
aws
SUMMIT
INDIA | MAY 25, 2023

SECR002

Security is top priority- How AWS Security operates under the hood

Vikas Sood
Head of Security Assurance
AWS India

Avanish Yadav
Sr. Networking Specialist SA
AWS India

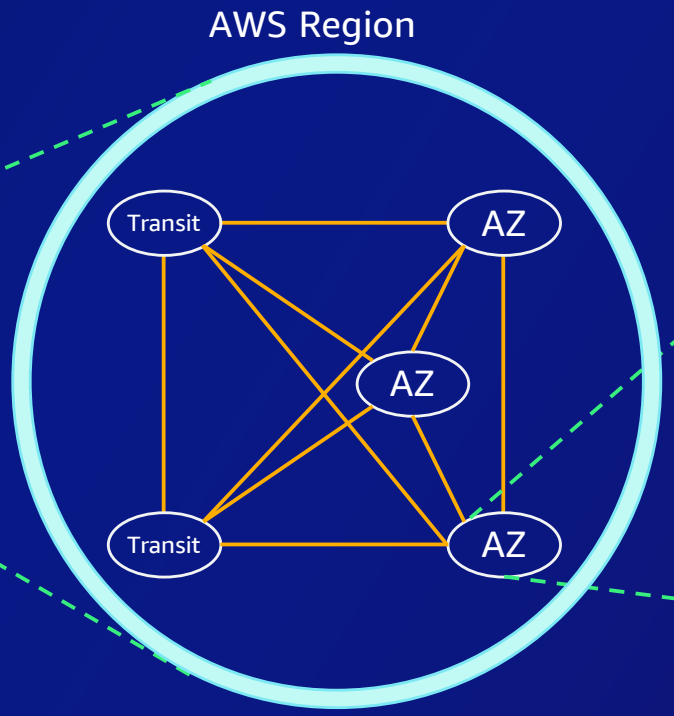
Agenda

- AWS Infrastructure
- Operational resiliency
- Data Centre security
- AWS NITRO system
- Shared Responsibility Model
- Security assurance - Continuous assessment and Compliance
  - SOC & ISO certifications
- Artifact

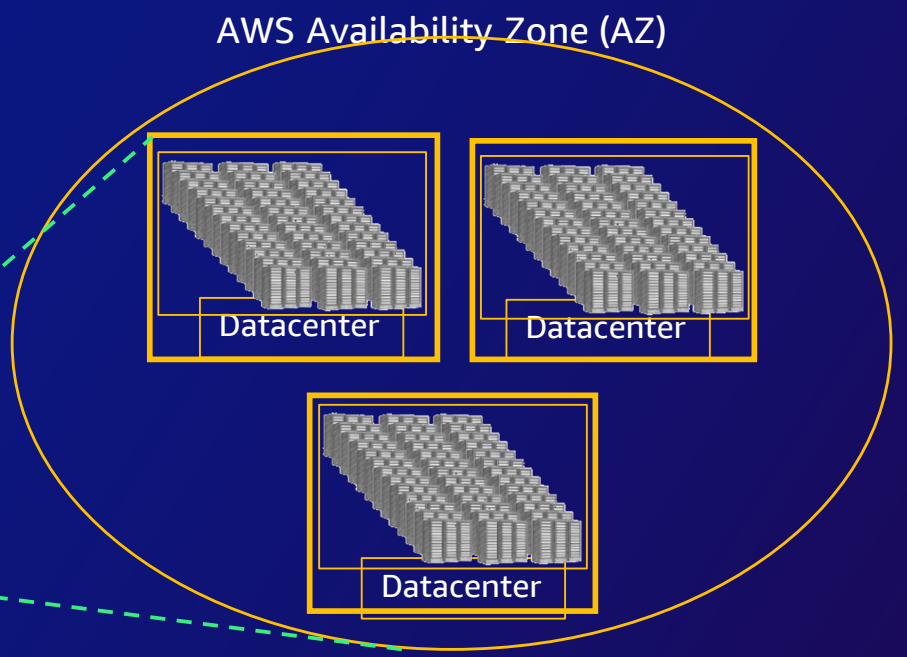
AWS Infrastructure

AWS Region design

AWS Regions are comprised of multiple AZs for **high availability, high scalability,** and high **fault tolerance.** Applications and data are replicated in real time and consistent in the different AZs.



A Region is a physical location in the world where we have multiple **Availability Zones.**



Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in separate facilities.

