aws

AWSOME DAY
ONLINE CONFERENCE

2025 | APJ

AWSOME DAY
ONLINE CONFERENCE

Introduction to AWS services
Networking & security

Peter Vandaele
Technical Trainer
AWS

Networking

Amazon Virtual Private Cloud (Amazon VPC)

Amazon VPC

AWS Cloud

VPC
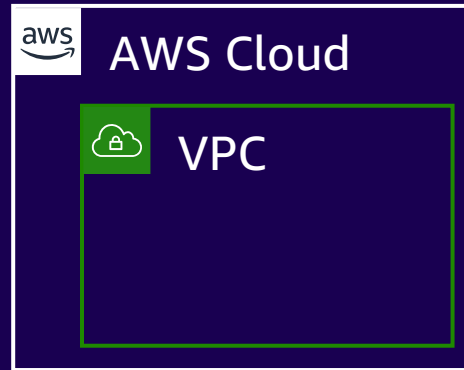
Your private network space in the AWS Cloud

Dev   Test

Provides logical isolation for your workloads

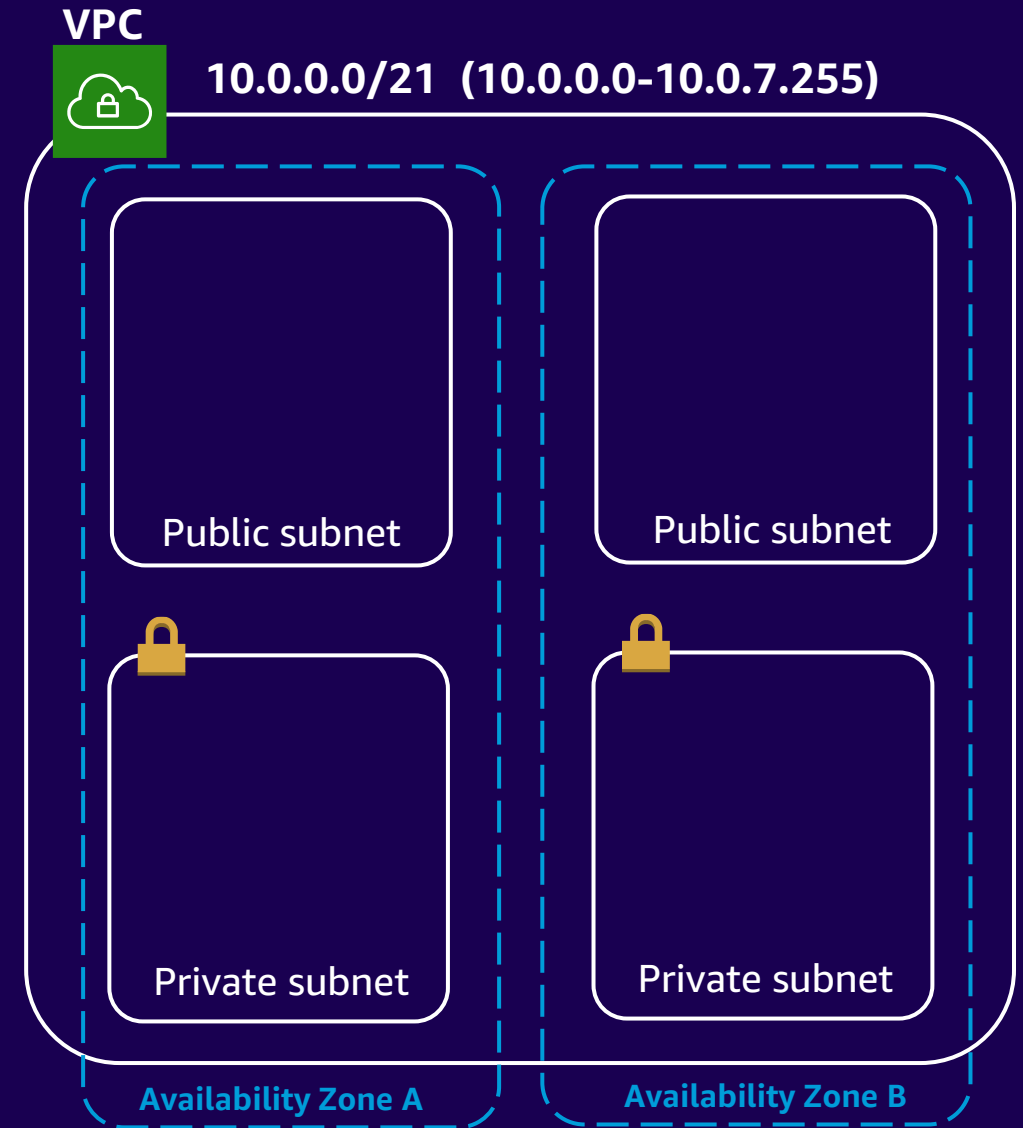Allows custom access controls and security settings for your resources

