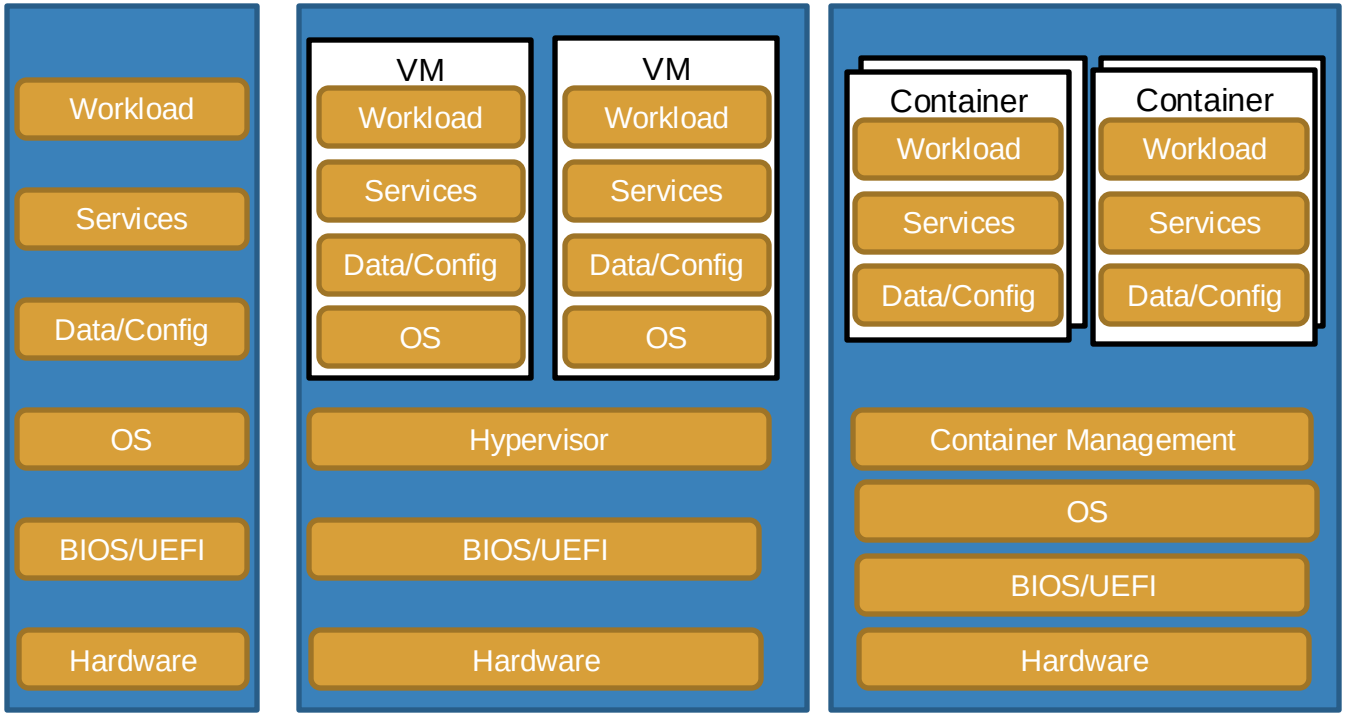
Containers

- Physical Hosting
- Virtualization
- Containers



Containers

- Physical Hosting
- Virtualization
- Containers



Container Lifecycle

Container Security

- Containers
  - “Supply chain” complexity
  - Container break-out
- Lifecycle
  - Each phase represents a vulnerability
- Solution Architecture
  - Typically, more complex
  - More things to secure

Serverless

Topics:

- What is Serverless
- Serverless Architecture
- Serverless Benefits
- Serverless Shared Responsibility
- Serverless Security

What Is Serverless?

There is No Cloud

There is just someone else's servers

What Is Serverless?

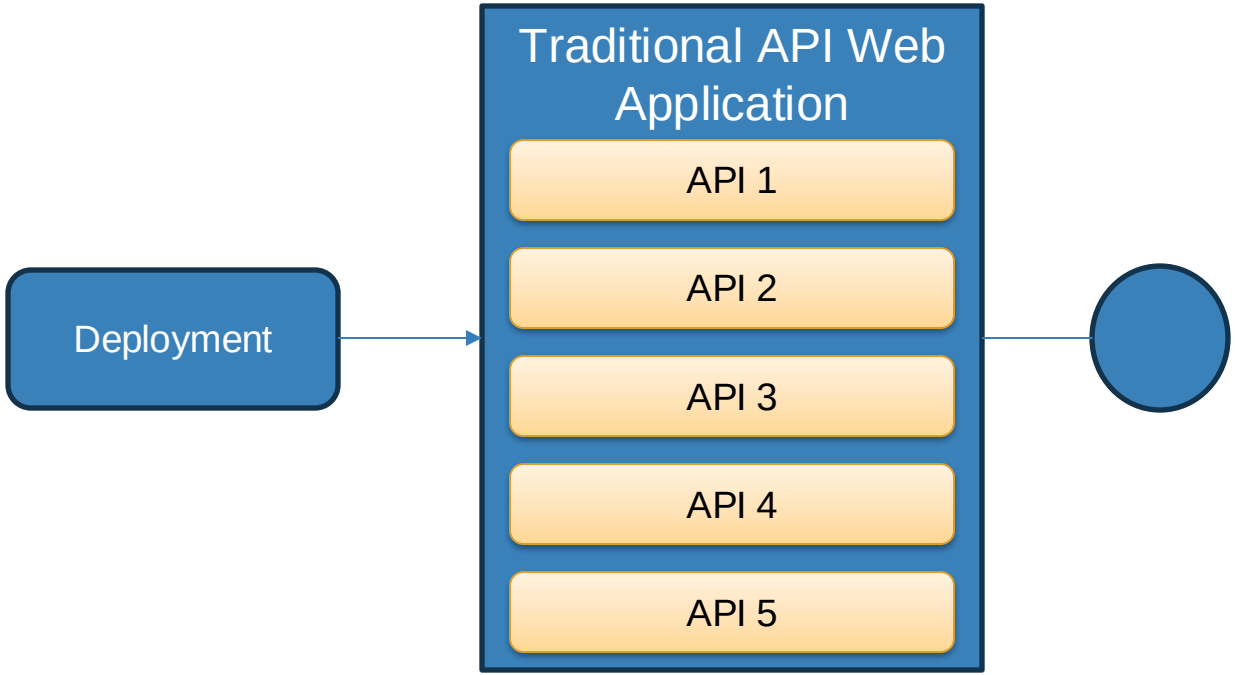
There is No Cloud

There is just someone else's servers

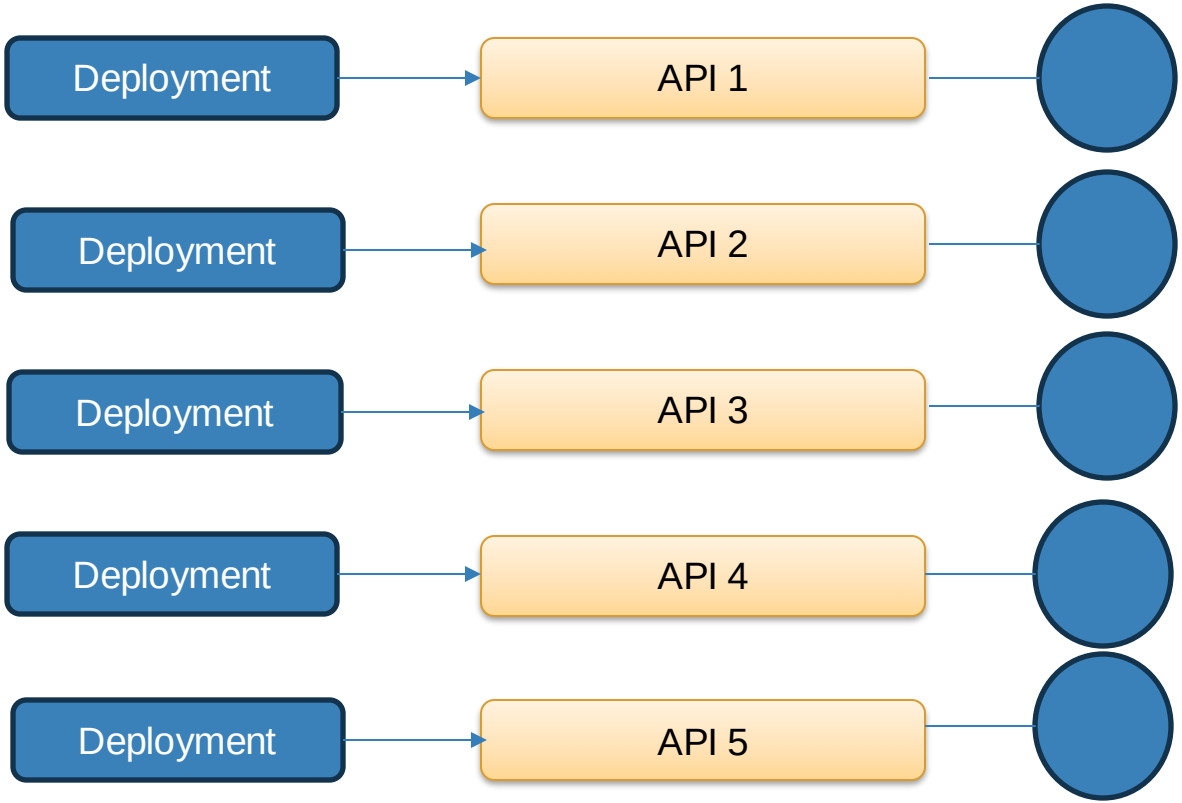
There is no such thing as serverless

It's just another way to host and bill cloud services.

