

A unique opportunity for you to be mentored by Amazonians



Batch 04

Week 2

15-July-2023



# Today's Session

Week 2  
15-July



# Virtualization Analogy



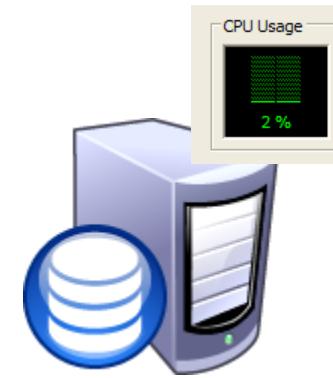
# Legacy Datacentre

1:1 Mapping

One Application : One Server



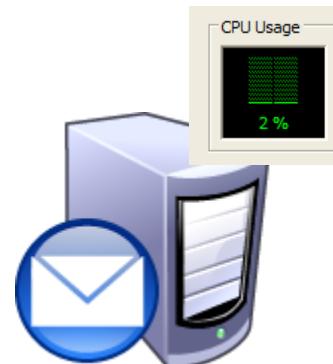
Web Server



Database Server



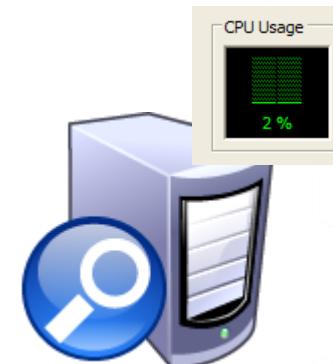
Active Directory



Mail Server



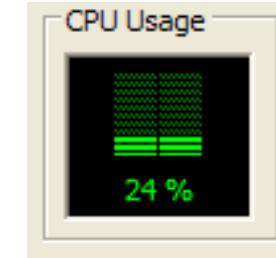
Print Server



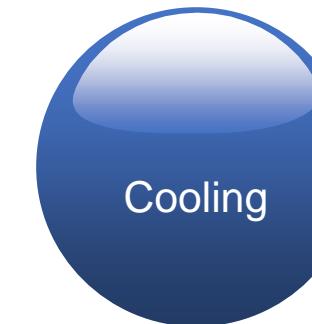
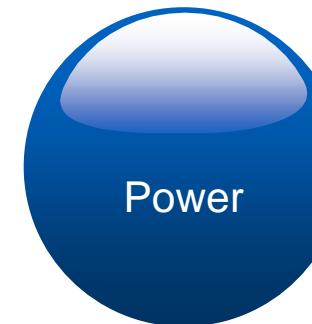
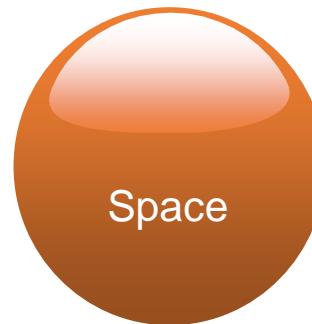
Search Server

# Legacy Datacentre

Low utilized servers



All require...



