Welcome to AWS Cloud Practitioner

Your instructor:

Michael J Shannon

CISSP #42221 / #524169,
CCNP-Security, PCNSE7,
Security+, GIAC GSEC,
OpenFAIR, and
ITIL 4 Managing Professional

Class will begin at 10:00 A.M. Central Standard Time (CST)

AWS Cloud Practitioner Exam

AWS Certified Cloud Practitioner (CLF-C01)

For candidates who have the skills and knowledge required to successfully validate a general understanding of the AWS Cloud

There are two types of questions:

- Multiple-choice: Has one correct response and three incorrect responses (distractors)
- Multiple-response: Has two correct responses out of five options

AWS Cloud Practitioner Exam

Uses a scaled score from 100 through 1000, with a minimum passing score of 700

The examination uses a compensatory scoring model, which means that you do not need to “pass” the individual sections, only the overall examination

The exam is $100 USD and candidates have 90 minutes to complete the exam

Exam Domains

Domain	% of Exam
Domain 1: Cloud Concepts	28%
Domain 2: Security	24%
Domain 3: Technology	36%
Domain 4: Billing and Pricing	12%
Total	**100%**

Cloud Computing Defined

According to Amazon Web Services (AWS): “Cloud computing is the on-demand delivery of compute power, database, storage, applications, and other IT resources via the internet with pay-as-you-go pricing.”

Cloud Computing Defined

Cloud Computing has many advantages

- No need for large upfront investments
- No need to spend time managing hardware
- Provision the exact computing resource

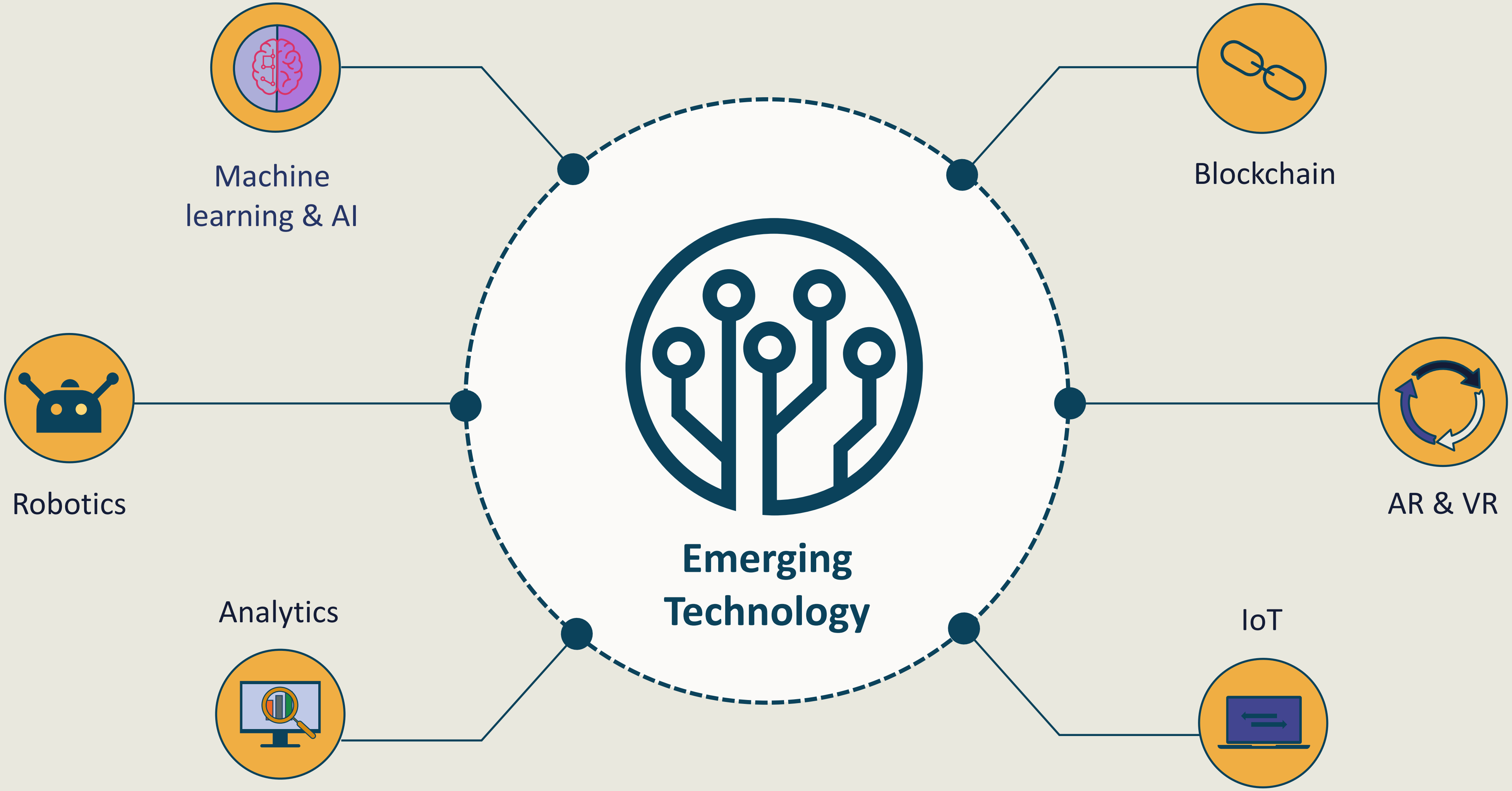
Cloud Computing Defined

- Servers
- Storage
- Databases
- Application services

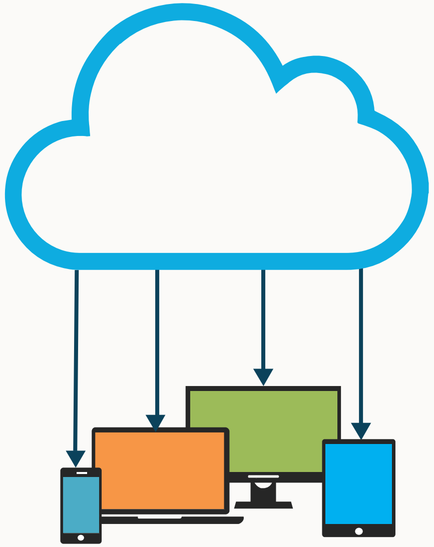
5 Characteristics of Cloud Services

- The traditional cloud model promotes availability and is composed of five essential characteristics:
  - On-demand self-service
  - Broad network access
  - Resource pooling
  - Rapid elasticity
  - Measured Service

Cloud Computing and Emerging Technology

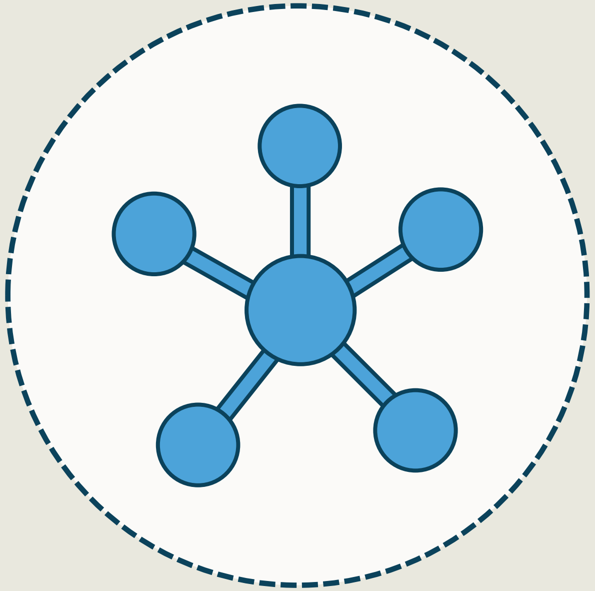


Cloud Computing Types

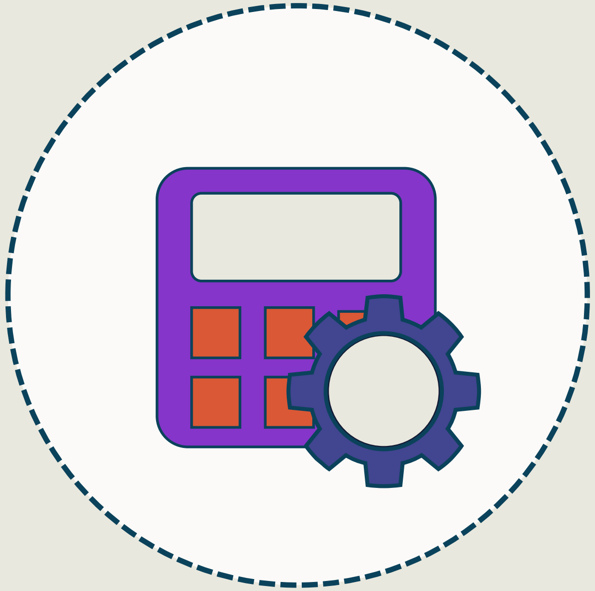


- Infrastructure-as-a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)

Infrastructure-as-a-Service (IaaS)



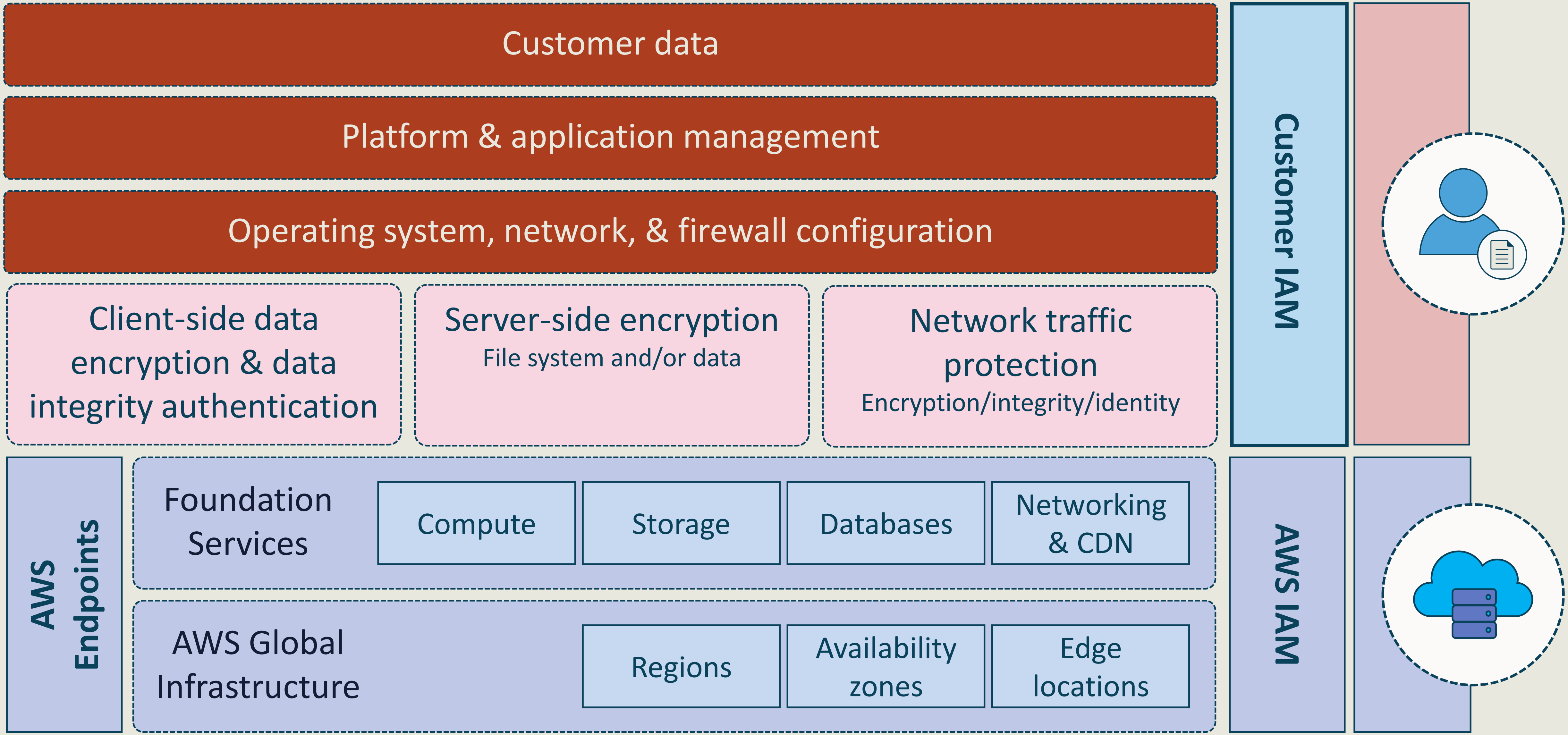
Networking and
Content Delivery



Compute

Storage & Database

IaaS at Amazon Web Services



Customer data

Platform & application management

Operating system, network, & firewall configuration

Client-side data encryption & data integrity authentication

Server-side encryption
File system and/or data

Network traffic protection
Encryption/integrity/identity

Customer IAM

AWS Endpoints

Foundation Services

Compute

Storage

Databases

Networking & CDN

AWS Global Infrastructure

Regions

Availability zones

Edge locations

AWS IAM

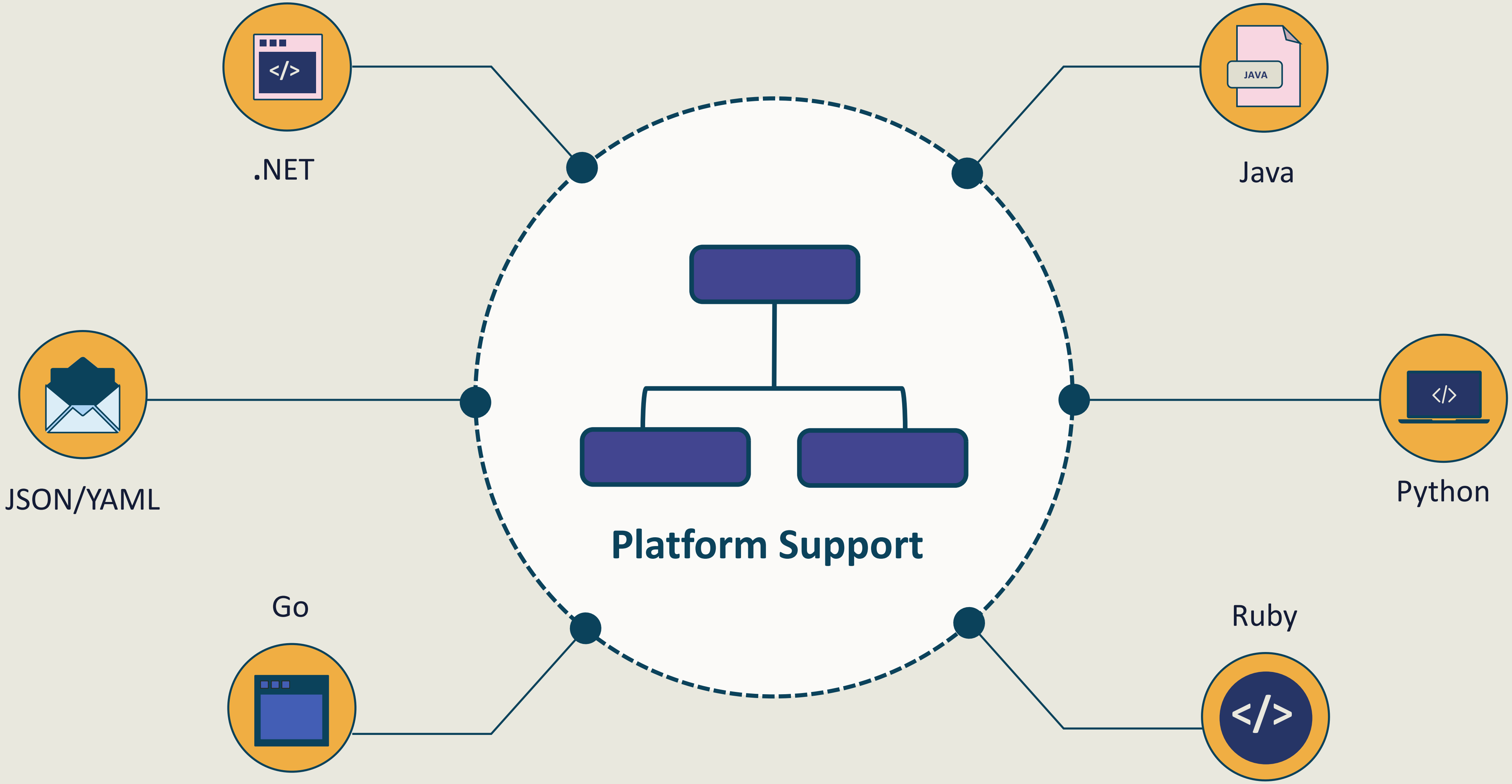
Example: AWS Virtual Private Cloud (VPC)

- Provision a logically isolated portion of the AWS Cloud
- Have complete control over your environment
  - Choosing your own IPv4 or IPv6 address ranges, subnet design
  - Configure route tables and network gateways