Using subnets to divide your VPC

A subnet is a segment or partition of a VPC's IP address range where you can isolate a group of resources
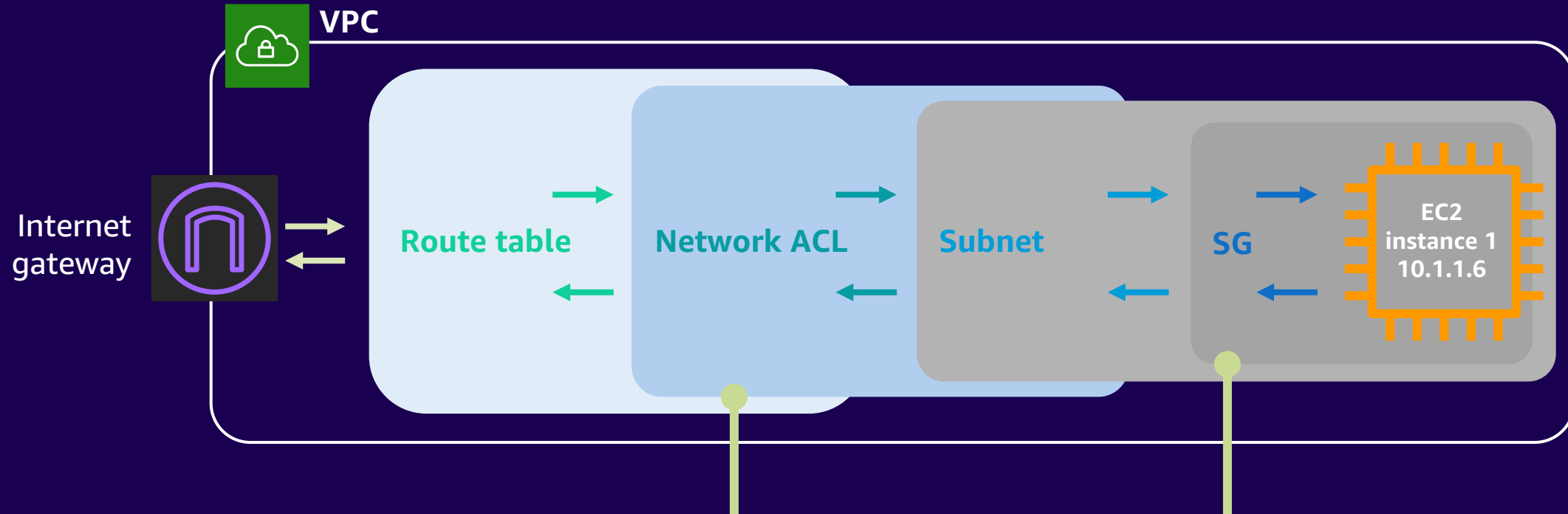
Subnets define internet accessibility

Private subnets

- No routing table entry to an internet gateway

- Not directly accessible from the public internet

VPC

10.0.0.0/21 (10.0.0.0-10.0.7.255)

Public subnet

Public subnet

Private subnet

Private subnet

Availability Zone A

Availability Zone B

Structure your infrastructure

VPC

Internet gateway → Route table → Network ACL → Subnet → SG → EC2 instance 1 10.1.1.6