# Users care about applications



# What is required to run an application?

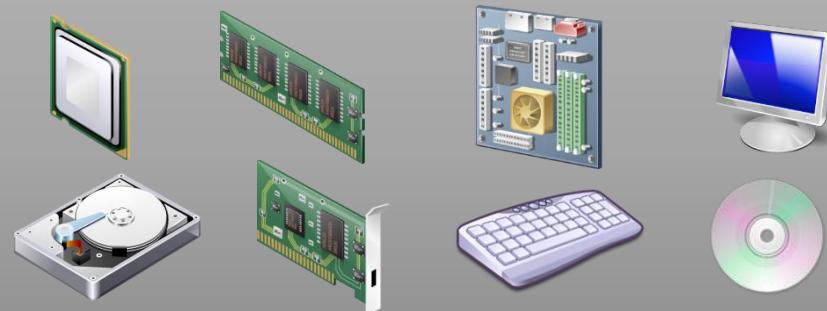
## Application



## Operating System



## Hardware Resources



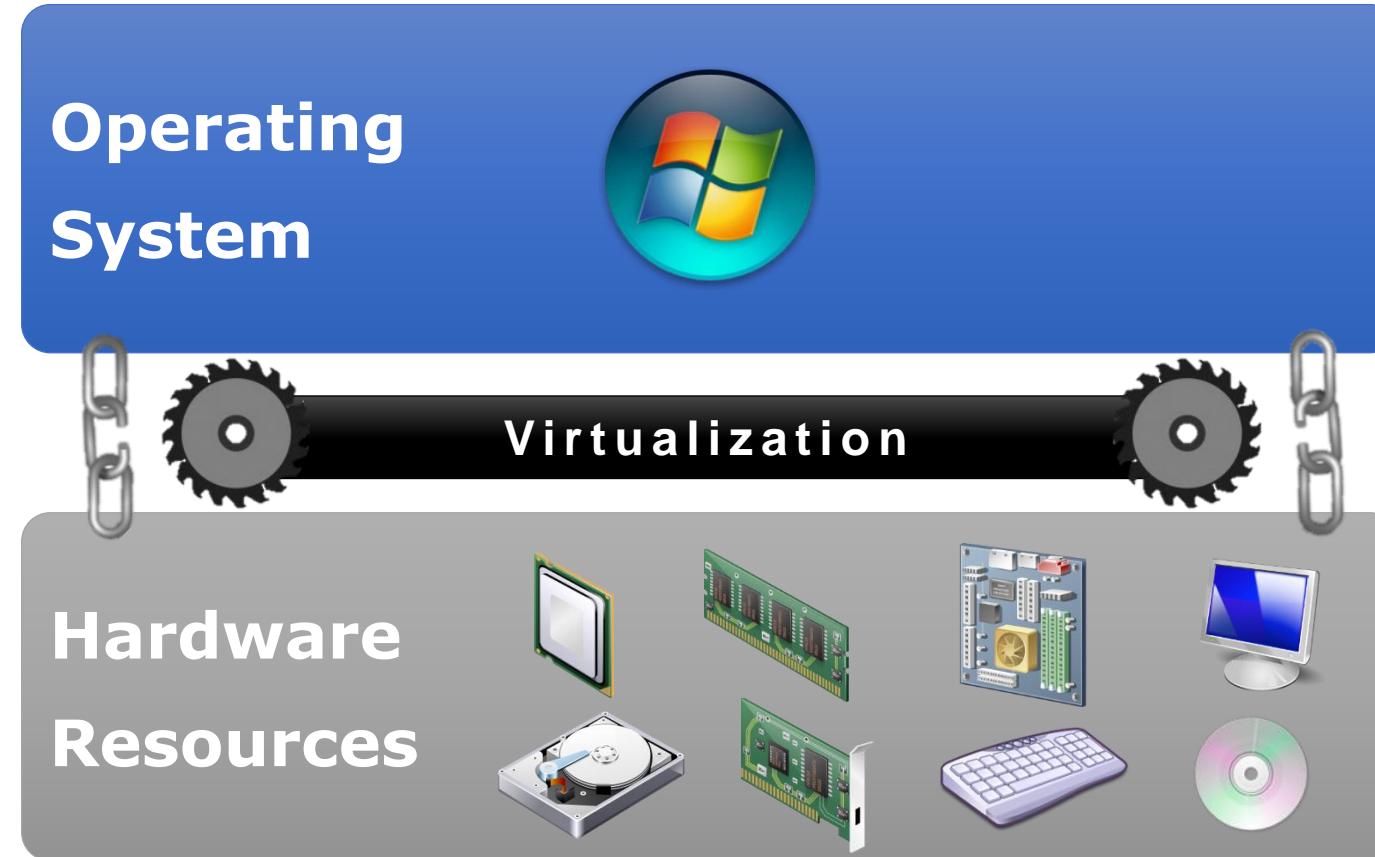
# Traditional Approach

- In traditional approach hardware is coupled with an OS



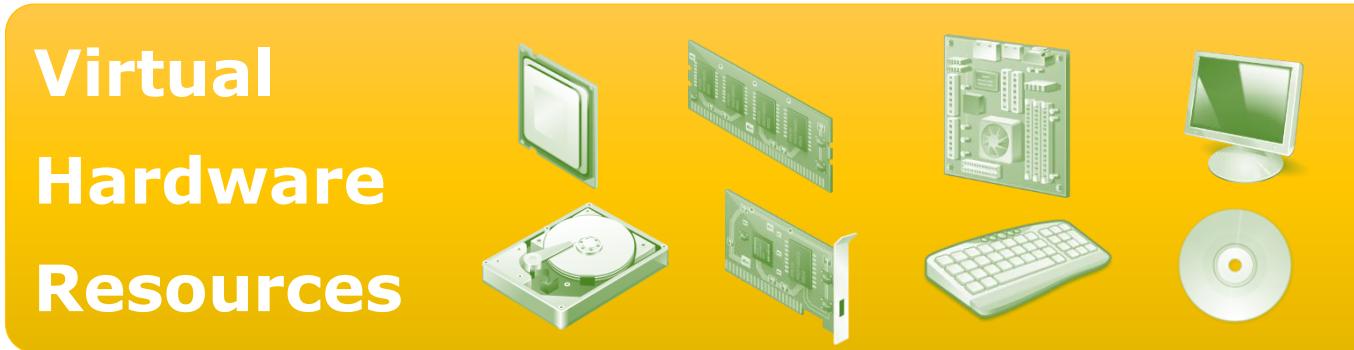
# Virtualization Approach

- Virtualization decouples the hardware from OS

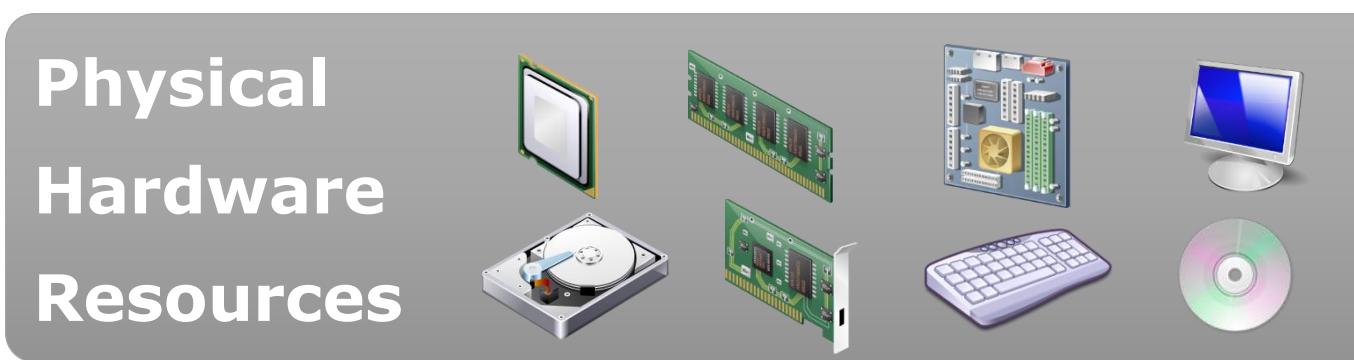


# Virtualization Approach

- It creates virtual hardware resource out of physical hardware resources

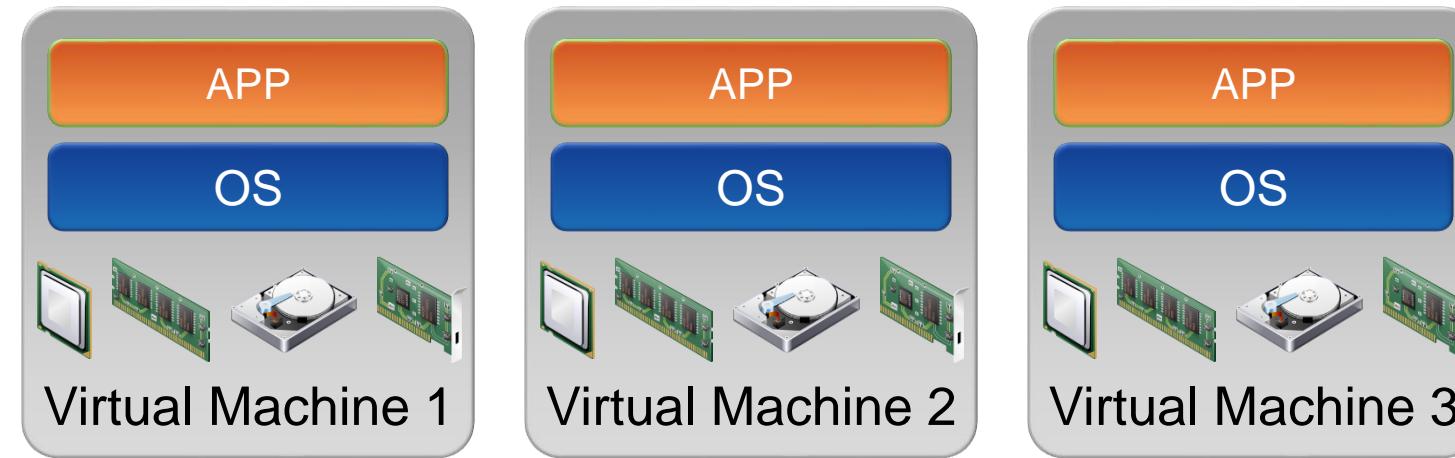


Virtualization Layer



# Virtualization Approach

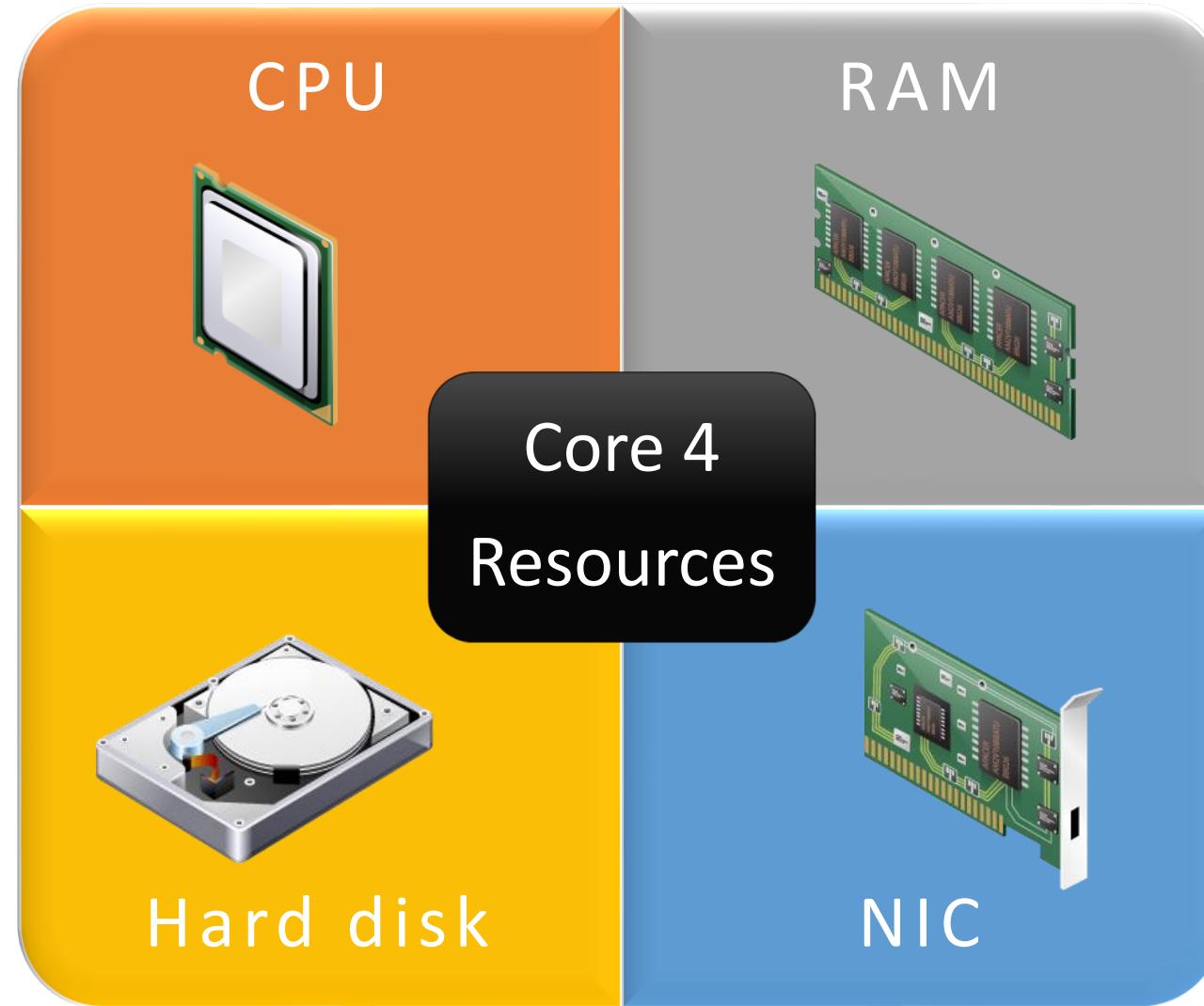
- The virtualized hardware resources can be assigned to different Virtual Machines.



