ARC321

DIGITAL NATIVE BUSINESS

# Using Multi-account strategy to enable hyperscale

Purna Sanyal (he/his)

Senior Solutions Architect
AWS

Yulia Chiaburu (she/her)

Leader, Solution Architecture
AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Agenda

- Digital Native Business (DNB) characteristics
- Hyperscale
- DNB customers migration journey
- Multi-account best practices
- Call to action

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Digital Native Business (DNB) characteristics

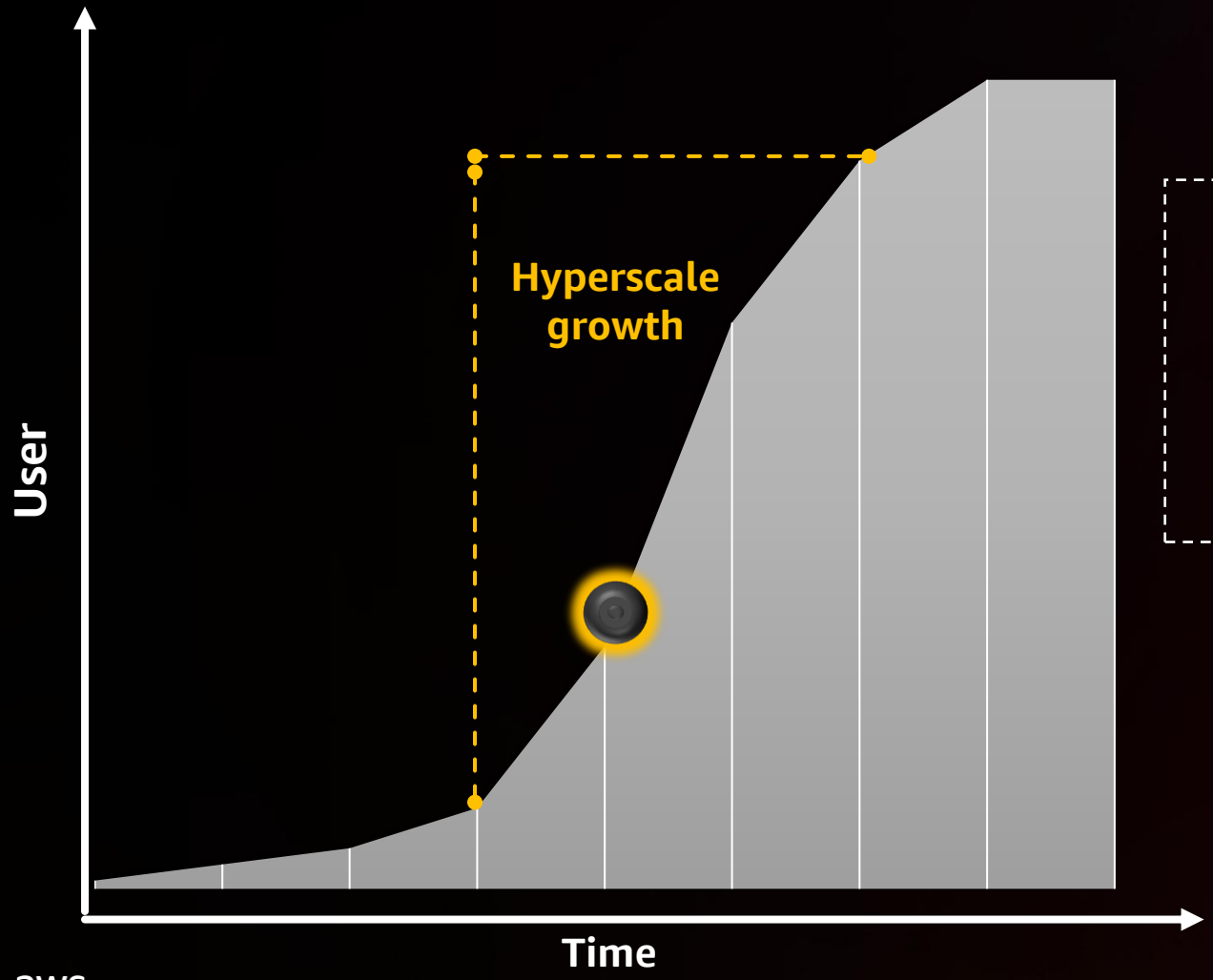
Digital Native Businesses are

- Companies born in the cloud (B2C, B2B2C)
- Consumer-centric
- Tech-savvy
- Agile mindset
- Transform their industries