Serverless Architecture



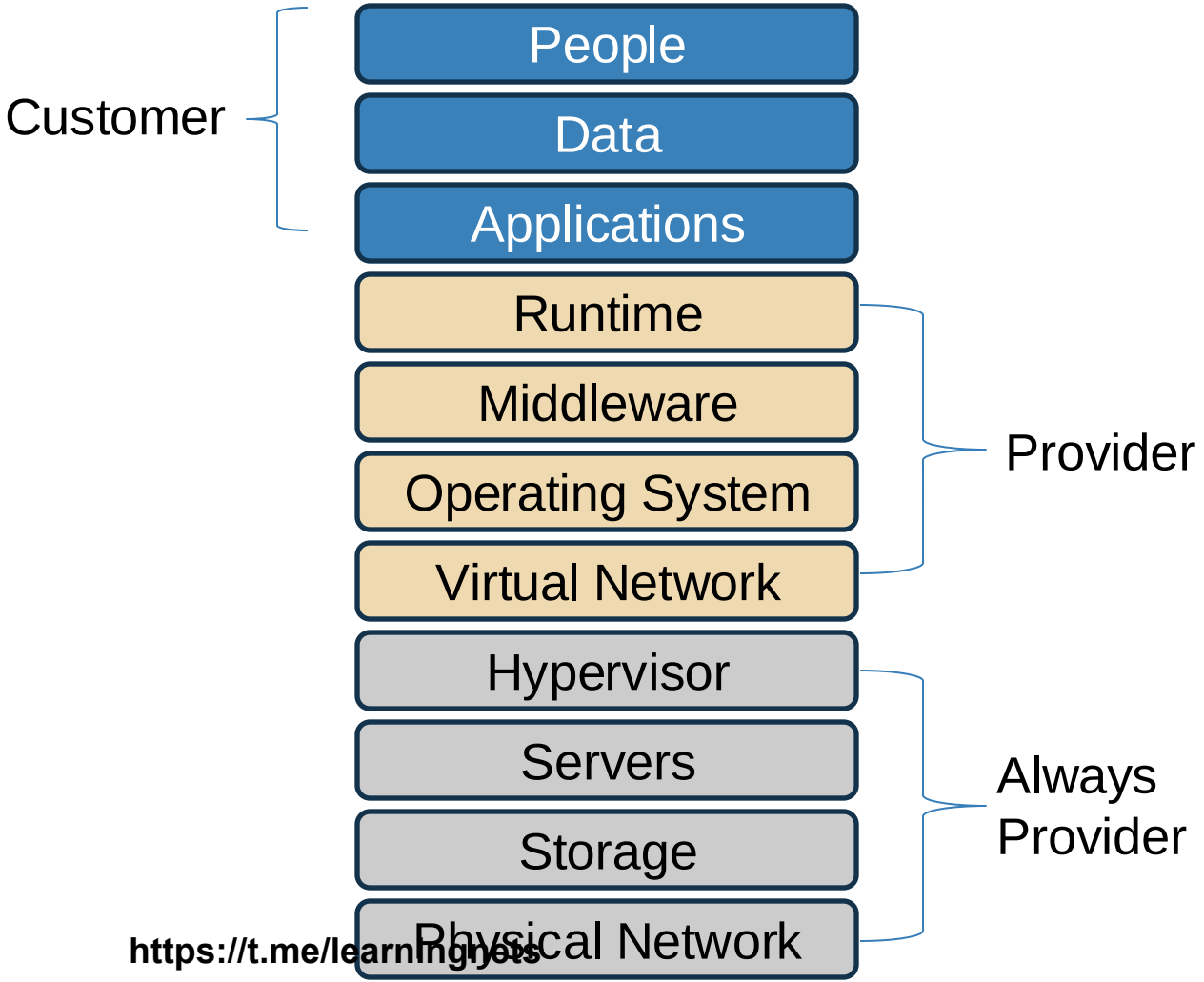
Serverless Architecture



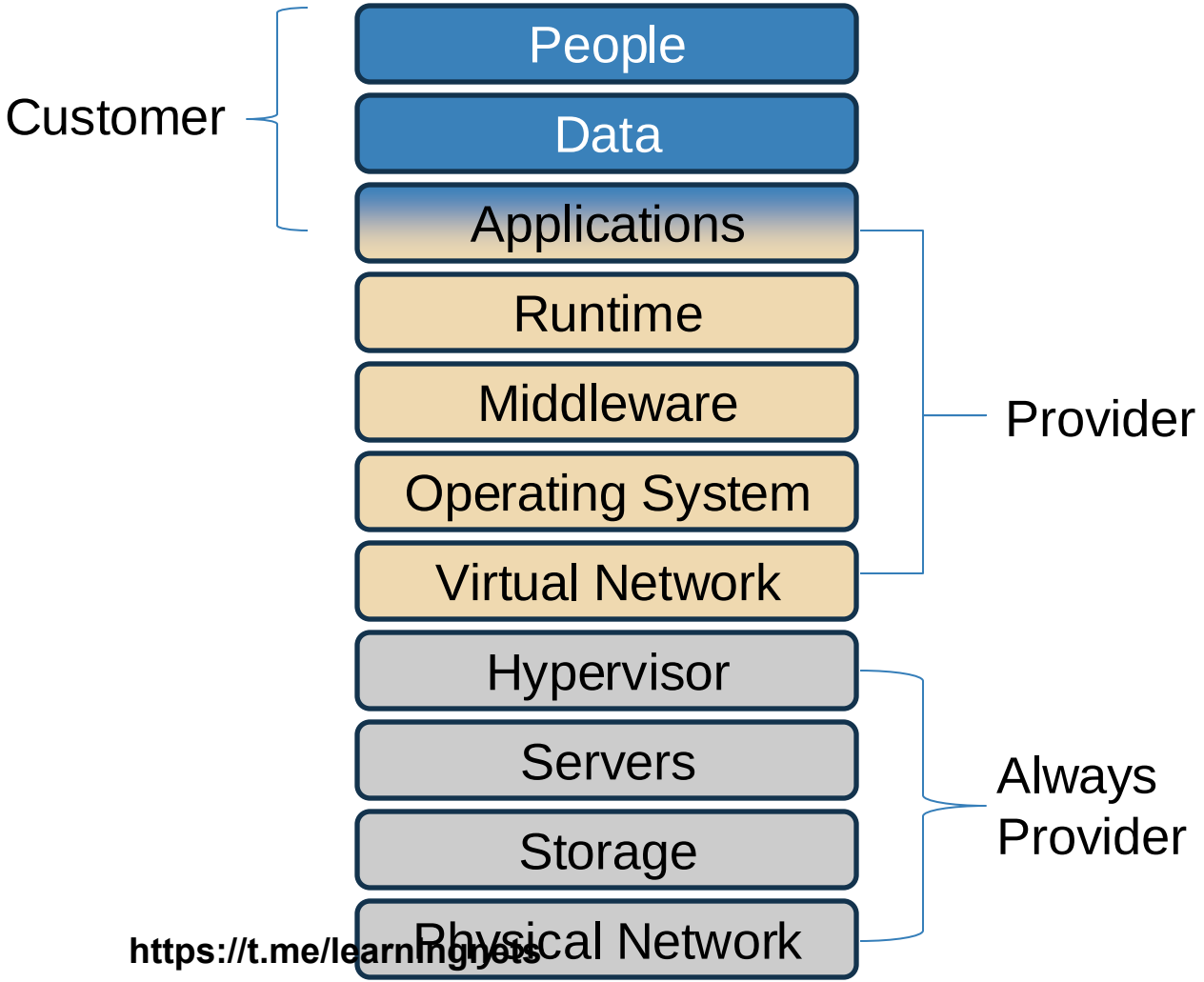
Serverless Benefits

- Scalability
- Deployment / Redeployment
- Consumption-based billing
  - Some traditional cloud services have a serverless option – i.e. databases