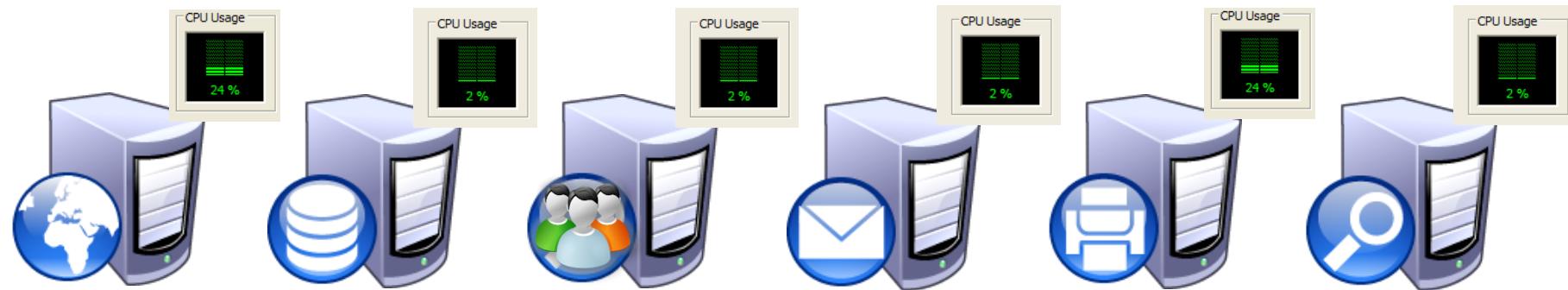
**Virtual  
Hardware  
Resources**



# Virtualization Approach



# Virtualization Approach



After Virtualization



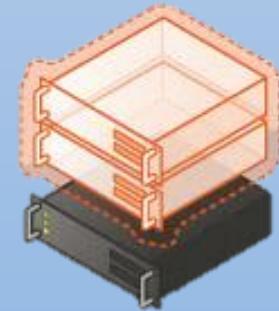
# Enablers for Virtualization

- Decreasing cost of Powerful Hardware

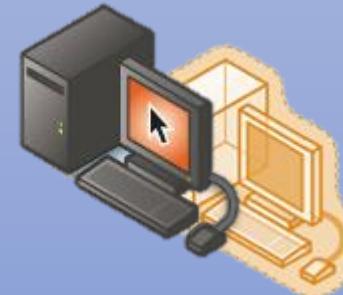


# Types of Virtualization

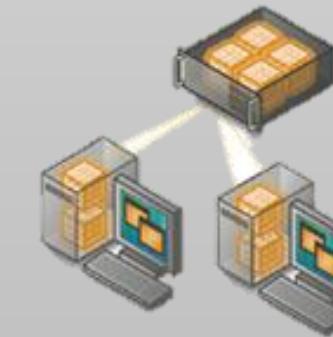
Server Virtualization



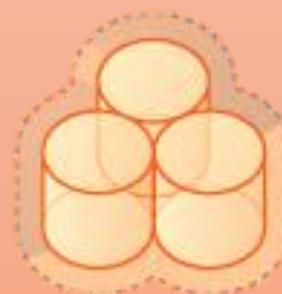
Desktop Virtualization



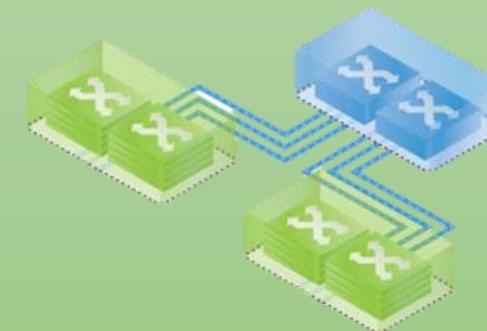
Application Virtualization



Storage Virtualization

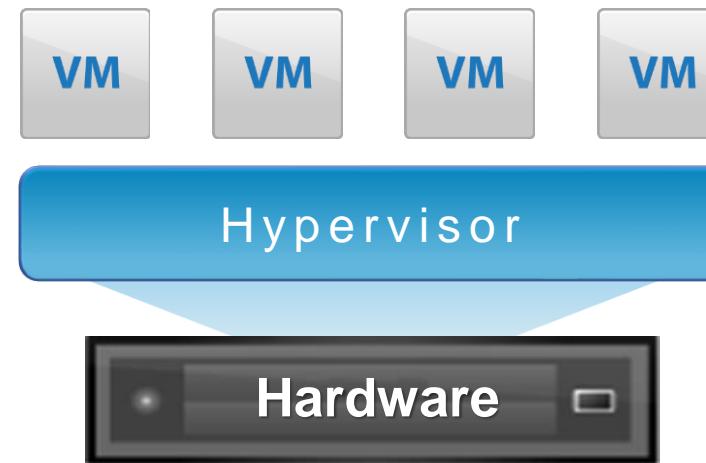


Network Virtualization



# Hypervisor

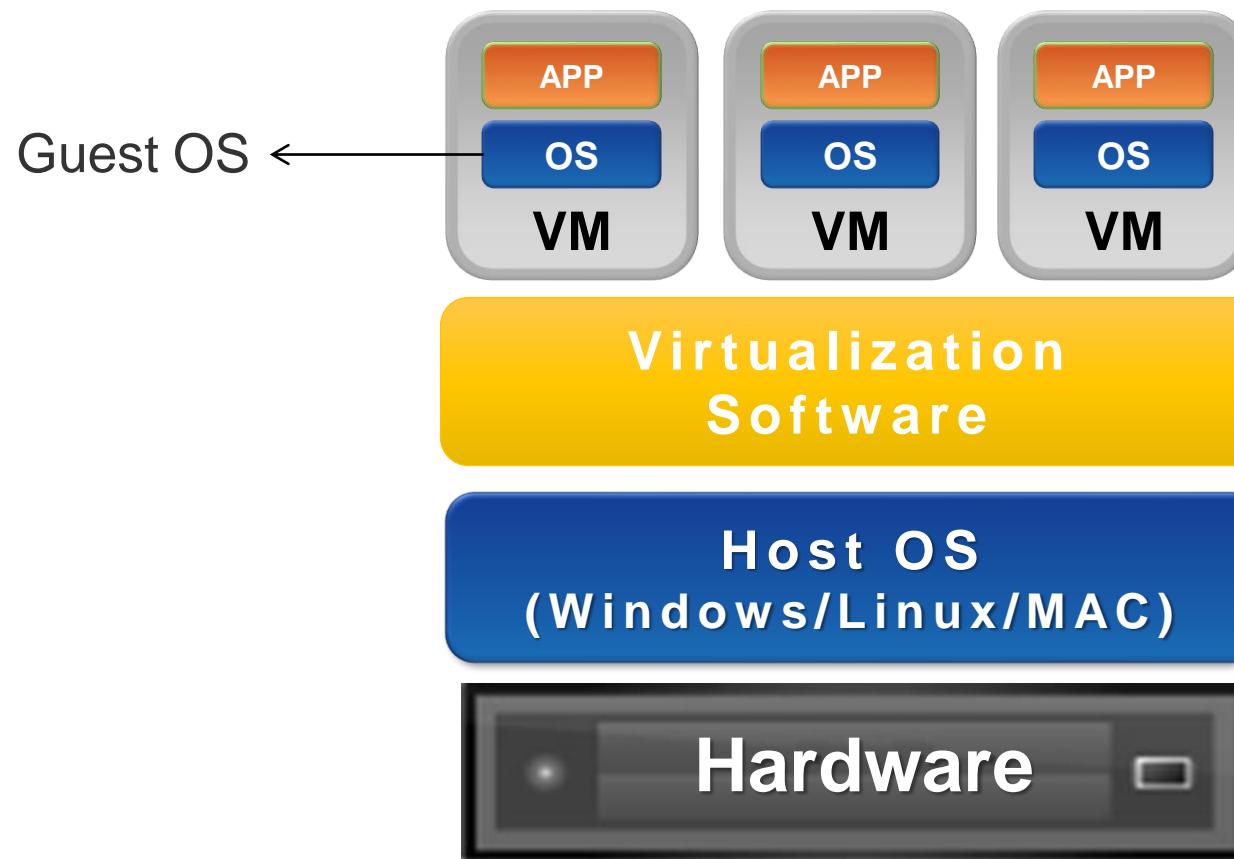
- A program that allows multiple operating systems to share a single hardware host.
- Each operating system appears to have the host's processor, memory, and other resources all to itself. However, the hypervisor is actually controlling the host resources.



- Also known as Virtualization Layer, Virtual Machine Manager (VMM)

## Type 2 Hypervisor – Host OS based (Hosted) Hypervisor

- A host-based virtualization system requires an operating system (such as Windows or Linux) to be installed on the computer.
- It runs as an application on the Host Operating System



## Type 1 Hypervisor – Bare-Metal Hypervisor

- A bare-metal hypervisor system does not require an operating system.
- The hypervisor is the operating system.



# Big Players in Virtualization Space

vmware®

Microsoft

cITRIX®

---

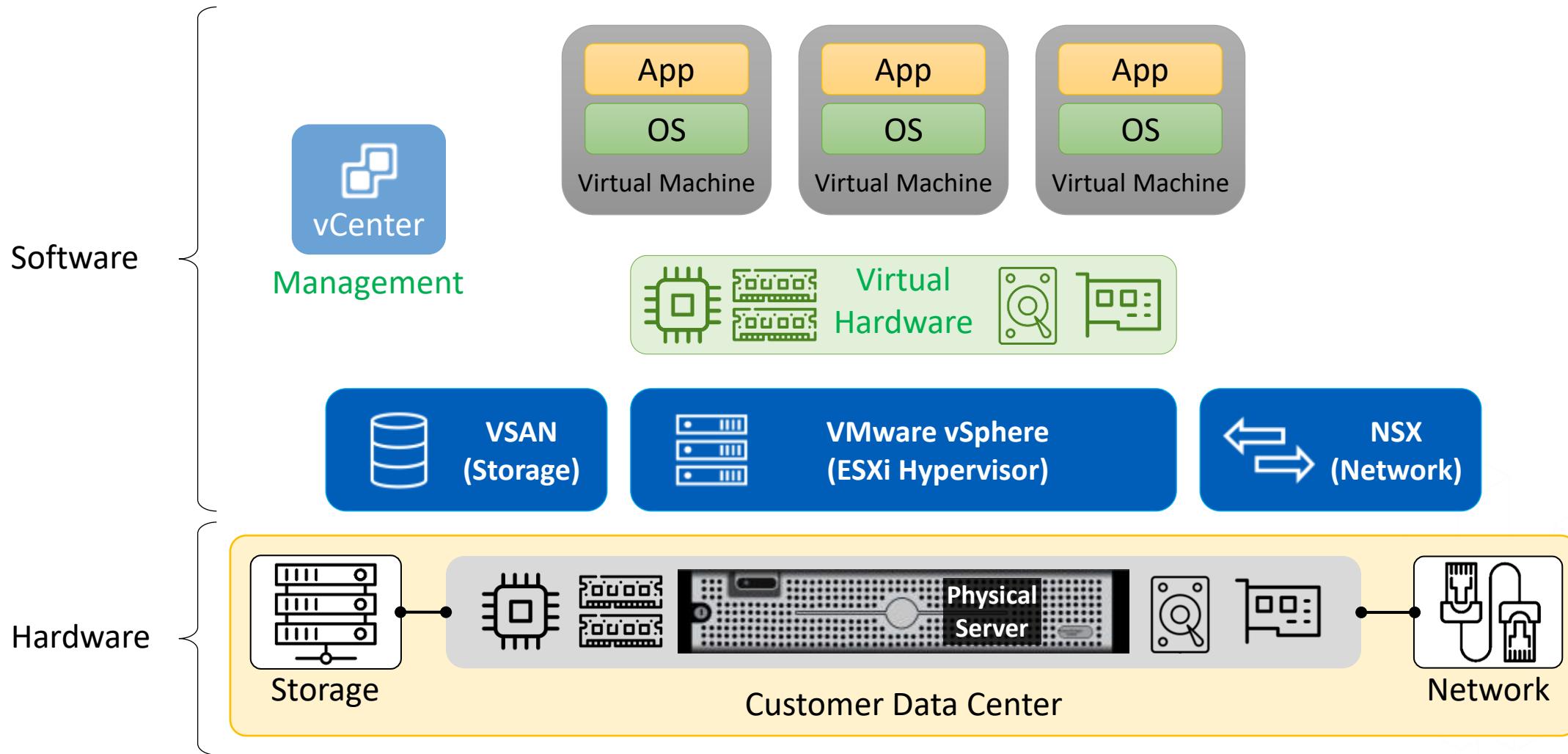
Others

ORACLE®

|| Parallels™

 redhat.