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# DNB hyperscale growth




**Hyperscale growth (10x or more ..)**

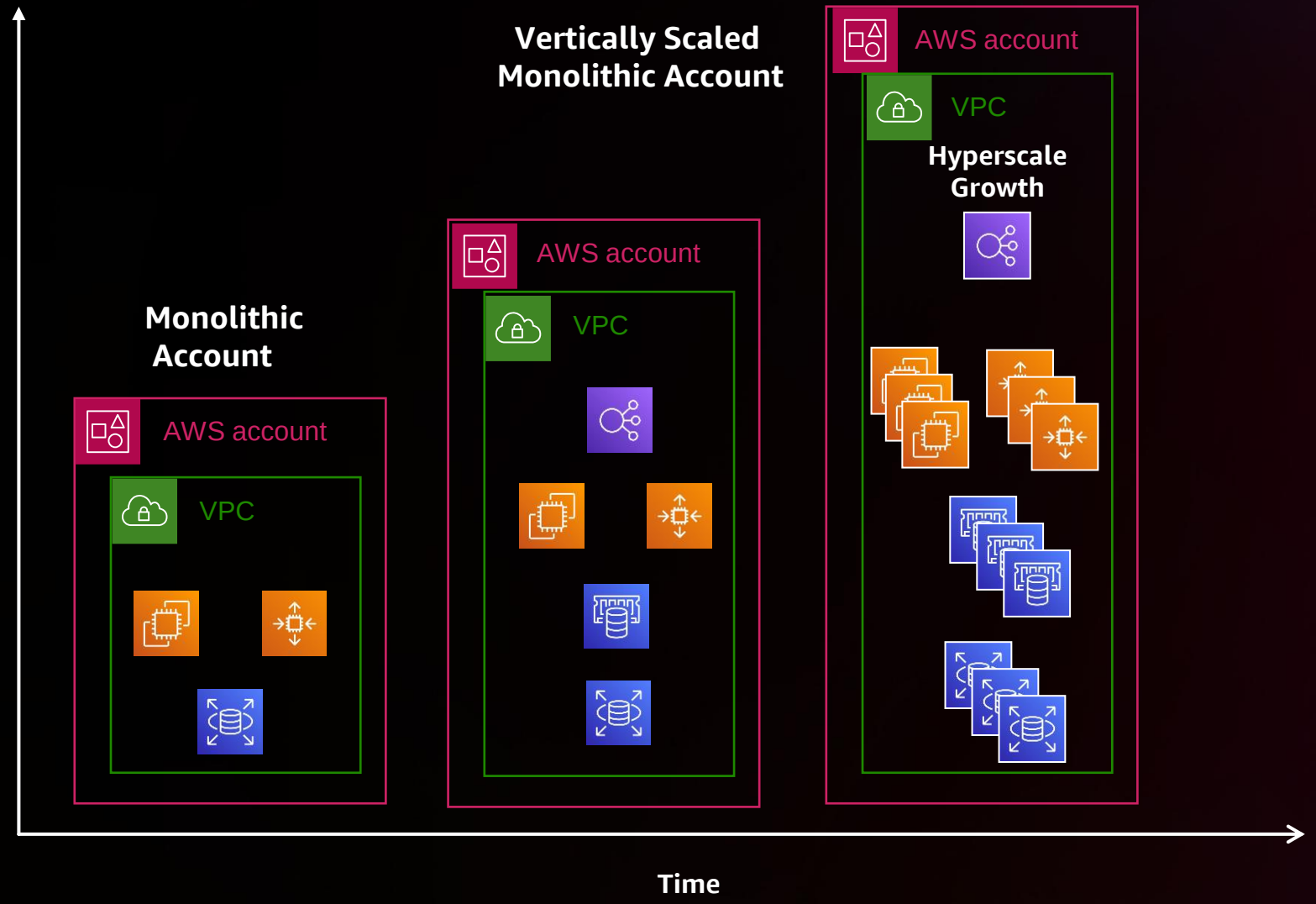
- ❑ Millions of users / customers
- ❑ Billions of transactions

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Will your architecture support this hyperscale growth ?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Hyperscale growth vs underlining architecture




Business Impact

- ❑ Increased blast radius
- ❑ Hitting hard limits
- ❑ Innovation **slows down**

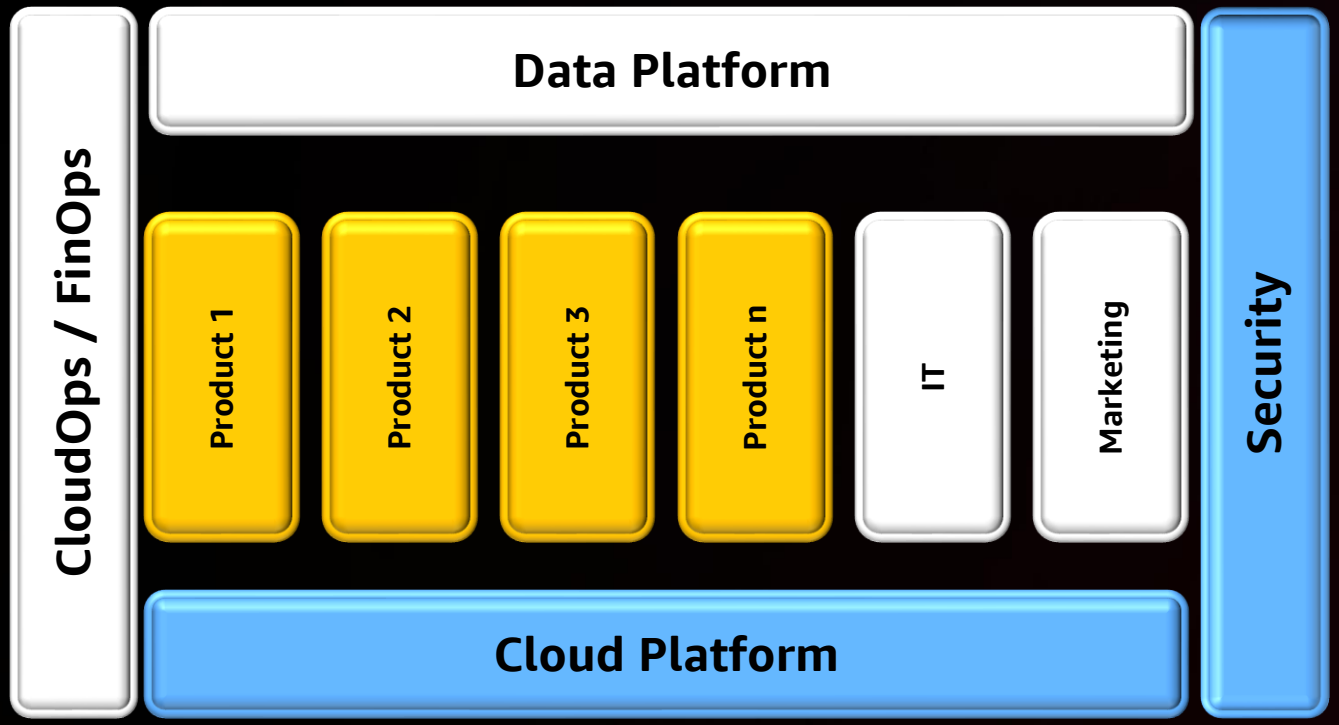


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Are you able to sustain the innovation pace and scale faster than traditional businesses?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# How monolithic account impacts innovation?

