A unique opportunity for you to be mentored by Amazonians

BeSA

Become a Solutions Architect

Batch 04

Week 2

15-July-2023

Today's Session

Week 2
15-July

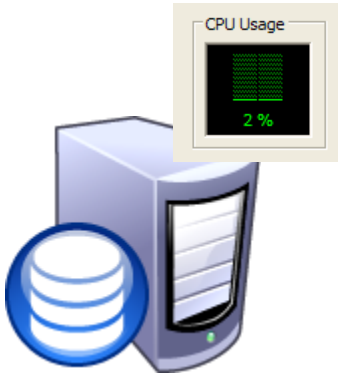
Virtualization Analogy

Legacy Datacentre

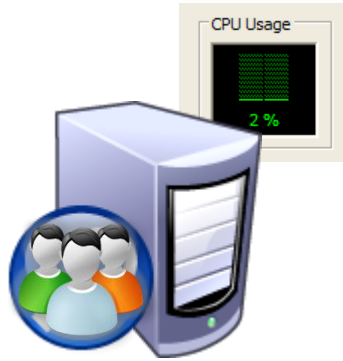
1:1 Mapping

One Application : One Server

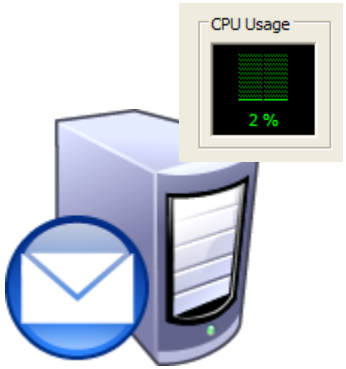
Web Server



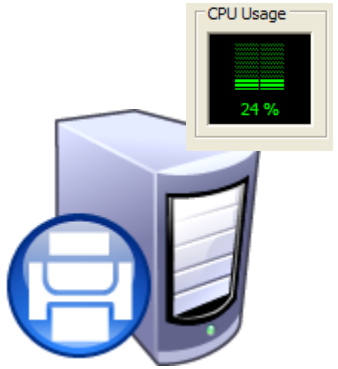
Database Server



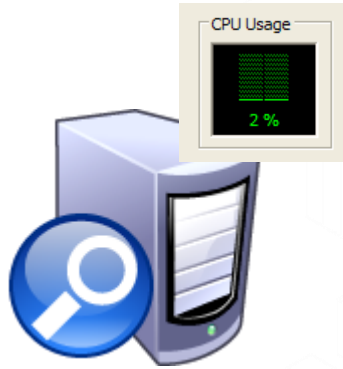
Active Directory



Mail Server



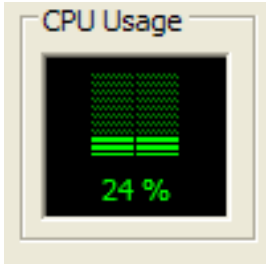
Print Server



Search Server

Legacy Datacentre

Low utilized servers



All require…

- Space
- Power
- Cooling
- Maintenance

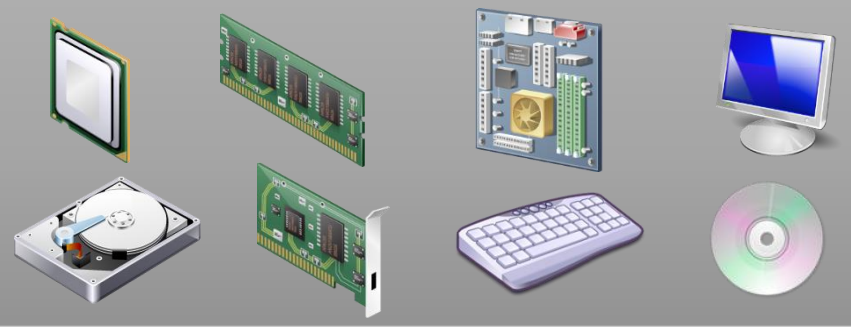
Users care about applications

What is required to run an application?