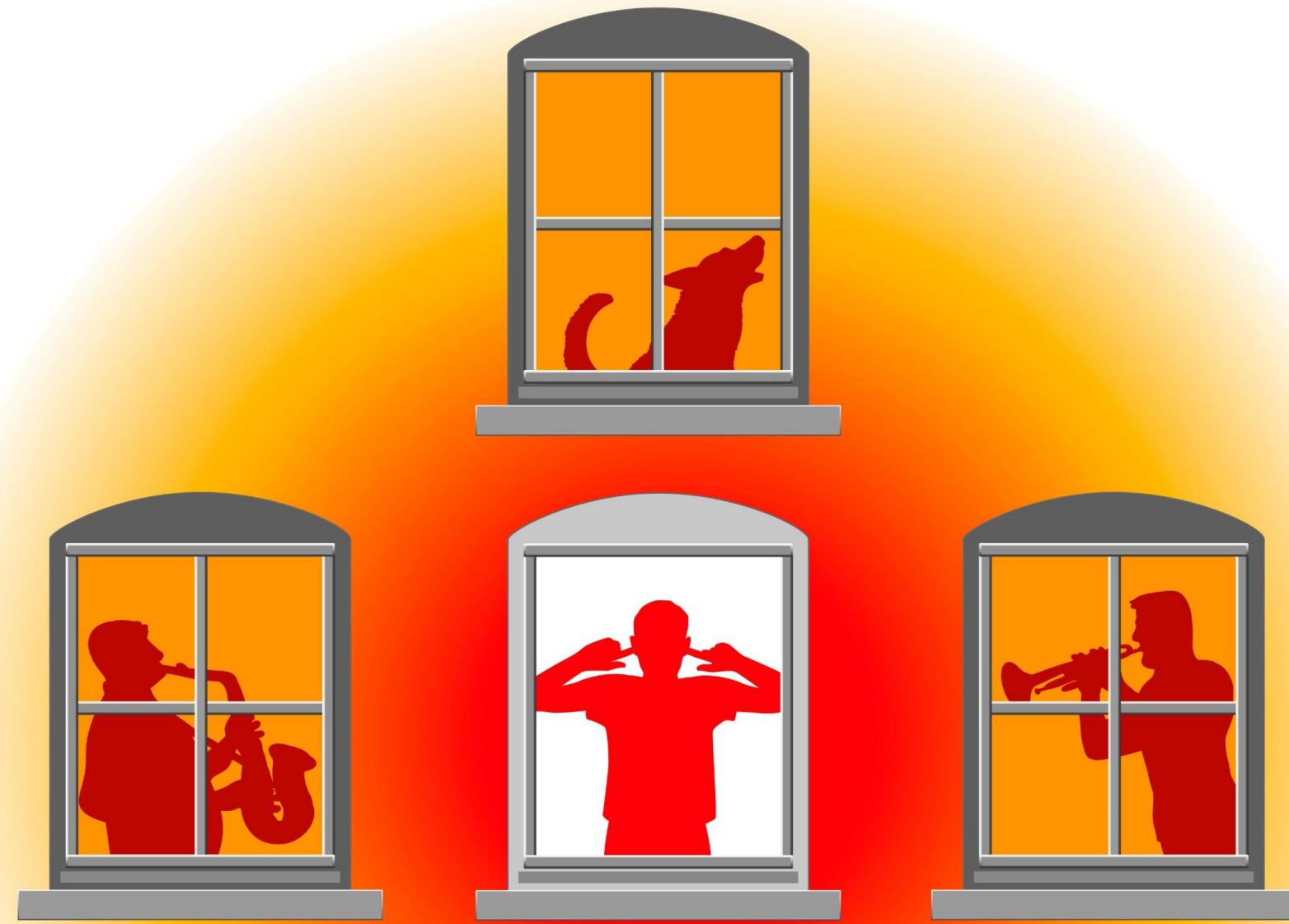
# VMware Software Defined Data Center (SDDC)