PaaS Shared Responsibility



Serverless Shared Responsibility



Serverless Security

Increasing Attack Surface*

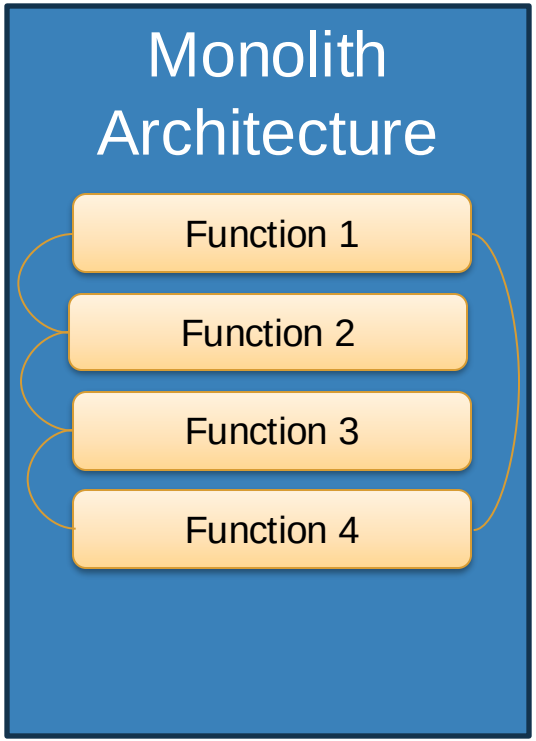
*Increasing opacity

Container Orchestration

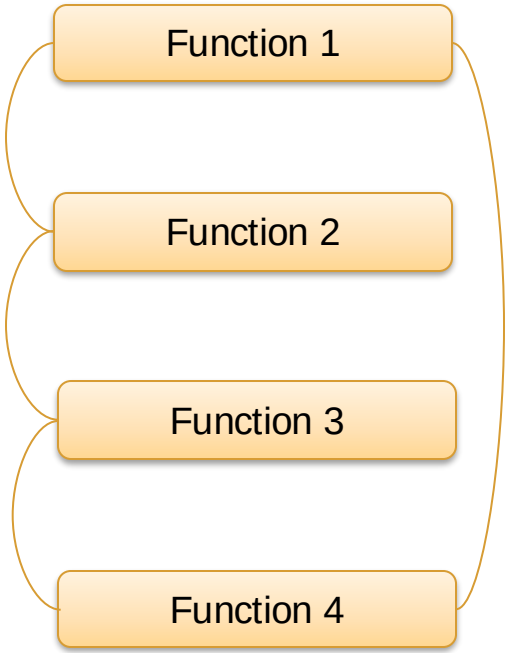
Topics:

- Container Complexity
- Container Orchestration
- Cloud Container Management

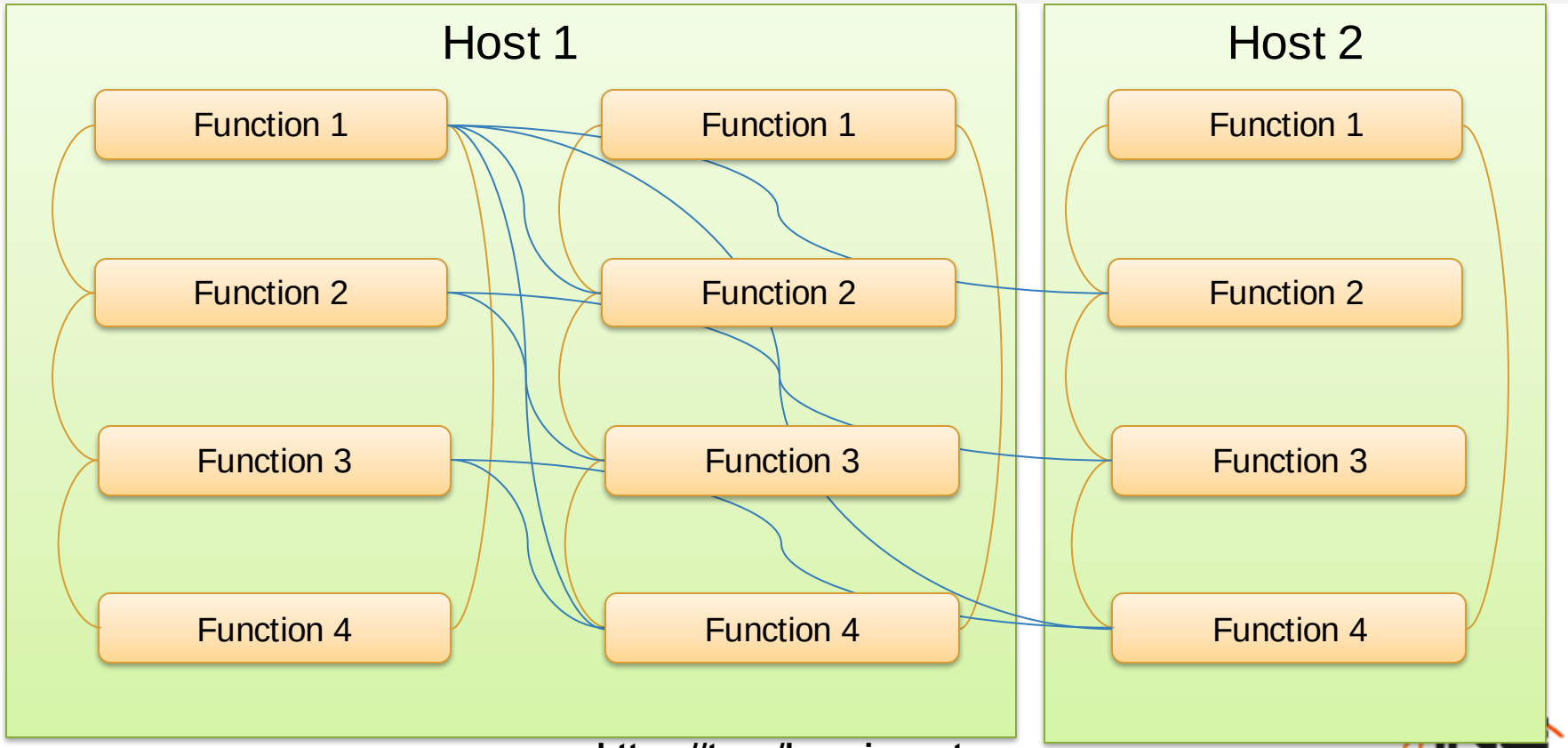
Container Complexity



Container Complexity



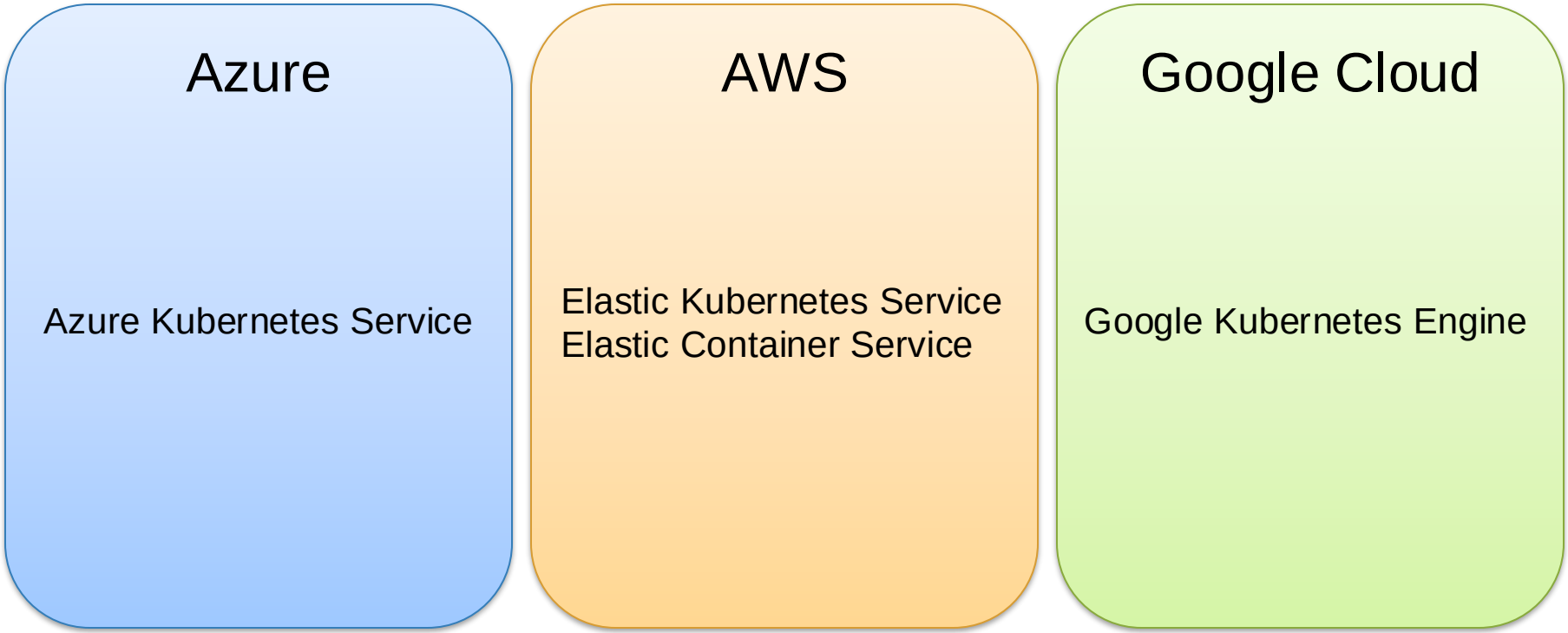
Container Complexity



Container Orchestration

- Single system for managing container hosting
  - Physical (or virtual) cluster
  - Container deployment
  - Scaling – cluster and containers
  - Networking
  - Availability
  - Security and IAM
- Frameworks
  - Kubernetes
  - Docker Swarm
  - Apache Mesos
  - Nomad

Cloud Container Orchestration

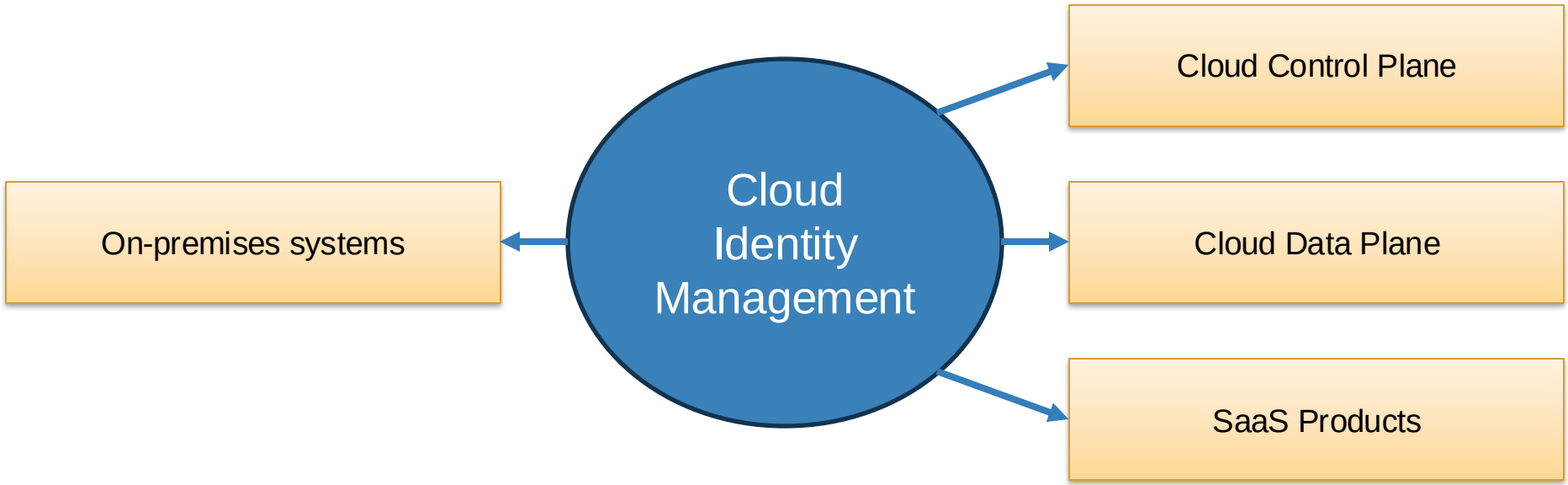


Cloud Security Requirements

Topics:

- Identity and Access control
- Regulatory Compliance
- Provider Responsibilities
- Shared Responsibilities

Identity and Access Management



Regulatory Compliance

- Shared responsibility
- Common regulations and frameworks
  - ISO/IEC 27002
  - EU-US Privacy Shield framework
  - ITIL
  - FEDRAMP
  - COBIT
- Provider needs to document their compliance
  - Major providers have on-line compliance centers
- You need to understand the compliance auditing process
- You need to know what you are responsible for

Provider Responsibility

- Secure facilities
- Employee training
- Separation

Shared Responsibilities

- Encryption
- SLAs
- Long-term viability
- Breach liability
- DR/BRP – regions/availability zones
- Data classification

Cloud Security Threats

Topics:

- Cloud Security Threats
- Multi-tenancy
- Hypervisor
- Virtual Machine metadata

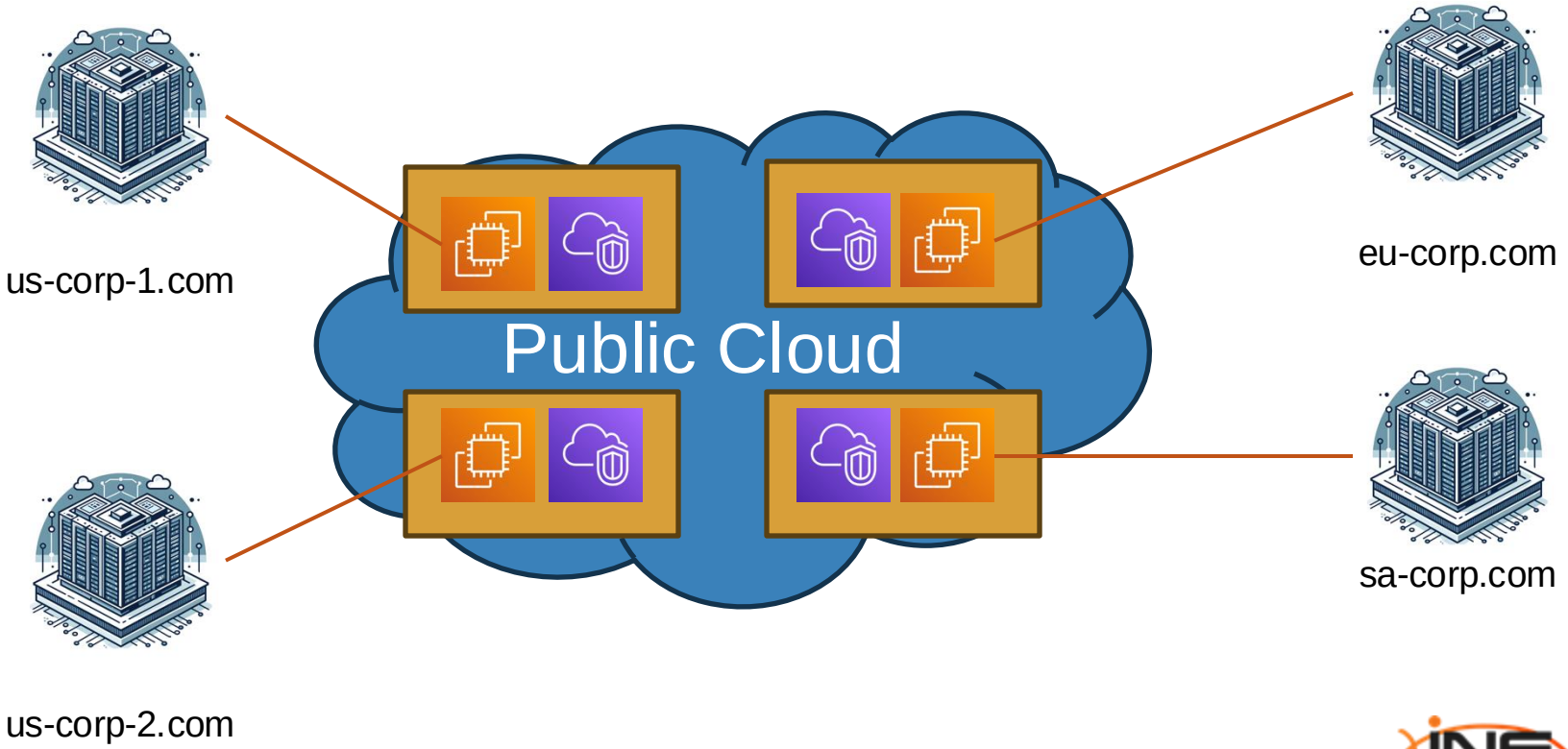
Cloud Security Threats

- Denial of Service (DoS)
- Session Hijacking
- DNS attacks
- Cross site scripting
- Multitenancy/shared technology
- Hypervisor attacks
- VM attacks (metadata service)
- Cross site forgery
- SQL injection
- Session riding
- DDoS
- Man in the middle
- Side channel
- Authentication
- API attacks