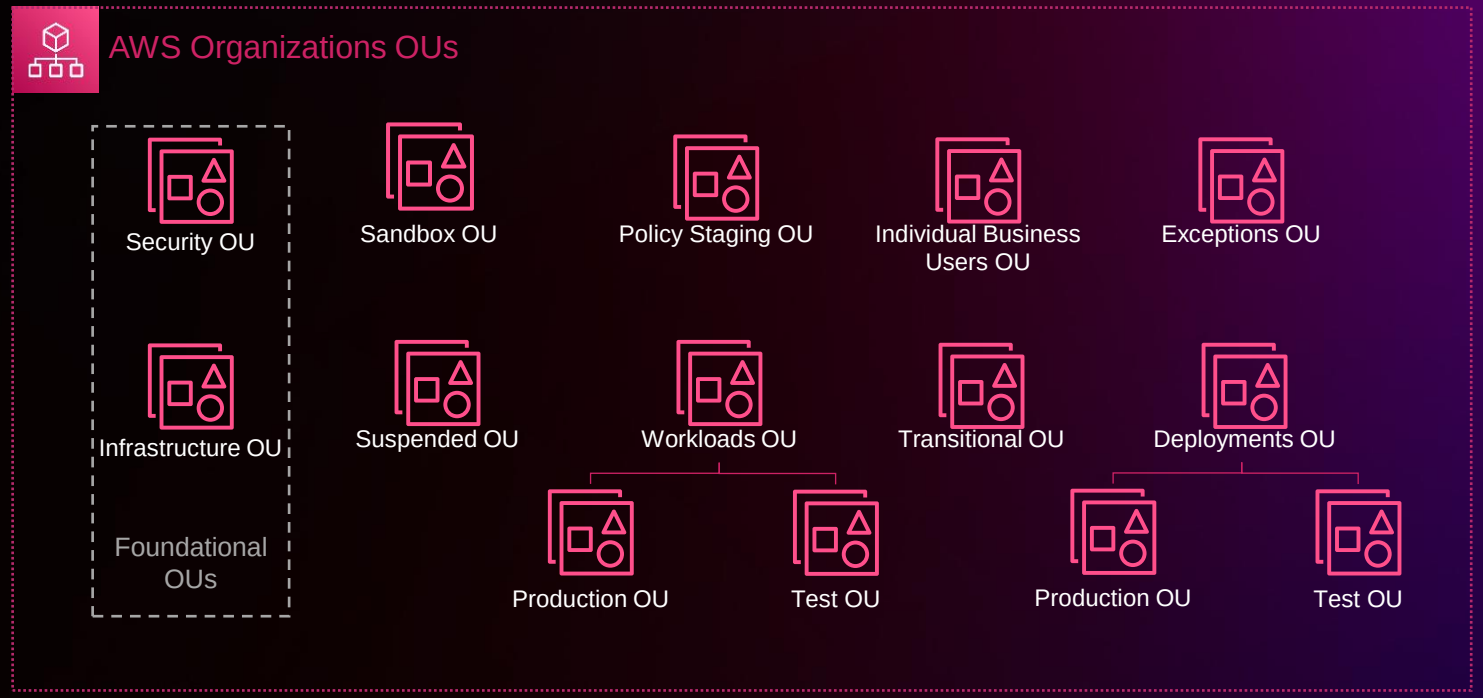



DNB Organization

- **Platform** - can not scale/ provision new resources - results in **outage**, bad customer experience
- **Security** - concern more about the **blast radius,** does not allow new services / tool in production and feel that it break the current production system
- **Product** - lack of new tools slows Innovation.

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Break the monolithic - move to Multi-account




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Why Multi-account?



Multiple teams



Multiple applications



Billing

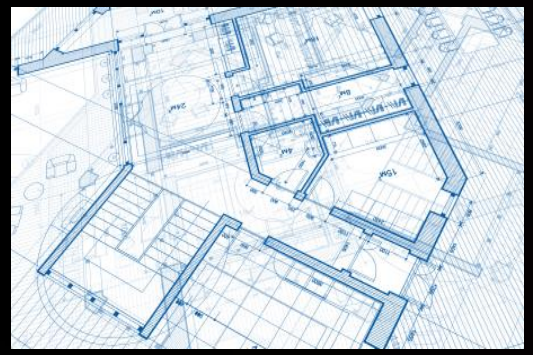


Isolation and security

Support hyperscale growth of the business

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

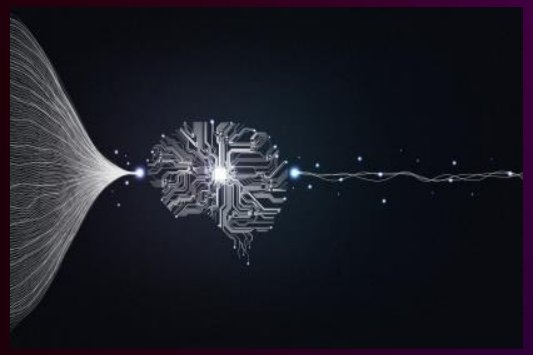
# How to move to Multi-account architecture?



Design



Build and deploy



Modernize

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# DNB Customer | Multi-account journey

**Tail-wind**
Platform become popular customer and developer community increased to 100K and 500K

**Move to Multi-account**
6 months to design and 12 months to break the monolithic



**Founded**
The mission is to transform the future of digital communication for the enterprises, developers and consumers

**Pandemic**
Point of Inflection, Platform can not support business growth (onboard millions new customers, launch new services)