Application

Operating System

Hardware Resources

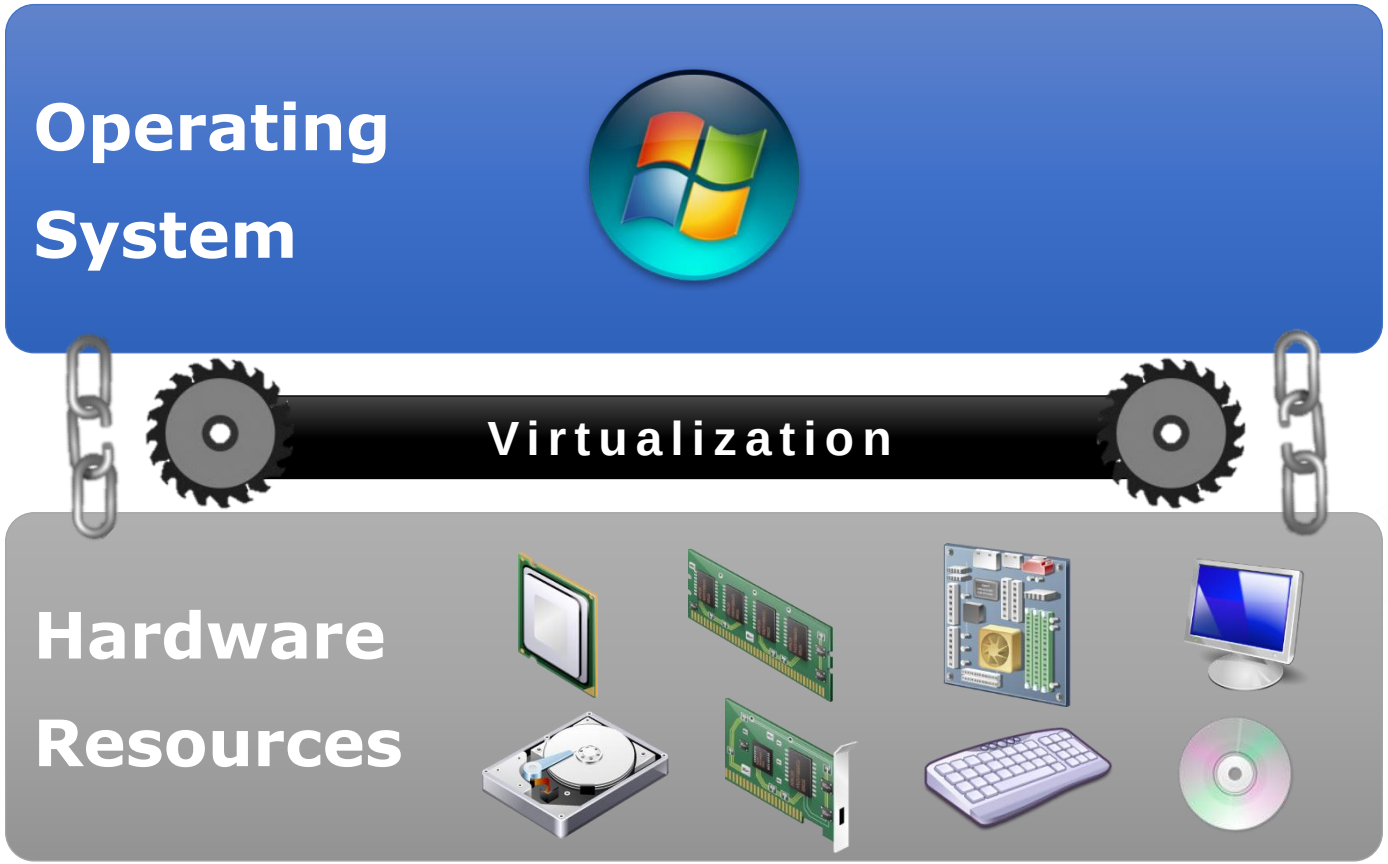


Traditional Approach

- In traditional approach hardware is coupled with an OS

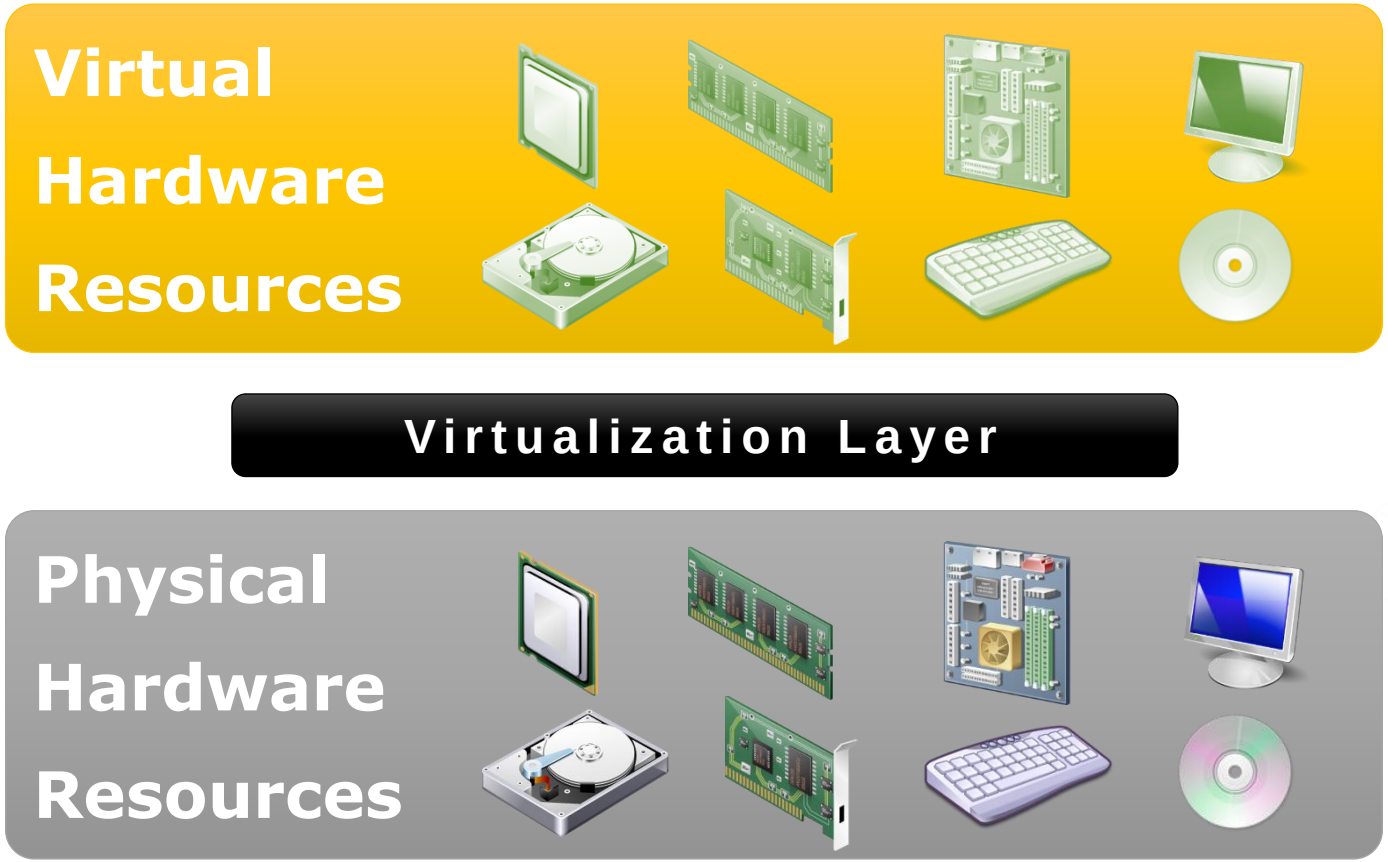
Virtualization Approach

- Virtualization decouples the hardware from OS



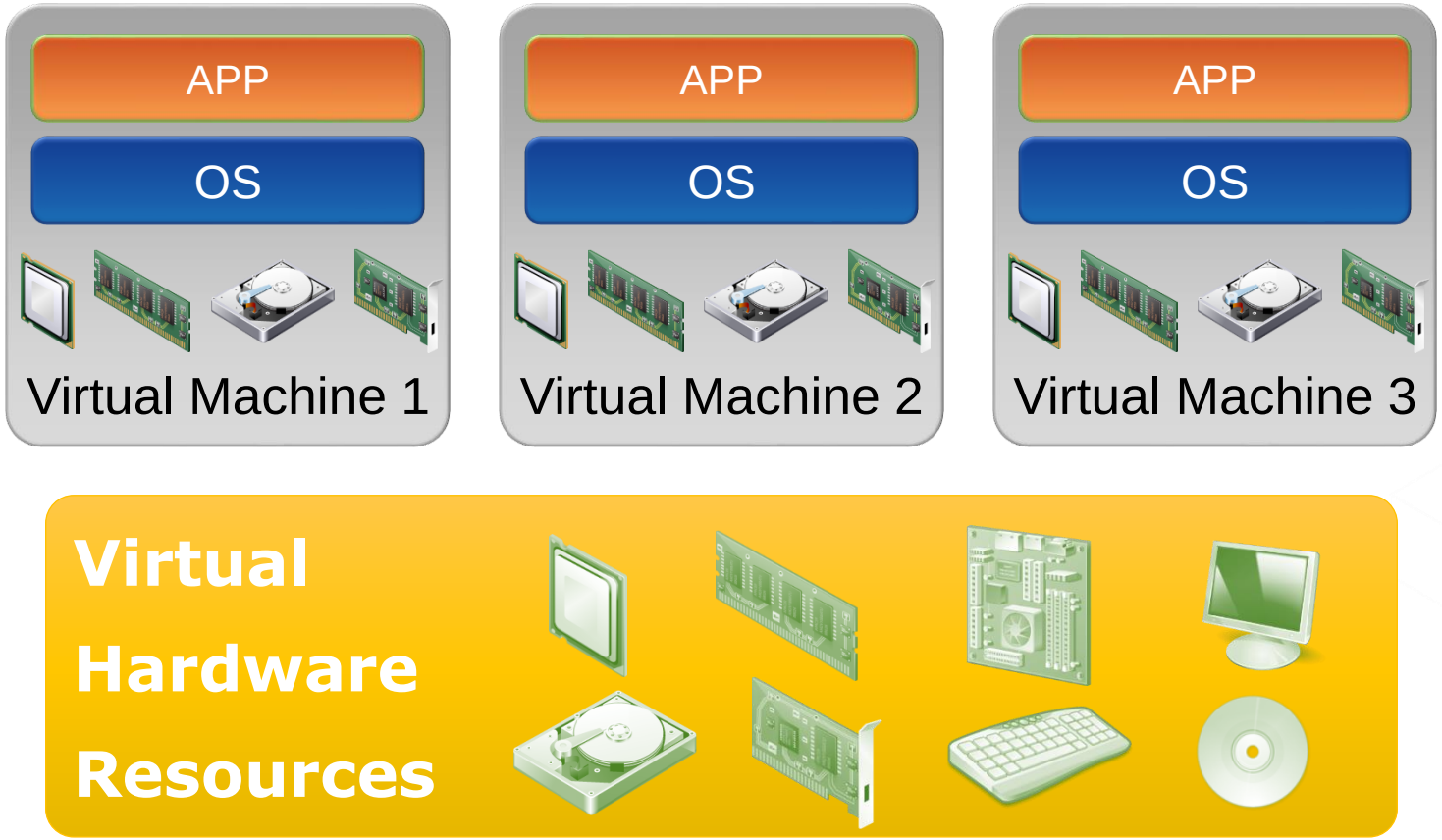
Virtualization Approach

- It creates virtual hardware resource out of physical hardware resources

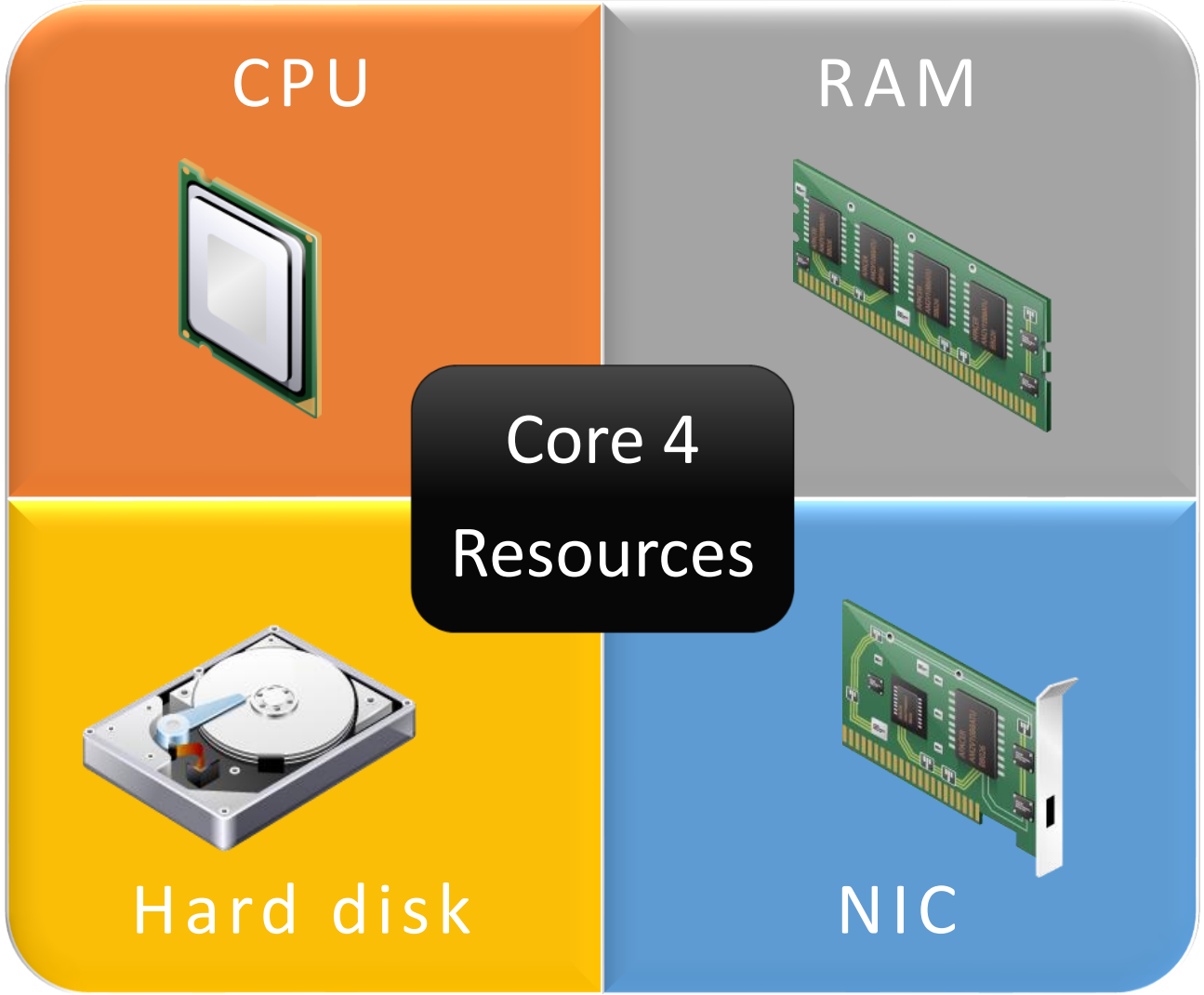


Virtualization Approach

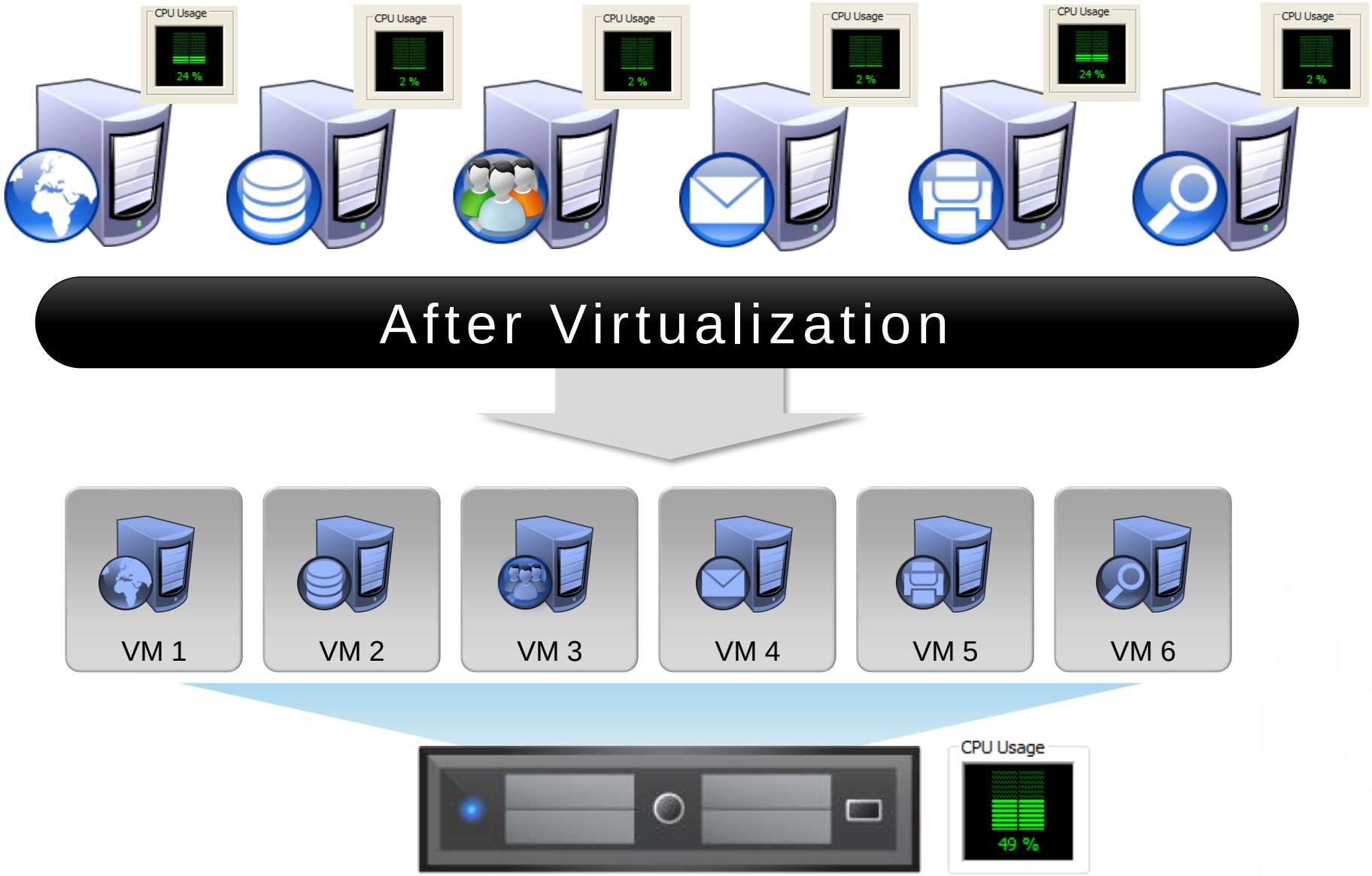
- The virtualized hardware resources can be assigned to different Virtual Machines.