## Some challenges



# Noisy neighbours



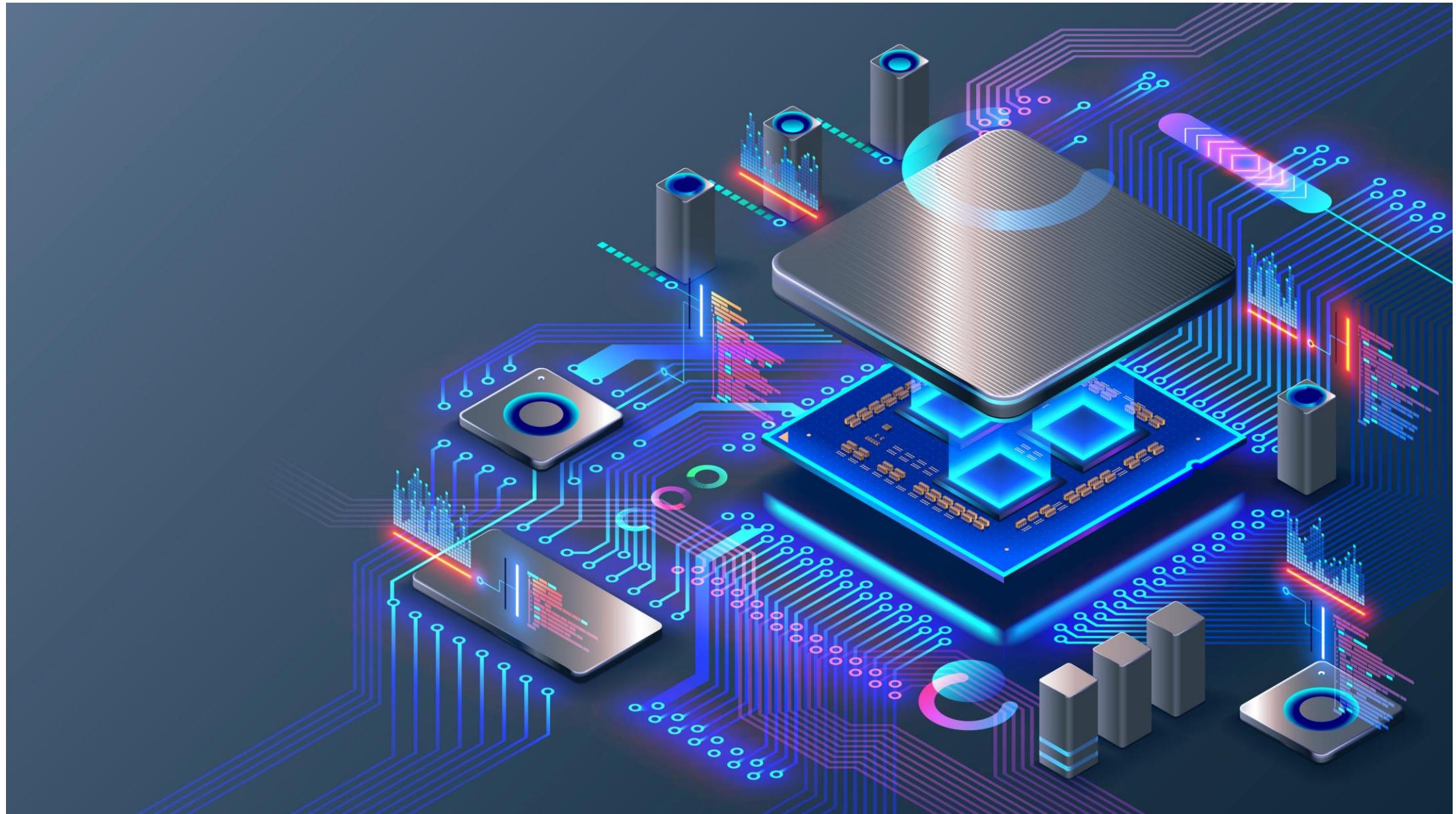
# Management overhead



# Cost



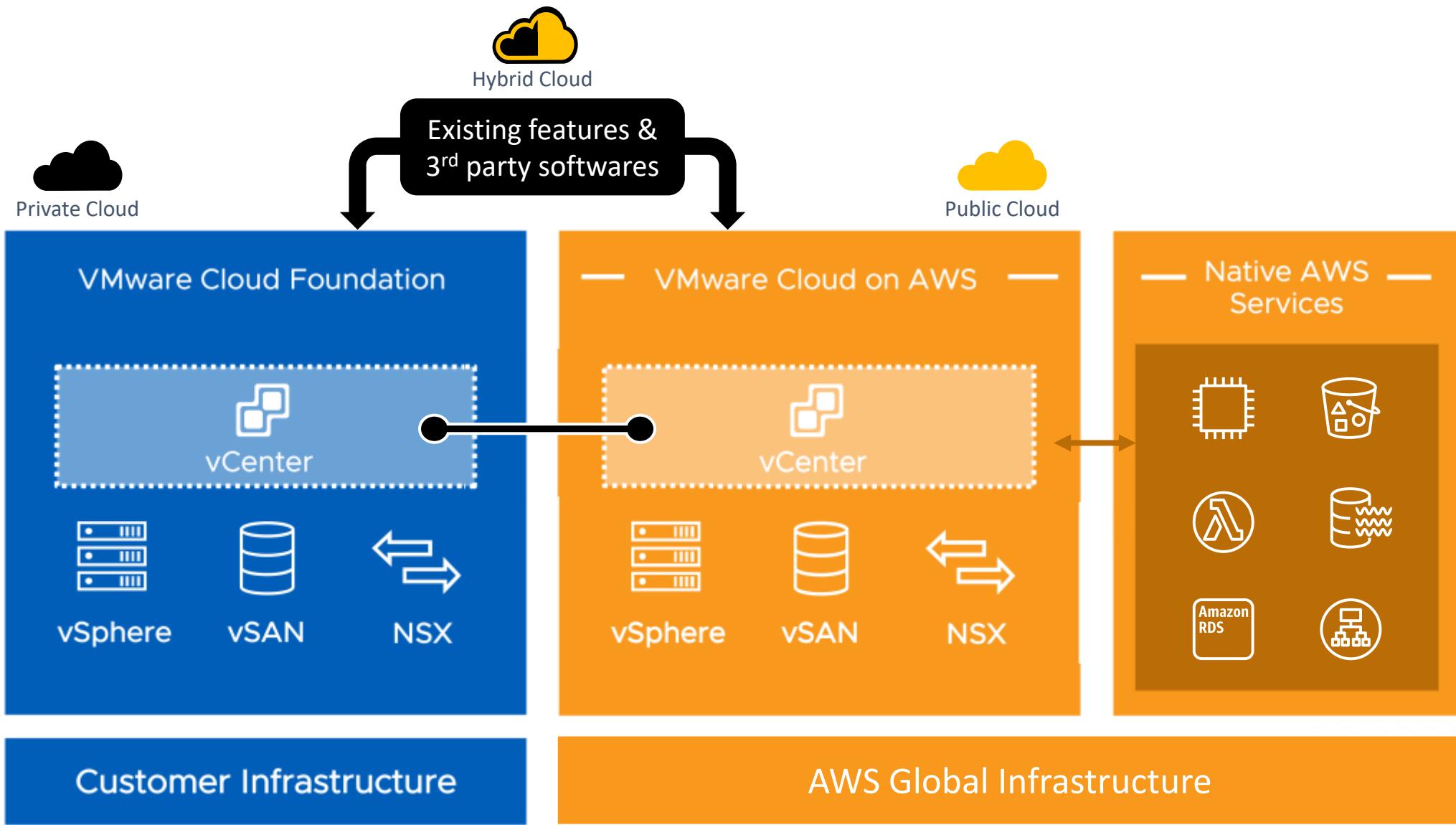
# Apps needing BareMetal access





VMware Cloud on AWS

# VMware Cloud on AWS (VMC on AWS)



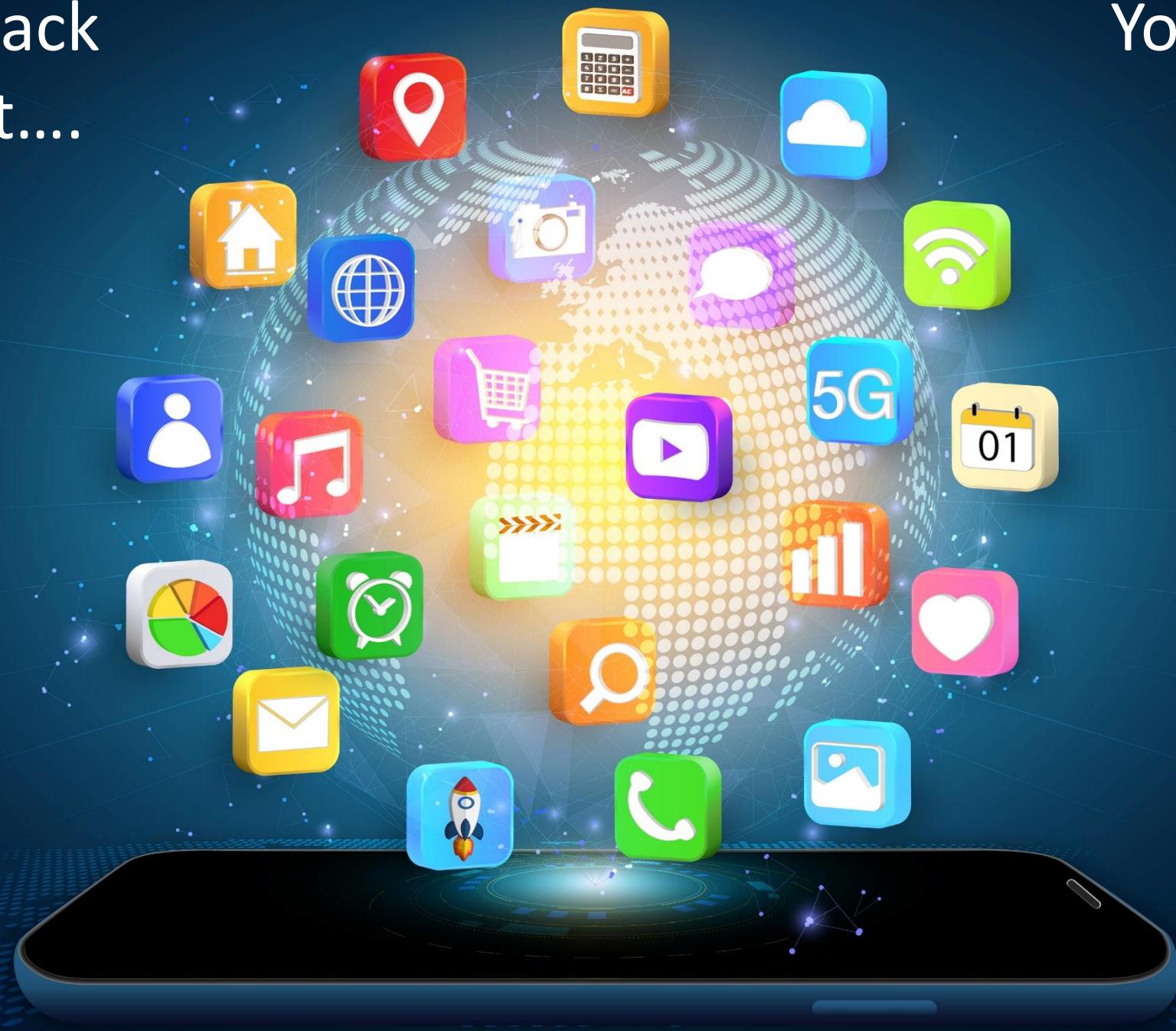


5 Minutes  
Break



If you are back  
type in chat....