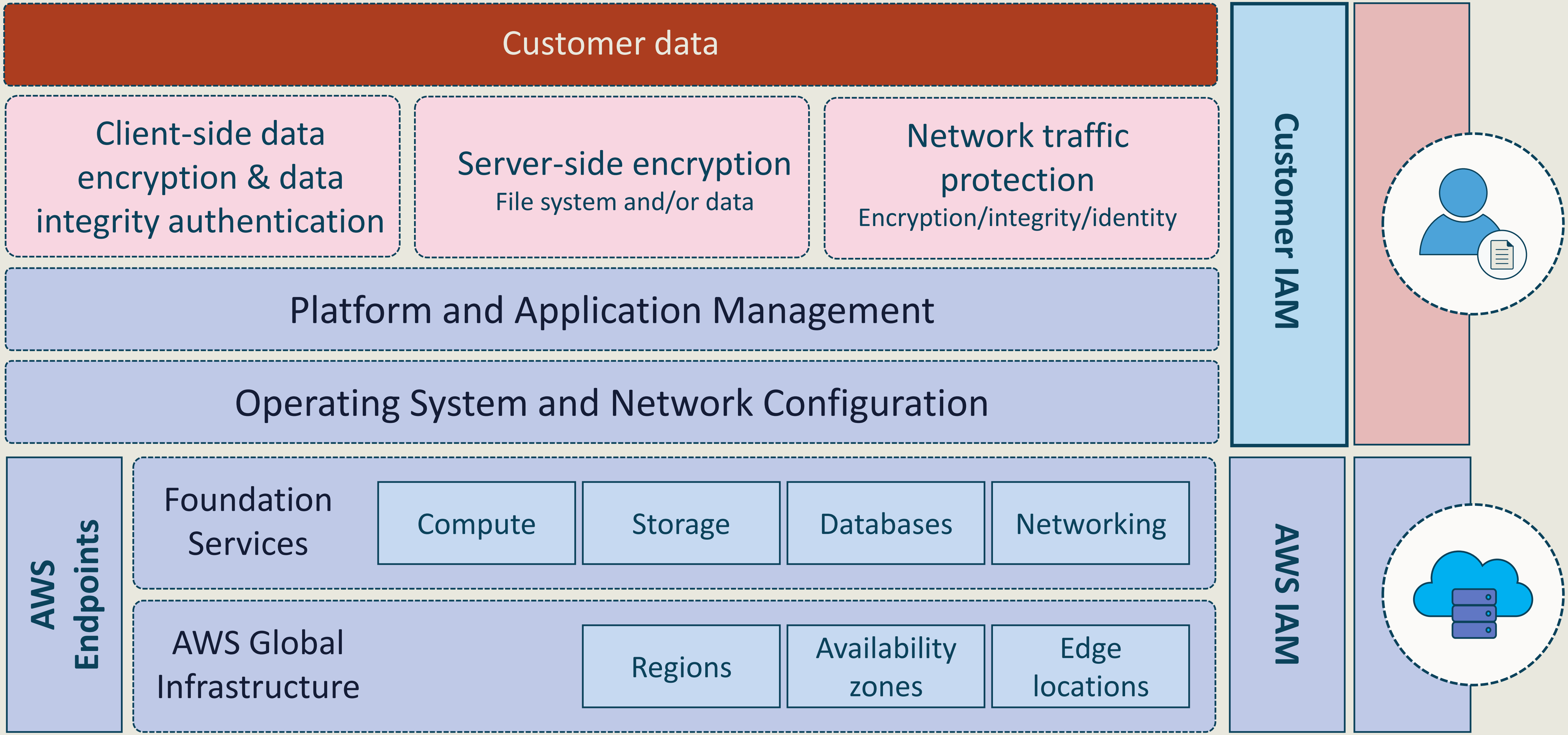
Platform-as-a-Service (PaaS)

- Customers still do not manage/control the AWS infrastructure
- Consumers control applications and services
- Programming languages, libraries, services, and tools
- Some services are more “managed” by AWS than others

Platform-as-a-Service (PaaS)



PaaS at Amazon Web Services



Customer data

Client-side data encryption & data integrity authentication

Server-side encryption
File system and/or data

Network traffic protection
Encryption/integrity/identity

Platform and Application Management

Operating System and Network Configuration

Customer IAM

AWS Endpoints

Foundation Services

Compute

Storage

Databases

Networking

AWS Global Infrastructure

Regions

Availability zones

Edge locations

AWS IAM

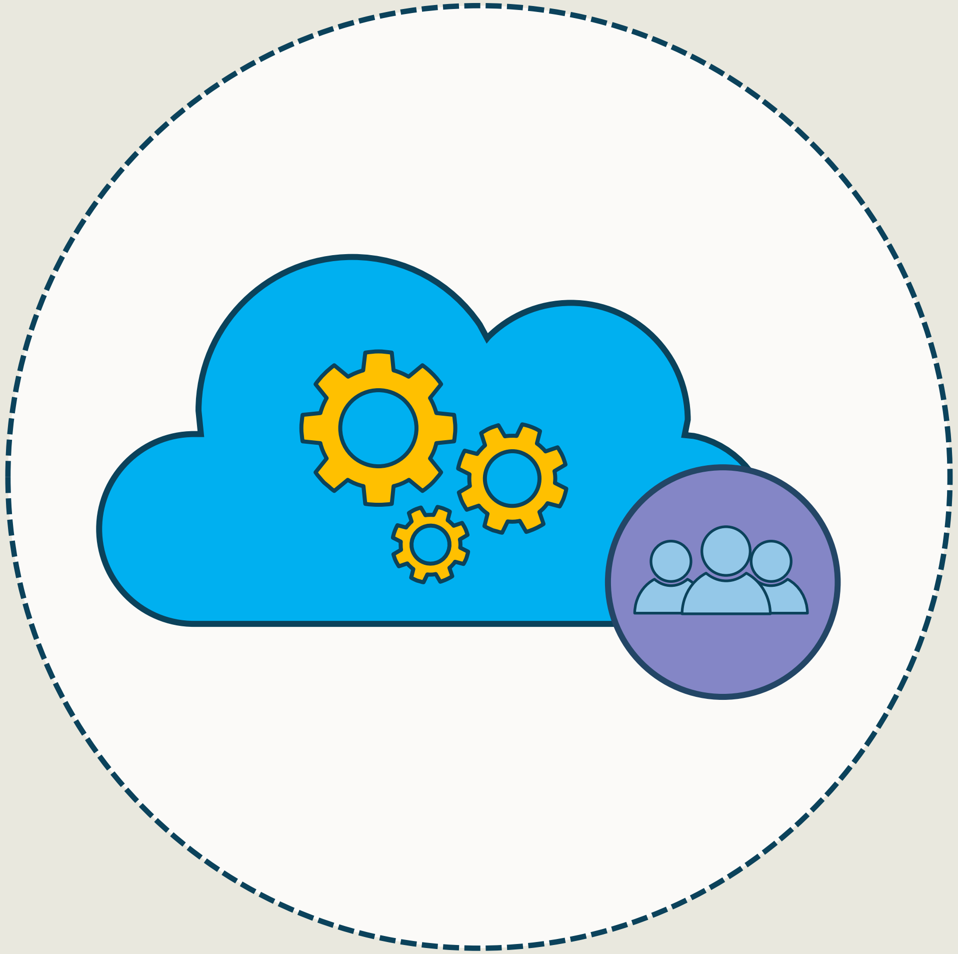
Example: Amazon Lightsail

Offers everything needed to build an application or website using a cost-effective

Provides virtual servers, storage, databases, and networking

Excellent for simple web applications and sites, business software, and development/testing

Software-as-a-Service



The consumer uses the service provider’s applications running on a cloud infrastructure

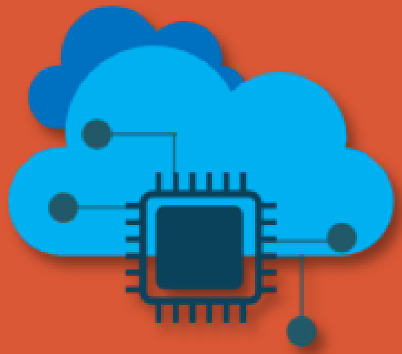
The consumer often does not even manage or control the individual application capabilities

AWS Cloud Deployment Models

- Cloud-based
- Hybrid
- On-premises

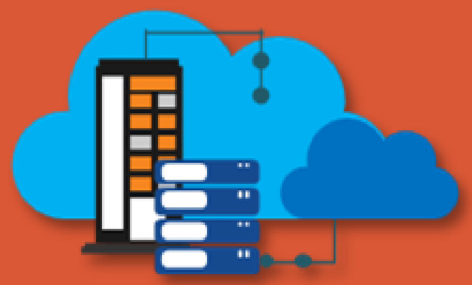
Cloud-based Cloud Deployment

- A fully deployed solution in the AWS Cloud
- Every component of the application operates in the cloud infrastructure
- Cloud-based applications have either been generated in the cloud or have been transferred from an existing enterprise
- Can be built on low-level virtualized infrastructure components
- Can also leverage higher level services that abstract from the management, architectural, and scaling needs of the core infrastructure



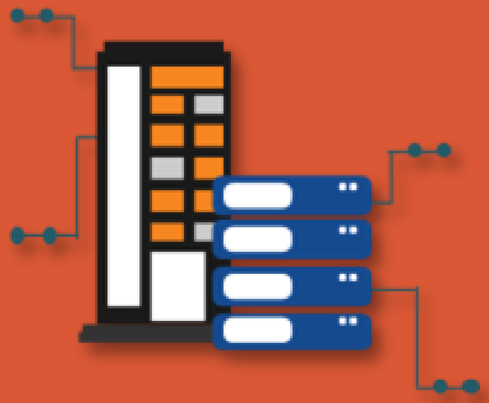
Hybrid Cloud Deployment

- A method for connecting infrastructure and applications between AWS Cloud-based resources and other resources that are not placed in the cloud
- The most common type of hybrid deployment is between the provider's cloud and a standing on-premises enterprise
- Can be used to migrate, expand, or grow an organization's infrastructure into a cloud solution while linking internal systems to AWS Cloud resources
- Often used by organizations to "burst up" to the cloud during peak demand times or special situations

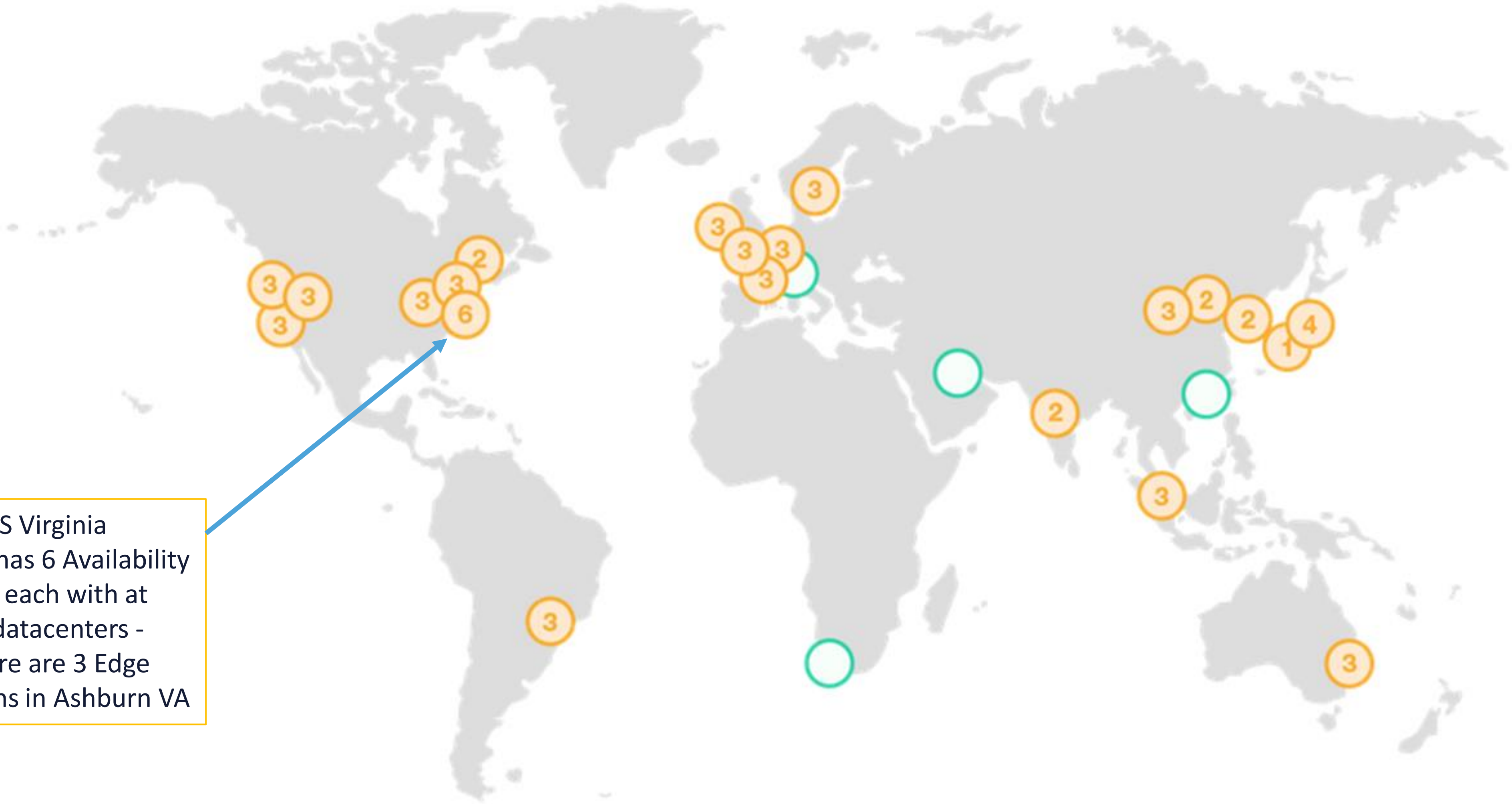


On-Premises Cloud Deployment

- Entails using virtualization and resource management tools on-site only
- Sometimes called a "private cloud" deployment although resources can be hosted privately at AWS
- Does not offer benefits of cloud computing but is often needed for regulations and governance
- This deployment model is very similar to a traditional IT infrastructure
- The difference is that the entity is using hypervisors, application management, and other virtualization technologies to attempt to enhance resource utilization and lower costs



Introduction to Amazon Web Services



The AWS Virginia Region has 6 Availability Zones – each with at least 2 datacenters - and there are 3 Edge Locations in Ashburn VA

AWS Value Proposition

AWS as the producer, we as the consumer to co-create value and deliver data, applications, services, and solutions to the world

- **Agility**
- **Elasticity**
- **Cost**
- **Flexibility**
- **Security**

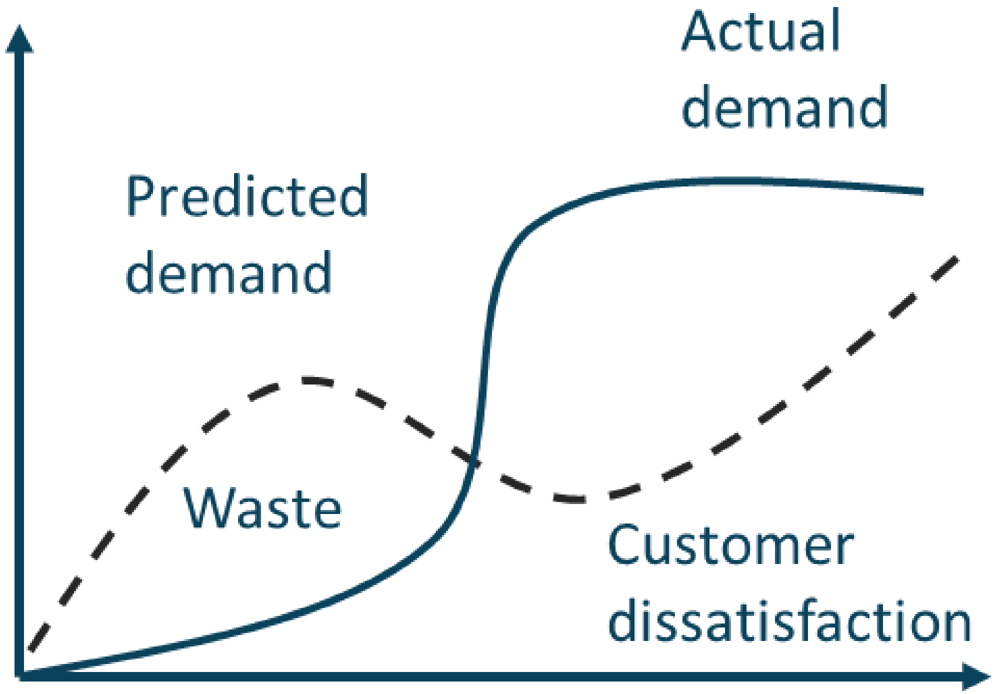
Agility

- Leveraging for rapid deployment, testing, experimentation, & innovation
- Overcoming geographical limitations
- Getting content as close to the consumer as possible
- Reducing time and cost for testing and experimentation
- Allows consumers better innovation