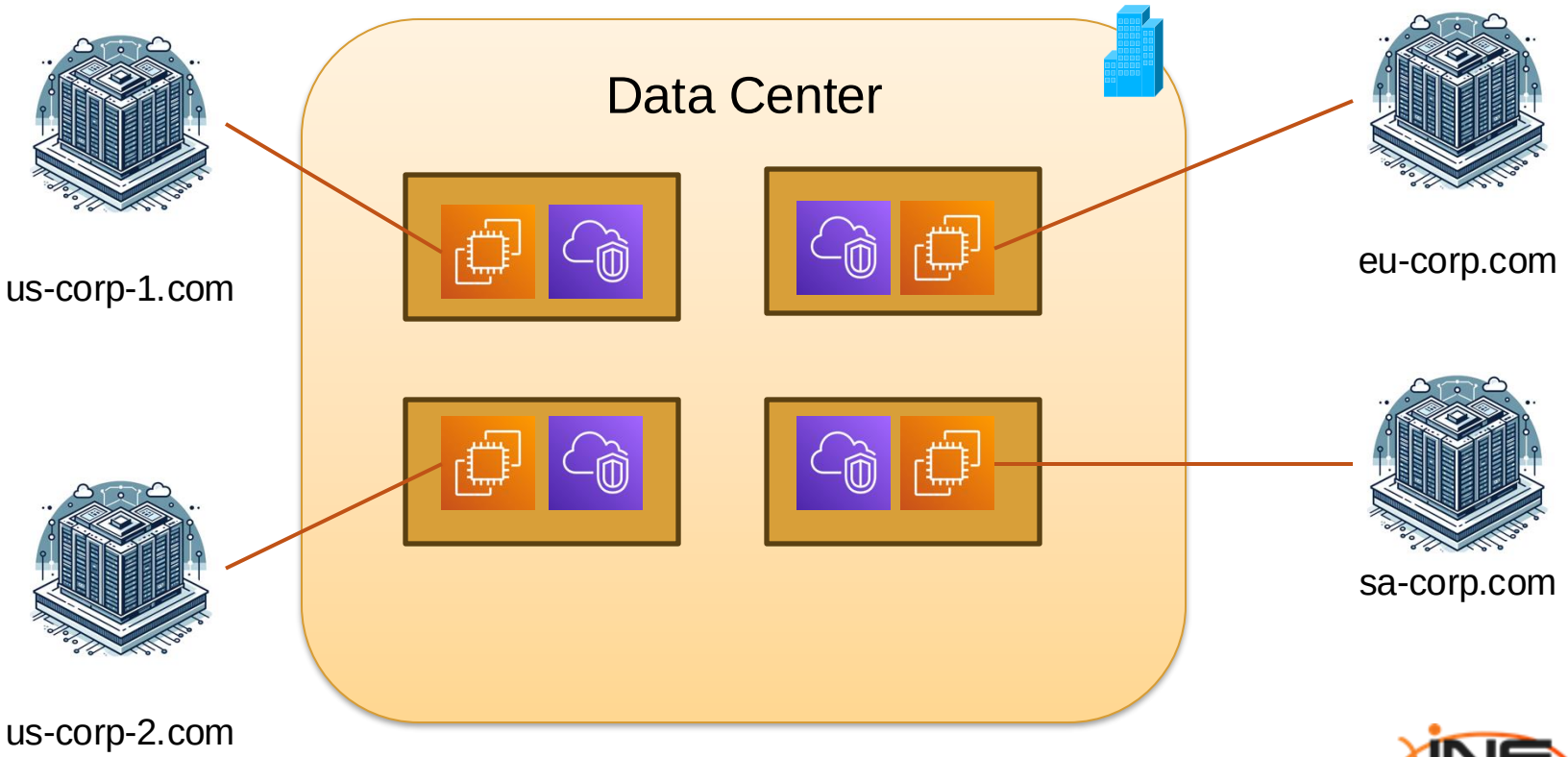
Cloud Security Threats

- Denial of Service (DoS)
- Session Hijacking
- DNS attacks
- Cross site scripting
- Multitenancy/shared technology
- Hypervisor attacks
- VM attacks (metadata service)
- Cross site forgery
- SQL injection
- Session riding
- DDoS
- Man in the middle
- Side channel
- Authentication
- API attacks