Virtualization Approach



Virtualization Approach

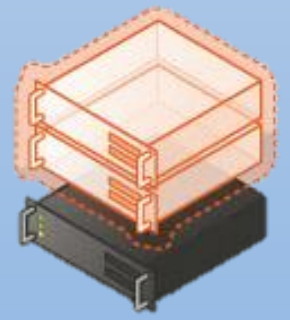


Enablers for Virtualization

- Decreasing cost of Powerful Hardware

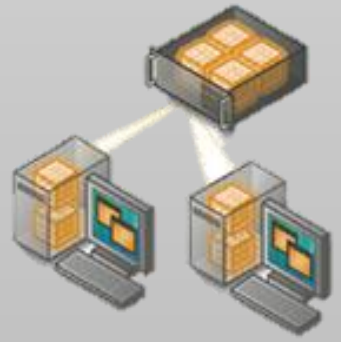
Types of Virtualization

Server Virtualization

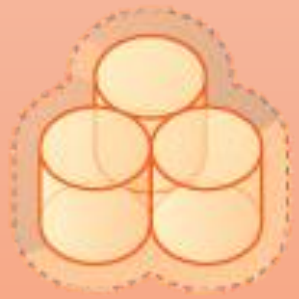


Desktop Virtualization

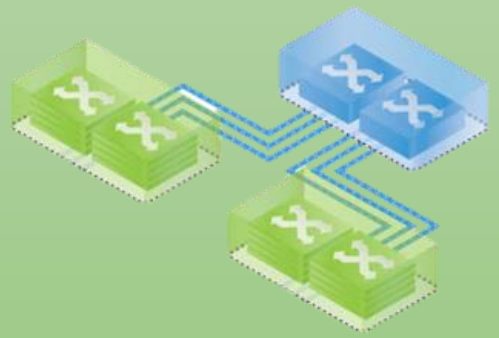
Application Virtualization



Storage Virtualization

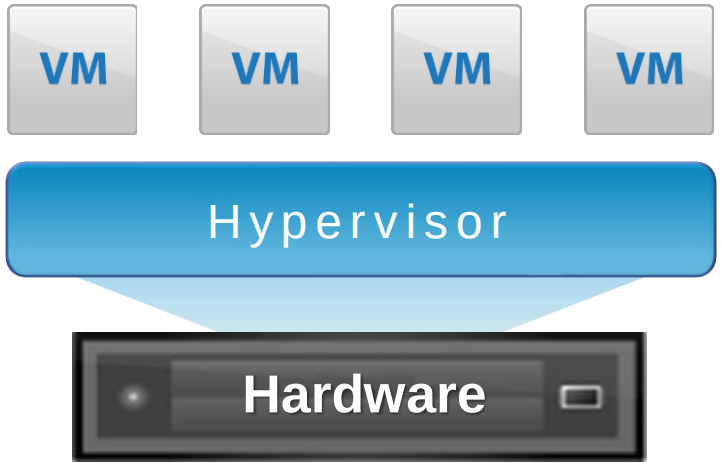


Network Virtualization



Hypervisor

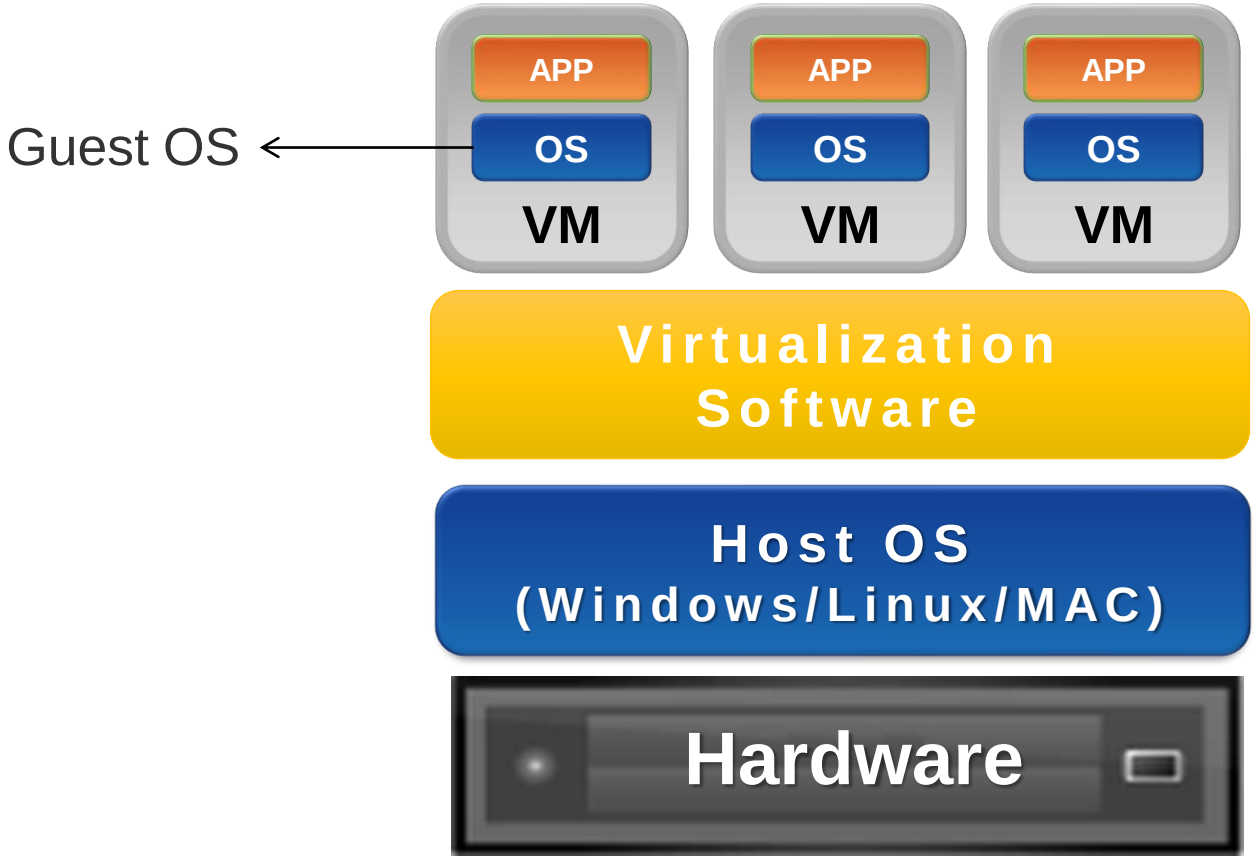
- A program that allows multiple operating systems to share a single hardware host.
- Each operating system appears to have the host's processor, memory, and other resources all to itself. However, the hypervisor is actually controlling the host resources.



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

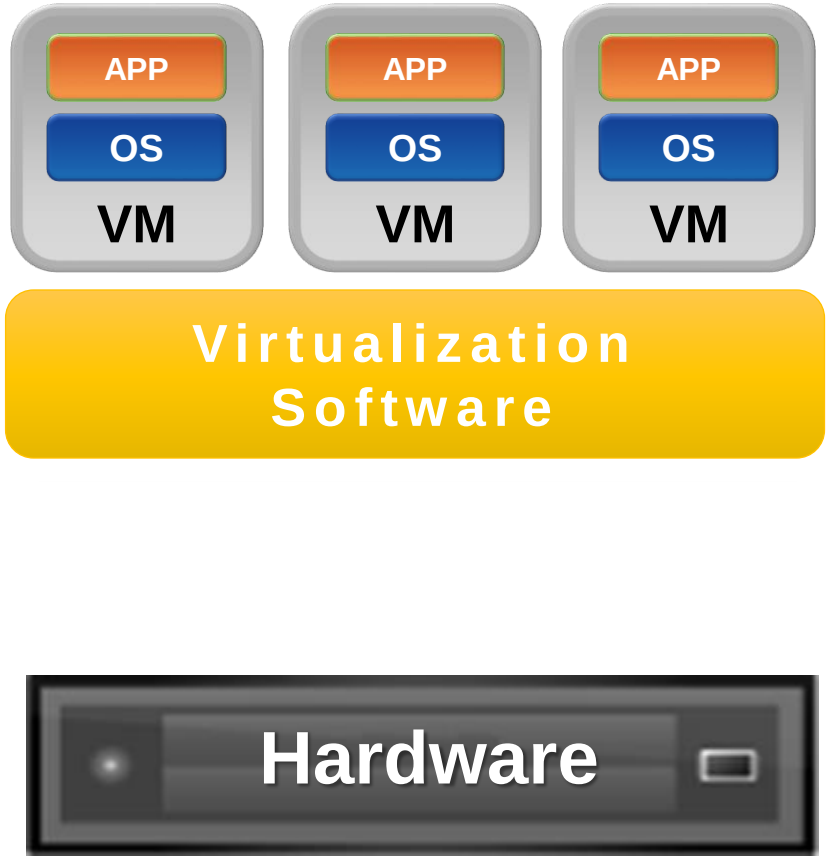
Type 2 Hypervisor – Host OS based (Hosted) Hypervisor

- A host-based virtualization systems 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®