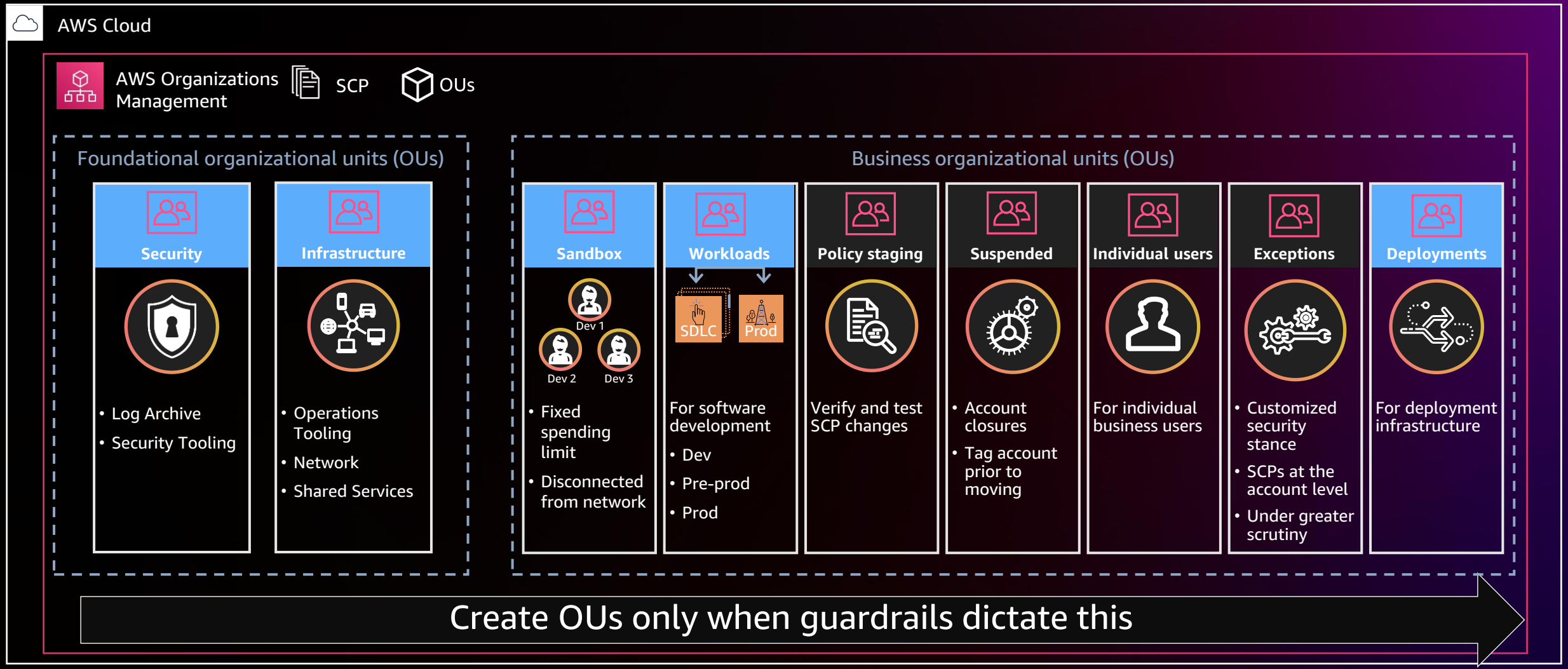
**Results**
Platform is scalable, user base increased by 10x, product launch time reduction by 30%

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Whiteboard

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Structure your Multi-account environment




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Hyperscale VPC networks

An environment can be considered “**Hyperscale”** once it supports **thousands of application endpoints** and **hundreds of gigabits of traffic per second**.

Hyperscale environments on AWS favor simple and agile network designs.

This allows you to integrate new use cases, and maximize the effectiveness of network and infrastructure components

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Hyperscale networking options



| Use case | Scalability | Traffic pattern | Cost |
|---|---|---|---|

AWS PrivateLink

VPC Sharing

Peering connection

AWS Transit Gateway

AWS account

VPC

Instance

PrivateLink Endpoints

AWS account

VPC

Instances

AWS account

VPC

Instance

PrivateLink Endpoints

Amazon API Gateway

Amazon S3

Amazon Public services/endpoints

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Hyperscale networking options



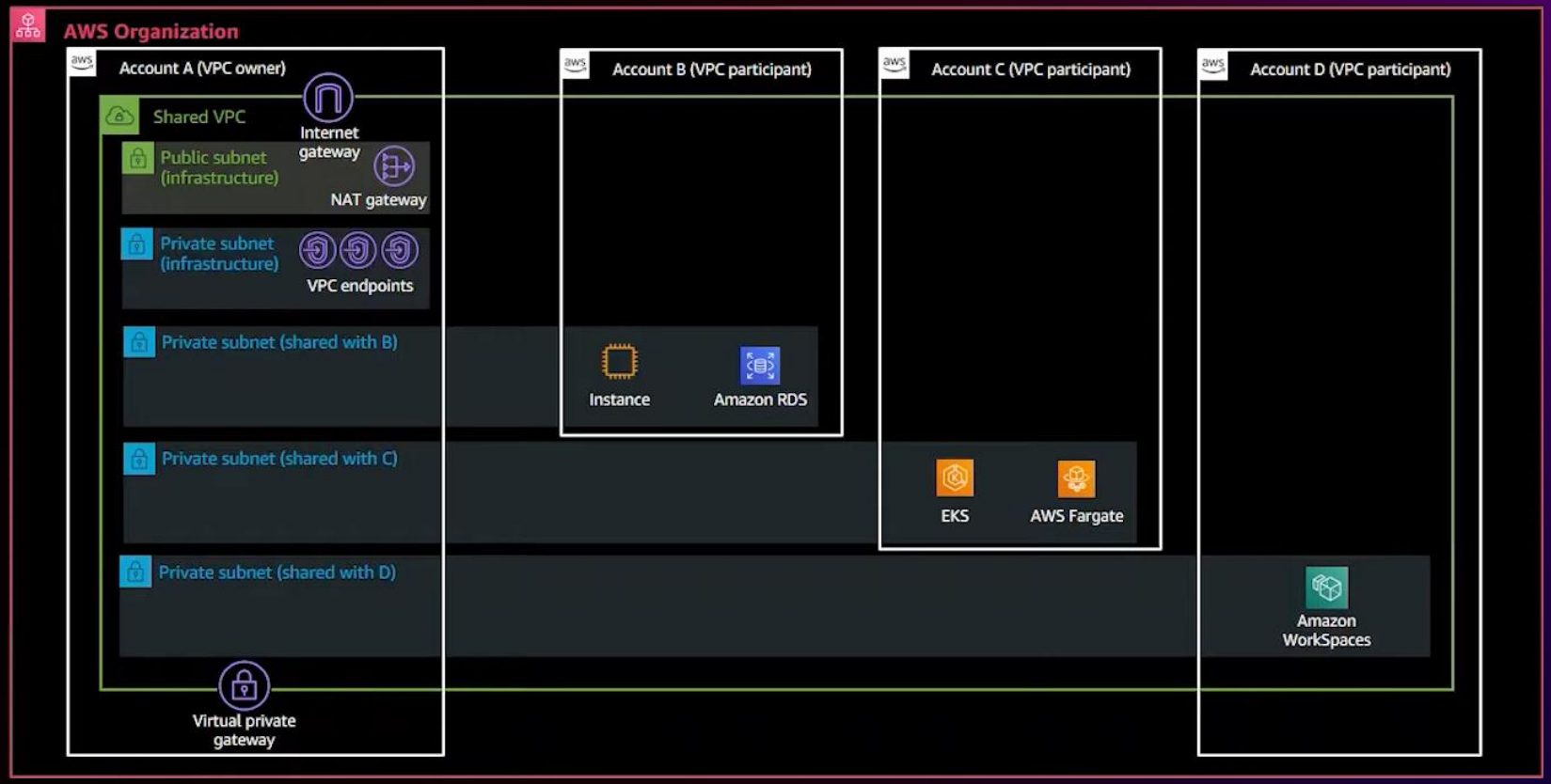
| Use case | Scalability | Traffic pattern | Cost |
|---|---|---|---|