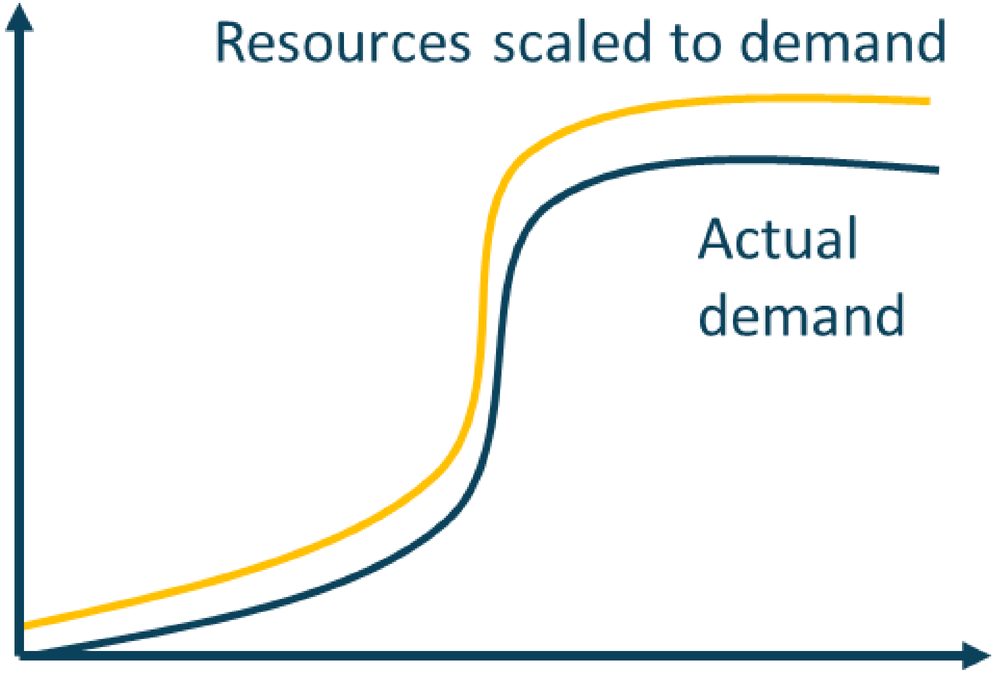
Elasticity

- Elasticity is the ability to almost instantly provision and de-provision resources
- Challenges with predicting demand leads to higher costs
- Leveraging dynamic auto-scaling technologies
- “Elasticity of the cloud allows us to add thousands of virtual servers and petabytes of storage within minutes, making such an expansion possible. Leveraging multiple AWS cloud regions, spread all over the world, enables us to dynamically shift around and expand our global infrastructure capacity, creating a better and more enjoyable streaming experience for Netflix members wherever they are."
  - - Yury Izrailevsky, VP Cloud and Platform Engineering, Netflix (from Netflix Media Center)

Elasticity



Rigid On-premises Resources



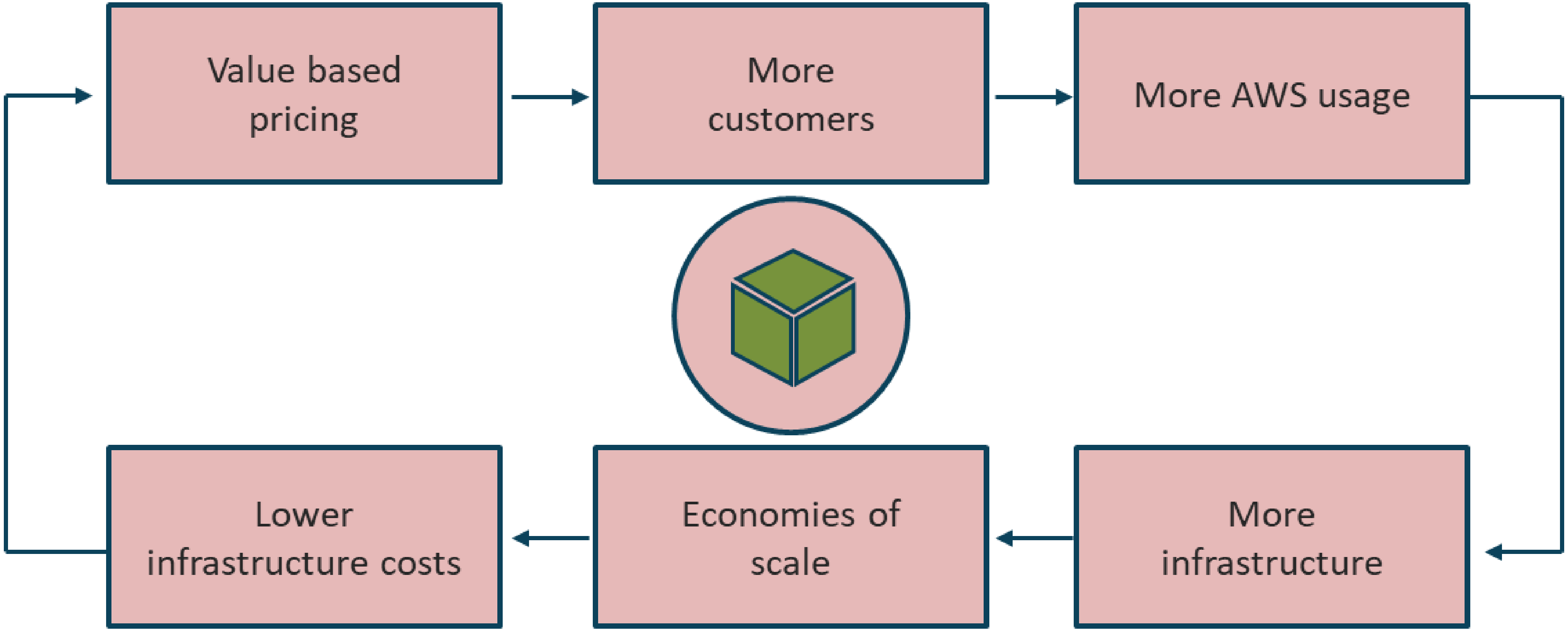
Elastic Cloud-based Resources

Cost

For many organizations, using the cloud to reduce costs is the dominant factor in the value proposition

- Cabling
- Cooling
- Power
- Networking
- Racks
- Ongoing maintenance and upgrades
- Racks
- Servers
- Storage
- Training and Certifications
- Labor

Cost



Value based pricing

More customers

More AWS usage

More infrastructure

Economies of scale

Lower infrastructure costs

Flexibility

- AWS delivers a continuously increasing set of infrastructure and software services
- These can be leveraged by all types of public and private organizations of all sizes and sectors
- These services empower organizations to:
  - Better engage with their customers
  - Manage their internal processes
  - Analyze data from internal and external sources to gain competitive advantage

Security

Secure non-descript datacenters

IAM

Secure endpoints

KMS

VPNs

VPC security

Introduction to Cloud Economics

AWS offers an enormous variety of services, products and solutions that empower organizations to be successful and profitable in meaningful and measurable ways

- Reports from various entities like Gartner and International Data Corporation (IDC) point out that AWS customers get important financial benefits that help increase growth, drive productiveness, and realize important long-term cost reductions

Source: “Cloud Economics Center". August 15, 2017. https://aws.amazon.com/economics/

Cloud Economics

- 62% realize a more efficient IT infrastructure staff
- 51% achieve lower 5-year cost of operations
- 90% use less staff time to deploy new storage
- 25% attain more productive development teams
- 6 months to payback outlays

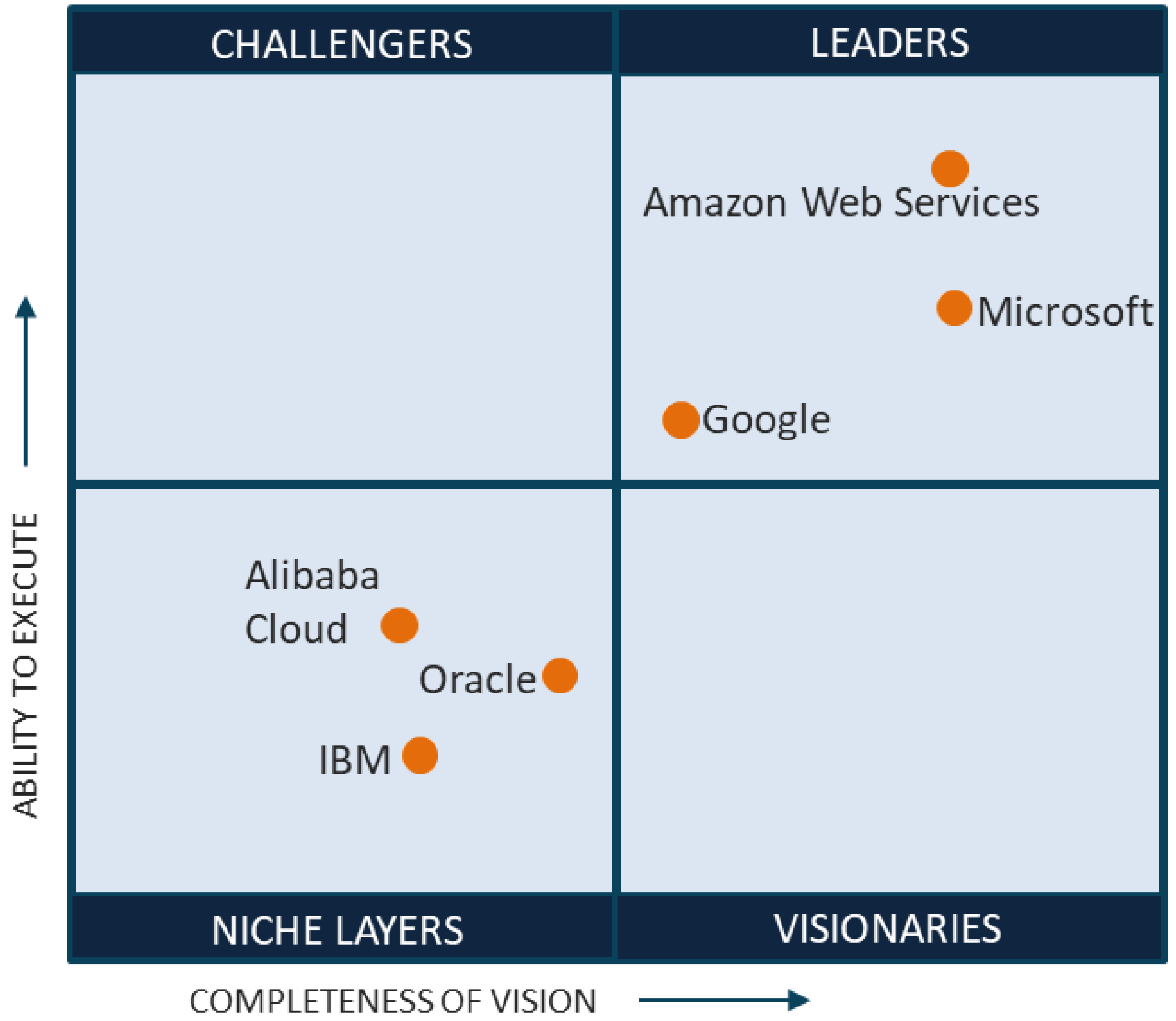
Source: “Cloud Economics Center". August 15, 2017. https://aws.amazon.com/economics/

Cloud Economics

- Gartner rates AWS the best cloud provider
- In the 2019 Magic Quadrant for Cloud Infrastructure as a Service, Worldwide, Gartner placed Amazon Web Services in the "Leaders" quadrant and rated AWS as having both the furthest completeness of vision and the highest ability to execute

Source: “Cloud Economics Center". August 15, 2019. https://aws.amazon.com/economics/

Gartner Compares Cloud Providers



Source: "Magic Quadrant for Cloud Infrastructure as a Service, Worldwide". https://www.gartner.com/en/documents/3738058/magic-quadrant-for-cloud-infrastructure-as-a-service-wor.

Comparing AWS to Other Providers

- Enterprises make larger annual financial commitments to AWS
- Organizations deploy more mission-critical workloads on AWS
- AWS has a broader range of customer profiles, ranging from startups and small and midsize businesses (SMBs) to large enterprises
- AWS is the most mature, enterprise-ready provider, with the strongest track record of customer success and the most useful partner ecosystem

Source: “Cloud Economics Center". August 15, 2017. https://aws.amazon.com/economics

AWS Free Tier Model

12 Months Free

Always Free

Trials

12 Month Free Tier Option

- The AWS Free Tier provides customers the ability to explore and try out AWS services free of charge up to specified limits for each service
- Services with a 12-month Free Tier allow customers to use the product for free up to itemized limits for one year from the date the of account creation
- If your usage exceeds the free tier limits, you simply pay standard, pay-as-you-go service rates

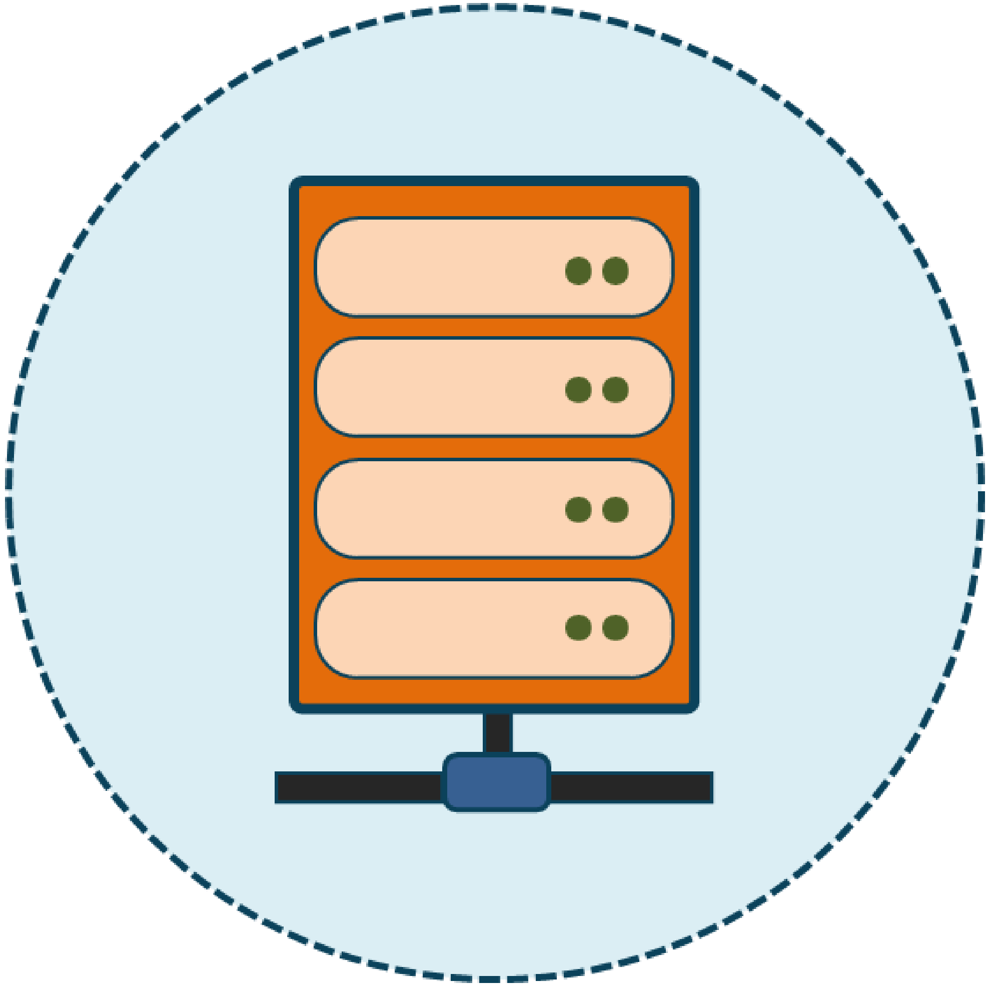
Pay As You Go Pricing

- AWS offers a "pay-as-you-go” approach to pricing for their large array of cloud products and services
- You will only pay for the specific services that you need and only for the time that you are utilizing them
- You will only incur fees for the actual resources and services that your enterprise uses

Pay As You Go

Easily adapt to changing business needs

- No more necessity to overcommit on budgets
- Improve reaction and response to changes
- Adapt business to real needs and not forecasts
- Reduce risks of over-positioning or missing capacity



Pay As You Go

- Organizations stay agile and reactive
- Always able to meet scaling demands
- Redirect focus to innovation and modernization
- Reduce the difficulty and complexity of procurement
- Empower the business to be fully elastic

Save When You Reserve

- AWS offers a Reserved Instance option for certain services like EC2 and RDS
- If your enterprise pays a higher upfront fee, you will enjoy a better discount
- According to AWS, you can save up to 75% over similar demand by reserving capacity
- With Reserved Instances, you can save up to 75% over equivalent on-demand capacity
- Reserved Instances are available in 3 options:
    - All up-front (AURI)
    - Partial up-front (PURI)
    - No upfront payments (NURI)

Save When You Reserve

EC2
m4
large

1 Year No Upfront

32% SAVINGS

$955/year (on demand) vs. $650/year (NURI)

EC2
m4
large

1 Year Partial Upfront

42% SAVINGS

$955/year (on demand) vs. $554/year (PURI)