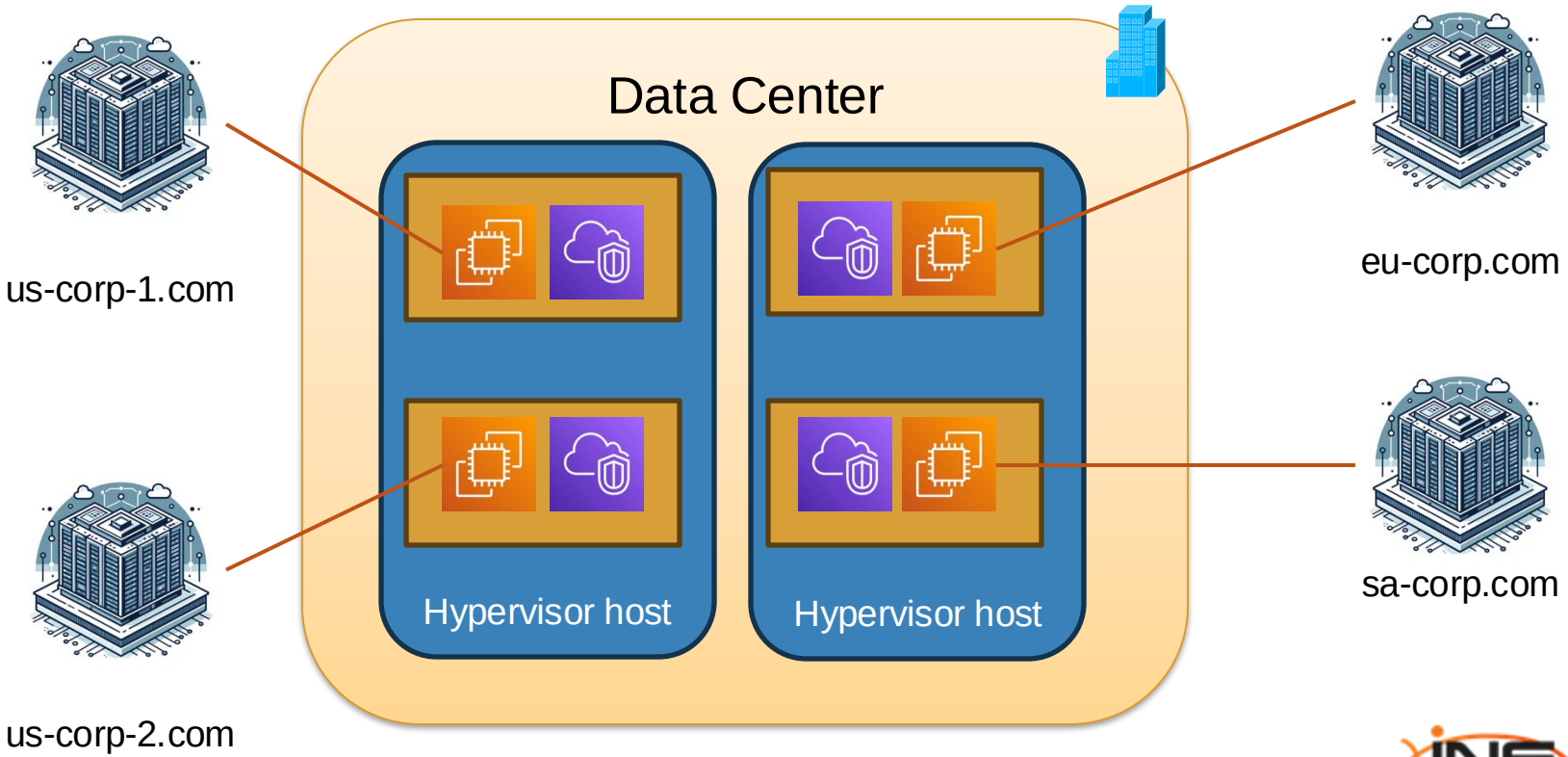
Multitenancy/Shared Technology



Multitenancy/Shared Technology

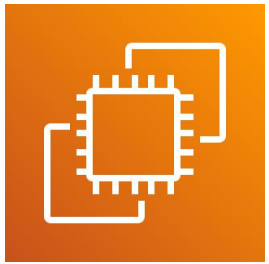


Hypervisor Attack

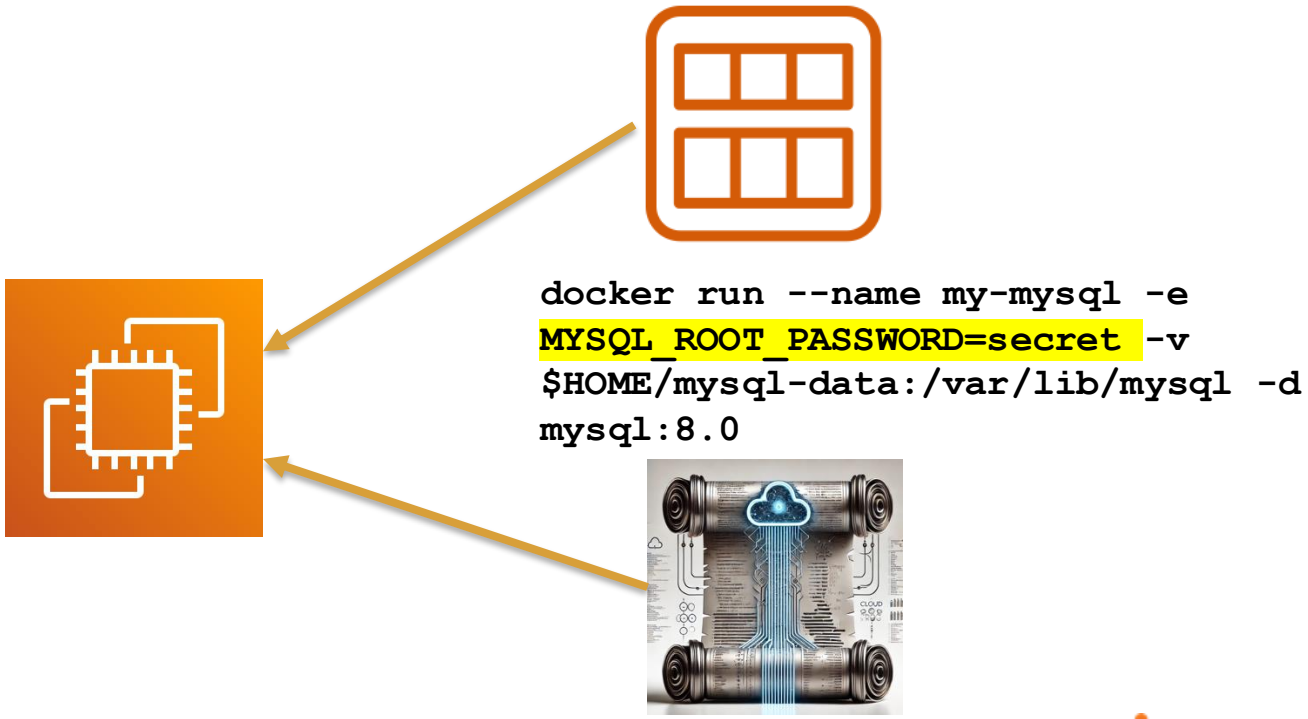


VM (Metadata) Attack

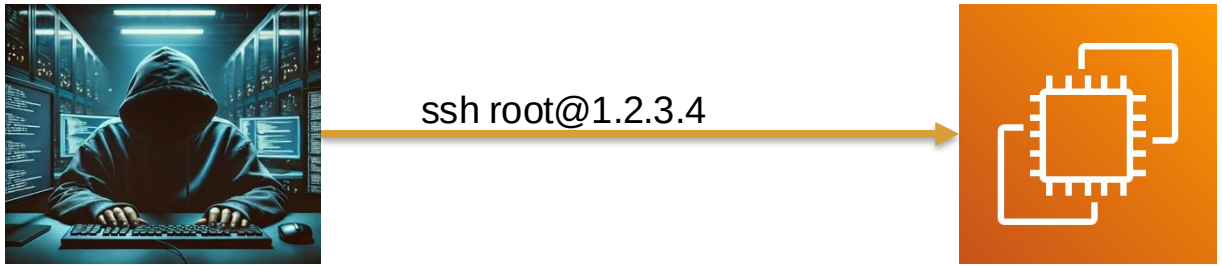
MySQL server for production database



VM (Metadata) Attack

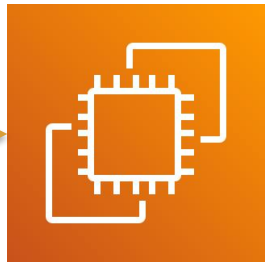


VM (Metadata) Attack



VM (Metadata) Attack

ssh root@1.2.3.4

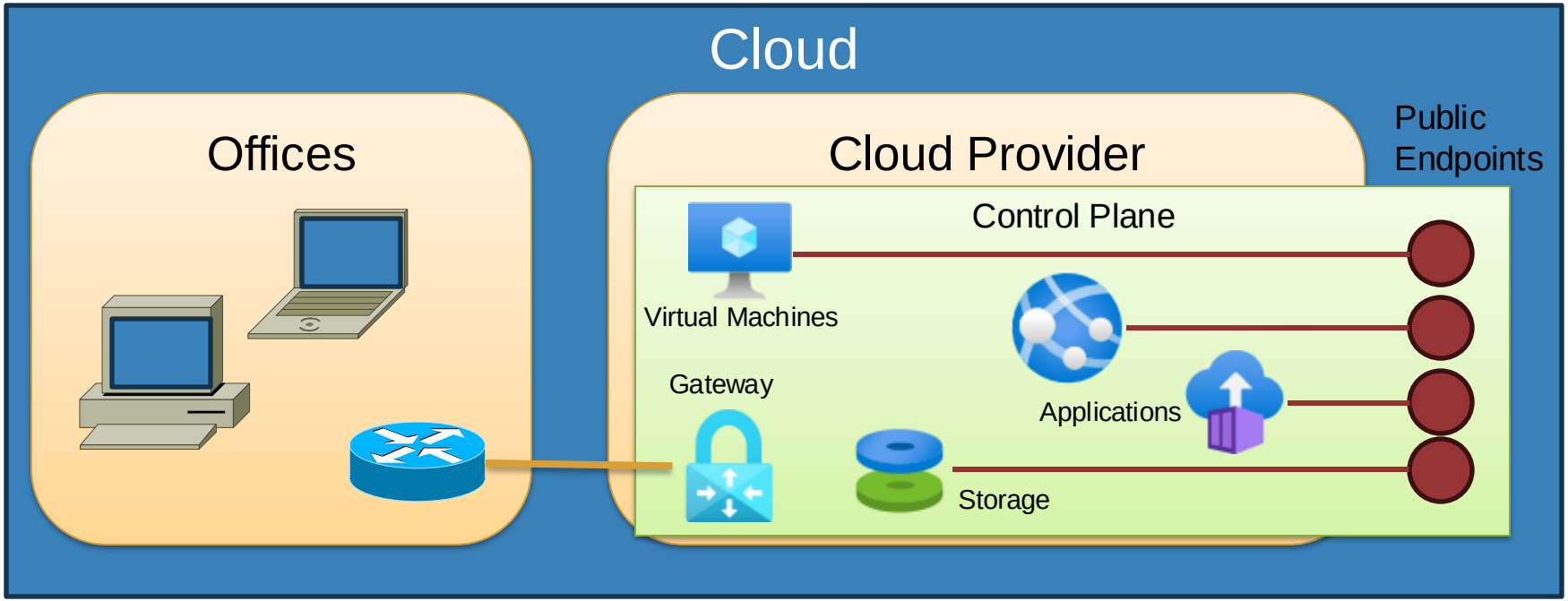


```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" ... ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-data
```