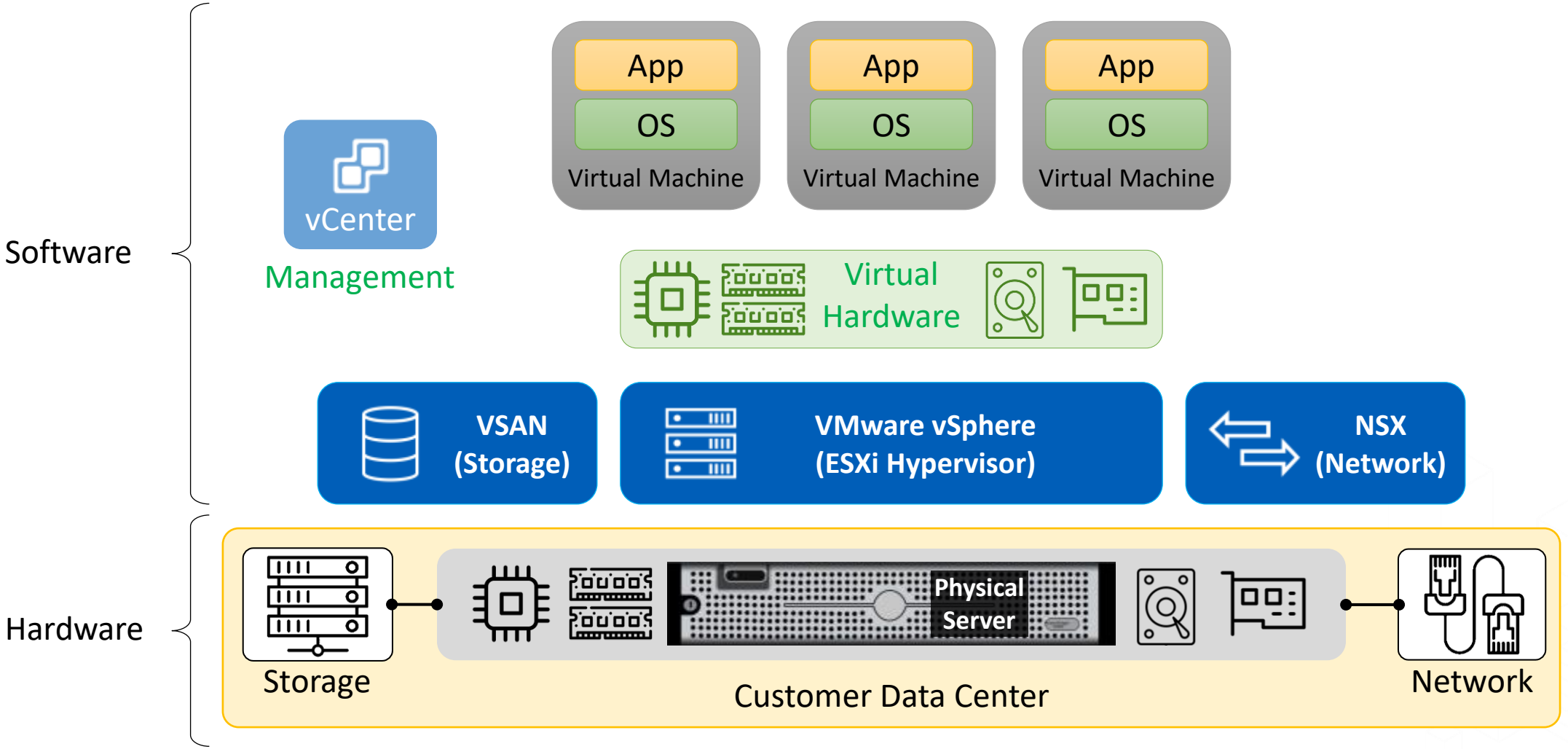
Others

ORACLE®

Parallels™

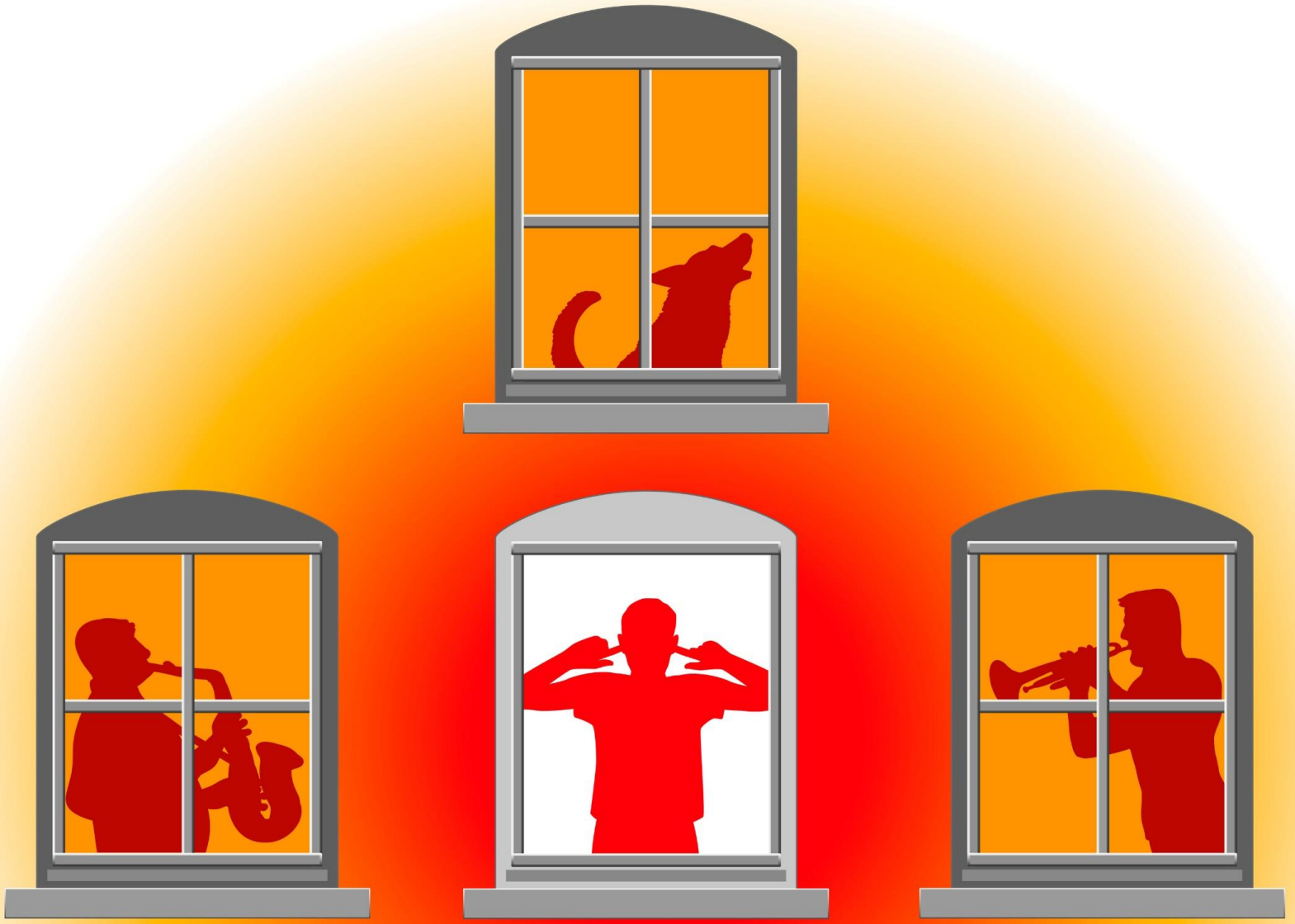
redhat.

VMware Software Defined Data Center (SDDC)