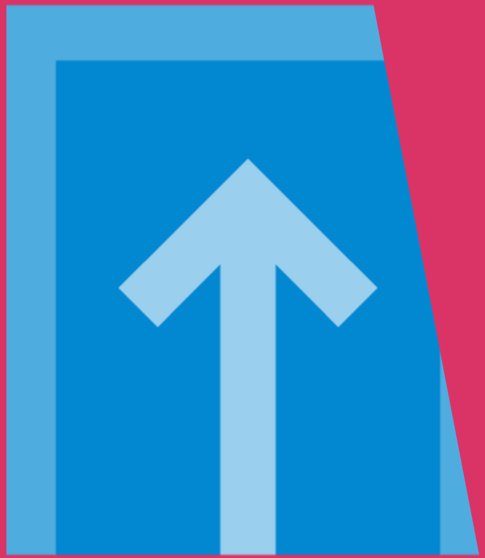
EC2
m4
large

1 Year All Upfront

43% SAVINGS

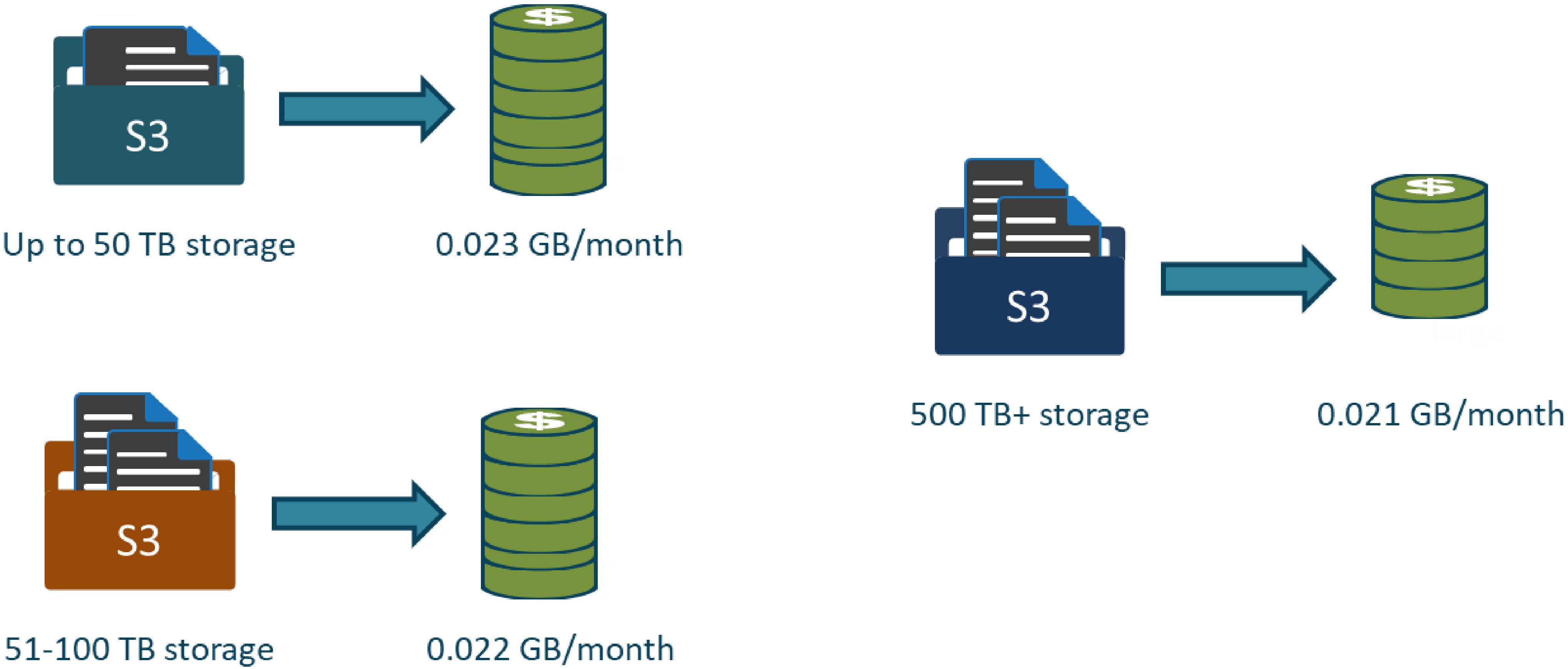
$955/year (on demand) vs. $545/year (AURI)

Pay Less When You Use More



- Use managed services to help address needs
- Get volume-based discounts
- Gain substantial savings as usage increases
- Take advantage of S3 tier-based pricing

Save When You Use More



Up to 50 TB storage

0.023 GB/month

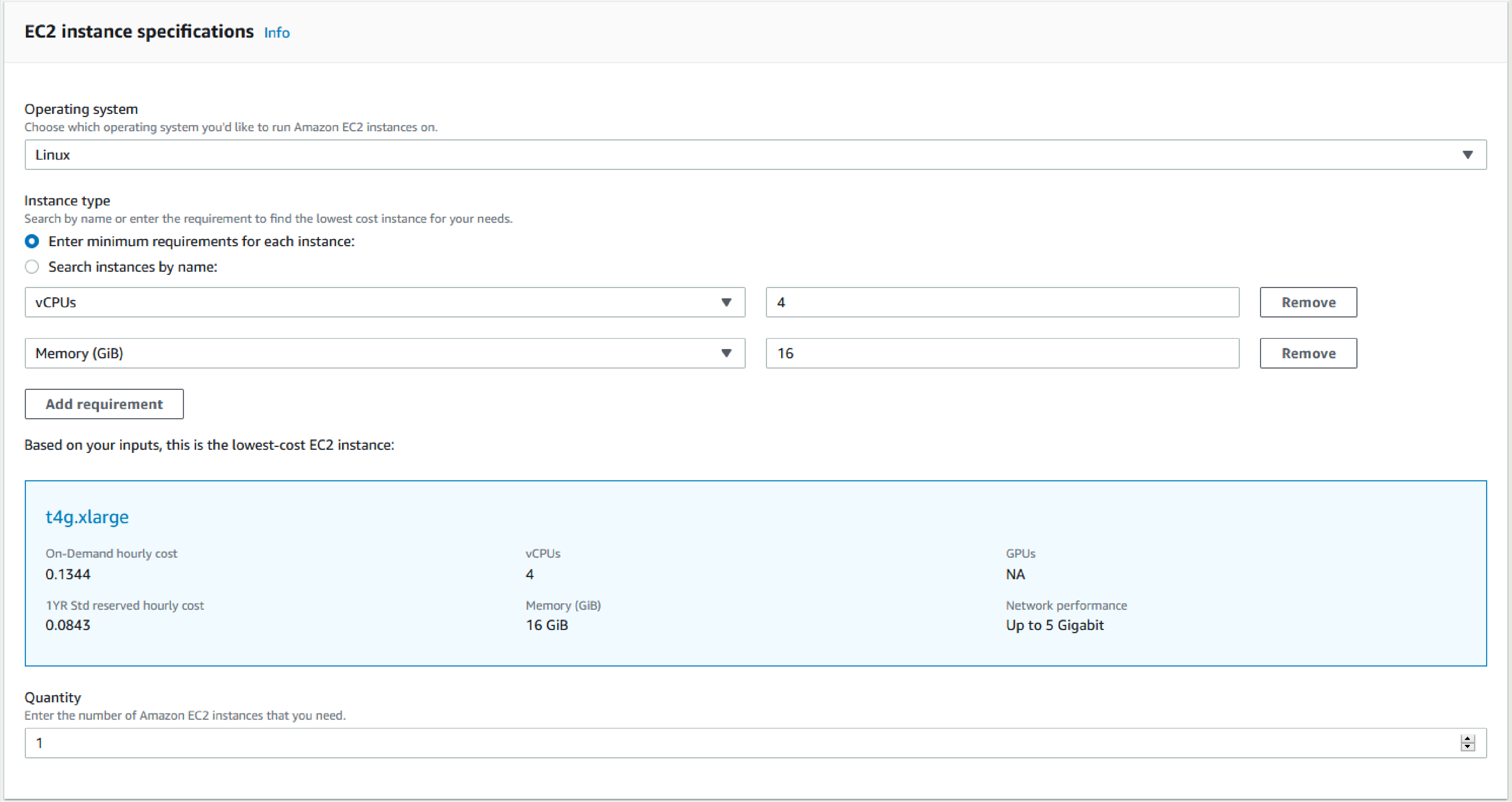
51-100 TB storage

0.022 GB/month

500 TB+ storage

0.021 GB/month

AWS Pricing Calculator



EC2 instance specifications

Operating system

Choose which operating system you'd like to run Amazon EC2 instances on.

Linux ▼

Instance type

Search by name or enter the requirement to find the lowest cost instance for your needs.

● Enter minimum requirements for each instance:

○ Search instances by name:

vCPUs ▼	4	Remove
Memory (GiB) ▼	16	Remove

Based on your inputs, this is the lowest-cost EC2 instance:

t4g.xlarge

On-Demand hourly cost 0.1344	vCPUs 4	GPUs NA
1YR Std reserved hourly cost 0.0843	Memory (GiB) 16 GiB	Network performance Up to 5 Gigabit

Quantity

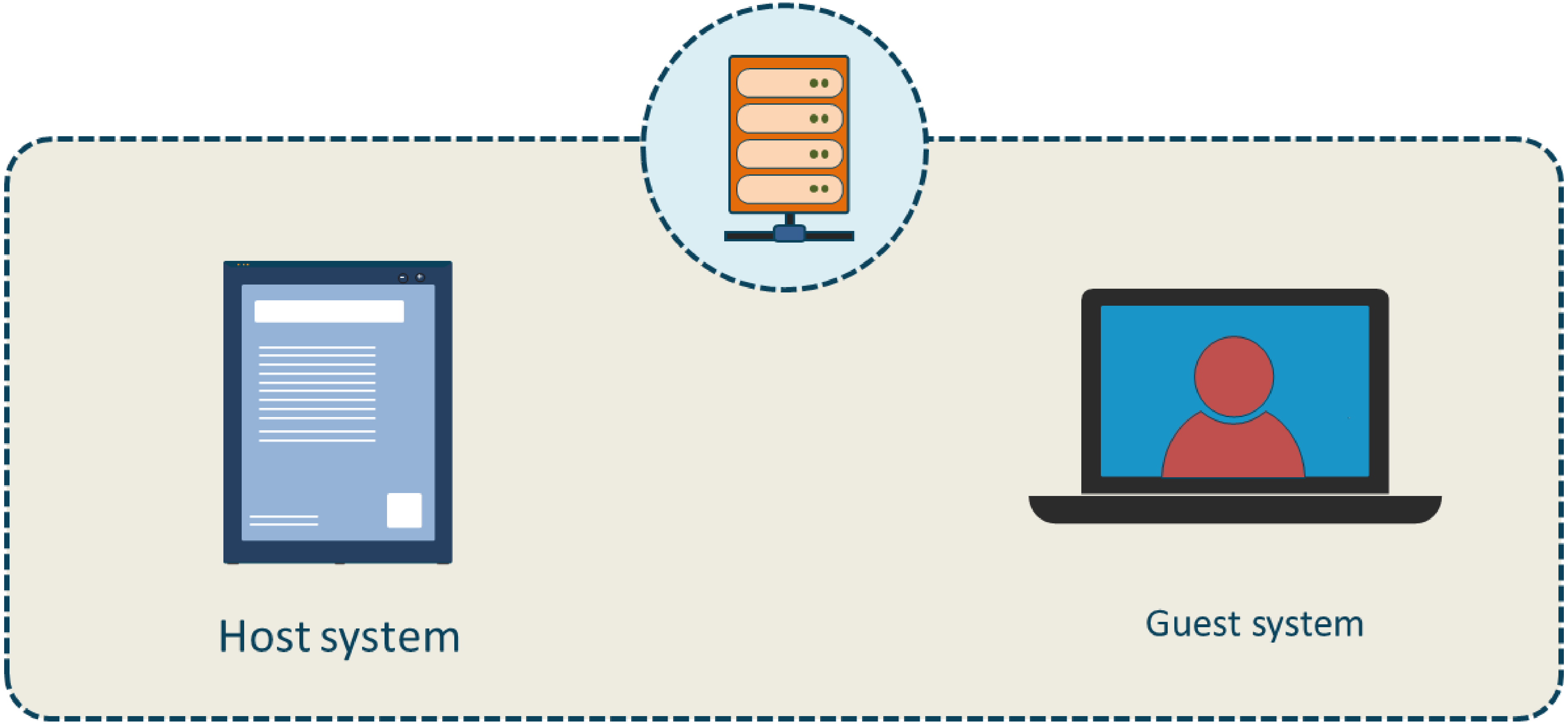
Enter the number of Amazon EC2 instances that you need.

1

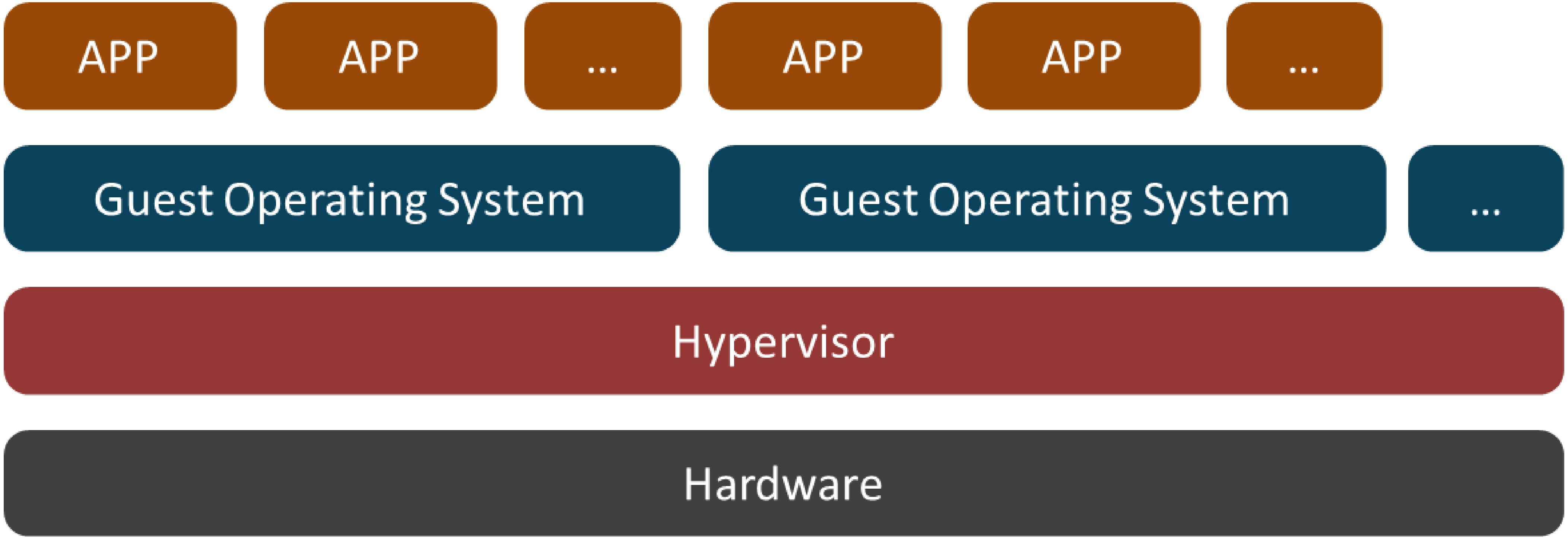
Virtualization

- A hypervisor is the software that produces and manages a virtual infrastructure, allowing multiple operating systems to run and share resources on a single physical machine