AWS PrivateLink

VPC Sharing

Peering connection

AWS Transit Gateway




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Hyperscale networking options



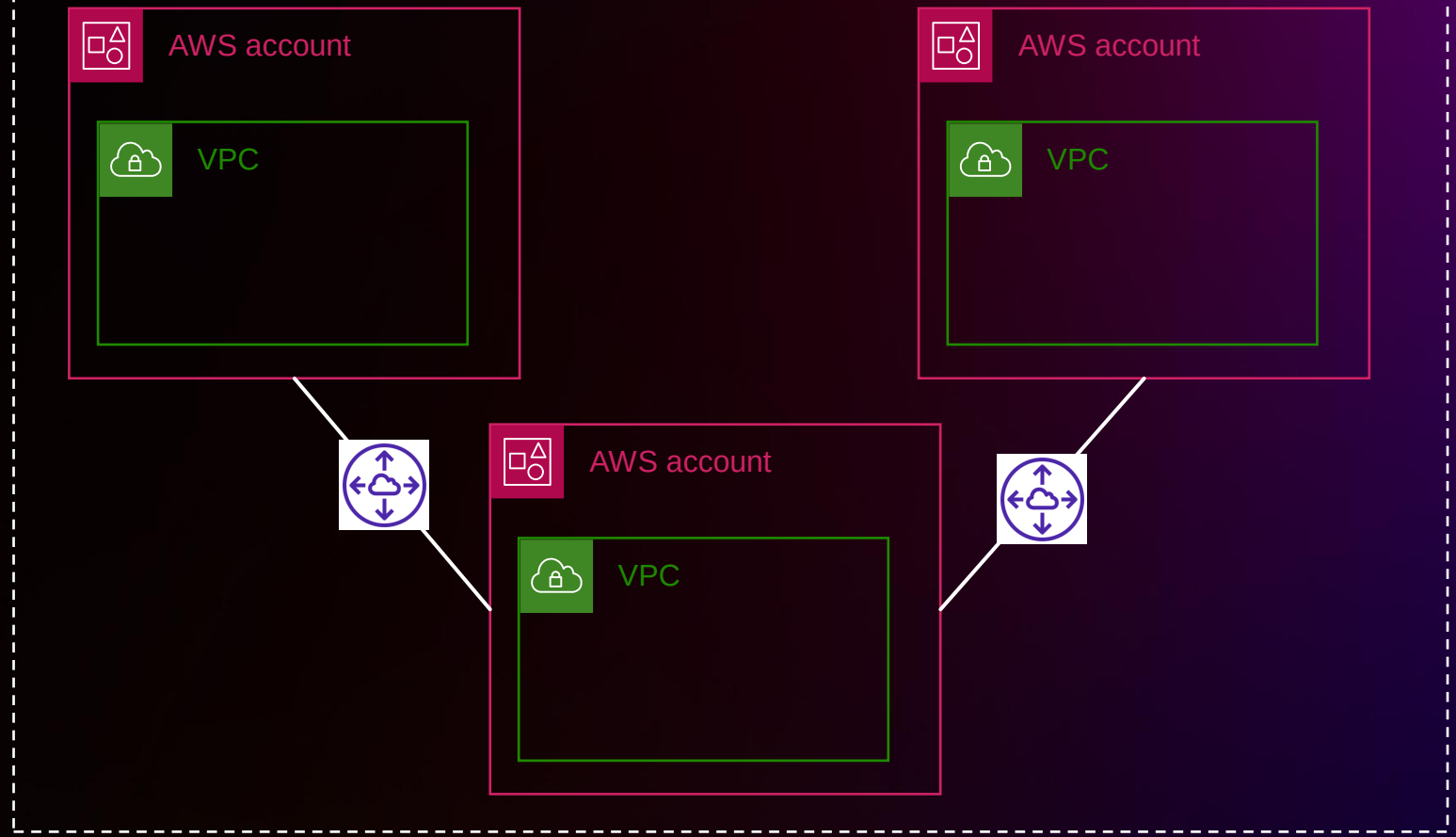
| Use case | Scalability | Traffic pattern | Cost |
|---|---|---|---|

AWS PrivateLink

VPC Sharing

Peering connection

AWS Transit Gateway




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Hyperscale networking options