- **Network access control lists (ACLs)**
- Allow/deny traffic in and out of subnets
- Hardens security as a secondary level of defense at the subnet level

Security groups
- Used to allow traffic to/from at the network interface (instance) level
- Usually administered by application developers

Elastic Load Balancing (ELB)

Elastic Load Balancing
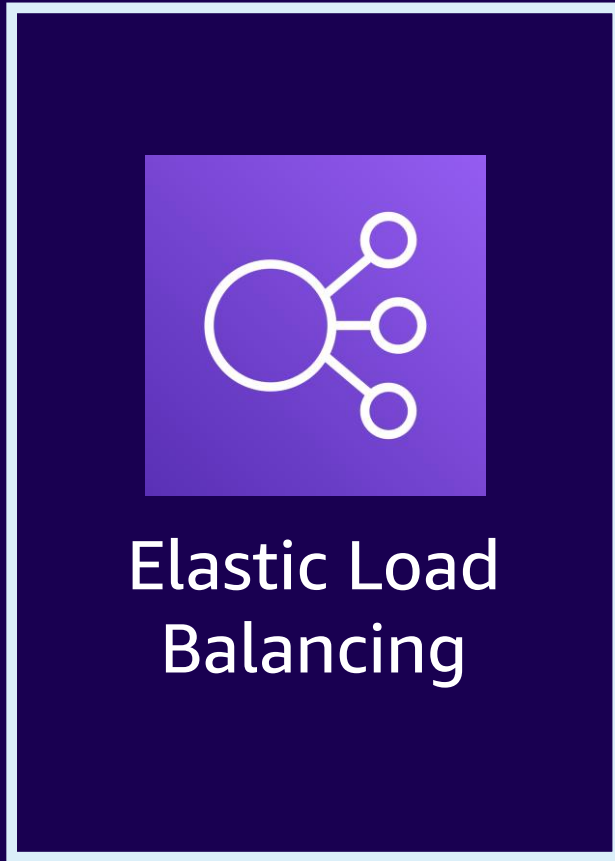
A managed load balancing service that distributes incoming application traffic across multiple Amazon EC2 instances, containers, and IP addresses
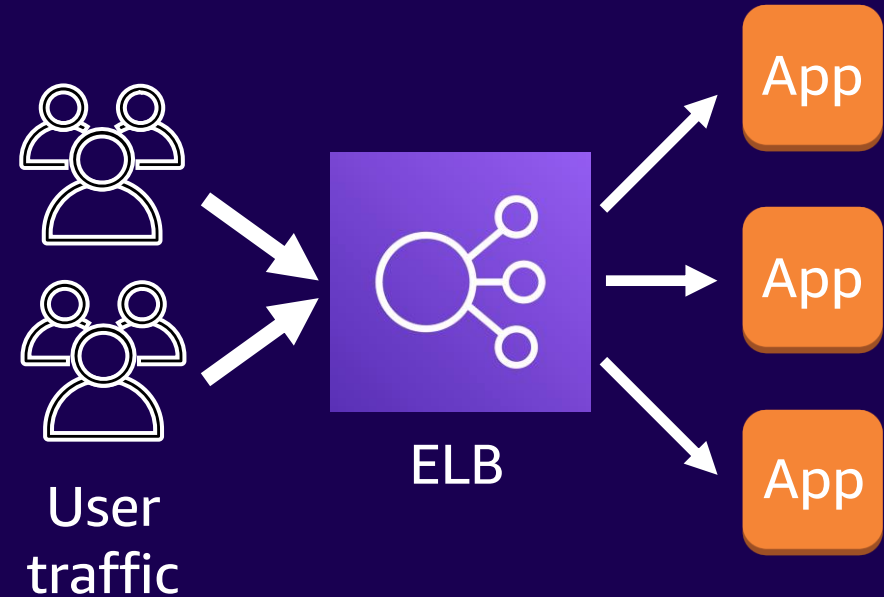
High availability