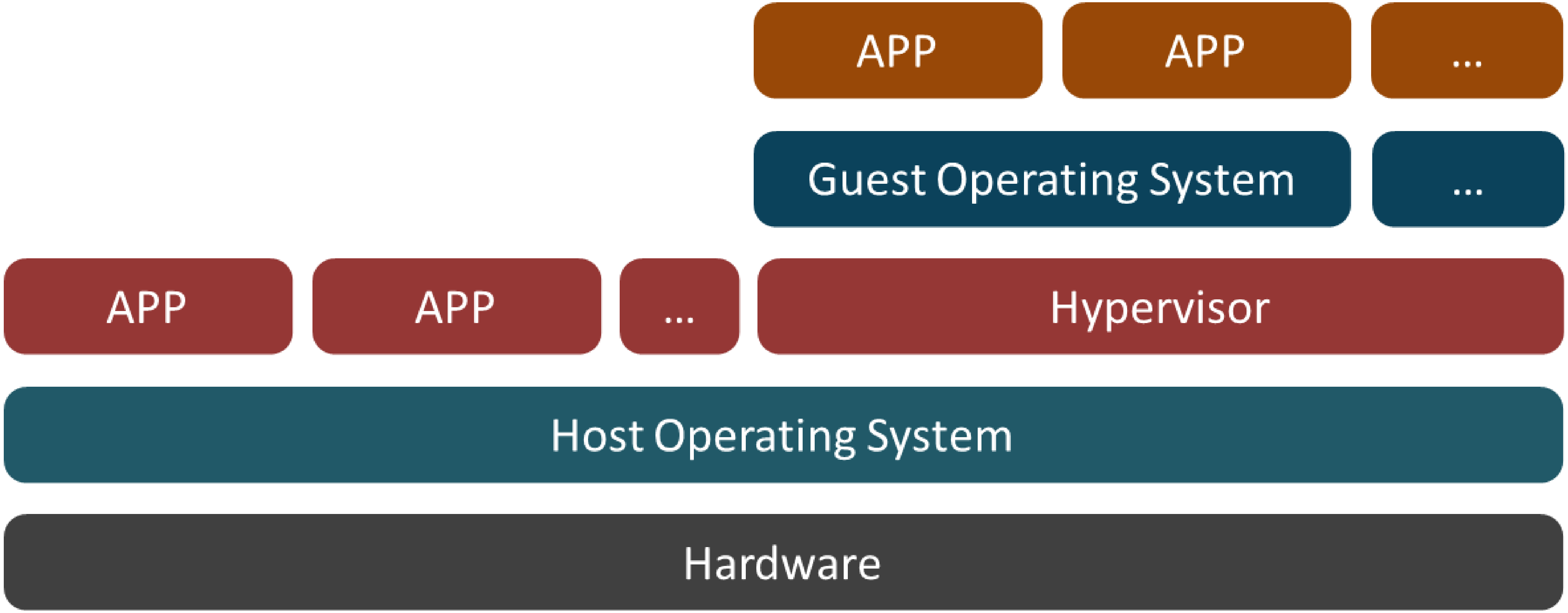
Hypervisors



Type 1 Hypervisors



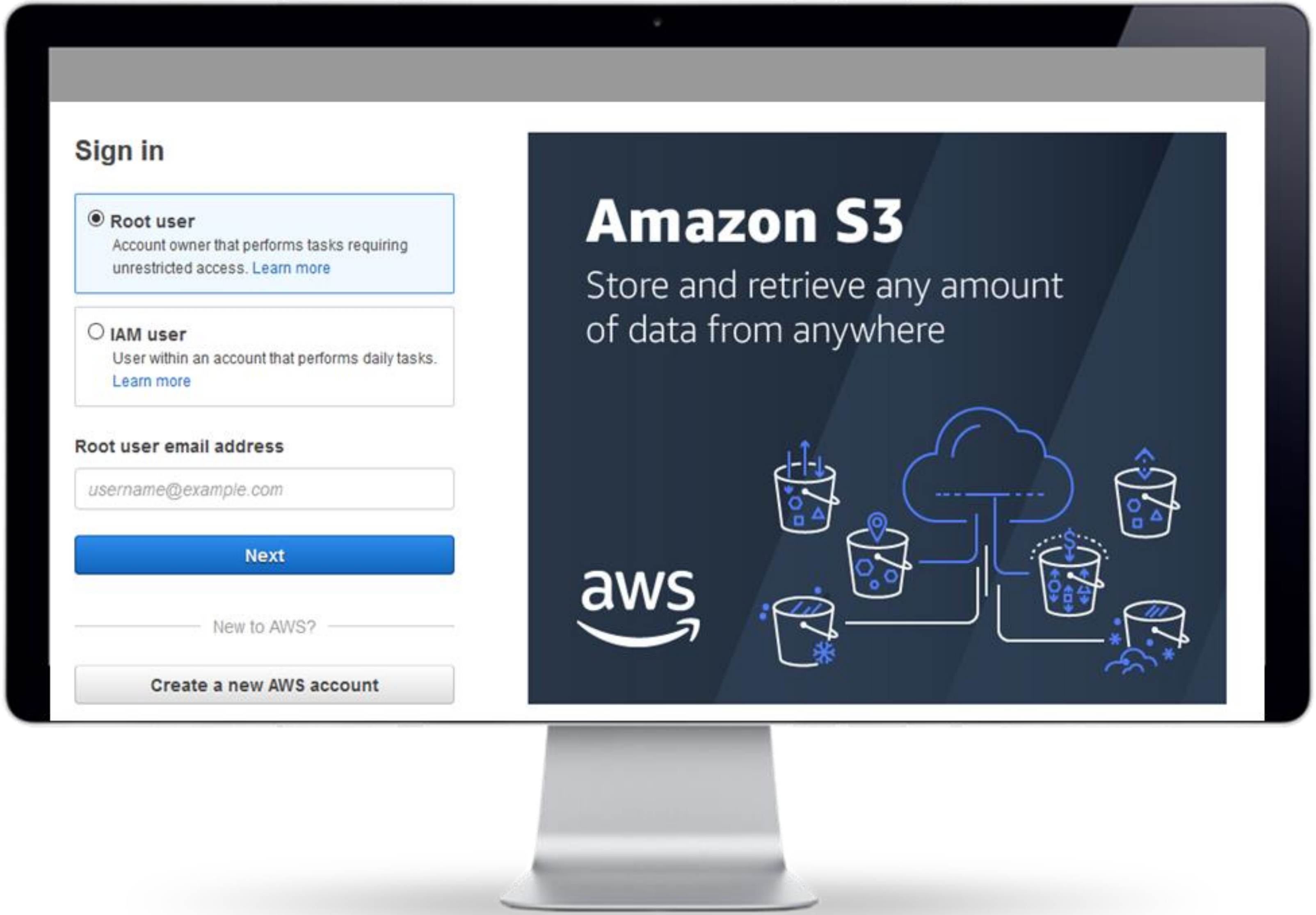
Type 2 Hypervisors



Containers

- In AWS, you can also build and run containerized applications
- A container is a discrete environment within an operating system where one or more applications can run, typically assigned all the resources and dependencies needed to function
- You can also use containers for processes and workflows in which there are important requirements for security, reliability, and scalability
- Amazon Elastic Container Service (Amazon ECS) is a fully managed container orchestration service

Understanding the Root Account



Sign in

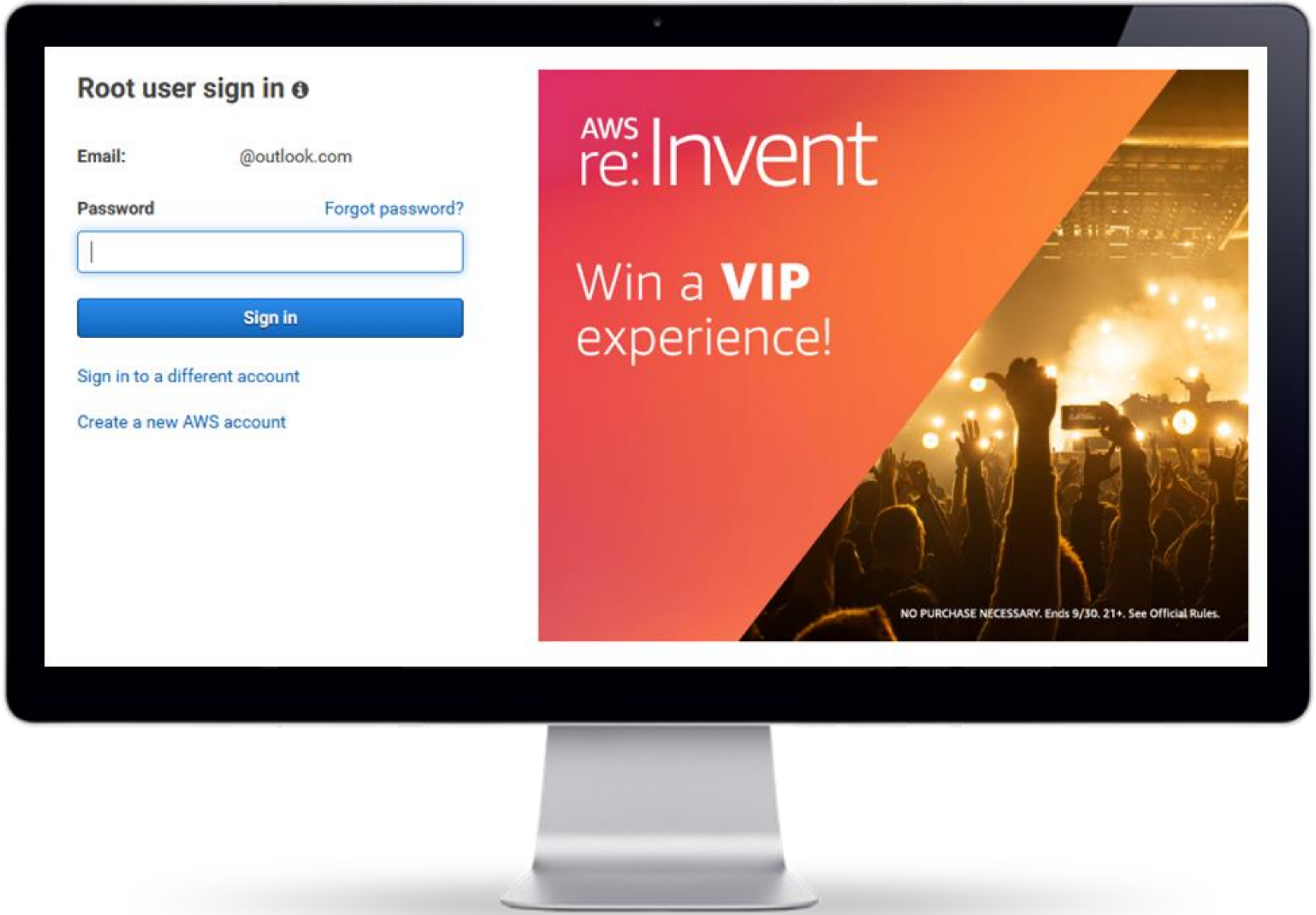
● Root user
Account owner that performs tasks requiring unrestricted access. Learn more

○ IAM user
User within an account that performs daily tasks. Learn more

Root user email address

username@example.com

Understanding the Root Account



Root user sign in

Email: @outlook.com

Password Forgot password?

Sign in

Sign in to a different account

Create a new AWS account

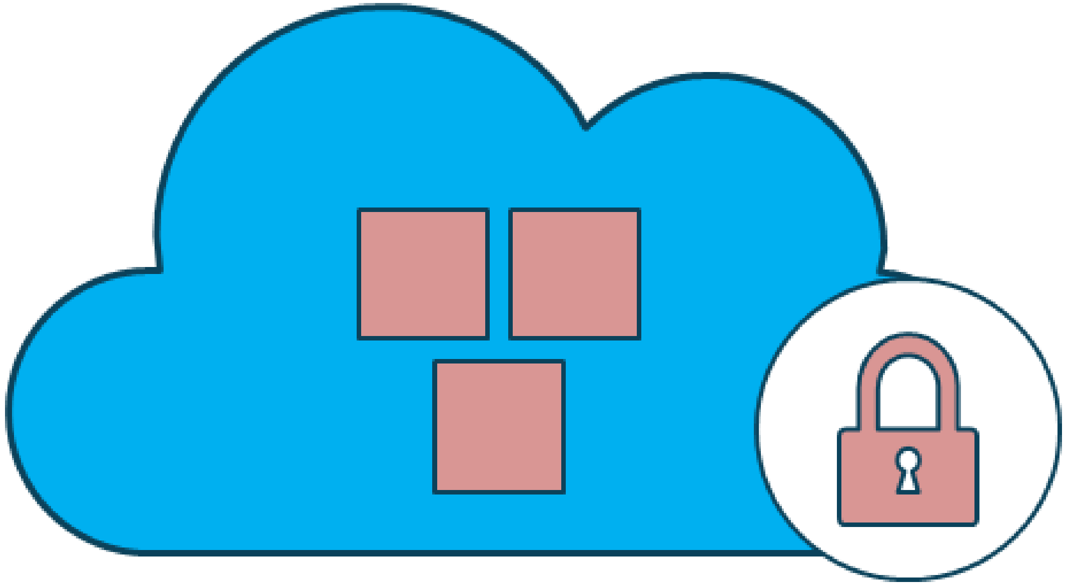
Root Account Distinctives

- IAM password policy does not apply to the root account
- Change the support plan, payments options, and billing
- Close an AWS account or sign up for GovCloud
- Transfer a Route 53 domain to another account
- Create an AWS-created X.509 signing certificate

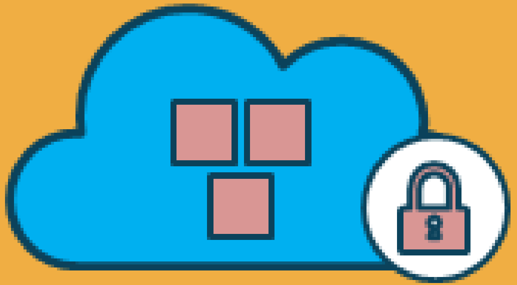
AWS Virtual Private Clouds (VPC)

The AWS virtual network service

- Amazon Virtual Private Cloud (Amazon VPC) lets you launch (spin-up) AWS resources into a virtual network that you've defined
- This virtual network closely emulates a traditional network in your own data center



Virtual Private Networks



- A VPC is a virtual network dedicated to your AWS account
- It is logically isolated from other virtual networks in the AWS Cloud
- You typically launch resources like EC2 Linux and Windows instances in the VPC
- Activities include creating subnets, specifying IP address ranges, and configuring route tables, NACLs, and security groups
- You can also leverage the AWS Marketplace

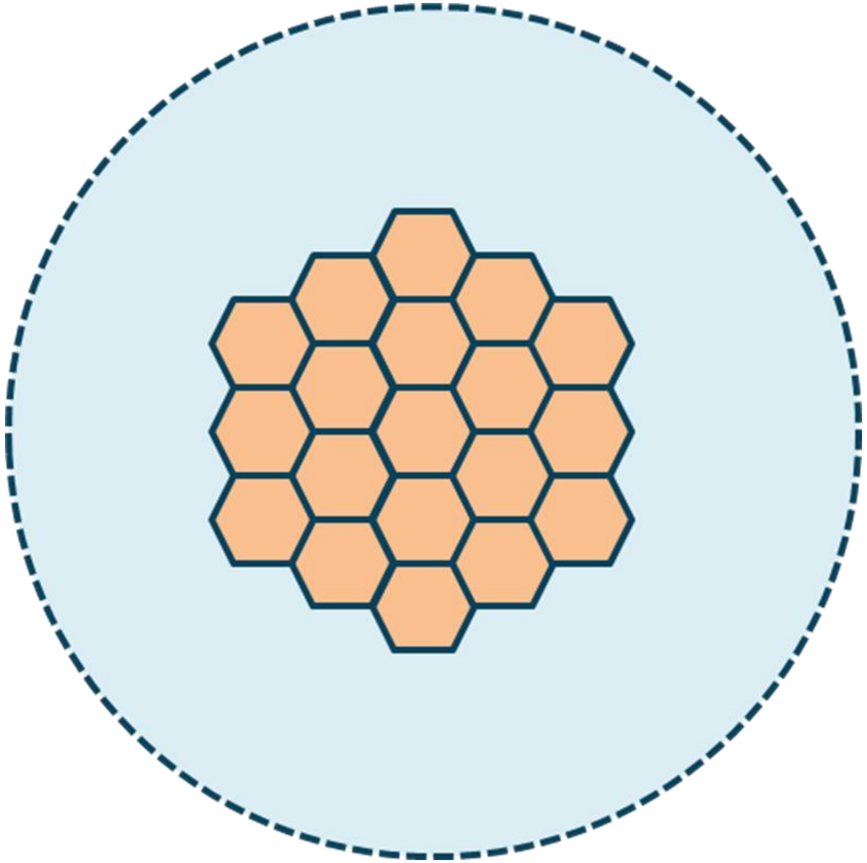
Amazon Machine Images (AMIs)

- AMIs provide the necessary information to launch an instance of an operating system
- When launching an instance in AWS you must determine the preferred AMI
- When you desire more than one instance with a similar configuration, you can also spin up multiple instances derived from a single AMI

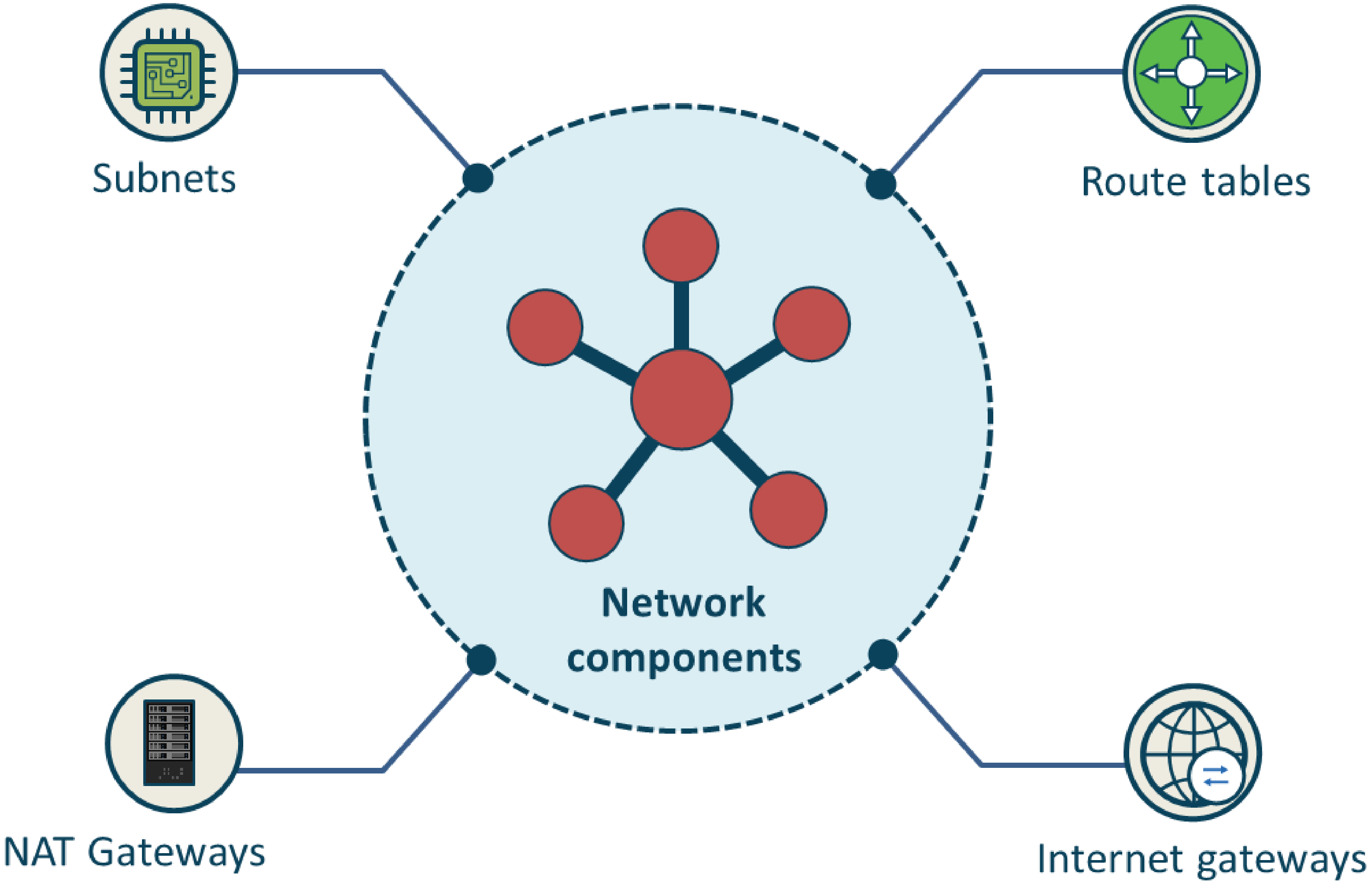
Amazon Machine Images

An AMI includes:

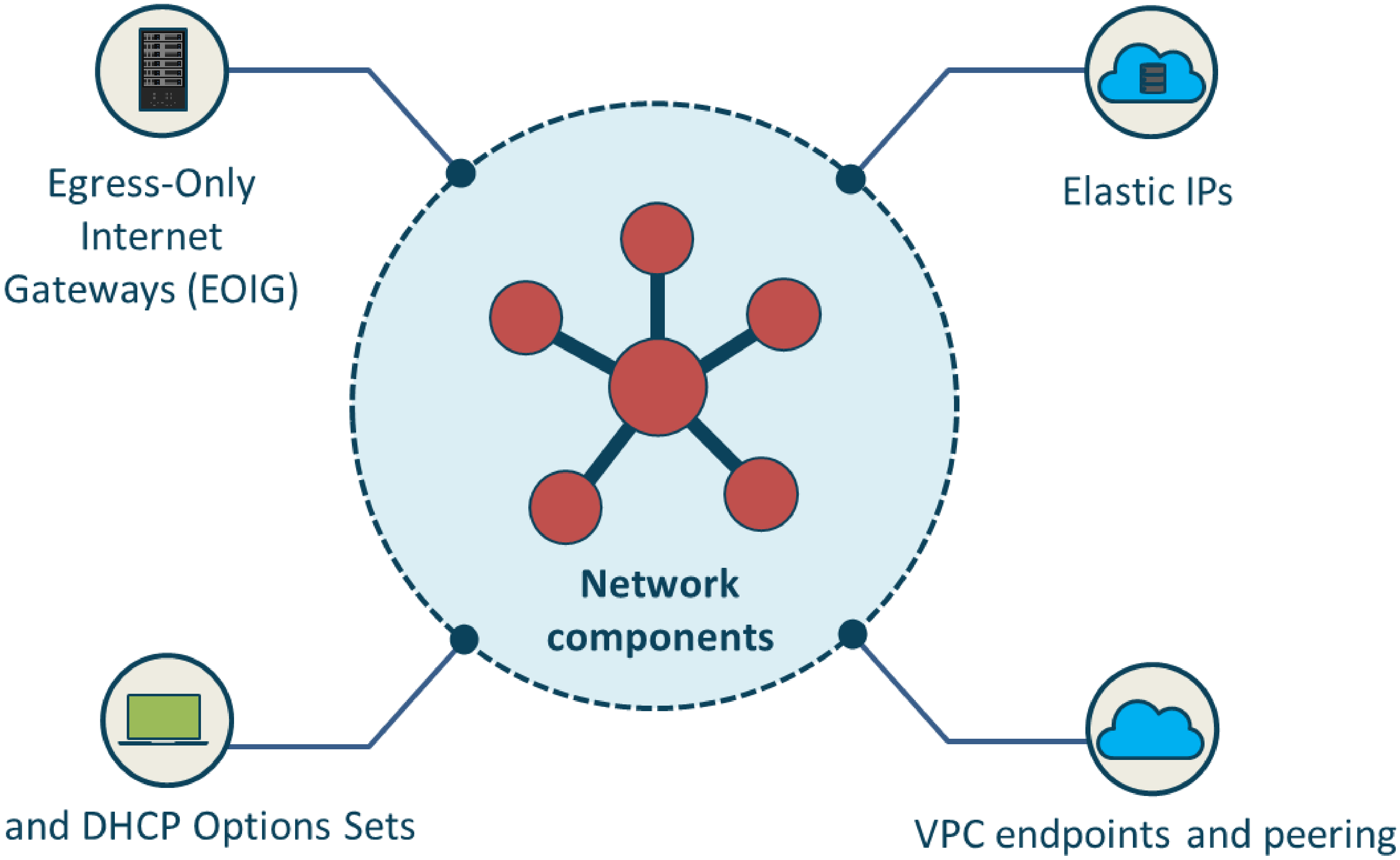
- An instance root volume template or one or more Elastic Block Storage (EBS) snapshots
- Permissions that allow you to manage the AWS accounts that launch instances using the AMI
- Specifications of the attachable volumes to use when launching an AMI based on a block device mapping



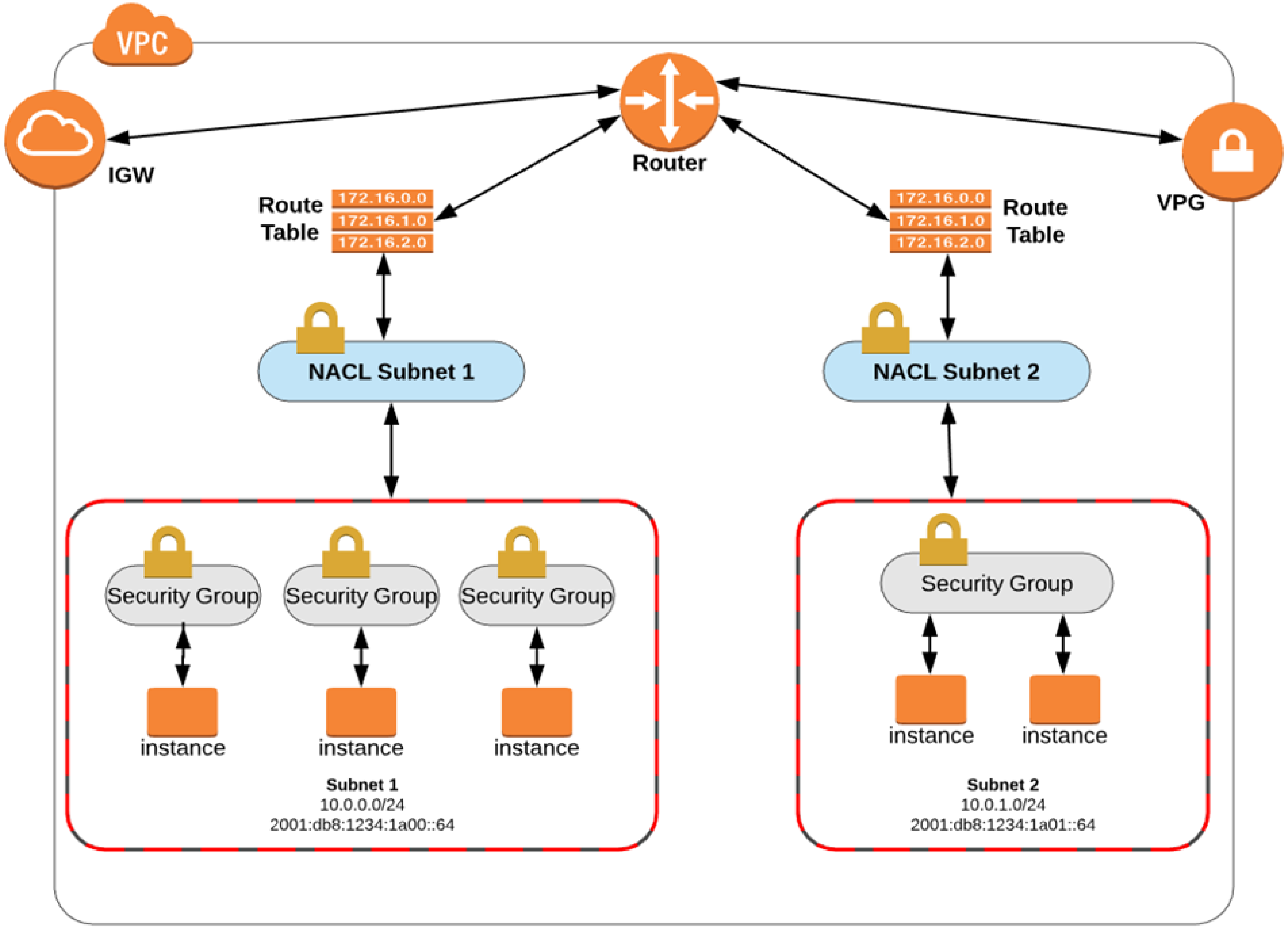
Networking Fundamentals



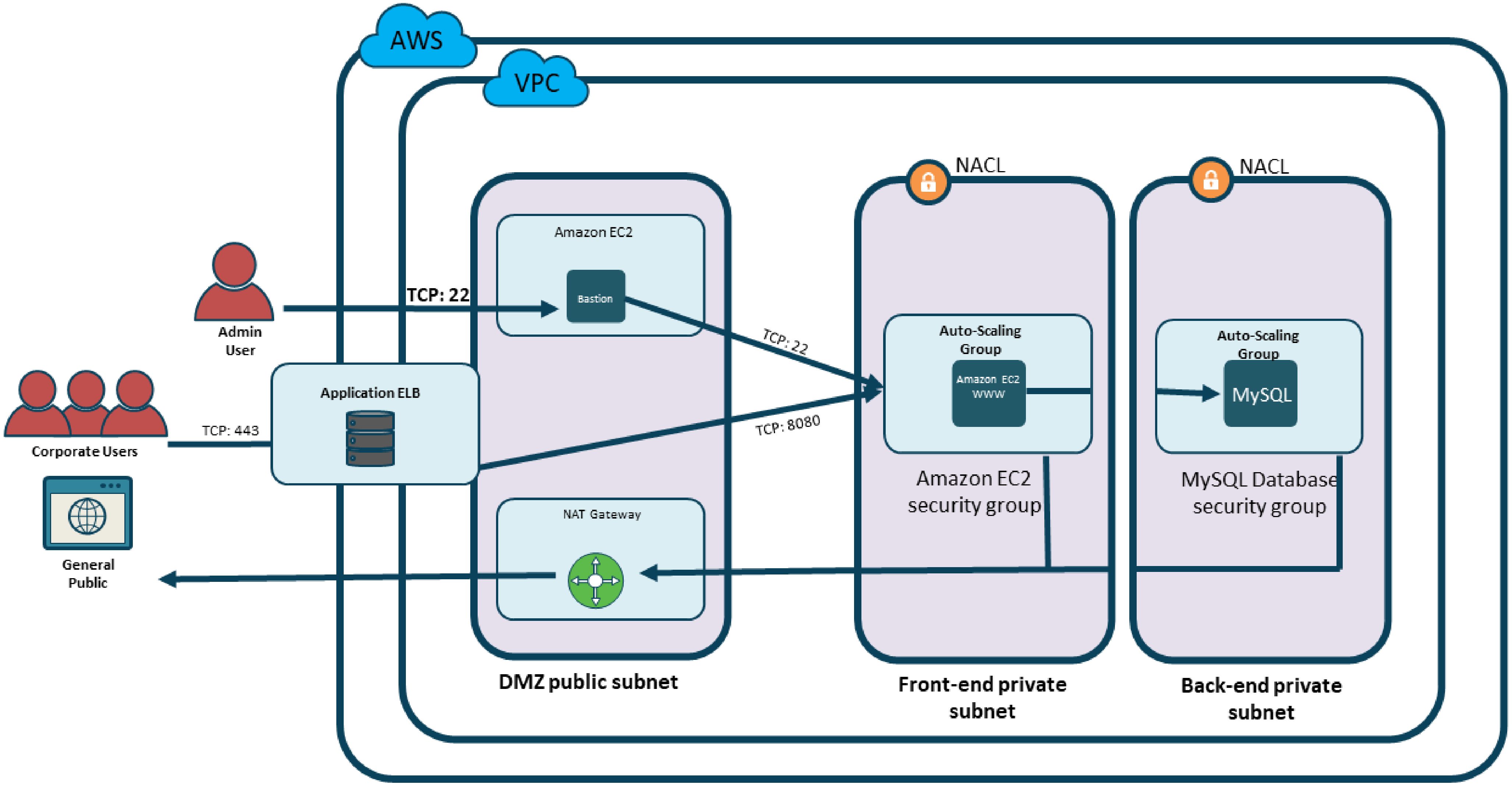
Networking Fundamentals


Egress-Only Internet Gateways (EOIG)
Elastic IPs
Network components
DNS and DHCP Options Sets
VPC endpoints and peering

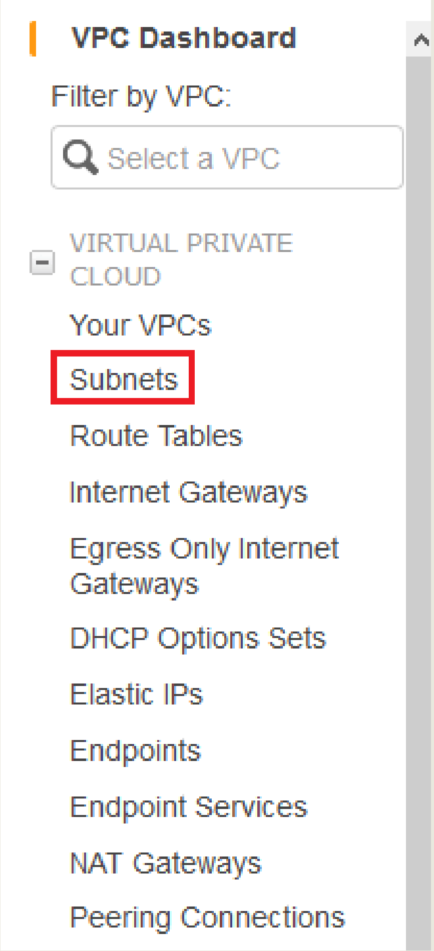
Networking Begins with Design



Networking Begins with Design

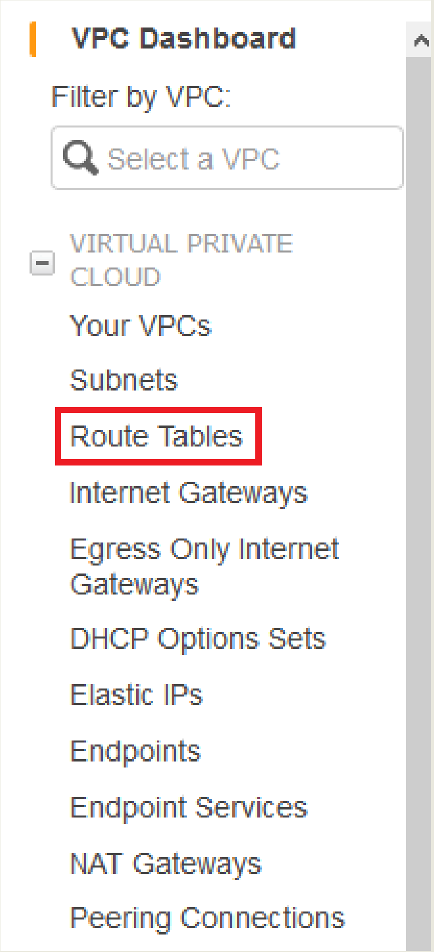


Subnets



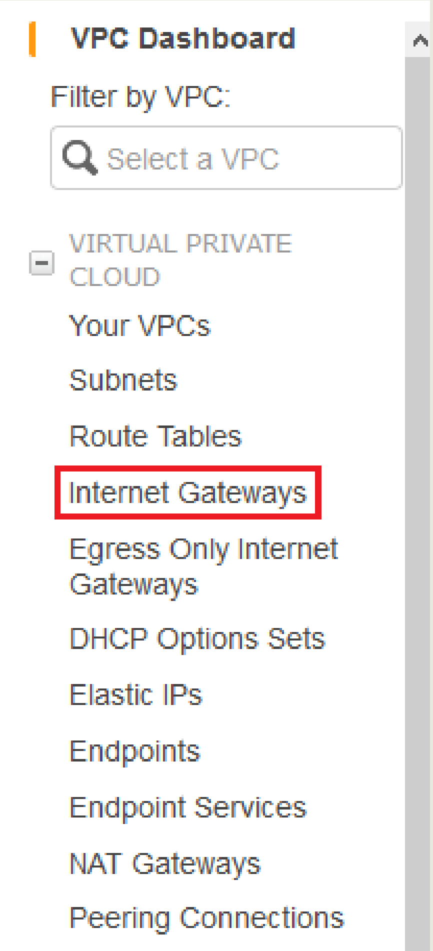
- A subnet is a range of IP addresses in your VPC
- A subnet is distinguished based on the entries in the Route Table assigned to it
- There are 3 Types of Subnets:
  - Private – there is no entry in the route table out of the subnet itself
  - Public – there is an entry in the table to an IGW
  - VPN-only – there is an entry to a VPG

Route Tables



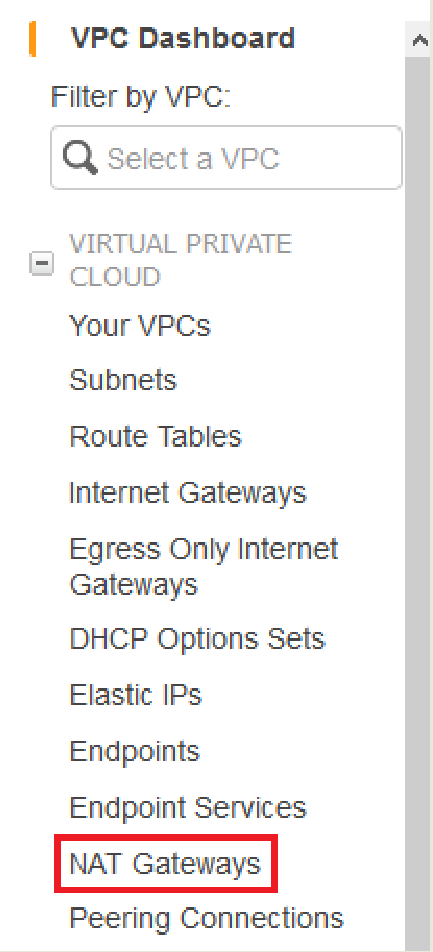
- Route tables contain a set of rules, called routes, that are used to determine where network traffic is directed
- The entries in your route tables determine the type of subnet you have deployed
- Default limit is 50 routes with 1000 route hard limit (new in 2019)
- Check out: https://docs.aws.amazon.com/vpc/latest/userguide/route-table-options.html

Internet Gateways (IGW)