Some challenges

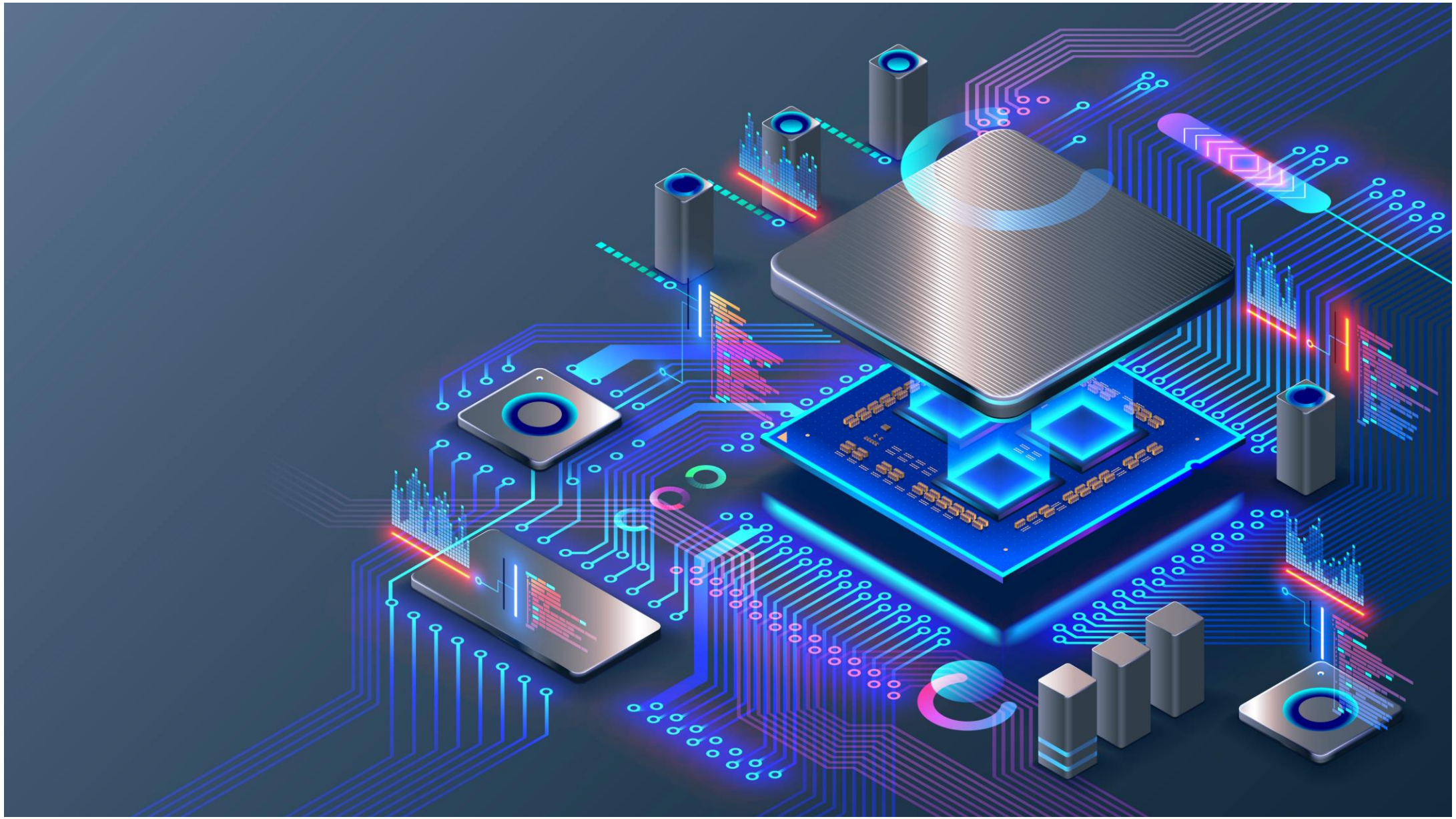
Noisy neighbours



Management overhead

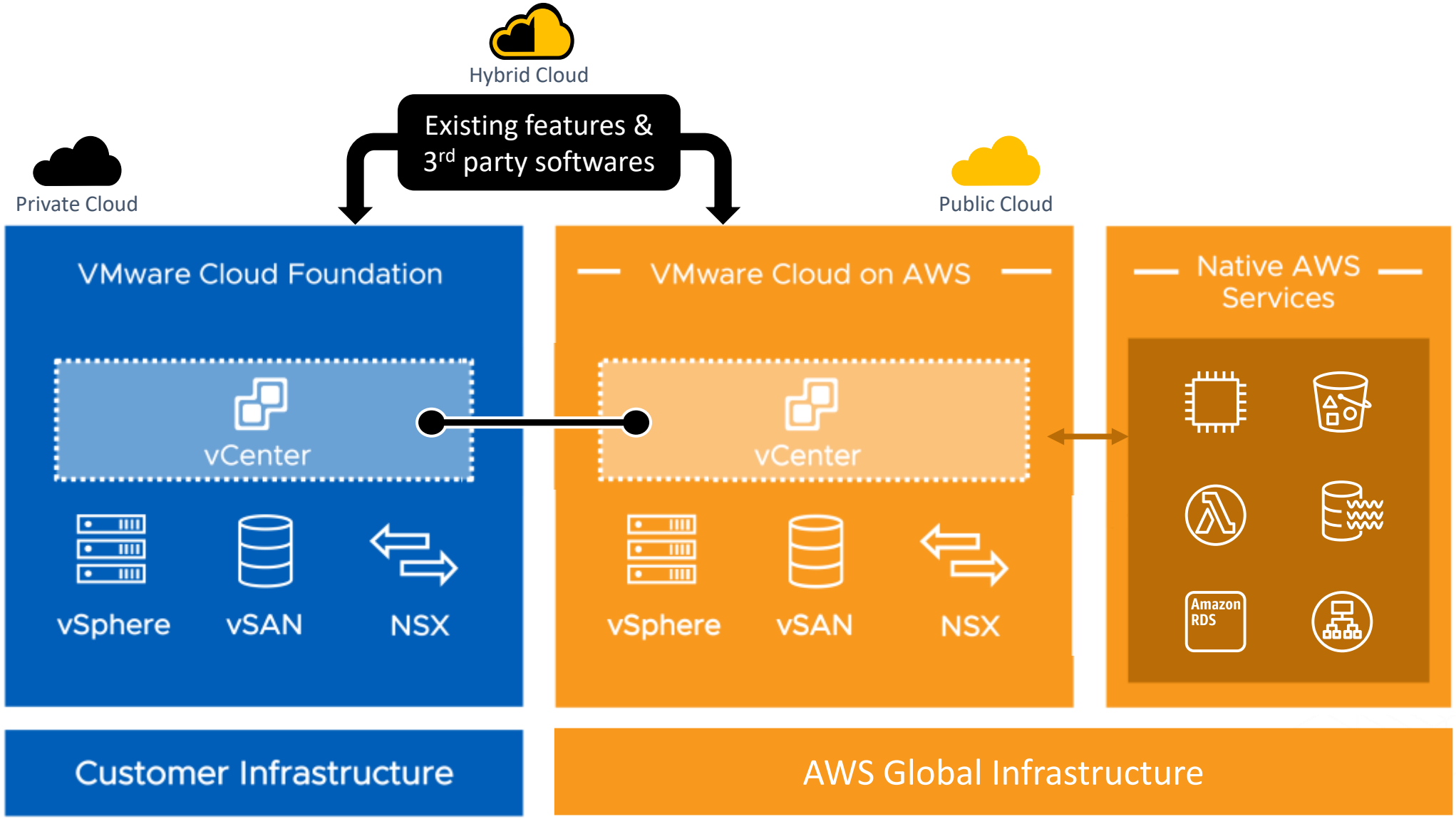
Cost

Apps needing BareMetal access



VMware Cloud on AWS

VMware Cloud on AWS (VMC on AWS)



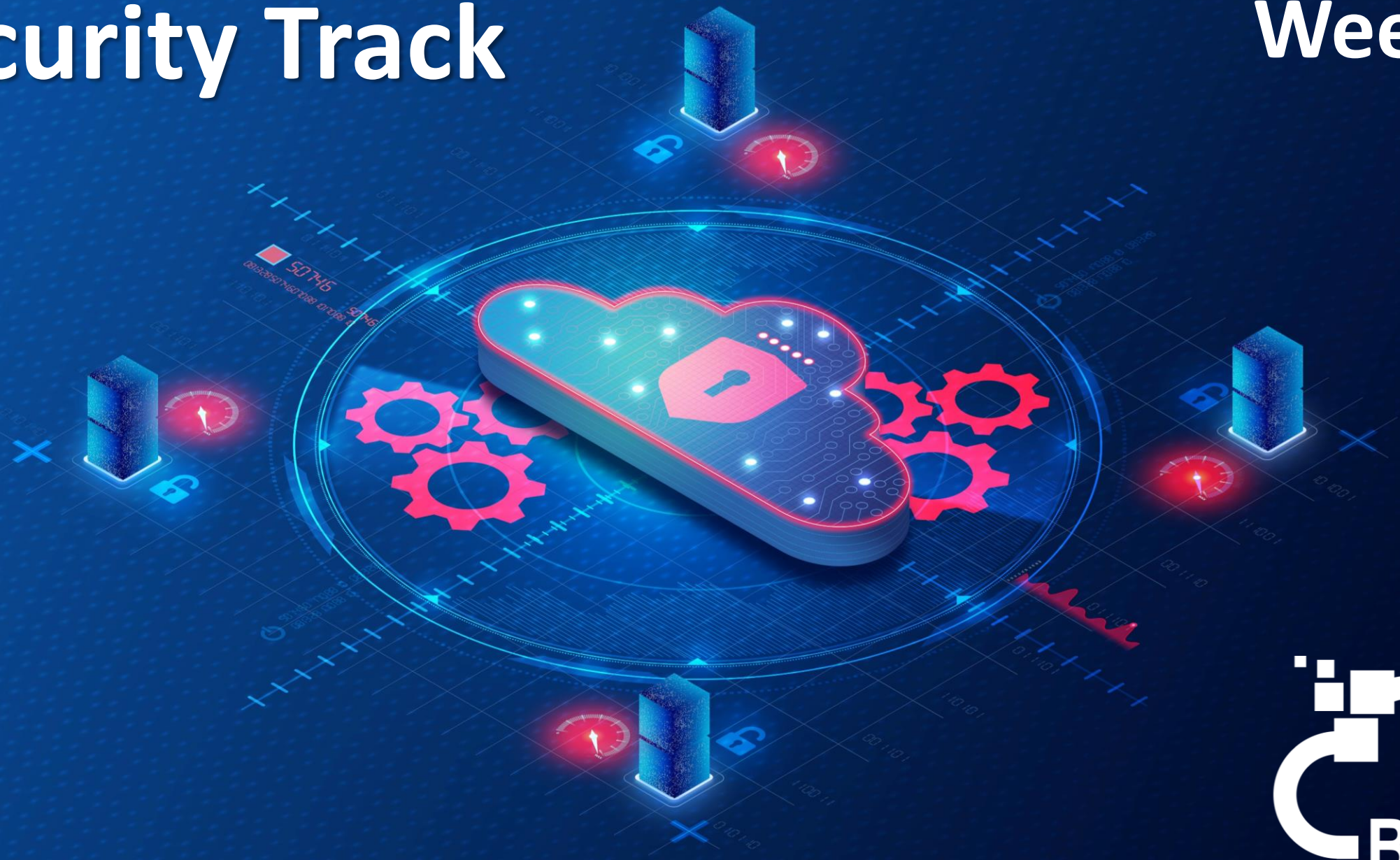
5 Minutes Break

If you are back type in chat….