Health checks

Security features

User traffic → ELB → App, App, App

Amazon Route 53

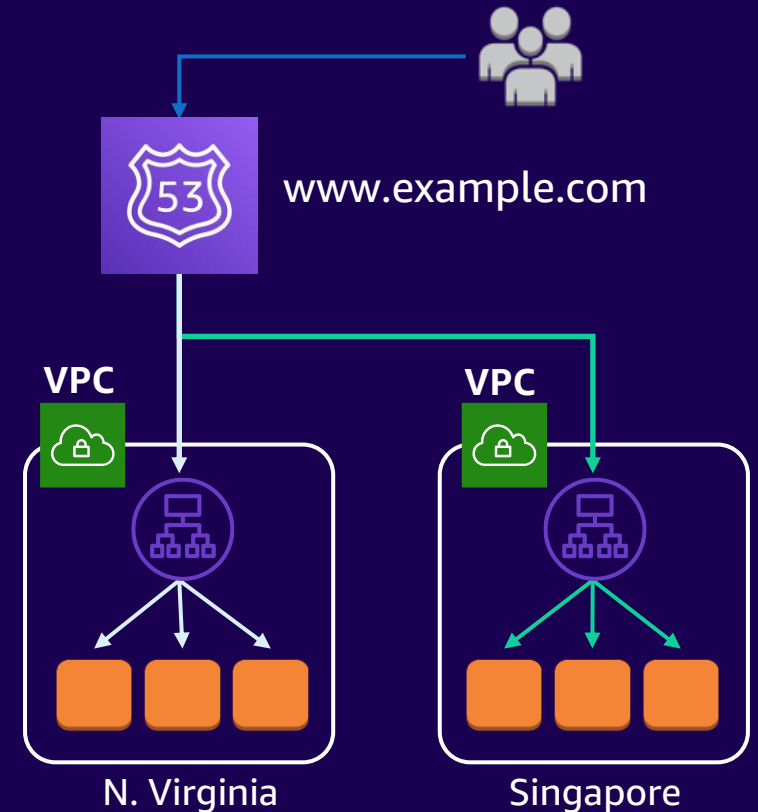Amazon Route 53

Route 53 is a highly available and scalable cloud Domain Name System (DNS) service

- DNS translates domain names into IP addresses

- Able to purchase and manage domain names and automatically configure DNS settings

- Provides tools for flexible, high-performance, highly available architectures on AWS