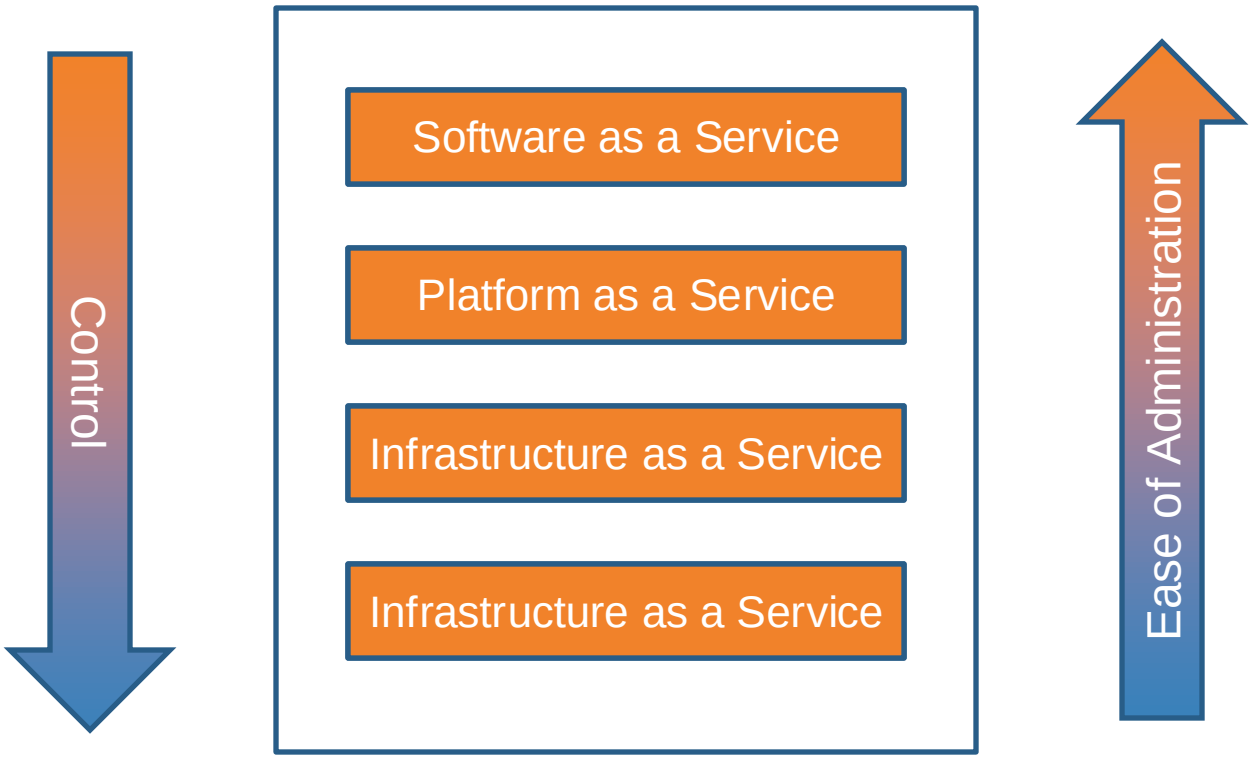
```
docker run --name my-mysql -e
MYSQL_ROOT_PASSWORD=secret -v
$HOME/mysql-data:/var/lib/mysql -d
mysql:8.0
```

Cisco CyberOps Introduction to Cloud Security

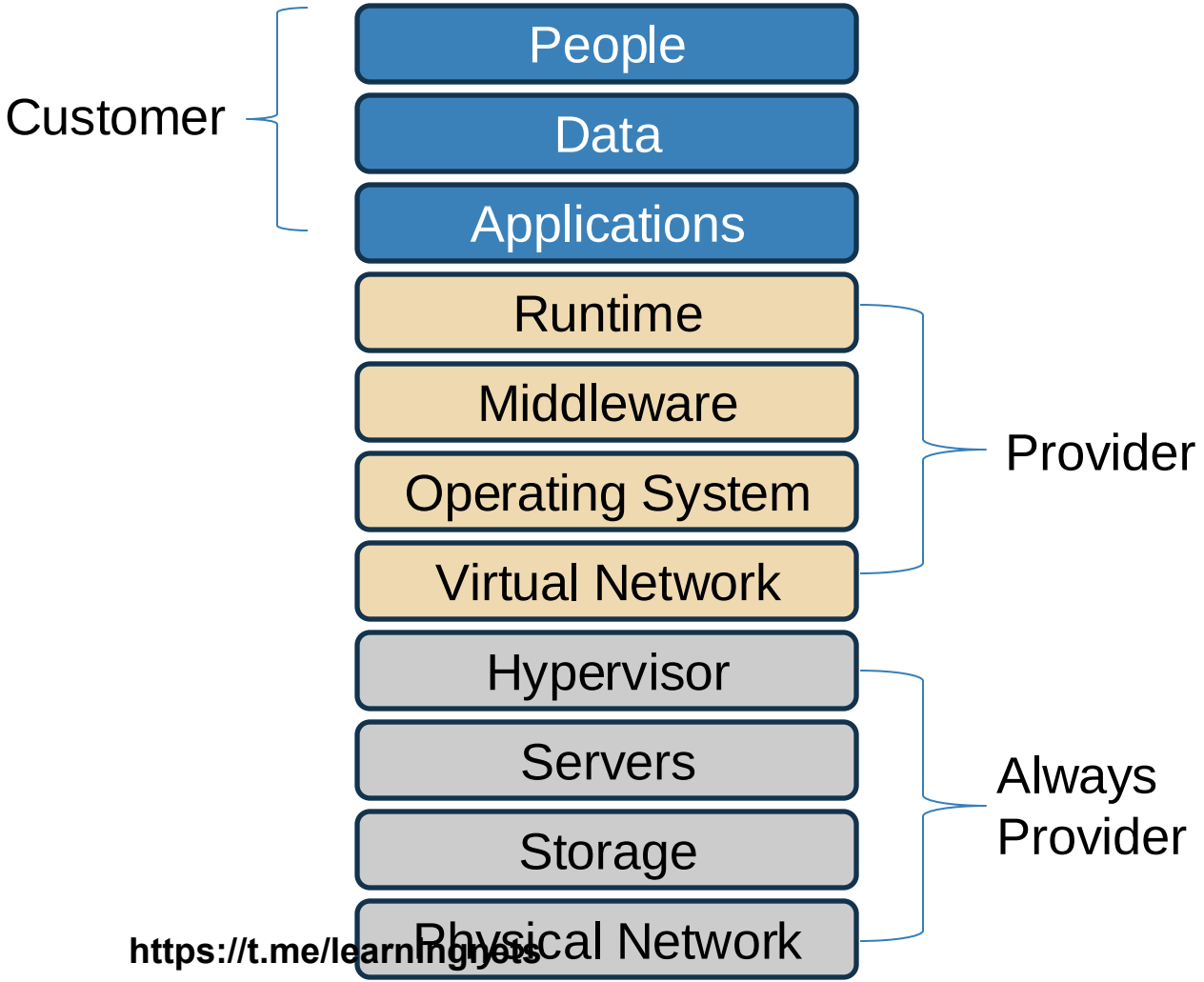
What is the Cloud?