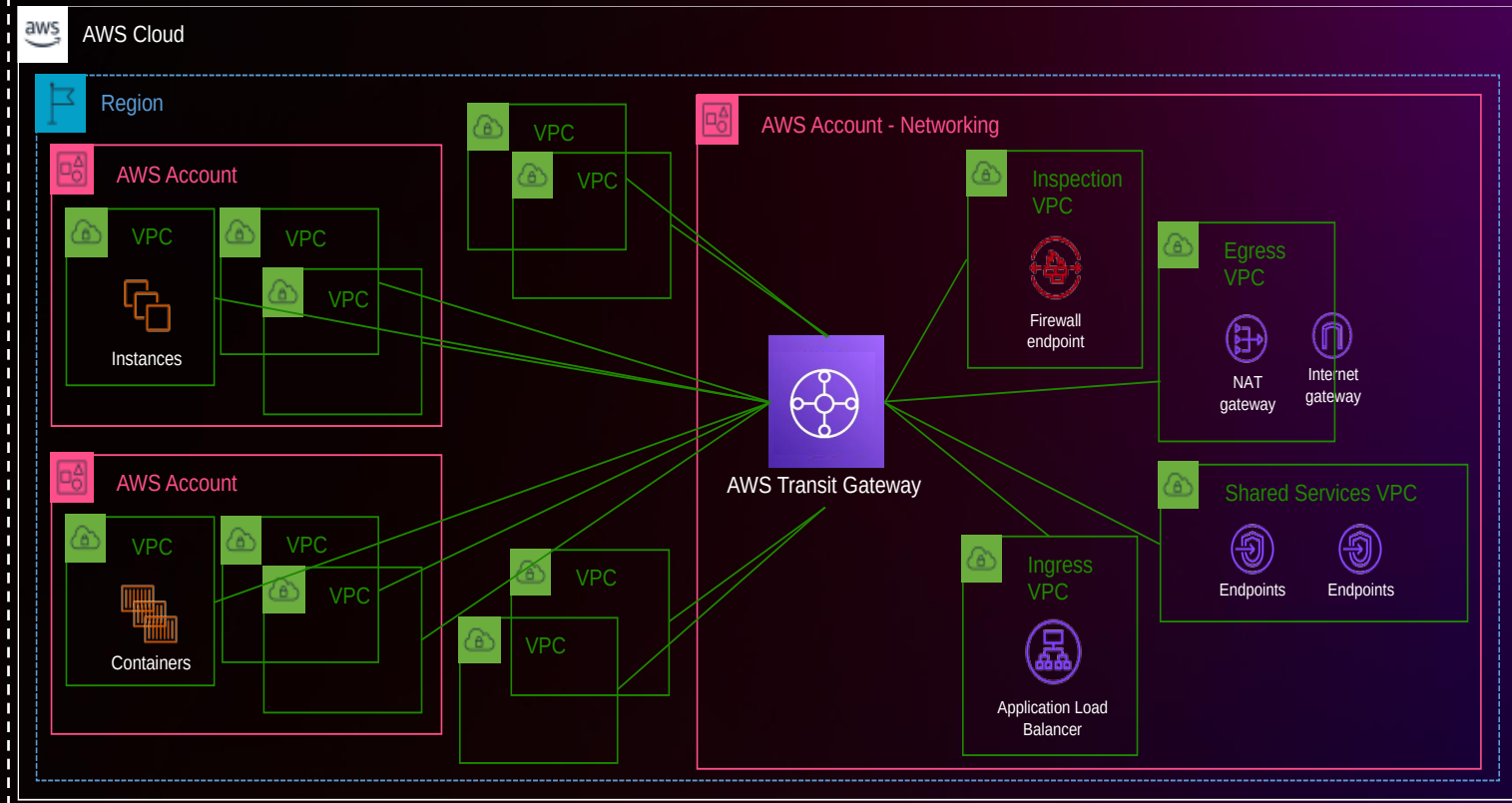
| Use case | Scalability | Traffic Pattern | Cost |
|---|---|---|---|