- Multiple routing options

www.example.com

VPC

VPC

N. Virginia

Singapore

Putting it all together

Amazon
Route 53

AWS Cloud

Amazon EC2
Auto Scaling group

Clients

Internet
gateway

ELB

EC2 instances
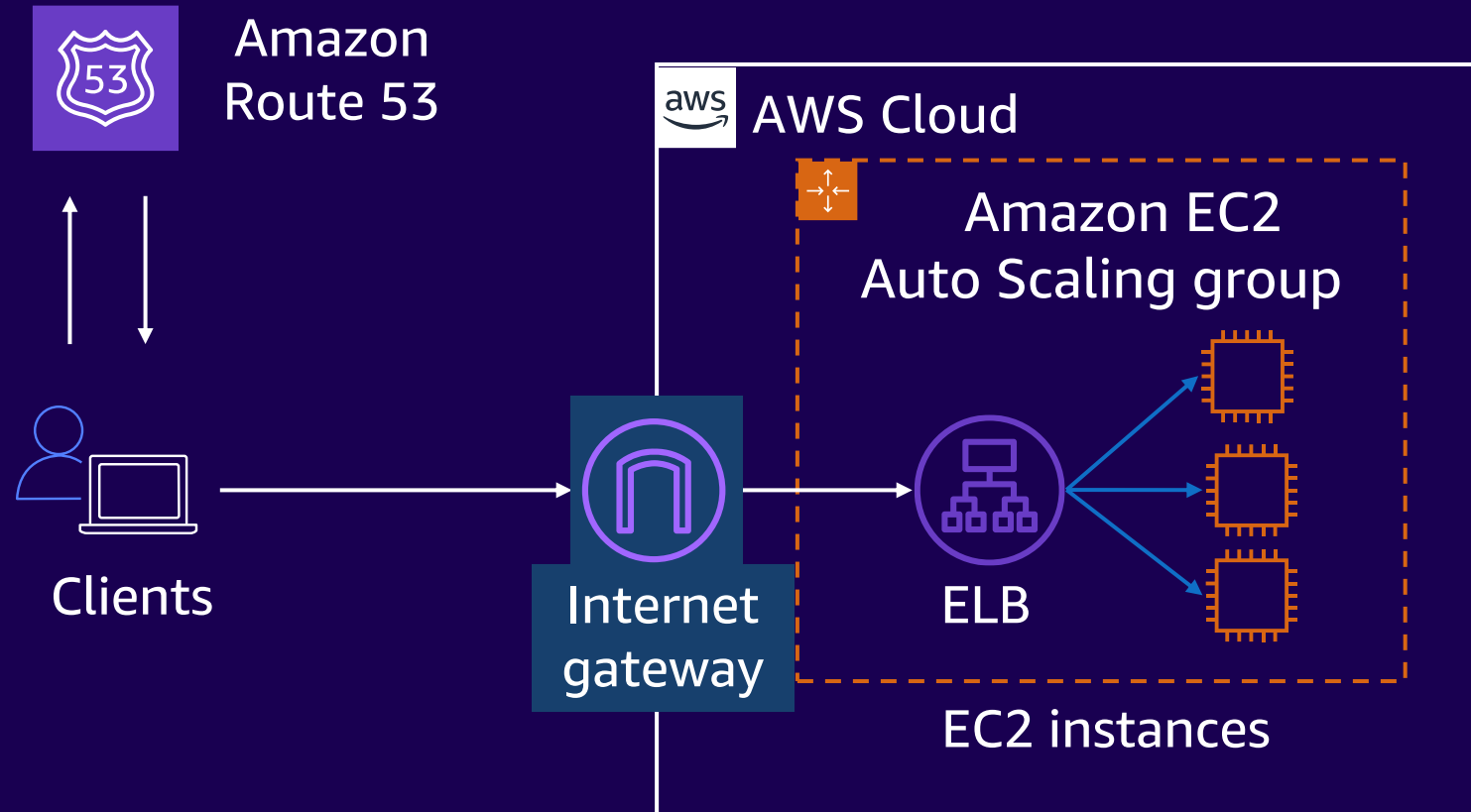
Connecting with your infrastructure