Types of Cloud Services



PaaS Shared Responsibility



Cloud Security Tools

Azure

Defender 365
Microsoft Defender for Cloud
Microsoft Sentinel

AWS

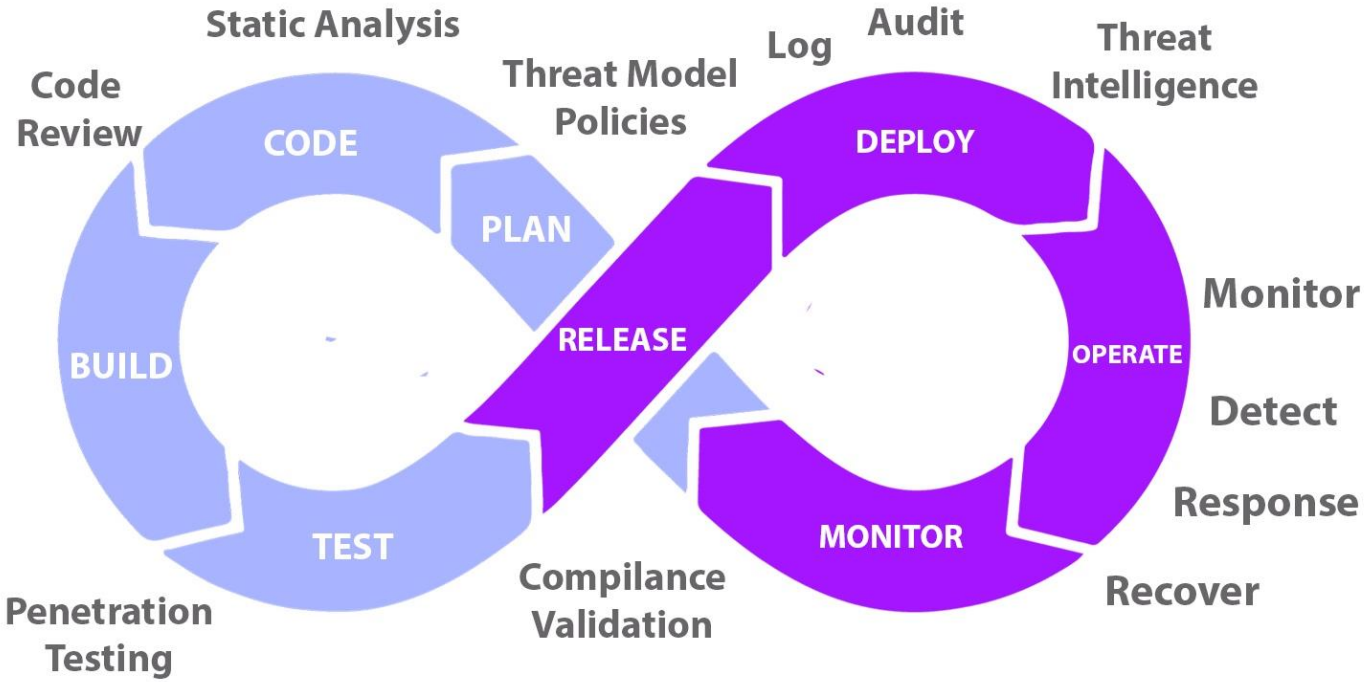
AWS Guard Duty

Google Cloud

Security Command Center

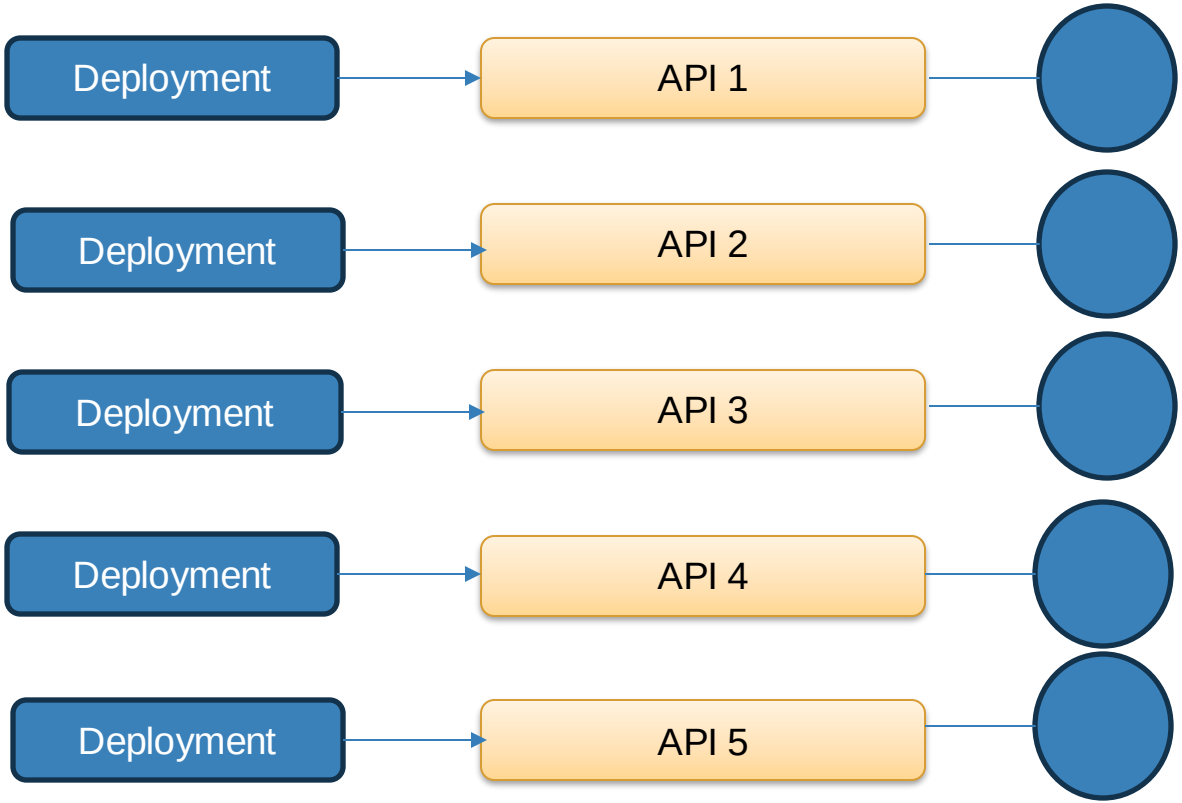
All platforms have network protection and compute protection and support third party security solutions

DevSecOps

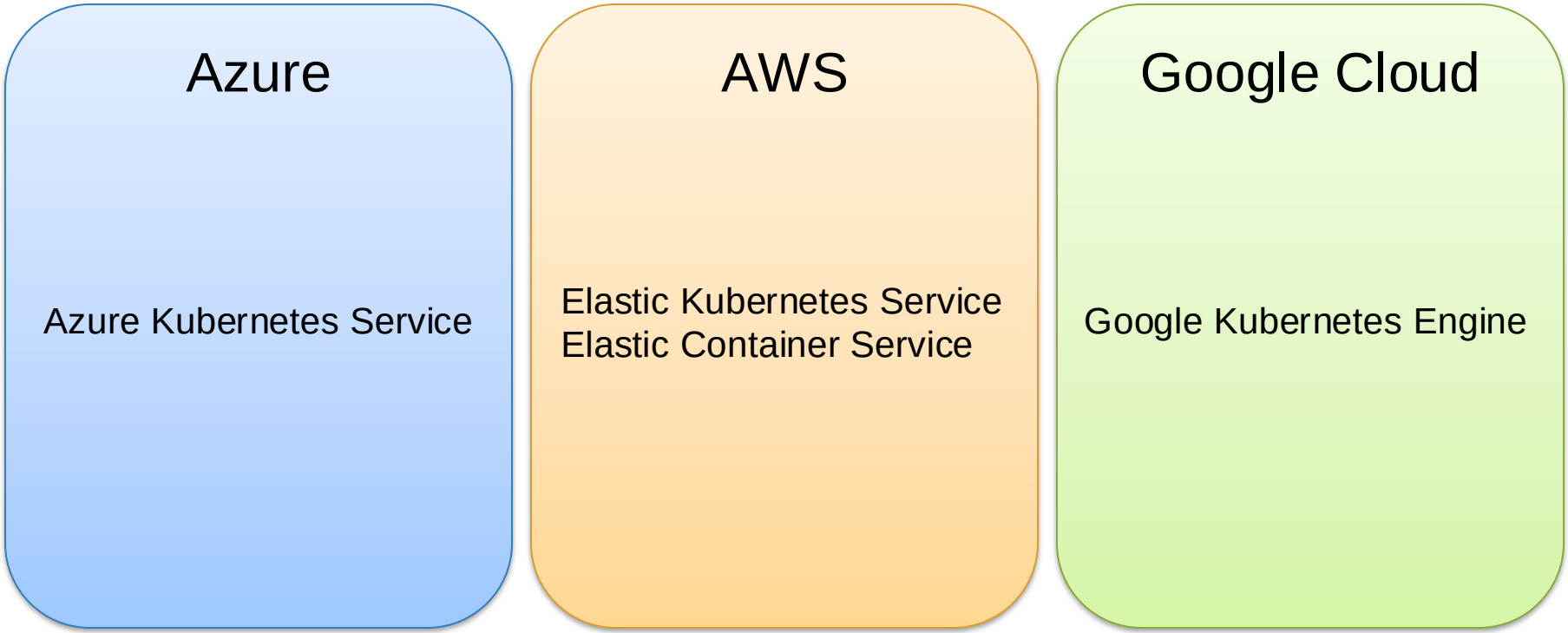


https://kodershop.com/wp-content/uploads/2023/03/DevSecOps.jpg

Serverless Architecture



Cloud Container Management



Regulatory Compliance

- Shared responsibility
- Common regulations and frameworks
  - ISO/IEC 27002
  - EU-US Privacy Shield framework
  - ITIL
  - FEDRAMP
  - COBIT
- Provider needs to document their compliance
  - Major providers have on-line compliance centers
- You need to understand the compliance auditing process
- You need to know what you are responsible for

Cloud Security Threats

- Denial of Service (DoS)
- Session Hijacking
- DNS attacks
- Cross site scripting
- Multitenancy/shared technology
- Hypervisor attacks
- VM attacks (metadata service)
- Cross site forgery
- SQL injection
- Session riding
- DDoS
- Man in the middle
- Side channel
- Authentication
- API attacks

Introduction to Cloud Security - Summary

Key Concepts - Recap

- Cloud Concepts
- Cloud Security
- Cloud Compute
- Cloud Workload Security

Learning Outcomes Recap

+ Understand the fundamental concepts of cloud computing, including the definition and characteristics.
+ Describe the various cloud deployment models: Public, Private, Hybrid, and Community.
+ Define the shared responsibility model in cloud computing.
+ Understand the integration of DevOps practices with cloud technologies
+ Identify the key security requirements for cloud deployments.
+ Recognize common cloud security threats

Next Steps

- Continue the CyberOps Associate learning path
- Dive into our Cloud and Cloud security content
- Get hands-on with plenty of cloud security labs in Skill Dive

Conclusion

Thank you!

EXPERTS AT MAKING YOU AN EXPERT