Your favourite  
Mobile App



# Security Track

Week 2



# AWS Foundational and Layered Security Services



AWS Security Hub



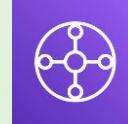
AWS Organizations



AWS Control Tower



AWS Trusted Advisor



AWS Transit Gateway



Amazon VPC



AWS IoT Device Defender



Amazon Cloud Directory



Amazon GuardDuty



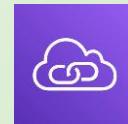
Amazon CloudWatch



AWS Step Functions



AWS OpsWorks



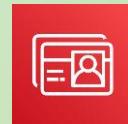
Amazon VPC PrivateLink



AWS Direct Connect



Resource Access manager



AWS Directory Service



Amazon Inspector



AWS Systems Manager



AWS Lambda



AWS CloudFormation

## Automate

Identify

Protect

Detect

Respond

Recover



AWS Service Catalog



AWS Config



AWS Shield



IAM



AWS Secrets Manager



KMS



Amazon Cognito



Amazon Macie



Amazon Detective



Amazon CloudWatch



AWS CloudTrail



Amazon S3 Glacier



AWS Well-Architected Tool



AWS Systems Manager



AWS WAF



AWS Firewall Manager



AWS Certificate Manager



AWS CloudHSM



AWS IAM Identity Center



AWS Security Hub



Personal Health Dashboard



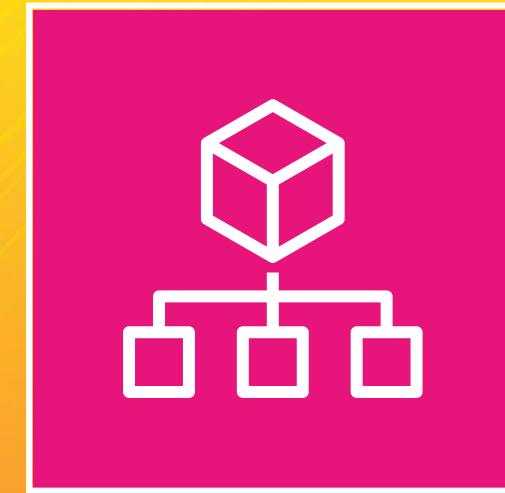
Amazon Route 53



Snapshot

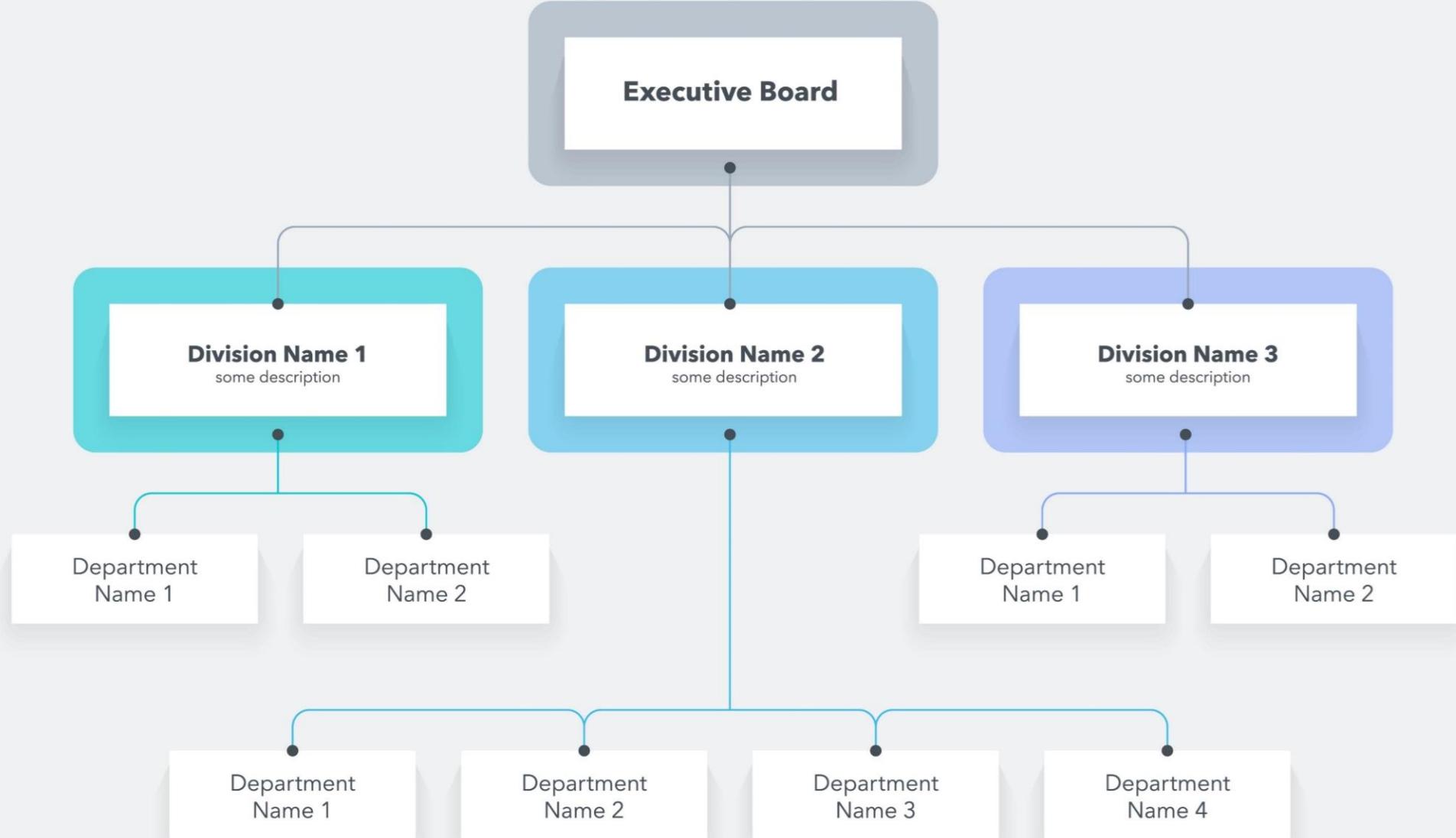


Archive



AWS Organizations

# A typical business organization structure



# Why multiple accounts?



Governance



Security Policies



Blast Radius



Account limits



Operational Boundary



Cost Visibility



Support Plan

# Challenges in Multi Account AWS Environment



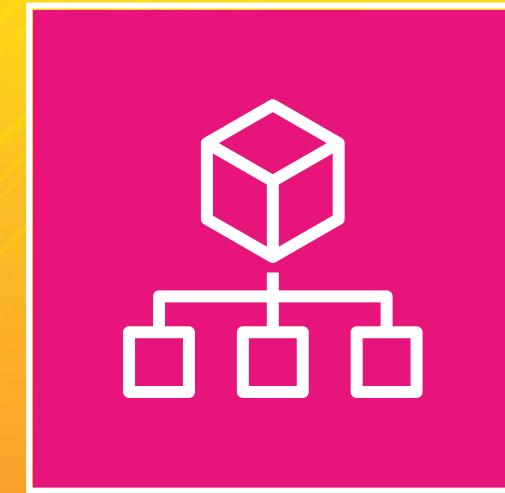
Operational Overhead



Individual Billing

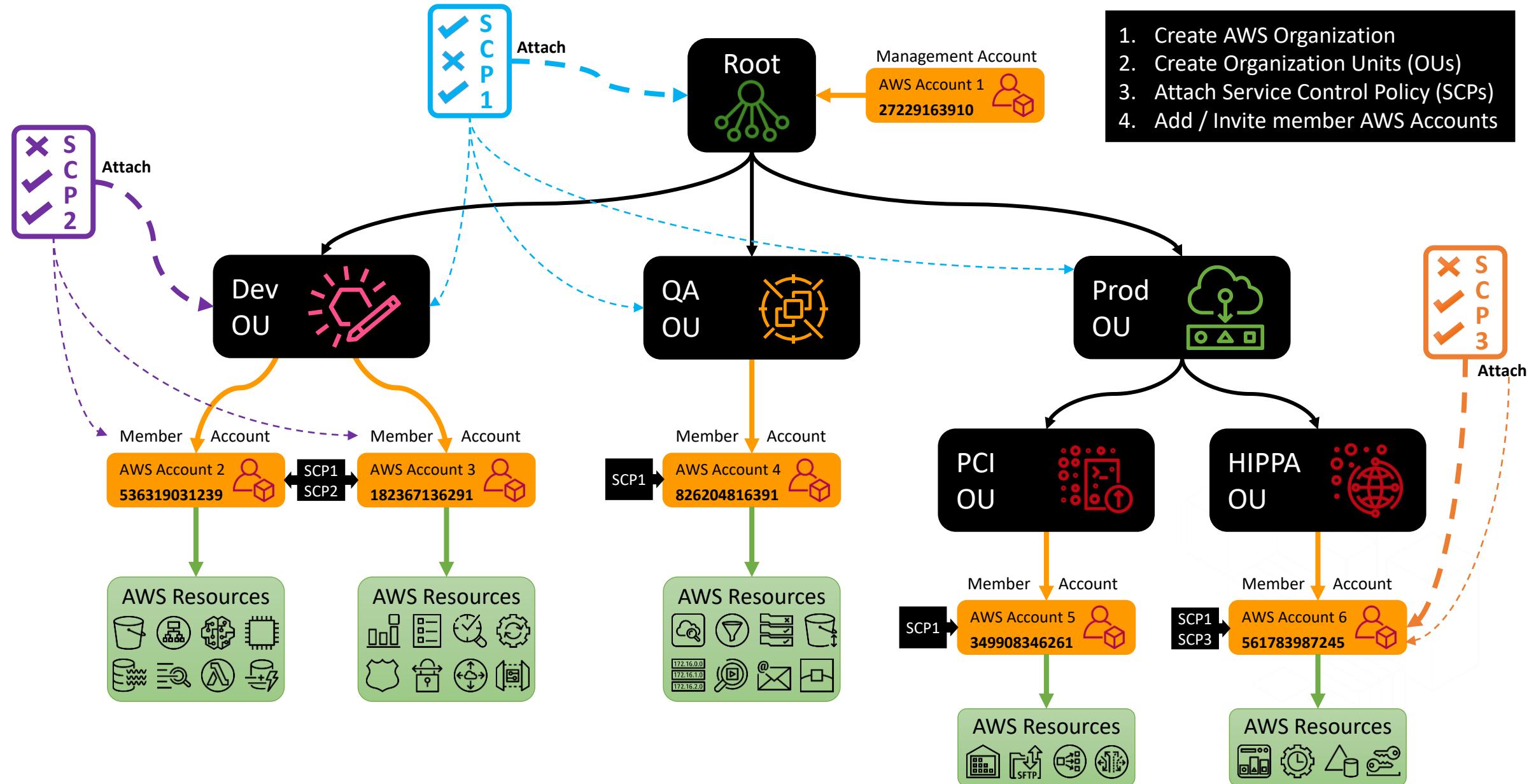


Security Control



AWS Organizations

# AWS Organization



# SCP Examples

## Allow example

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "EC2:*", "S3:*"  
      ],  
      "Resource": "*"  
    }  
  ]  
}
```

## Deny example

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Deny",  
      "Action": [  
        "SQS:*"  
      ],  
      "Resource": "*"  
    }  
  ]  
}
```

# Effective Permission

SCP



Allow: EC2:  
Allow: S3:

IAM



IAM  
Policies

Allow: EC2:  
Allow: SQS:



# SCP Examples

- No Internet Gateway for VPC

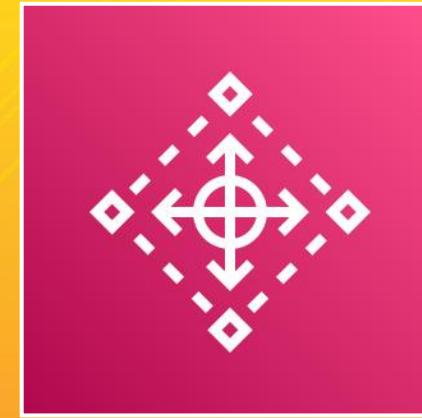
```
"Statement": [  
    {  
        "Effect": "Deny",  
        "Action": [  
            "ec2:AttachInternetGateway",  
            "ec2>CreateInternetGateway",  
            "ec2:AttachEgressOnlyInternetGateway",  
            "ec2:CreateVpcPeeringConnection",  
            "ec2:AcceptVpcPeeringConnection"  
        ],  
        "Resource": "*"  
    }  
]
```