AWS Cloud

VPC
10.0.0.0/16

Internet gateway

Internet

AWS Client VPN Endpoint

TLS
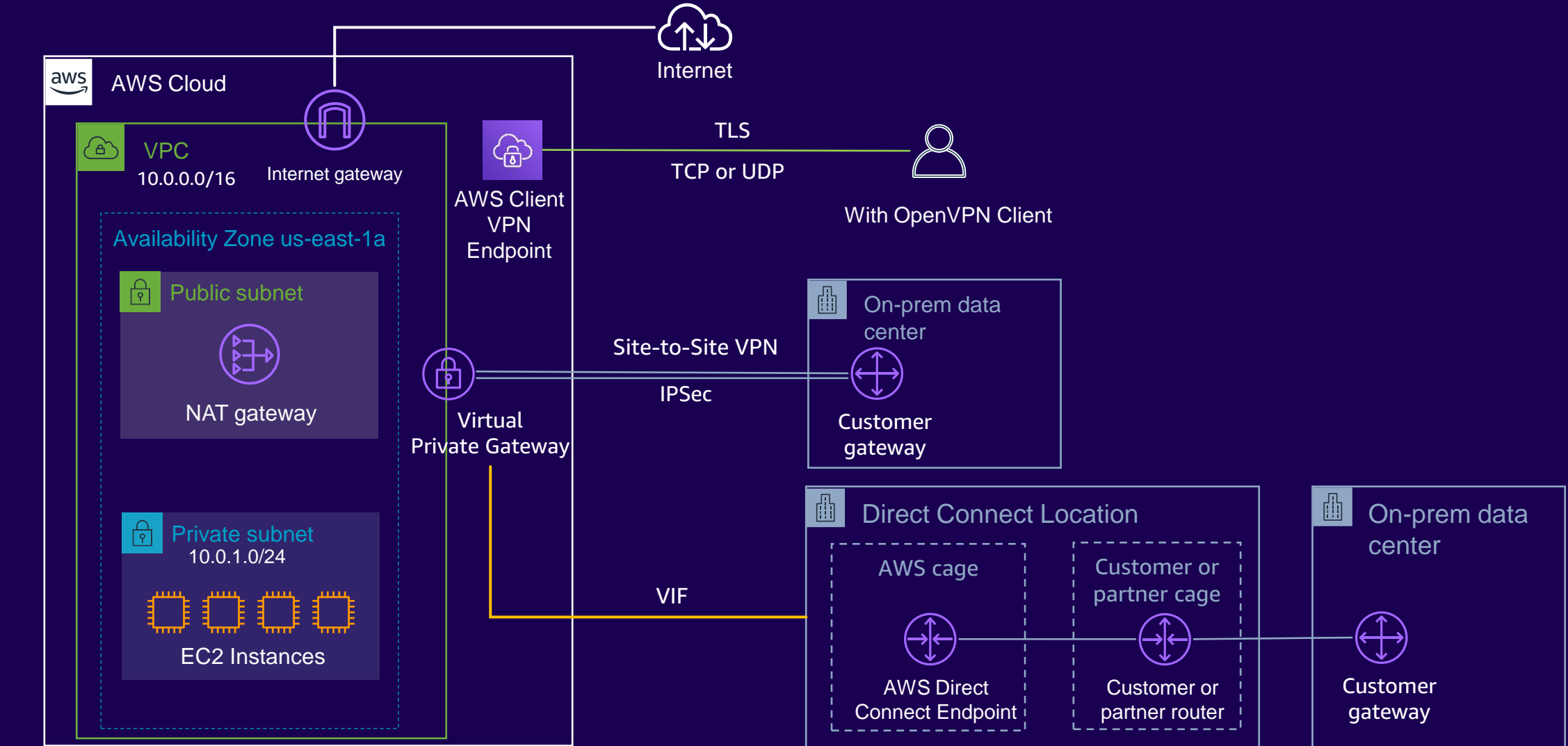
TCP or UDP

With OpenVPN Client

Availability Zone us-east-1a

Public subnet

NAT gateway

Private subnet
10.0.1.0/24

EC2 Instances

Virtual Private Gateway

Site-to-Site VPN

IPSec

On-prem data center

Customer gateway

VIF

Direct Connect Location

AWS cage

Customer or partner cage

AWS Direct Connect Endpoint

Customer or partner router

On-prem data center

Customer gateway

Key Takeaways

Amazon VPC provides:
- Logically isolated network to launch applications
- Security Groups, Network ACLs and Route tables to secure your deployments

There are three main ways customers connect to AWS:
- Client VPN
- Site-to-site VPN
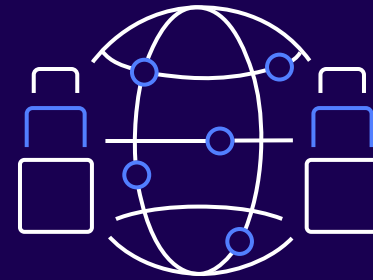- Direct Connect