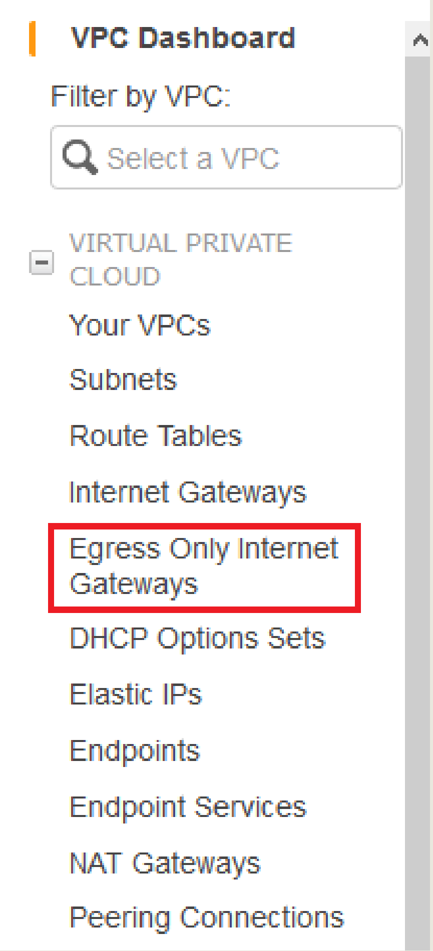
- An internet gateway (IGW) is a horizontally scaled, redundant, and highly available VPC component
- It facilitates communication between VPC instances and the internet
- It imposes no availability risks or bandwidth constraints on your network traffic
- An IGW serves two purposes:
  - To provide a target in your VPC route tables for traffic routable on the Internet
  - To perform network address translation (NAT) for instances that have been assigned public IPv4 addresses

NAT Gateways



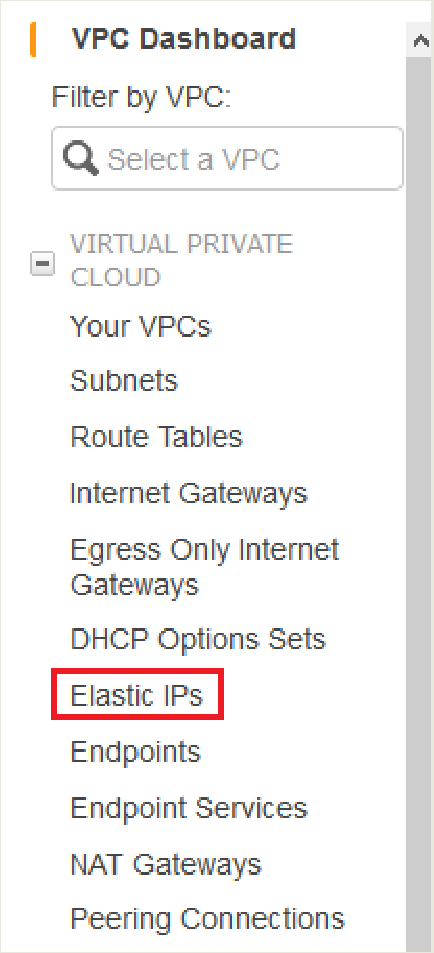
- NAT Gateways enable instances in a private subnet to connect to the internet or other AWS services, while preventing the internet from initiating a connection with those instances
- For example – Windows Update Services, upgrades, security fixes, etc.
- You are charged for creating and using a NAT gateway in your account with hourly usage and data processing rates applying

Egress-Only Internet Gateways (EOIG)



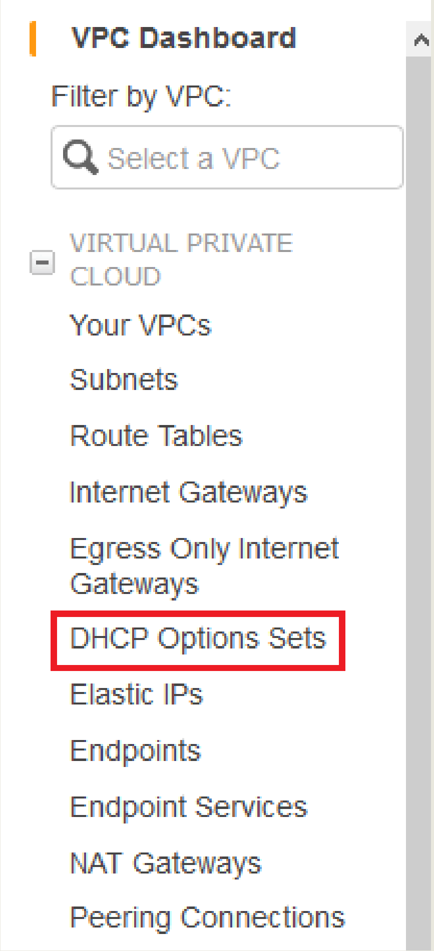
- An egress-only Internet gateway allows outbound communication over IPv6 from instances in your VPC to the Internet
- It prevents the Internet from initiating an IPv6 connection with your instances
- An egress-only Internet gateway is for use with IPv6 traffic only
- An internet gateway supports IPv4 and IPv6 traffic

Elastic IP Addresses



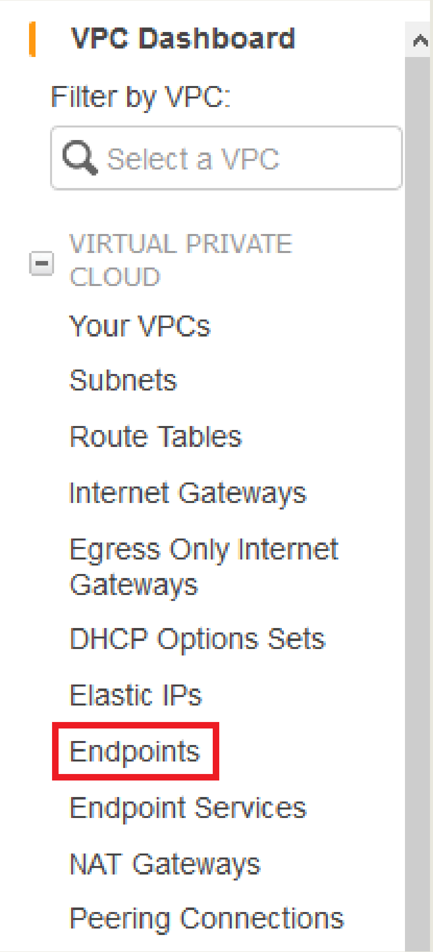
- An Elastic IP addresses (EIP) address is a static, public IPv4 address used for dynamic cloud computing
- You can associate an EIP with any instance or network interface for any VPC in your account then mask an instance failure by quickly remapping the address to another instance in the VPC
- Associate the EIP with the network interface instead of directly with the instance so that you can move all the attributes of the vNIC from one instance to another in a single step

DHCP Options Sets



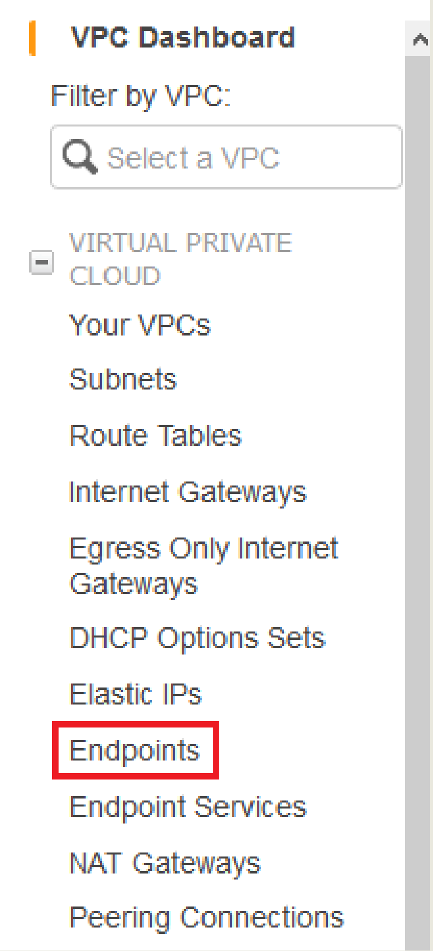
- EC2 instances launched into a nondefault VPC are private by default and they receive an unresolvable host name that AWS assigns
- You can assign your own domain name to your instances and use up to 4 of your own DNS servers by designating a special set of DHCP options to use with the VPC
- Available options: **domain-name-servers, domain-name, ntp-servers, netbios-name-servers, netbios-node-type**

Endpoints



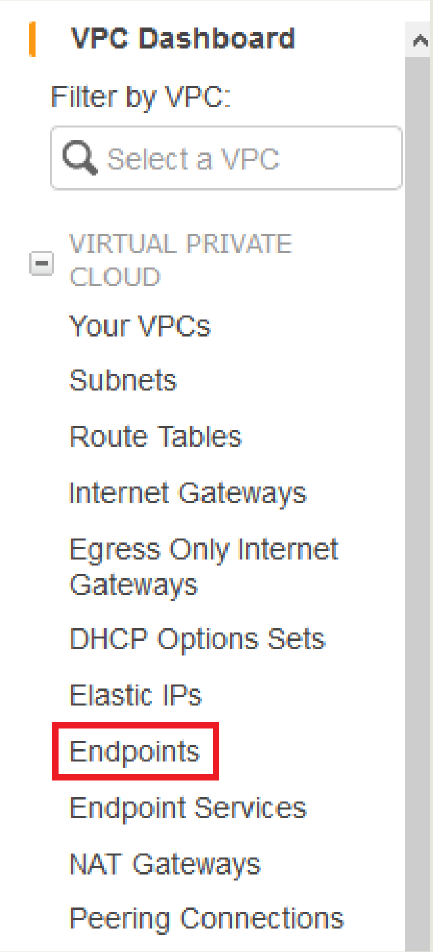
- VPC endpoints allow you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without needing an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection
- Instances in your VPC do not need public IP addresses to communicate with resources in the service since traffic between your VPC and the other service does not leave the Amazon network
- Endpoints are virtual VPC devices

Endpoints (cont.)



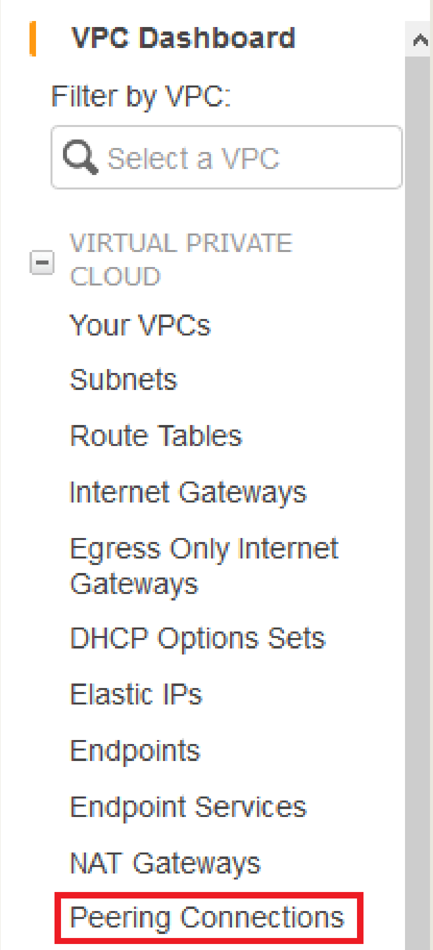
- When you generate a gateway endpoint, you simply designate the subnet route tables in your VPC that are used by the gateway endpoint
- A route is automatically added to each of the route tables with a destination that specifies the prefix list ID of the service (pl-xxxxxxxx), and a target with the endpoint ID (vpce-xxxxxxxxxxxxxxxxx)
- You cannot explicitly delete or modify the endpoint route, but you can change the route tables that are used by the endpoint

Endpoints (cont.)



- The following are the key concepts for VPC endpoints:
  - **Gateway** endpoints - a gateway that you designate as a target for a route in your route table for traffic destined to a supported AWS service
  - **Interface** endpoints - An interface endpoint is an elastic network interface with a private IP address from the IP address range of your subnet that serves as an entry point for traffic destined to a supported service
  - **Endpoint services** - Your own application in your VPC using PrivateLink. Other AWS principals can create a connection from their VPC to your endpoint service

VPC Peering



VPC Dashboard

Filter by VPC:

Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

- A VPC peering connection is a networking connection between two VPCs that lets you route traffic between them using private IPv4 or IPv6 addresses
- Instances in either VPC can communicate with each other as if they are within the same network
- You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account
- Intra-region or inter-region peering connections

Network-to-Amazon VPC Connectivity Options

Connecting to your VPC

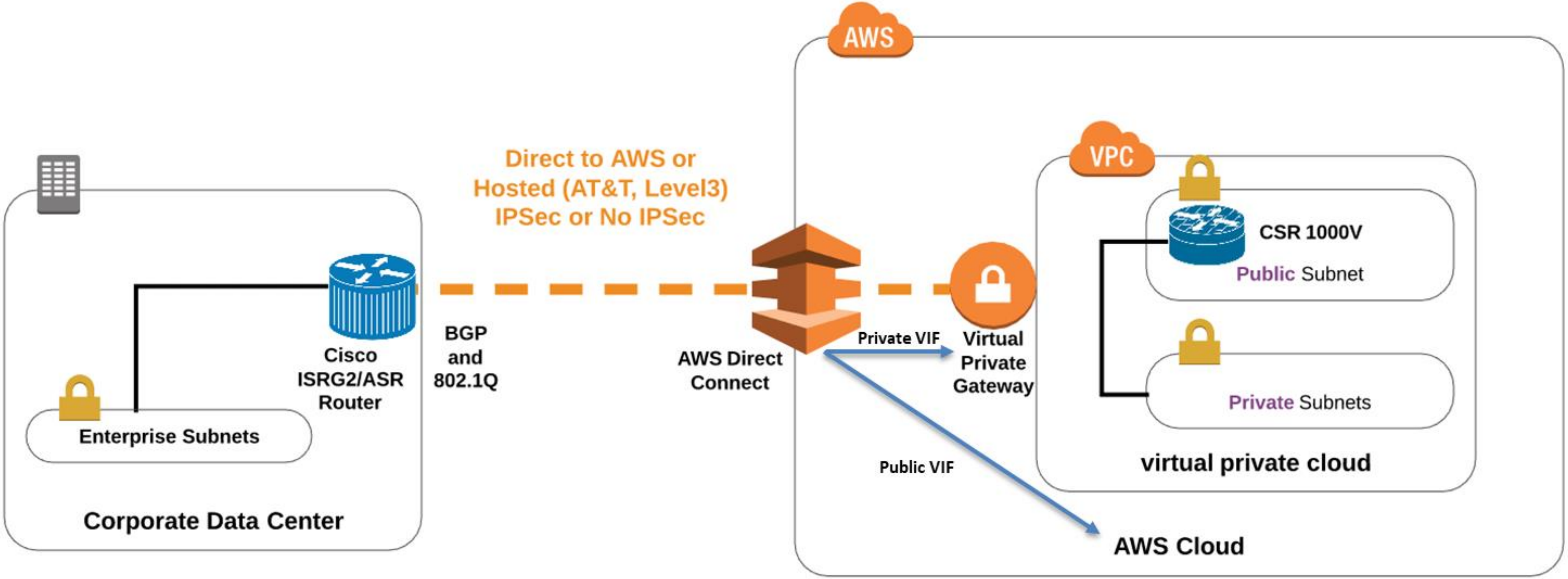
- AWS Site-to-Site (managed) VPN
- AWS Direct Connect
- AWS Direct Connect Plus VPN
- AWS VPN CloudHub
- Software VPN
- Transit Gateway (and/or transit VPC)
- Client VPN Endpoints

Amazon VPC-to-VPC Connectivity Options

Connecting between VPCs

- VPC Peering
- Software-to-AWS Site-to-Site (Managed) VPN
- AWS Site-to-Site (Managed) VPN
- AWS Direct Connect
- AWS PrivateLink
- AWS Transit Gateway

AWS Direct Connect



Benefits of Cloud Security

AWS has the most secure datacenters in the world

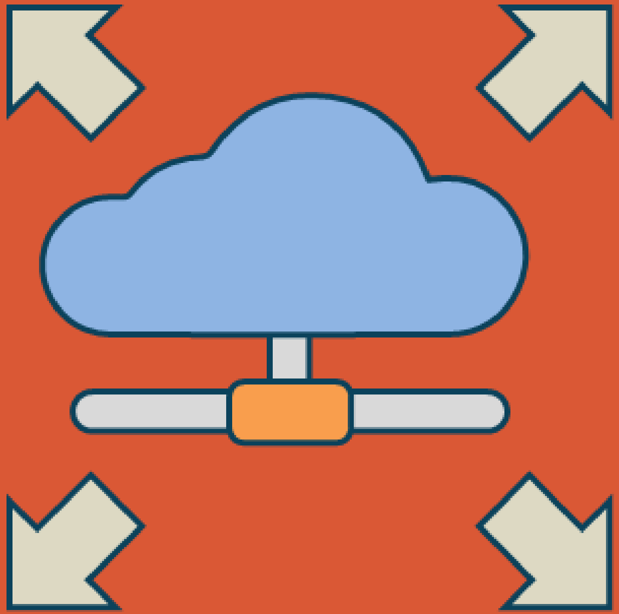
- Leverage the secure infrastructure and best practices of AWS
- Inherit all the guidelines, policies, architecture, and operational processes of Amazon Web Services
- Allows you to grow and innovate, while preserving a compliant and secure environment

Benefits of Cloud Security

- The AWS infrastructure uses strong safeguards to help protect the privacy of all data is stored in highly secure AWS data centers
- Maintain the highest standard of security without having to manage your own facility
- Security scales with your AWS Cloud usage so that no matter the size of the business, the AWS infrastructure will keep your data safe
- AWS manages dozens of compliance programs in its infrastructure so that segments of your compliance have already been completed