AWS PrivateLink

VPC Sharing

Peering connection

AWS Transit Gateway




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

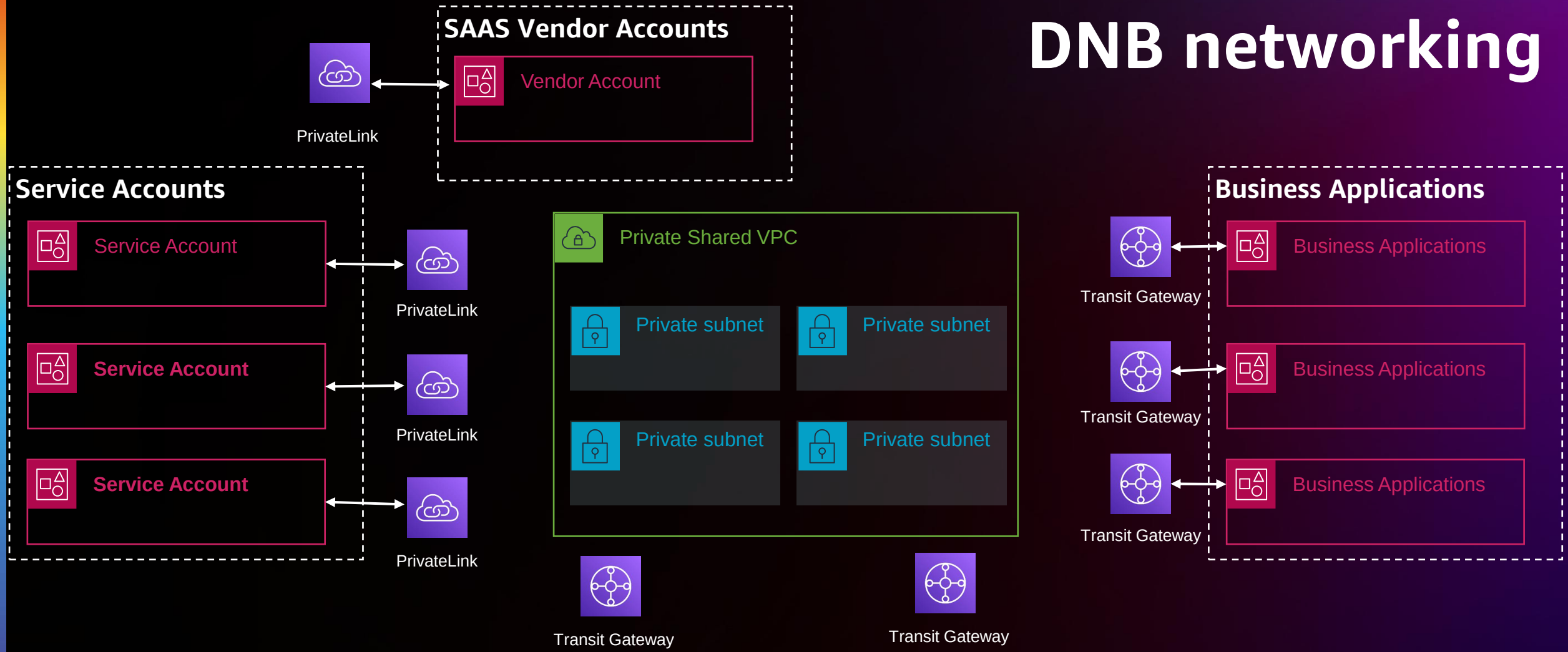
# Selection criteria



| Criteria | PrivateLink | VPC Peering | Transit Gateway |
|---|---|---|---|
| Architecture | Point-to-point private connection over AWS backbone | Full Mesh | Hub and Spoke |
| Use Cases | Secure private connection to AWS or internal services, SaaS provider-consumer or private cross-VPC communication | Simple connectivity between a few VPCs | Easily connect Amazon VPCs, accounts, and on-premises networks to a single gateway |
| Complexity | Low | Increases with VPC count | AWS Managed Service |
| Overlapping CIDR blocks | Allowed | Not allowed | Not allowed |
| Scalability | 200 interface endpoints / VPC | 125 Peers/VPC | 5000 Attachments |
| Supported flows | TCP | TCP, UDP | TCP, UDP |
| Segmentation and security | Built-in: Unidirectional initiation only by consumer. Service provider needs to allow-list and approve consumers | Customer Managed | Multiple Route Tables and ability to insert inline appliances |
| Latency | Hyperplane latency | Lowest | Hyperplane latency |
| Bandwidth Limit | Sustained 10 Gbps per AZ<br>Bursts of up to 100 Gbps | No Limit | Bursts of up to 50 Gbps per VPC Attachment |
| Visibility | VPC Flow Logs | VPC Flow Logs or VPC Traffic Mirroring | Transit Gateway Network Manager |
| Cross VPC Security Group references | Not applicable | Supported | Not Supported |
| TCO | Medium | Lowest | Medium |

vices, Inc. or its affiliates. All rights reserved.

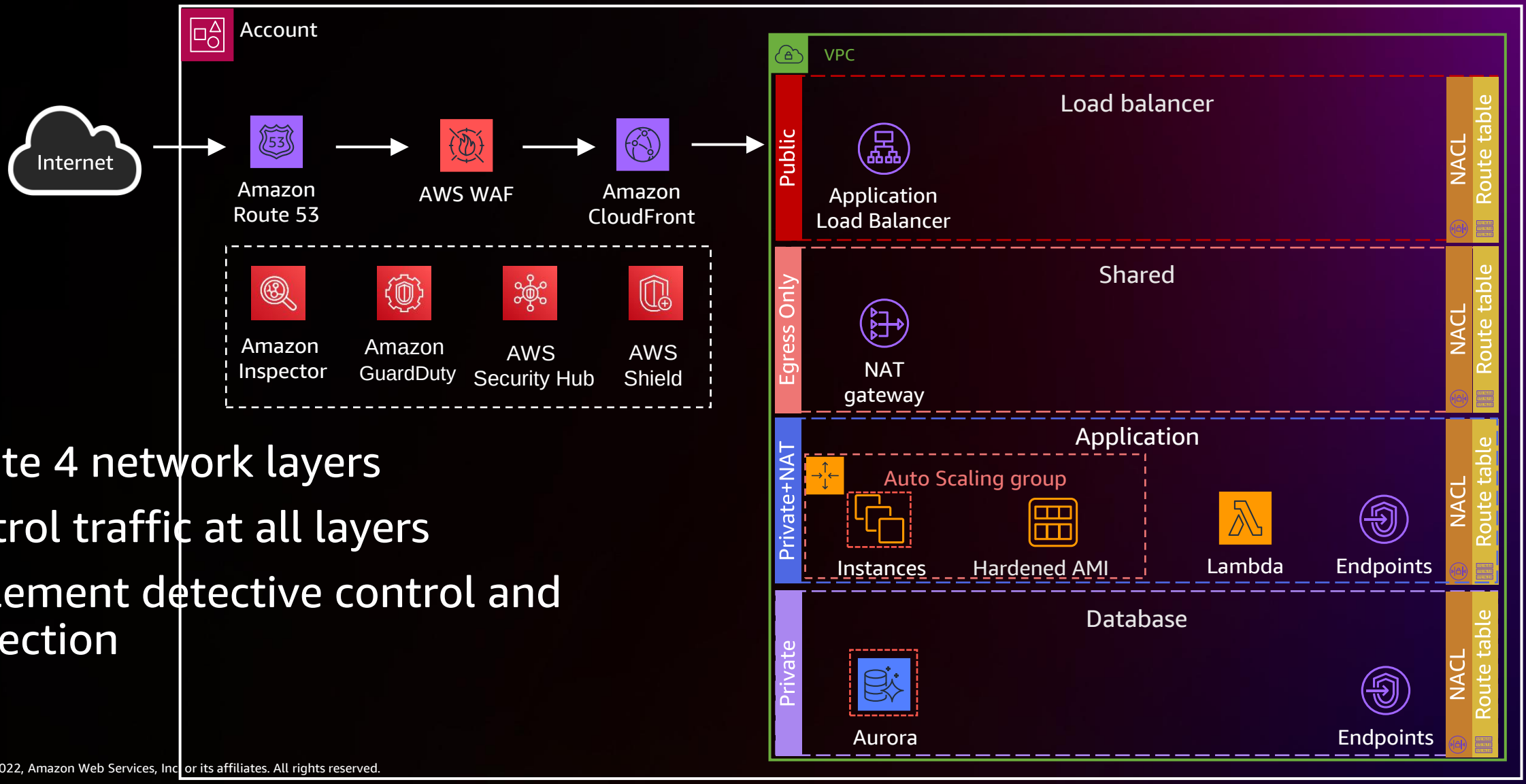
# DNB networking




aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Hyperscale infrastructure protection