Security

Security is our top priority

Designed for security
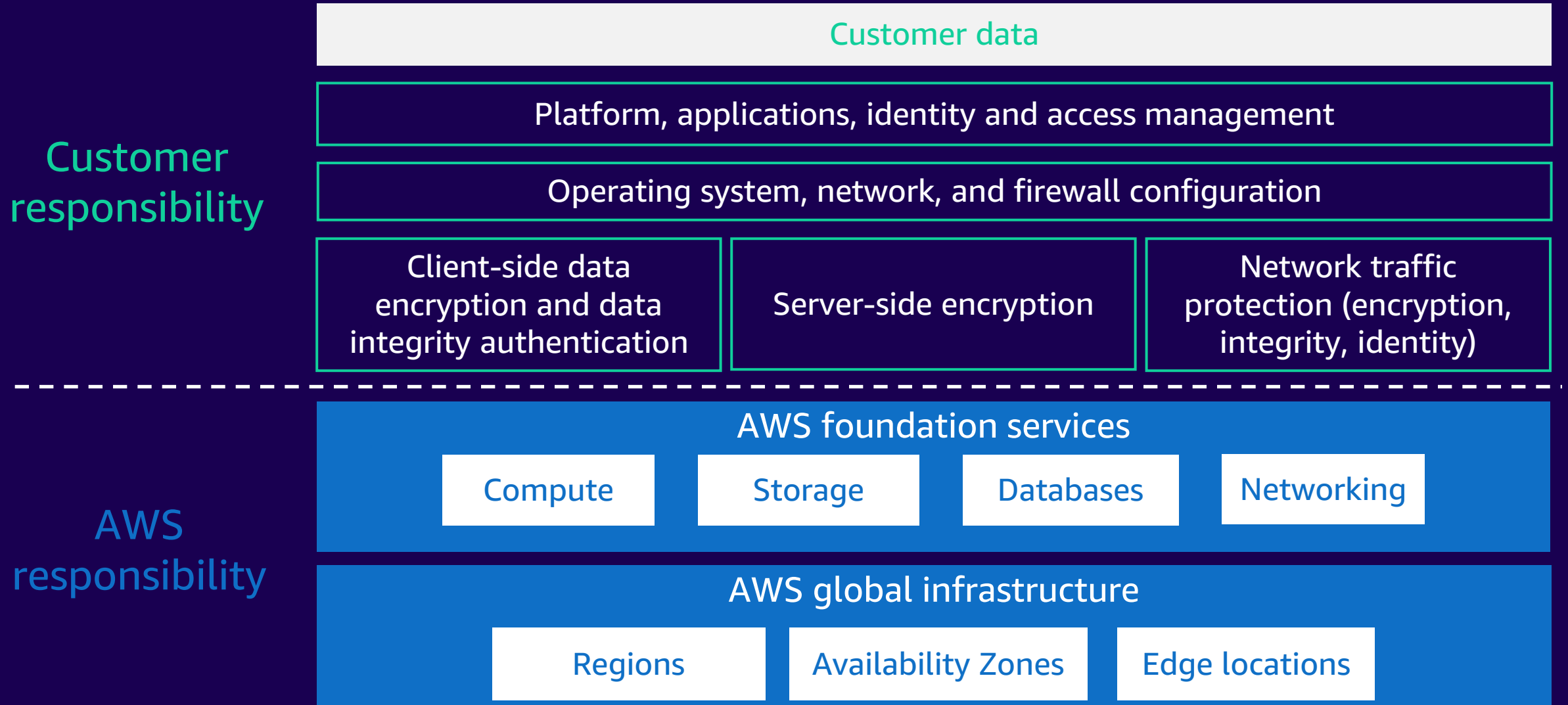
Constantly monitored

Highly automated

Highly available

Highly accredited

Shared responsibility model

Customer data

Customer responsibility

Platform, applications, identity and access management

Operating system, network, and firewall configuration

Client-side data encryption and data integrity authentication	Server-side encryption	Network traffic protection (encryption, integrity, identity)

AWS responsibility

AWS foundation services

Compute	Storage	Databases	Networking

AWS global infrastructure

Regions	Availability Zones	Edge locations

AWS Identity and Access Management (IAM)