Your favourite Mobile App

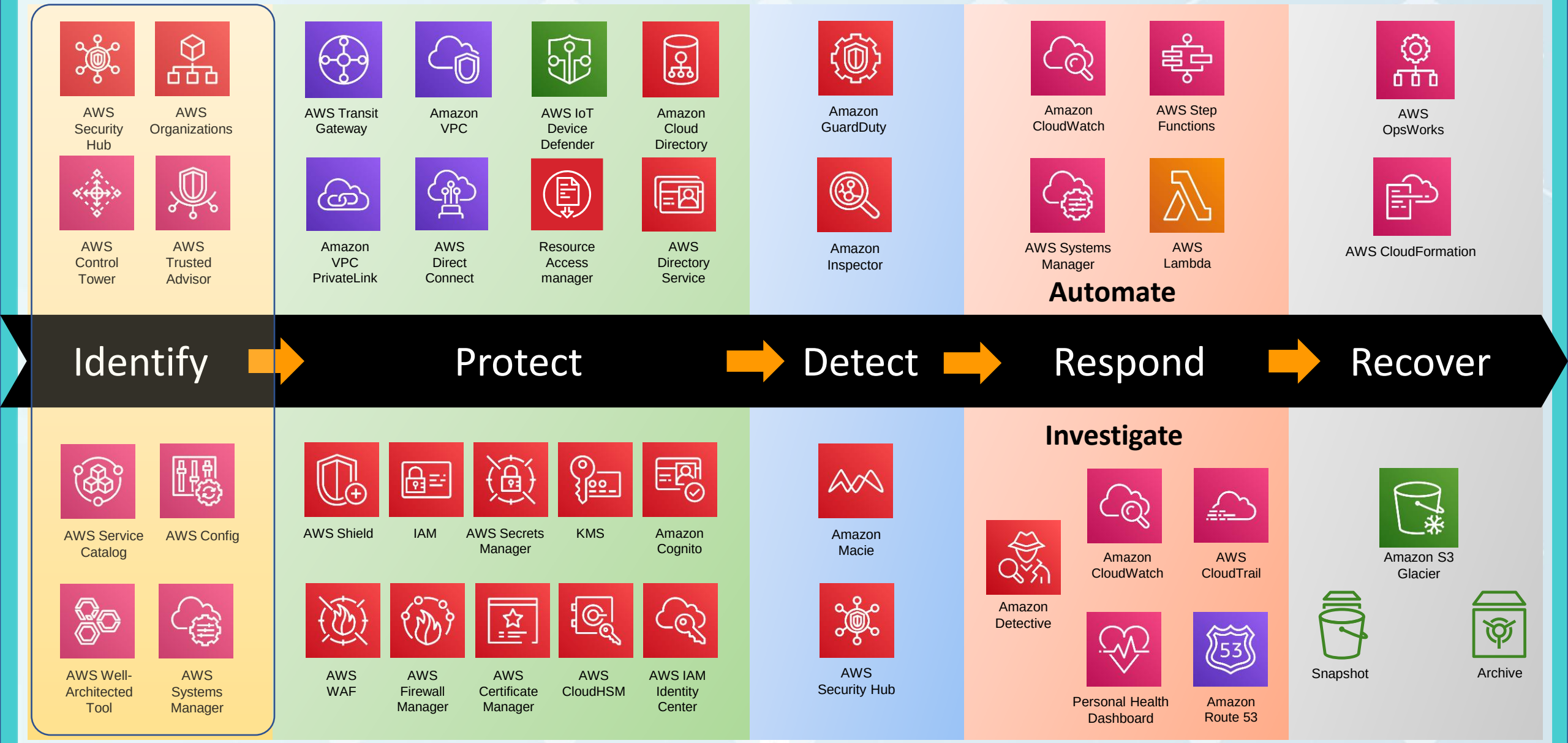
Security Track

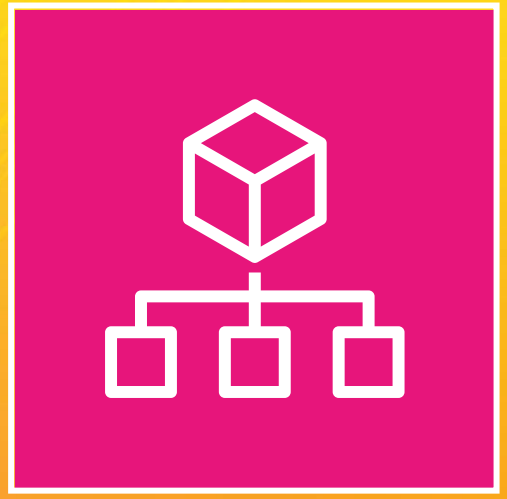
Week 2



BeSA

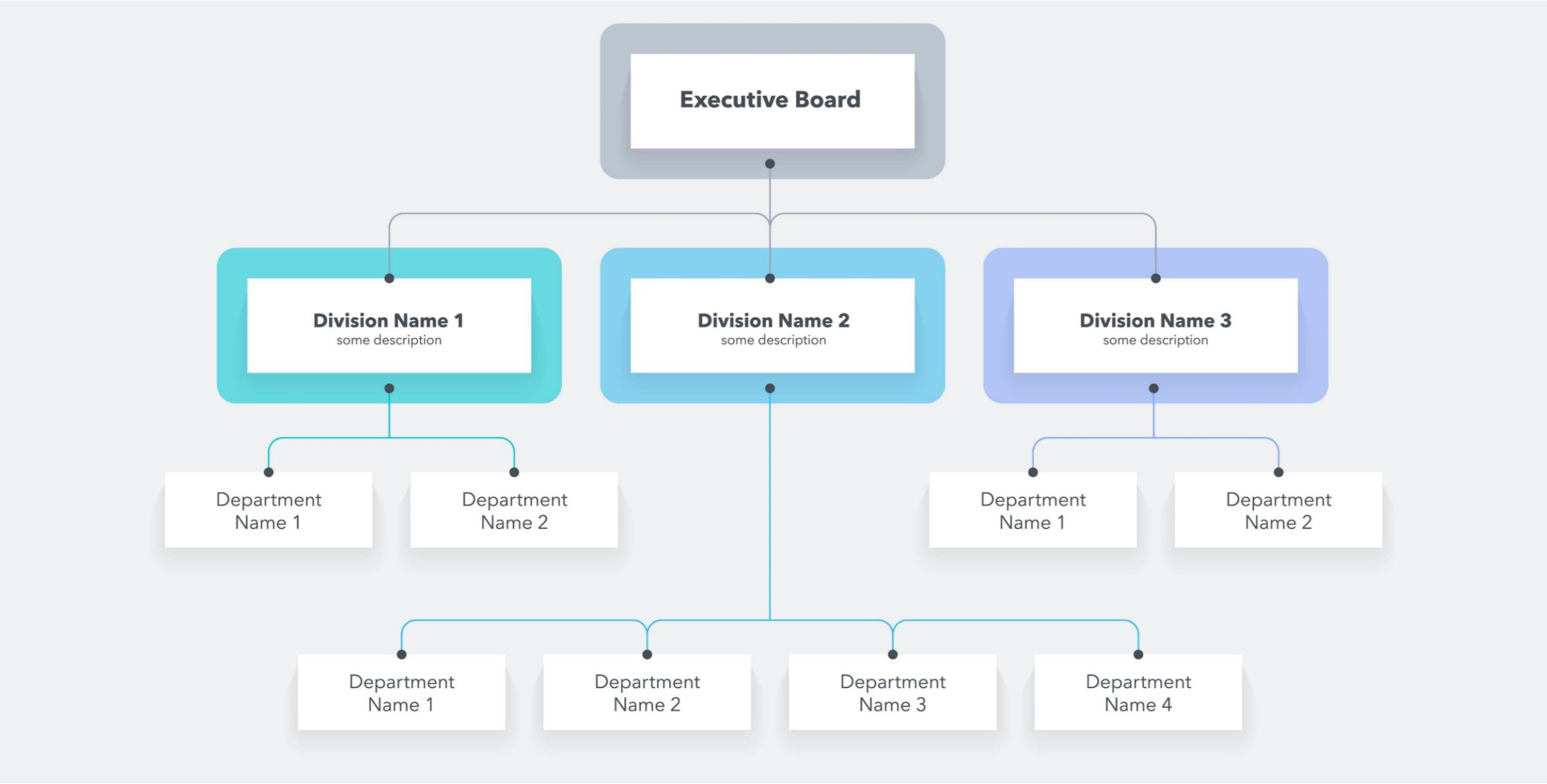
AWS Foundational and Layered Security Services





AWS Organizations

A typical business organization structure



Why multiple accounts?

Governance

Security Policies

Blast Radius

Account limits

Operational Boundary

Cost Visibility

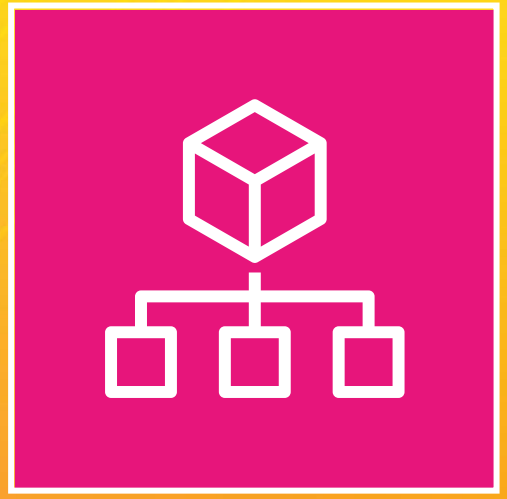
Support Plan

Challenges in Multi Account AWS Environment

Operational Overhead

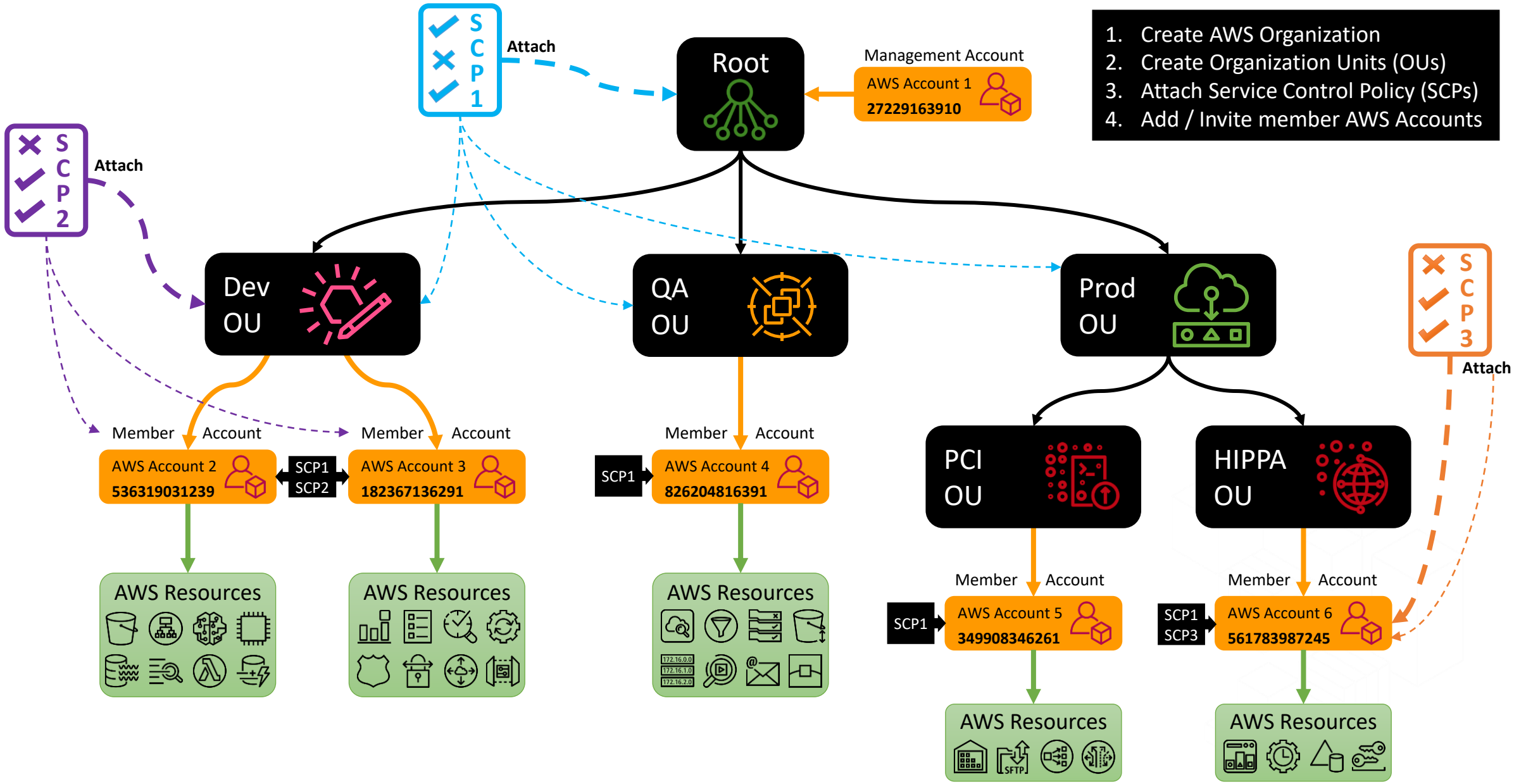
Individual Billing

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

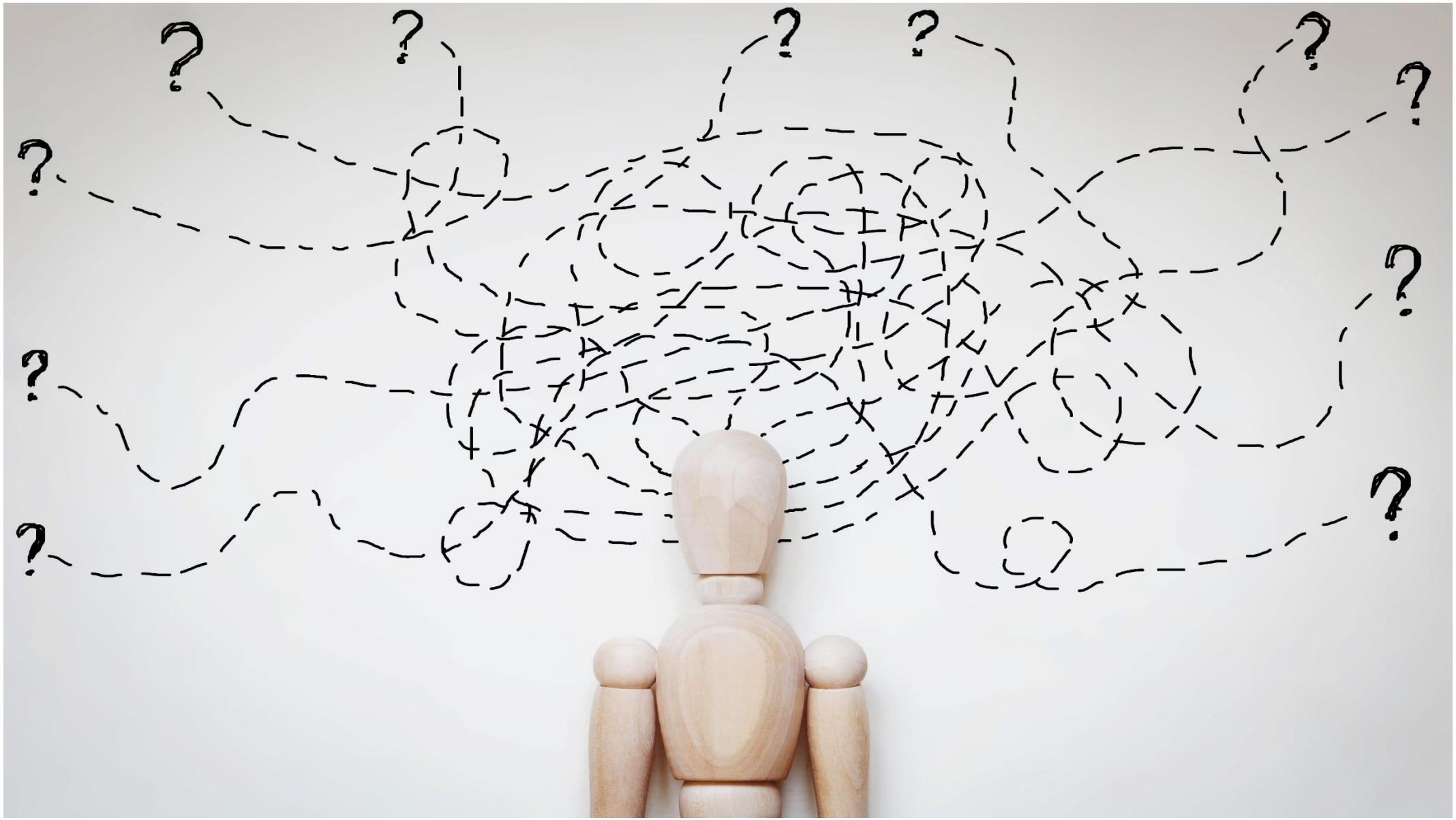
```
{
  "Version": "2012-10-17",
  "Statement": [
       {
      "Effect": "Deny",
      "Action": ”cloudtrail:StopLogging",
      "Resource": "*"
    }
  ]
}
```