- Stop CloudTrail from being disabled

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Deny",  
            "Action": "cloudtrail:stopLogging",  
            "Resource": "*"  
        }  
    ]  
}
```

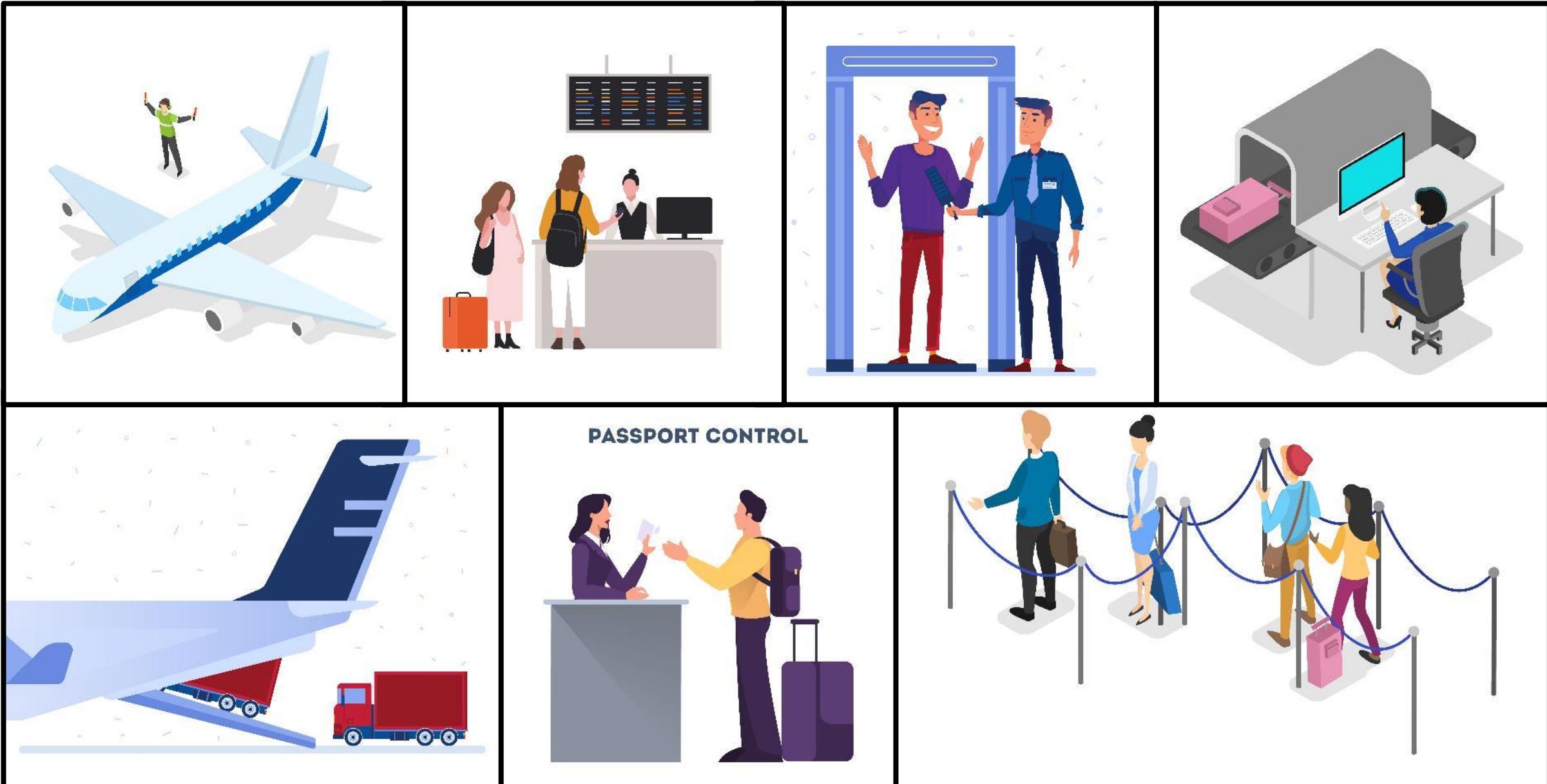


More Example service control policies

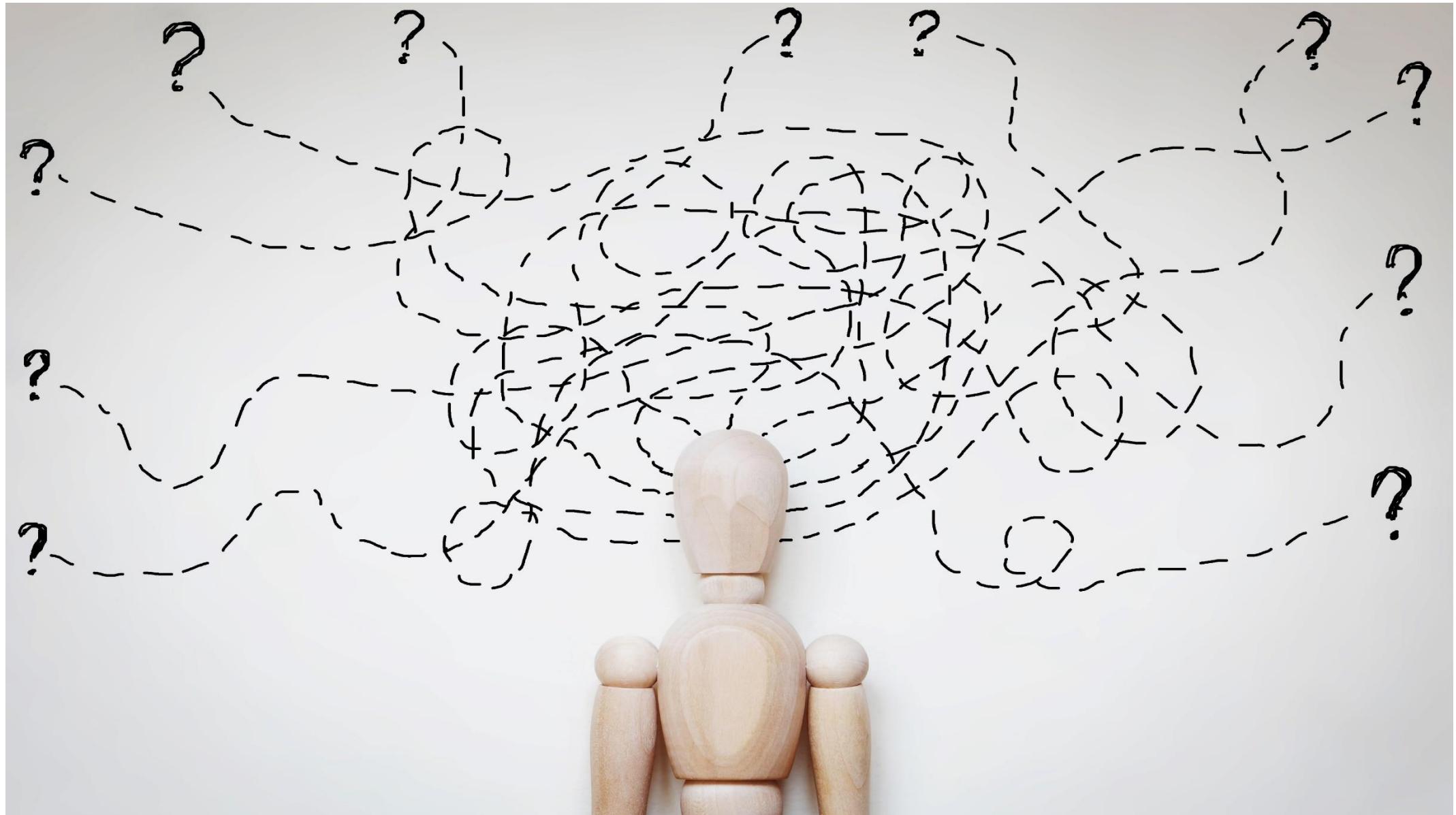


AWS Control Tower

# Can you design an airport?



# Where to start?



Lets use the best practices from other successful airport designs



# Setting up a new AWS Multi-account architecture

## Initial Setup

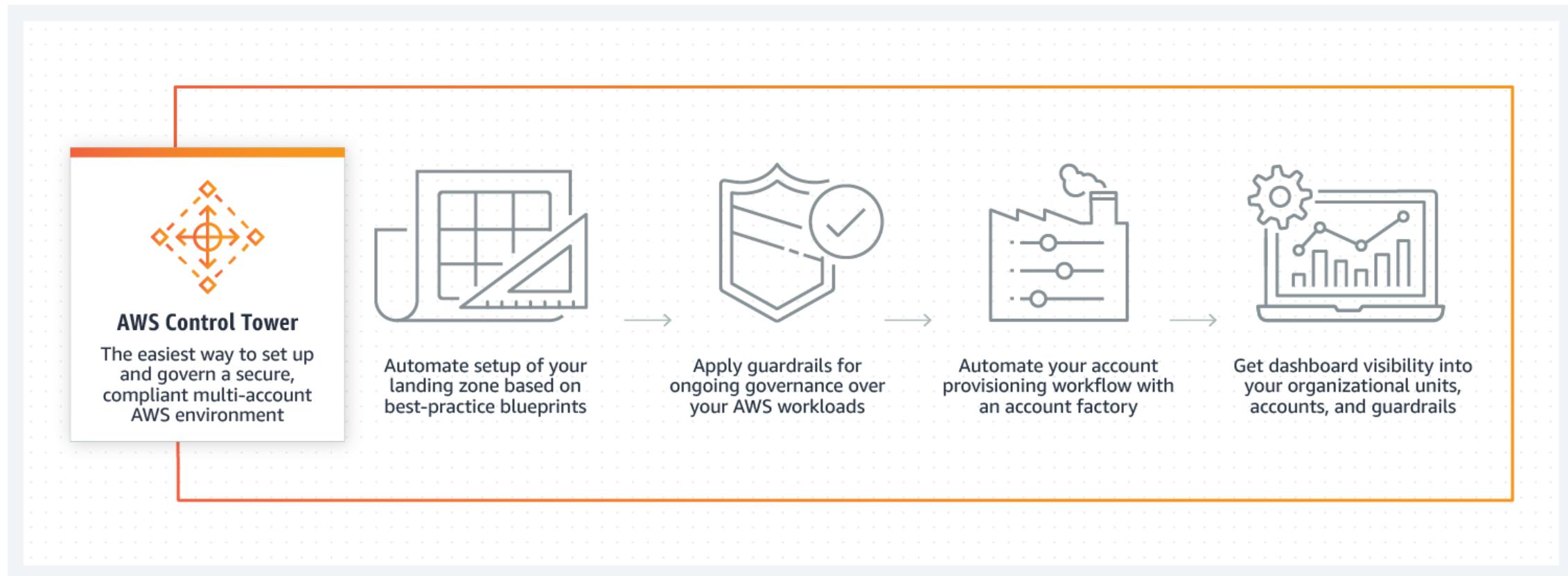
- Create Organization Management account
  - Create temporary Amazon S3 bucket of AWS CloudTrail logs
  - Enable CloudTrail locally
  - Enable AWS Organization full feature
- Create Log Archive account
  - Create bucket(s) for security logs
- Create Security account
  - Create Roles – Read Only | Power Users | Admin
- Create a Shared Services Account
  - Configure Single Sign-On (SSO)

## Repeat setup for every account

- Secure Root credentials
- Complex password policy
- Link to Organization Master account
- Enable CloudTrail
- Send Log to Archive account
- Enable Amazon GuardDuty
- Enable AWS Config
- Enable appropriate Config rules
  - Amazon S3 bucket encryption
  - Amazon S3 block public access
  - EBS Volume encryption
  - Etc...
- Create common cross-account Security role
  - Read Only | Power User | Admin
- Create VPC (non-overlapping IP space)
- Enable federation into account (SSO)
- Etc..

# AWS Control Tower

- AWS Control Tower provides the easiest way to set up and govern a secure, compliant, multi-account AWS environment based on best practices established by working with thousands of enterprises.



# AWS Control Tower

Landing zone



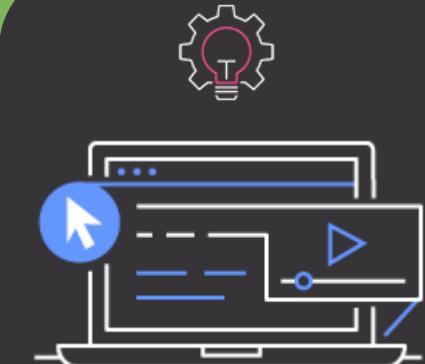
Guardrails



Account Factory



Dashboard



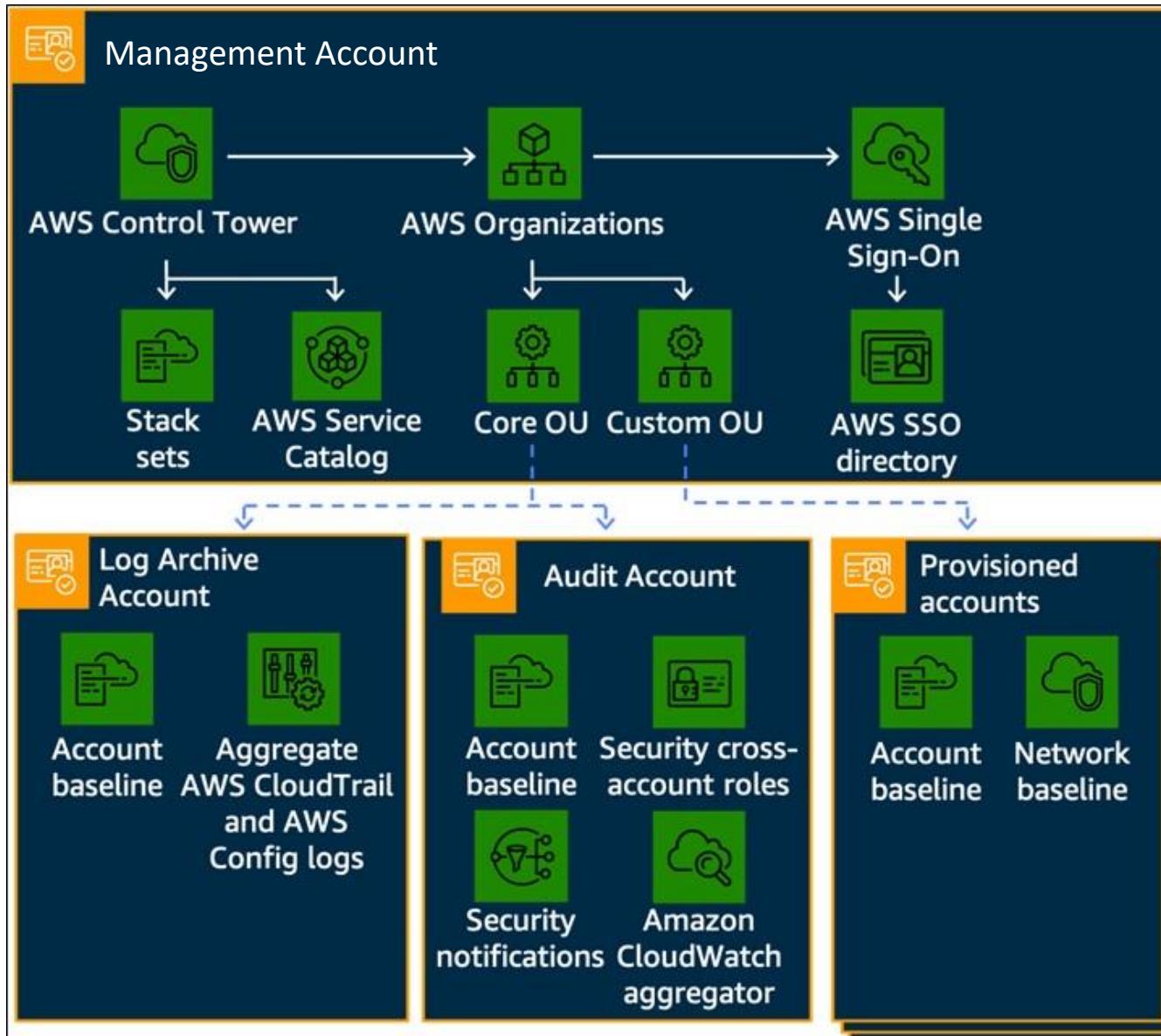
# AWS Control Tower – Landing Zone

## Landing zone

A well-architected, multi-account AWS environment based on security and compliance best practices.



# Landing Zone Structure



## Underlying services

[AWS Organizations](#)

[AWS Service Catalog](#)

[AWS Single Sign-on](#)

[AWS Config](#)

[AWS CloudFormation](#)

### ▼ View all underlying services

[Amazon CloudWatch](#)

[AWS CloudTrail](#)

[AWS Identity and Access Management](#)

[Amazon Simple Storage Service](#)

[Amazon Simple Notification Service](#)

[AWS Lambda](#)

[AWS Step Functions](#)

## Related services

[AWS Security Hub](#)

[AWS Systems Manager](#)

No additional charge exists for using AWS Control Tower.

# AWS Control Tower - Guardrails

## Landing zone

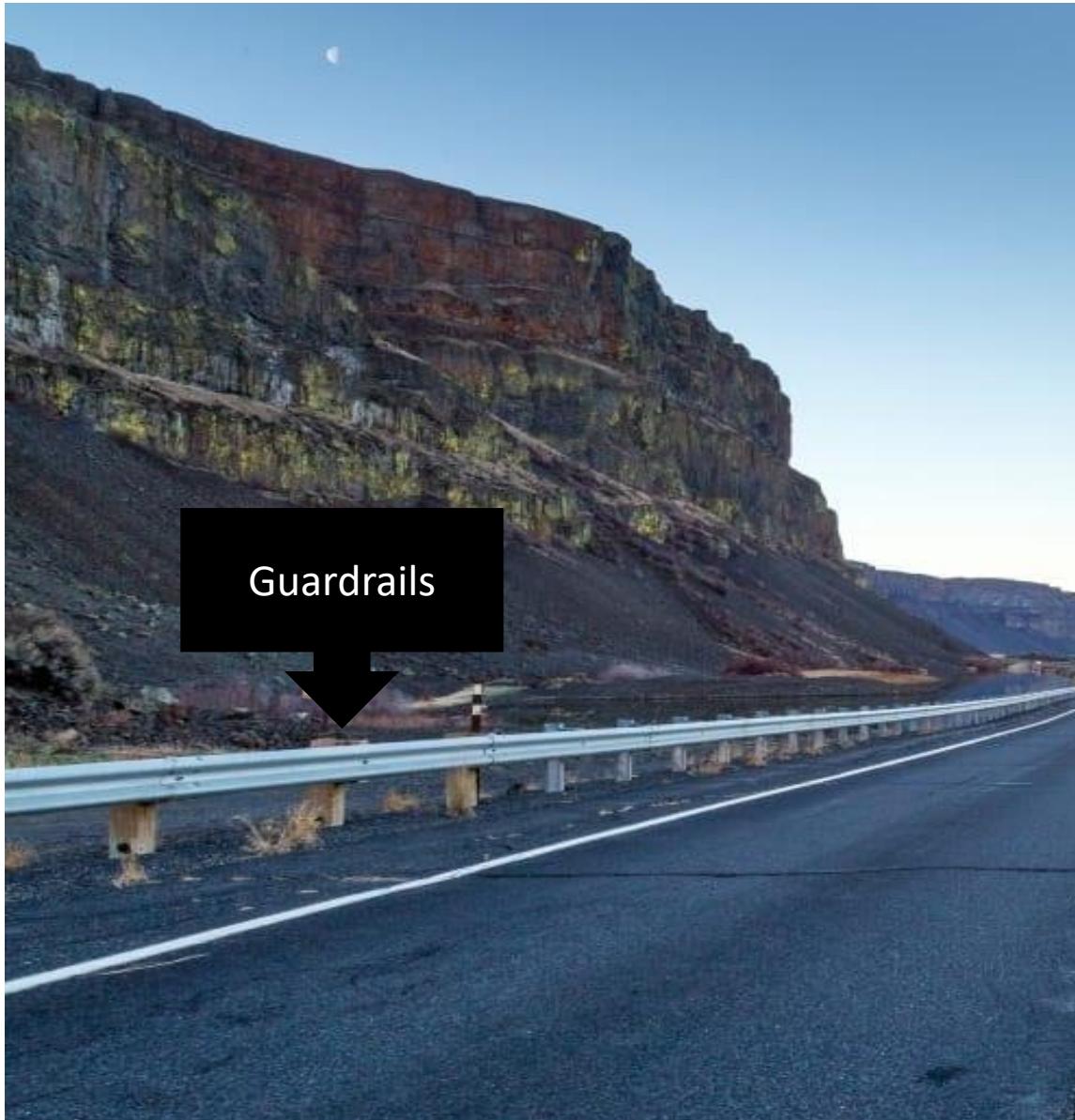
A well-architected, multi-account AWS environment based on security and compliance best practices.



## Guardrails

A high-level rule that provides ongoing governance for your overall AWS environment.

# Guardrails in real life



# Guardrails in AWS Control Tower

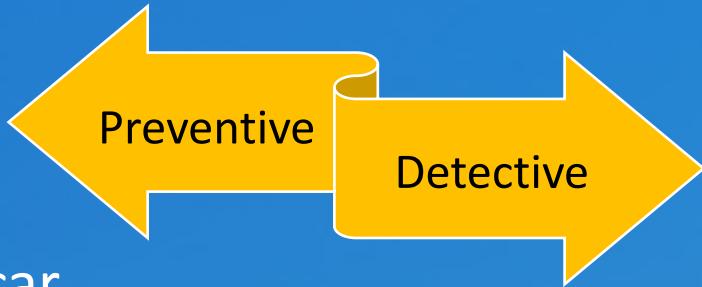
- A guardrail is a high-level rule that provides ongoing governance for your overall AWS environment. It's expressed in plain language.
- Through guardrails, AWS Control Tower implements **preventive** or **detective** controls that help you govern your resources and monitor compliance across groups of AWS accounts.

Goal/category	Example
IAM security	Require MFA for root user
Data security	Disallow public read access to Amazon S3 buckets
Network security	Disallow internet connection via Remote Desktop Protocol (RDP)
Audit logs	Enable AWS CloudTrail and AWS Config
Monitoring	Enable AWS CloudTrail integration with Amazon CloudWatch
Encryption	Ensure encryption of Amazon EBS volumes attached to Amazon EC2 instances
Drift	Disallow changes to AWS Config rules set up by AWS Control Tower



# Suggestions for Speed Limiting...

- Place speed limits and signs
- Put speed humps everywhere
- Put driving instructors in every car



- Random speed checks
- Mobile / fixed speed cameras



# AWS Control Tower – Account Factory

## Landing zone

A well-architected, multi-account AWS environment based on security and compliance best practices.