IAM

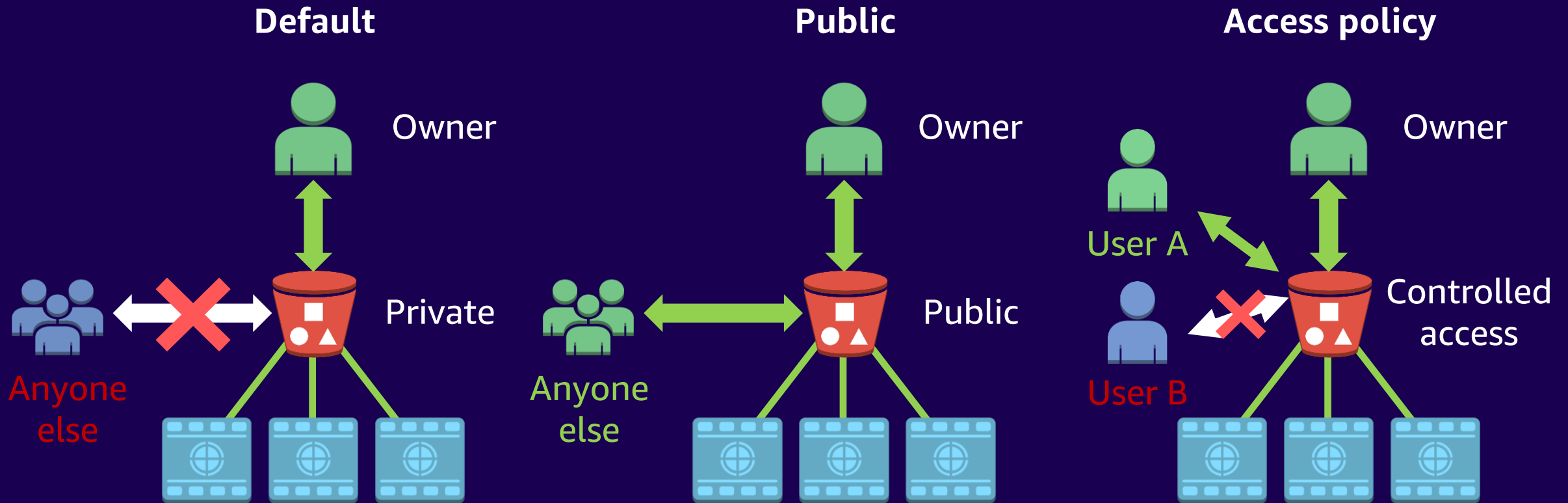Securely control access to your AWS resources

Assign granular permissions to users, groups, or roles

Share temporary access to your AWS account

Federate users in your corporate network or with an internet identity provider

Amazon S3 access control: General

Some services support resource-based policies, such as S3 bucket policies

Default

Owner

Anyone else

Private

Public

Owner

Anyone else

Public

Access policy

User A

User B

Owner

Controlled access

AWS CloudTrail

AWS CloudTrail

Track user activity and API usage in your AWS account

Continuously monitor user activities and record API calls

Useful for compliance auditing, security analysis, and troubleshooting

Log files are delivered to Amazon S3 buckets

Who?   What?   When?   Where?

API security-relevant information

What is AWS Trusted Advisor?

A service providing guidance to help you reduce cost, increase performance, and improve security

Cost optimization	Performance	Security	Fault tolerance	Service limits
0 ☑ 9 ⚠ 0 ⓘ	3 ☑ 7 ⚠ 0 ⓘ	2 ☑ 4 ⚠ 11 ❗	0 ☑ 15 ⚠ 5 ❗	37 ☑ 0 ⚠ 1 ❗

$7,516.87
Potential monthly savings

Key Takeaways

Security is EVERYONE'S responsibility

   Security IN the Cloud / Security OF the Cloud

IAM allows users to control access to AWS resources

   Apply policies to Users, Groups & Roles

When a S3 bucket is created, by default it is set to PRIVATE

CloudTrail records API calls in AWS

   Who, What, When, Where

AWS Trusted Advisor provides recommendations

   help you reduce cost, increase performance and improve security

Thank you for attending **AWSome Day Online Conference**

We hope you found it interesting! A kind reminder to **complete the survey.**
Let us know what you thought of today's event and how we can improve the event experience for you in the future.

aws-apj-marketing@amazon.com

twitter.com/AWSCloud

facebook.com/AmazonWebServices

youtube.com/user/AmazonWebServices

linkedin.com/company/amazon-web-services

twitch.tv/aws

Test your knowledge

Thank you!