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

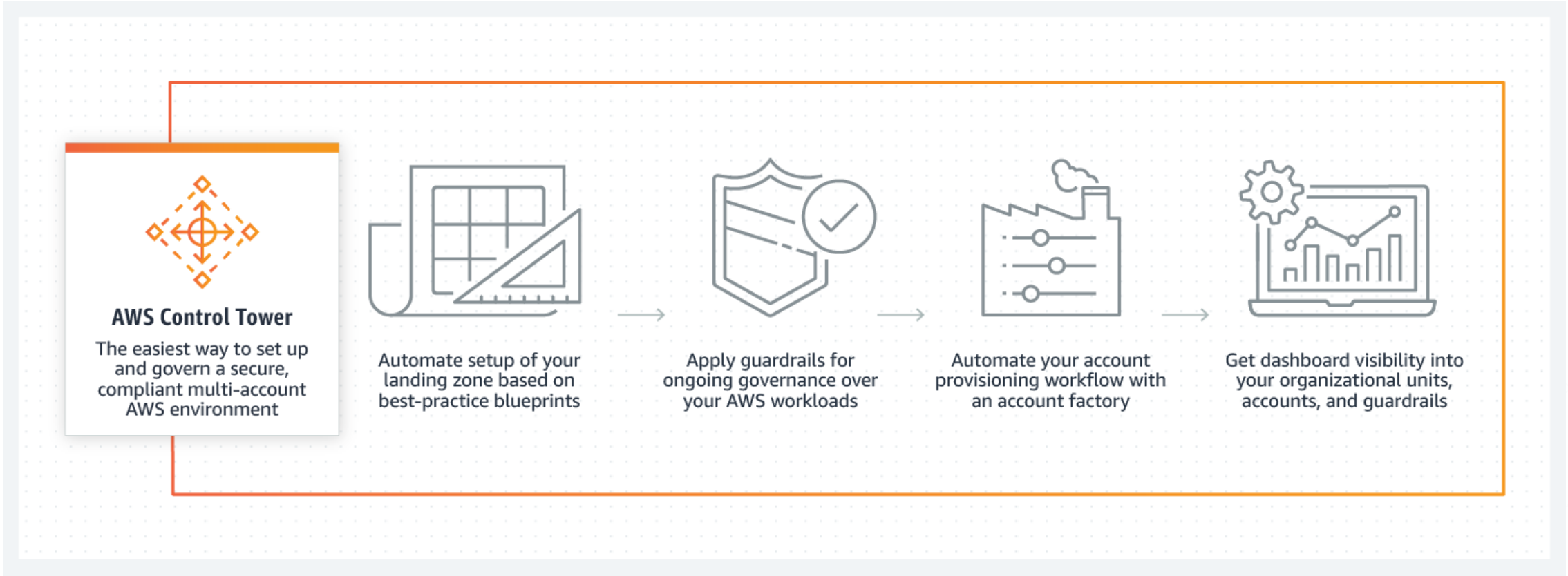
- Create Organization Management account
  - Create temporary Amazon S3 bucket of AWS CloudTrail logs
  - Enable CloudTrail locally
  - Enable AWS Organization full feature
- Create Log Archive account
  - Create bucket(s) for security logs
- Create Security account
  - Create Roles – Read Only | Power 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

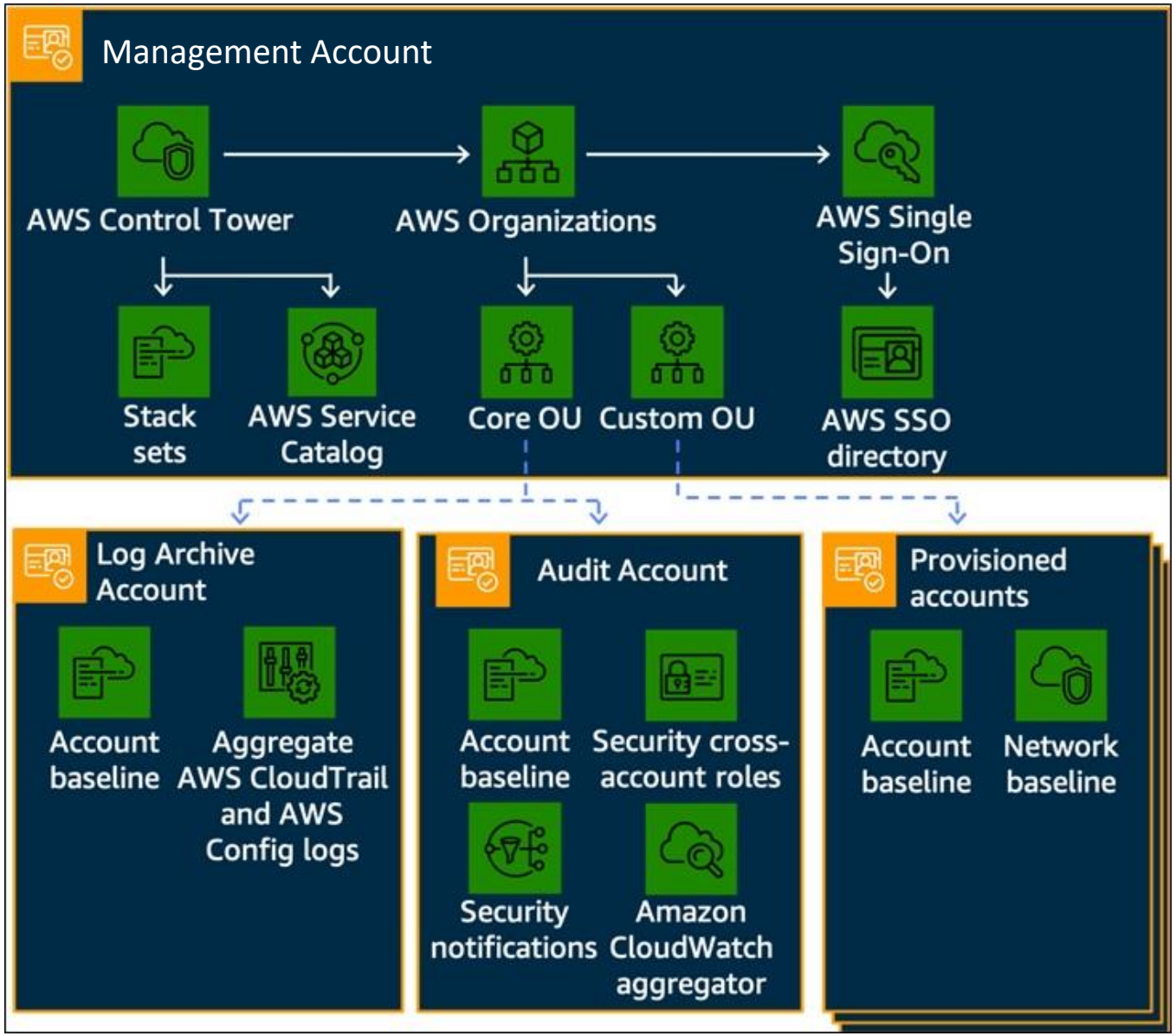
Dashboard

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

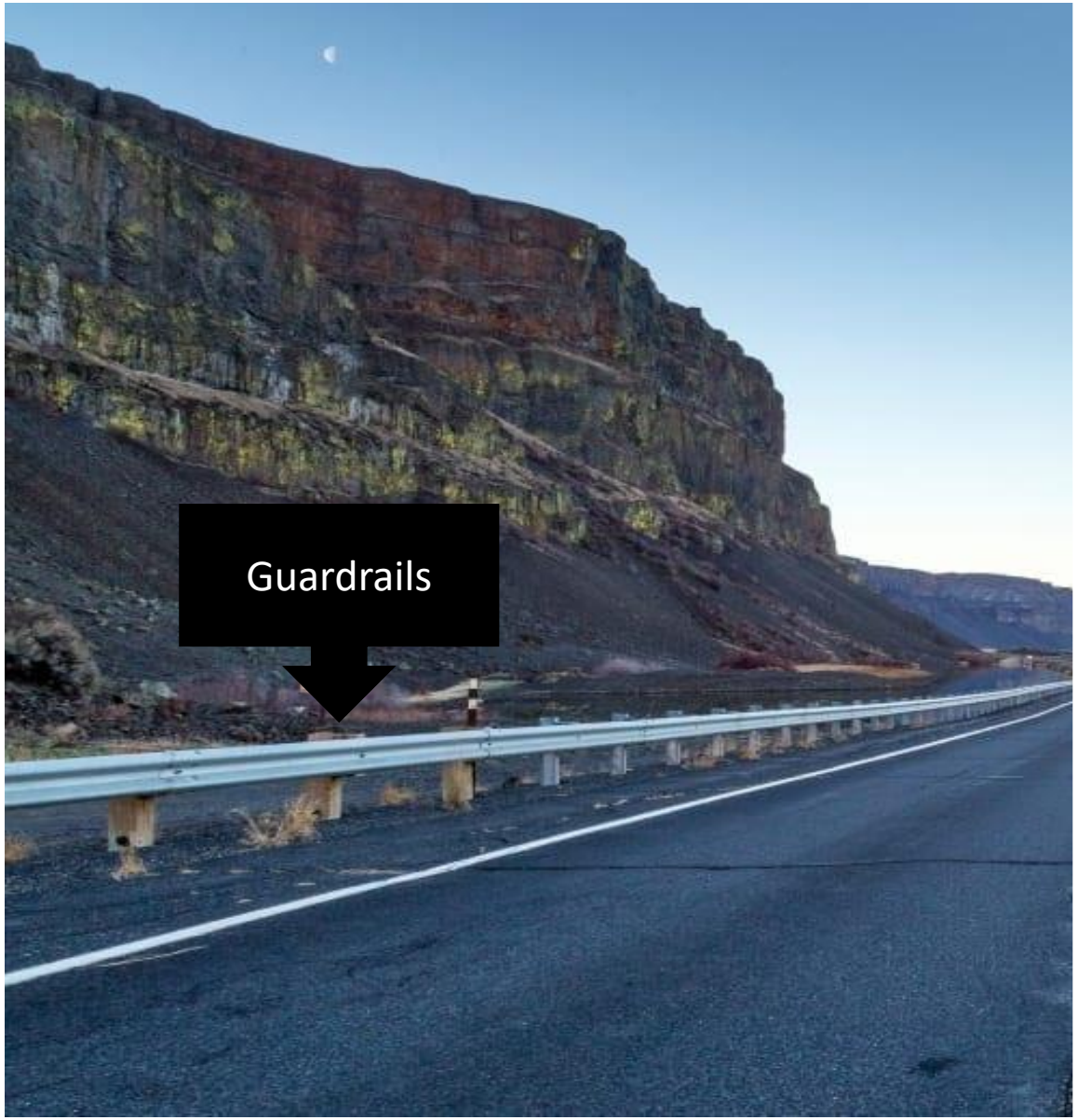
Landing zone

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

Preventive

Detective

- 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.