The Shared Responsibility Model

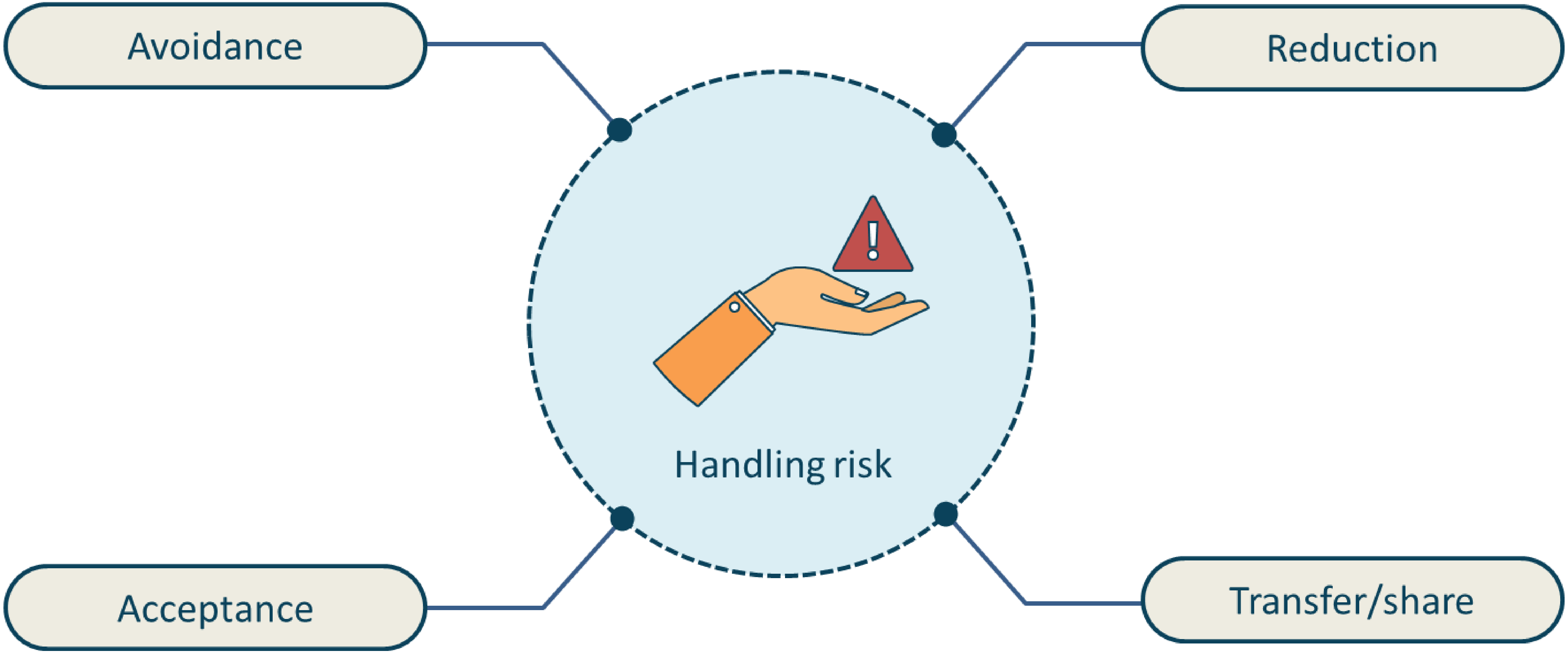
- Cloud resource security is quite a bit different than protecting your own data center on-premise
- When you migrate resources to a cloud service provider (CSP), the service level-agreement (SLA) becomes a joint shared responsibility between the provider and the consumer
- With IaaS and SaaS cloud models this relationship has a more distinct demarcation point
- With PaaS, however, the lines are often less clear and depend on how "managed" the service is by the CSP



Results of Shared Responsibility

- What content customers choose to store or migrate to AWS
- Which AWS services are used with that content
- In what country that content is stored
- The format and structure of that content
- Whether it is masked, anonymized or encrypted
- Who has access to that content
- How those access rights are granted, managed and revoked

Risk Treatment



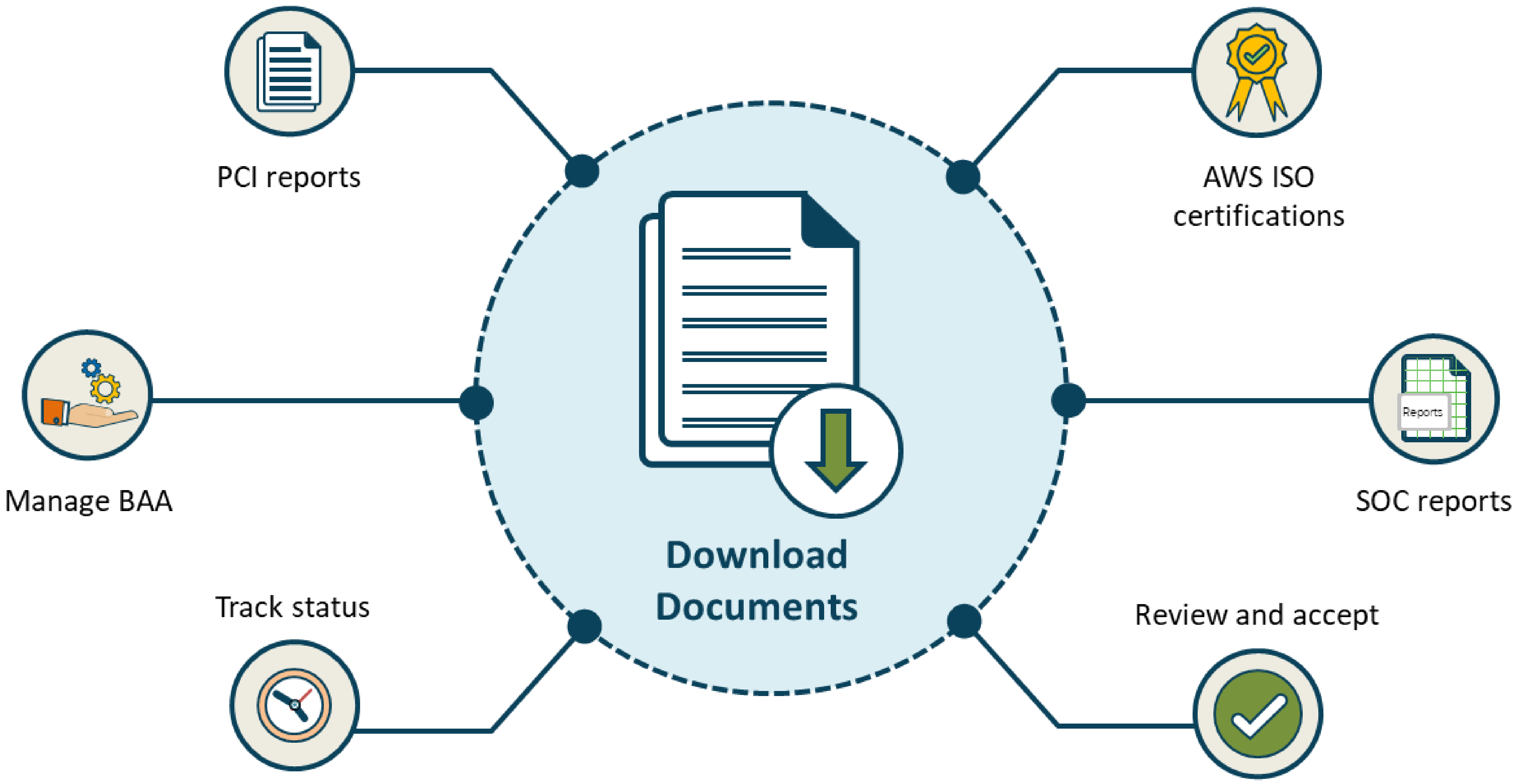
AWS Compliance

- Compliance services help you realize AWS controls
- Compliance responsibilities are part of shared responsibility
- Utilize "governance-focused" and "audit-friendly" services
- Enablers are constructed on traditional compliance programs
- AWS offers an extensive array of control information

AWS Artifact

- You may need to uphold specific standards as proven through an audit
- An audit or inspection will ensure that the company has met those standards
- Artifact is a console-based, on-demand self-service auditing object retrieval service that offers quick and easy access to AWS compliance documentation and agreements

Download Security and Compliance Documents



PCI reports

AWS ISO certifications

Manage BAA

SOC reports

Track status

Review and accept

Download Documents

AWS Artifact consists of two main sections: Agreements and Reports

- AWS Artifact **Agreements** lets you review, accept, and manage agreements for an individual account and for all your accounts in AWS Organizations
  - Different types of agreements are offered to address the needs of customers who are subject to specific regulations, such as HIPAA
- AWS Artifact **Reports** provides compliance reports from third-party auditors who have tested and verified that AWS is compliant with a variety of global, regional, and industry-specific security standards and regulations
  - AWS Artifact Reports remains up to date with the latest reports released
  - You can provide the AWS audit artifacts to your auditors or regulators as evidence of AWS security controls

Customer Compliance Center

- Contains resources to assist customers in learning more about AWS compliance
- Contains customer compliance stories and case studies to ascertain how organizations in regulated industries have solved various compliance, governance, and audit tasks
- The Customer Compliance Center includes an auditor learning path designed for individuals in auditing, compliance, and legal roles who need to learn more about how their internal operations can validate compliance using the AWS Cloud
- Customers can access compliance whitepapers and documentation on topics such as:
  - AWS answers to key compliance questions
  - An overview of AWS risk and compliance
  - An auditing security checklist

Cloud Security Alliance (CSA)

Consensus Assessment Initiative Questionnaire

Cloud Security Alliance (CSA) is a not-for-profit enterprise with a mission to "promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing."

CSA STAR Self-Assessment

CSA Star Level 1:

CSA STAR Self-assessment

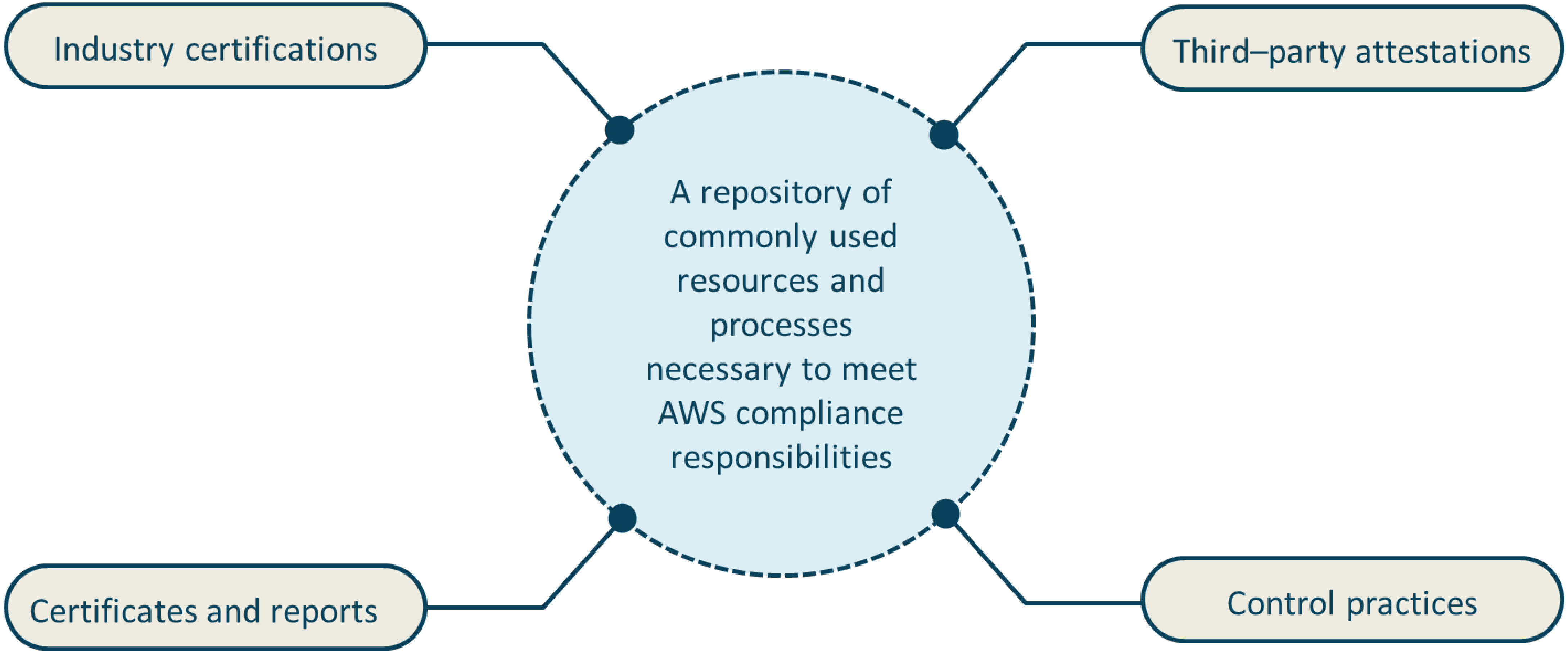
CSA Star Level 2:

CSA STAR Attestation and Certification

CSA Star Level 3:

Continuous Monitoring

AWS Compliance Solutions Guide



A repository of commonly used resources and processes necessary to meet AWS compliance responsibilities

Industry certifications

Third–party attestations

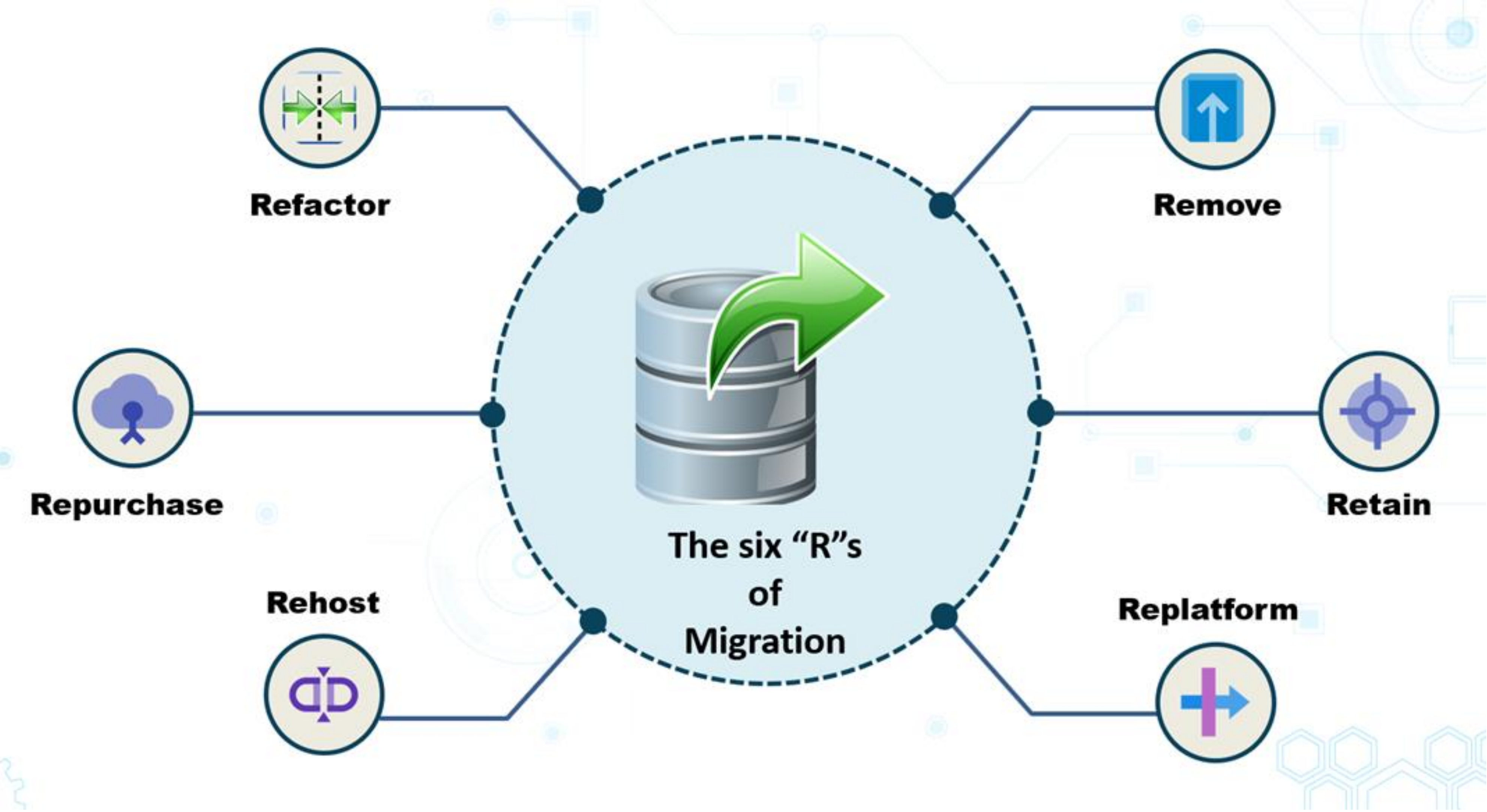
Certificates and reports

Control practices

Cloud Adoption Framework (AWS CAF)

- The AWS CAF organizes guidance into six areas of focus, called Perspectives
- Each Perspective speaks to discrete responsibilities
- The planning process assists the right stakeholders across the organization prepare for the coming changes
- In general, the Business, People, and Governance Perspectives focus on business capabilities
- The Platform, Security, and Operations Perspectives focus on technical capabilities

6 most common migration strategies


Refactor
Remove
Repurchase
Retain
Rehost
Replatform
The six "R"s
of
Migration