## Account Factory

A configurable account template that helps provisioning of new AWS accounts with pre-approved account configurations.



## Guardrails

A high-level rule that provides ongoing governance for your overall AWS environment.



# Account Factory

- Account factory for controls on account provisioning
  - Pre approved account baselines with VPC options
  - Pre approved configuration options

AWS Control Tower > Account factory

## Account factory Info

The account factory enables you to create standardized baselines and network configurations for accounts in your organization. Your users can configure and provision these new accounts in AWS Service Catalog.

### Network configuration

The following VPC configuration options are available to your users when they provision new accounts. You can modify these settings anytime.

Internet-accessible subnet Disallow	Address range (CIDR) for account VPCs 172.31.0.0/16	Regions for VPC creation EU (Ireland) US East (N. Virginia) US East (Ohio) US West (Oregon)
Maximum number of private subnets 1		
Availability Zone count 3		

**Provision new account**  **Edit**



AWS Control Tower > Account factory > Enroll account

## Enroll account Info

### Account details

Account enrollment provisions a new account or brings an existing account into AWS Control Tower governance.

**Account email**  
Specify a new email if you are creating a new account in your landing zone, or an existing email to extend governance to an existing AWS account.

Must be from 6 to 64 characters long.

**Display name**  
Name for account as it appears in AWS Control Tower

**AWS SSO email**  
Designate an SSO user.

Must be from 6 to 64 characters long.

**AWS SSO user name**  
First and last name intended for creating an AWS SSO user

Martha	Rivera
--------	--------

**Organizational unit**  
Defines governance for an account, and enables all guardrails on that OU

**Cancel** **Enroll account**

# AWS Control Tower

## Landing zone

A well-architected, multi-account AWS environment based on security and compliance best practices.



## Account Factory

A configurable account template that helps provisioning of new AWS accounts with pre-approved account configurations.



## Guardrails

A high-level rule that provides ongoing governance for your overall AWS environment.



## Dashboard

Offers continuous oversight of your landing zone to your team of central cloud administrators.

# Dashboard

- The Control Tower dashboard gives you continuous visibility into your AWS environment.
- You can view the number of OUs and accounts provisioned, the number of guardrails enabled, and the check the status of your OUs and accounts against those guardrails.
- You can also see a list of noncompliant resources with respect to enabled guardrails.

The screenshot shows the AWS Control Tower Dashboard. On the left, a sidebar menu includes Dashboard, Accounts, Organizational units, Guardrails, Users and access, Account factory, and Shared accounts. The main content area has several sections:

- Environment summary:** Shows 3 Organizational units and 34 Accounts.
- Guardrail summary:** Shows 28 Preventive guardrails and 12 Detective guardrails.
- Noncompliant resources:** A table listing three resources: a Volume (EC2, us-west-2, db-uswest-1-gamma, Custom) with a note to enable encryption for EBS volumes; another Volume (EC2, us-east-1, testing-beta-1, Project 1) with a note to enable encryption for EBS volumes; and a Security Group (EC2, eu-west-1, ops-test-4, Project 1) with a note to disallow internet connection through.
- Organizational units:** A table showing three OUs: Core (Parent OU: Root, Compliance: Compliant), Project 1 (Parent OU: Root, Compliance: Noncompliant), and Custom (Parent OU: Root, Compliance: Noncompliant).
- Accounts:** A table showing account details: Account name, Account email, Organizational unit, Owner, and Compliance status.



Become a Solutions Architect

A day in the life of an Amazonian



**Julie Elkins**

Senior Technical

Curriculum Developer



**Thank you for attending.  
See you next Saturday (22-July-2023)**



Become a Solutions Architect

For content check **Resources Link** on BeSA Home Page