Guardrails

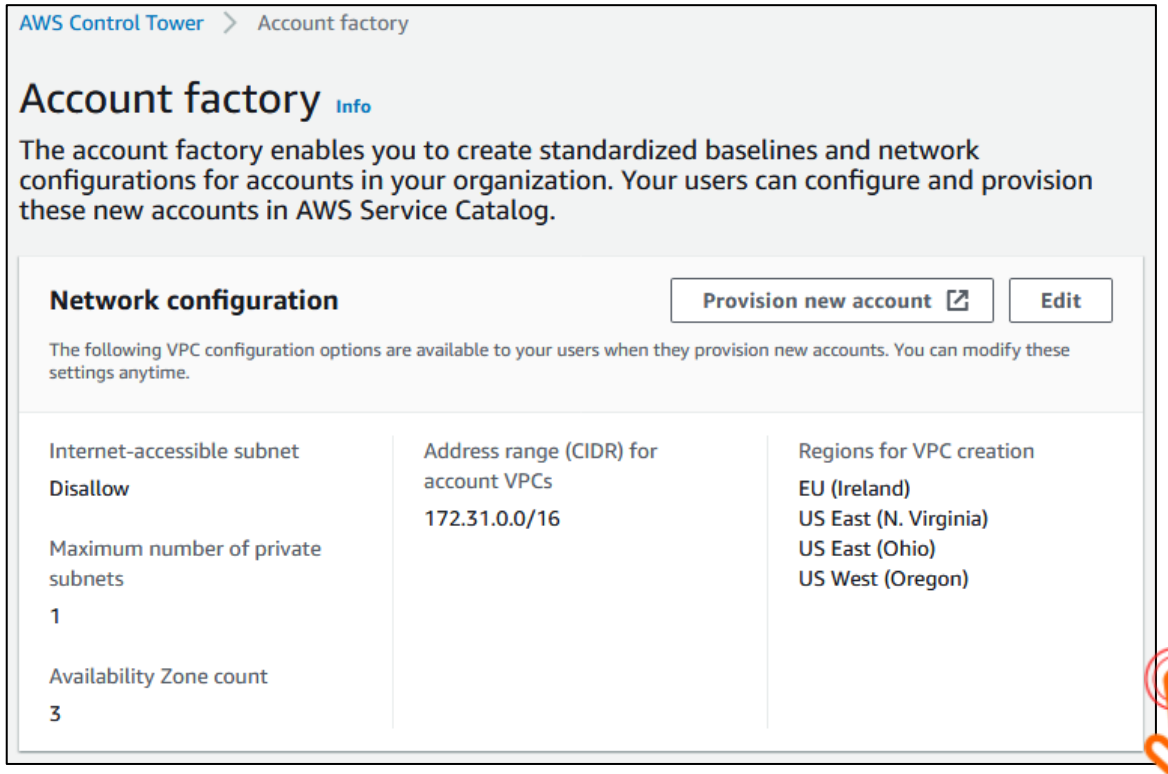
A high-level rule that provides ongoing governance for your overall AWS environment.

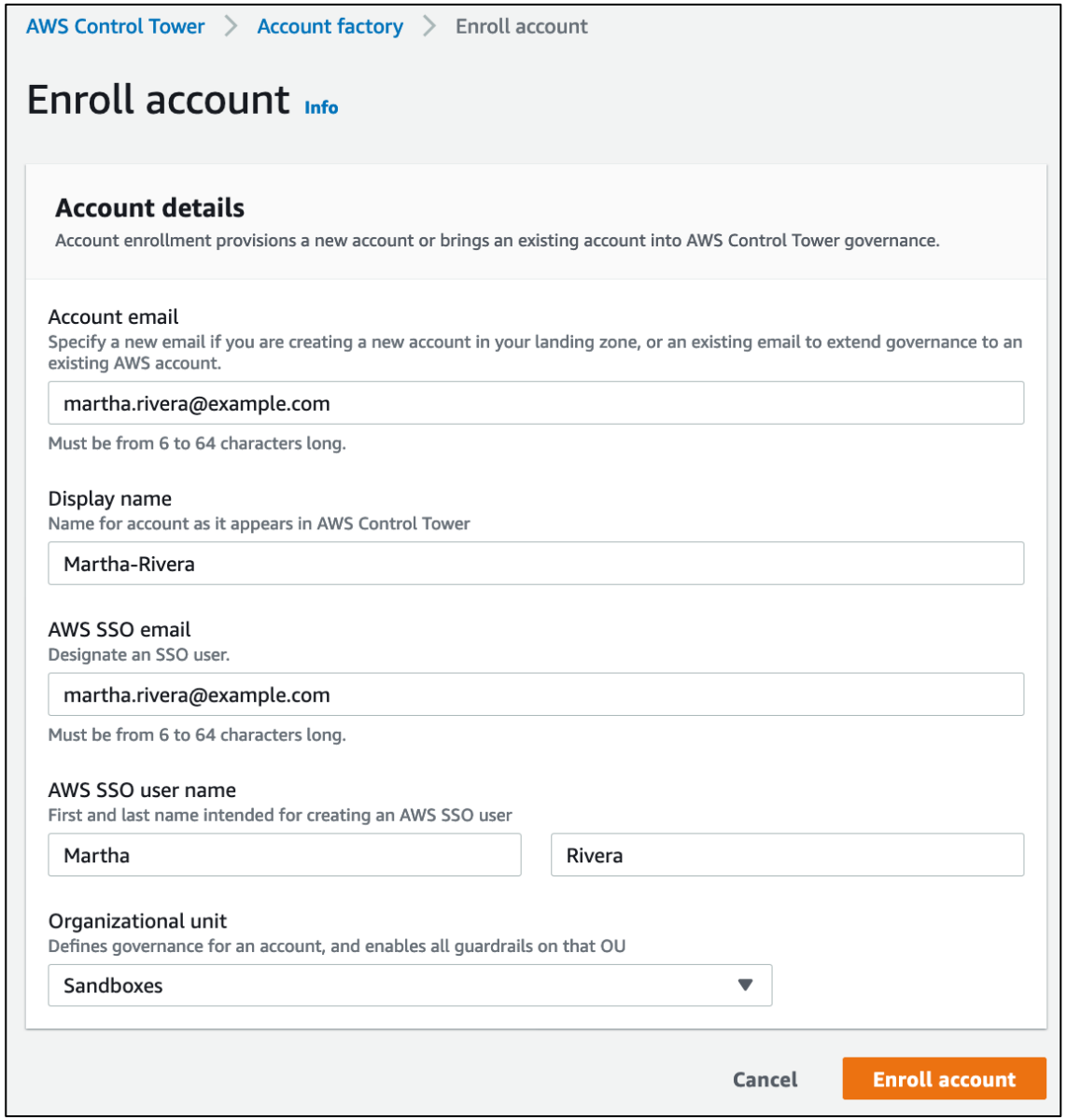
Account Factory

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

Account Factory

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





AWS Control Tower

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.

Account Factory

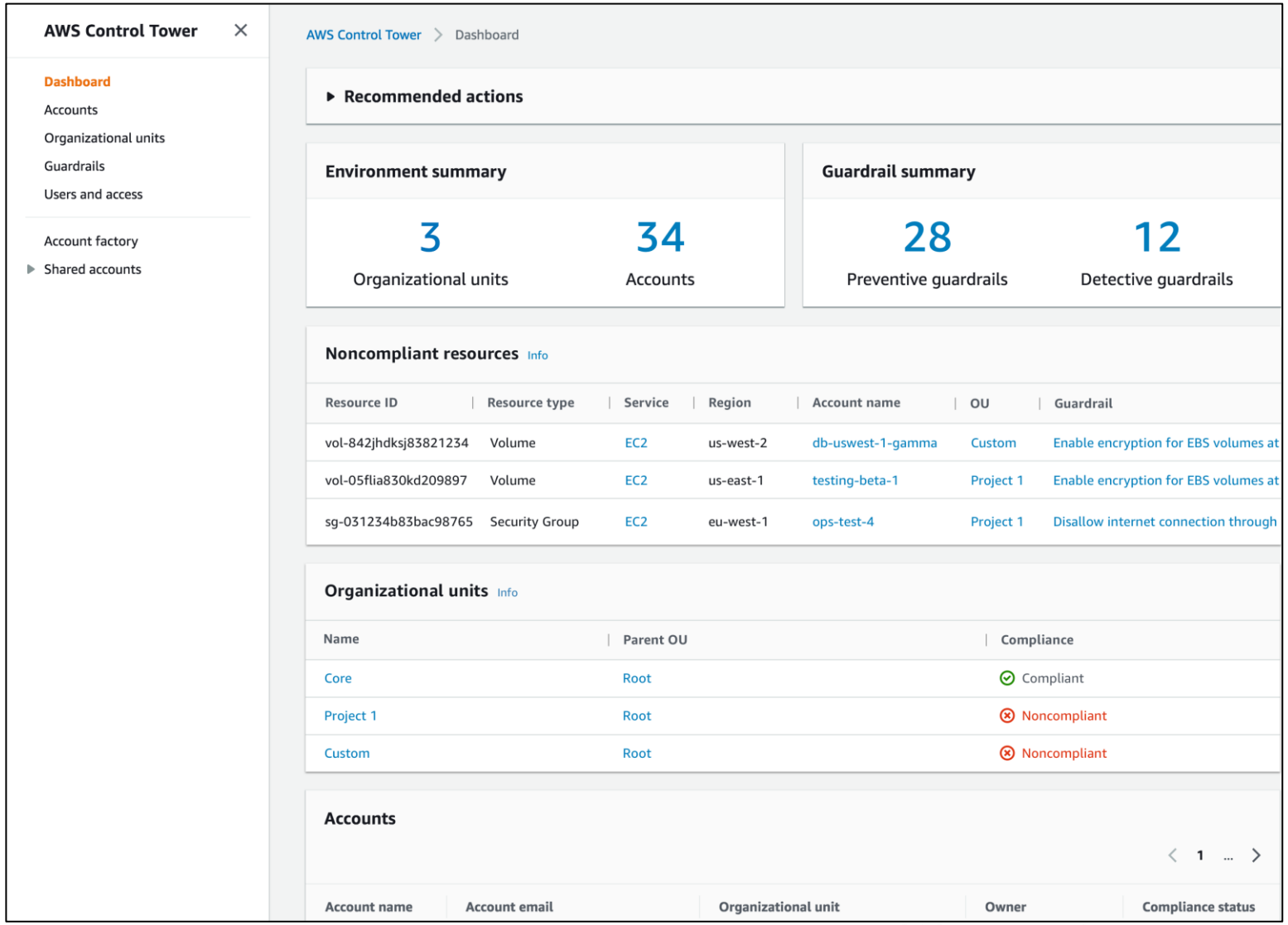
A configurable account template that helps provisioning of new AWS accounts with pre-approved account configurations.

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.



BeSA

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)

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