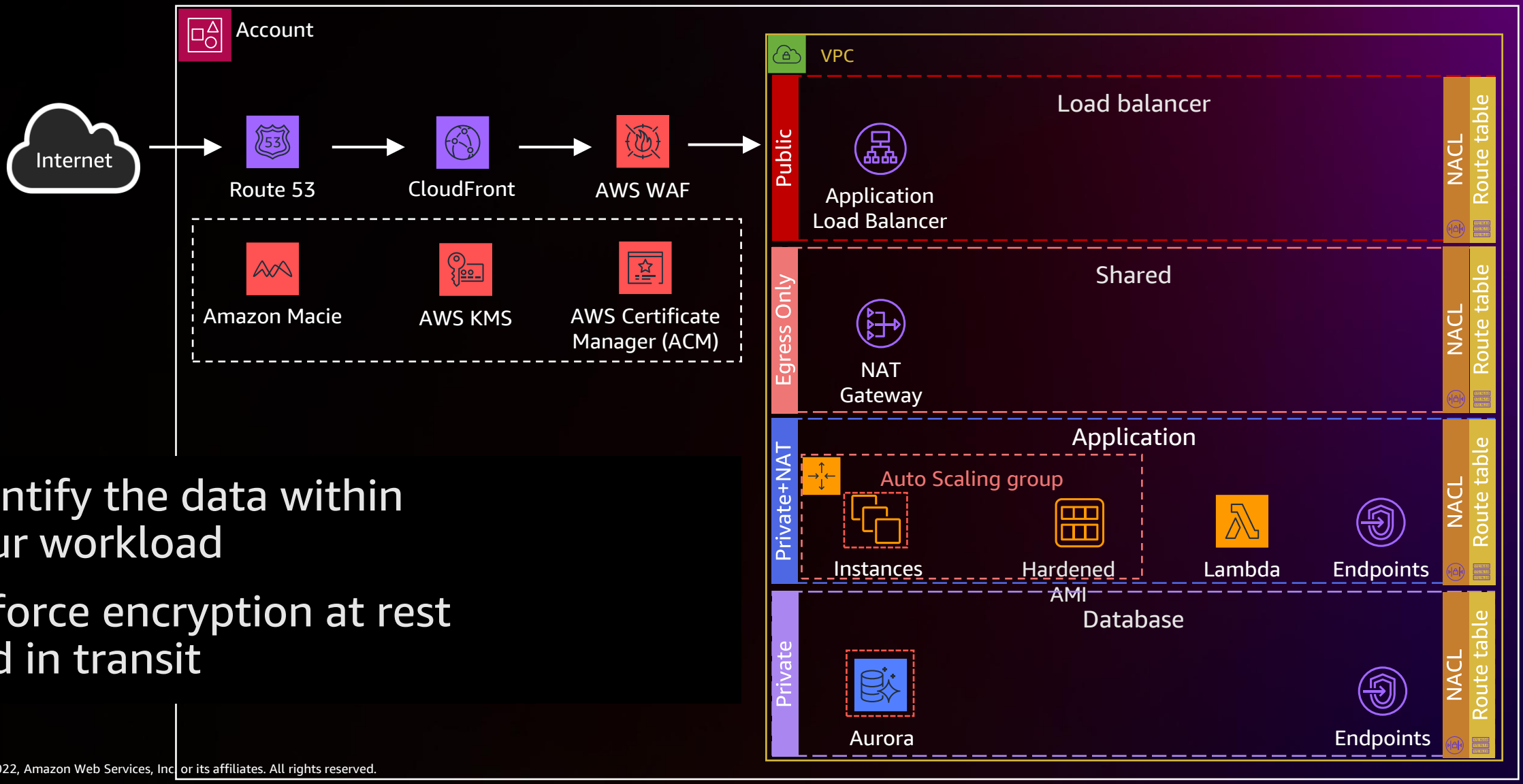



- Create 4 network layers
- Control traffic at all layers
- Implement detective control and protection

© 2022, Amazon Web Services, Inc or its affiliates. All rights reserved.

# Hyperscale data protection






- Identify the data within your workload
- Enforce encryption at rest and in transit

© 2022, Amazon Web Services, Inc or its affiliates. All rights reserved.

# Migration checklist










**Operations** **Account** **Resources**

[COP325 – Chalk Talk] Migrate AWS Accounts like a maestro

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Application modernization with Multi-account strategy



Microservice



Data Strategy



Machine Learning

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Call to action

- Start with Multi-account strategy **today**
- Engage early with AWS account team
- Move to modernize

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Cloud foundations and multi-account strategy sessions

## Chalk Talks

[DOP322 – Chalk Talk]

Optimizing runtime performance with AWS X-Ray and Amazon CodeGuru Profiler

[ARC317– Chalk Talk]

Architecting security and governance for your multi-account environment

[COP323– Chalk Talk]

Delegating access in a multi-account environment with IAM Identity Center

## Workshop

[COP206 - Workshop]

Build a complete DevSecOps pipeline on AWS

## Reference Material

[Whitepaper – Establishing your Cloud Foundation on AWS]

https://docs.aws.amazon.com/whitepapers/latest/establishing-your-cloud-foundation-on-aws/welcome.html

[Blog – Journey to Adopt Cloud-Native Architecture Series: #4 – Governing Security at Scale and IAM Baselining]

- Multi Account Strategy for Hyperscale
- Use of AWS Control Tower
- Migrate existing account under AWS Control Tower governance
- Start with Fundamental Multi Account Structure and improve

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Thank you!



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.