AWS Global Infrastructure

AWS REGIONS, LOCAL ZONES, EDGE LOCATIONS, AND GLOBAL BACKBONE

AWS Network Backbone
Redundant 400 GbE network and private capacity between all regions except China

Direct Connect:
100+ locations; customers can reach every AWS Region from their local Direct Connect PoP

aws

Region & number of Availability Zones (AZs)
31 geographical regions, 99 availability zones

United States

GovCloud (U.S.):
U.S.-East (3), US-West (3)

U.S. West
Oregon (4), Northern California (3)

U.S. East
N. Virginia (6), Ohio (3)

Canada

Central (3)

South America

São Paulo (3)

Africa

Cape Town (3)

Europe

Frankfurt (3)
Ireland (3)
London (3)
Milan (3)
Paris (3)
Spain (3)
Stockholm (3)
Zurich (3)

Middle East

Bahrain (3)
UAE (3)

Asia Pacific

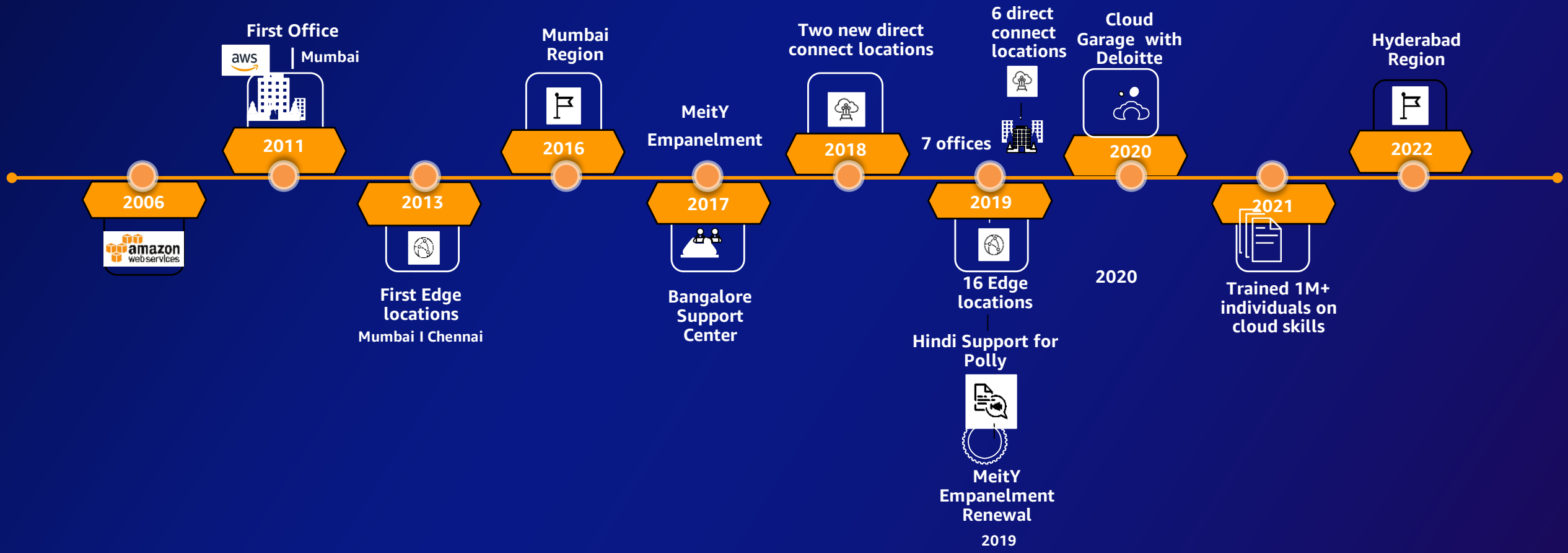
Beijing (2)
Hong Kong (3)
Hyderabad (3)
Jakarta (3)
Mumbai (3)
Ningxia (3)
Osaka (3)
Seoul (4)
Singapore (3)
Tokyo (4)

Australia

Sydney (3)
Melbourne (3)

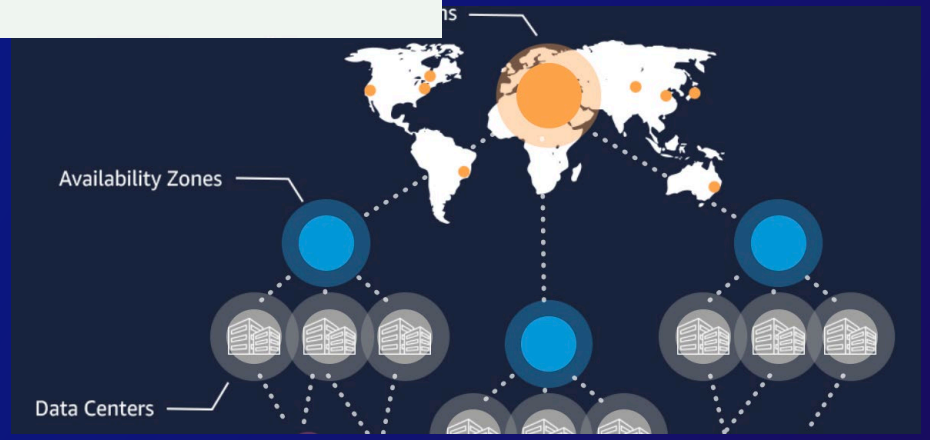
Announced Regions: **4** Regions and 12 AZs in Canada, Israel, New Zealand, and Thailand

The AWS journey in India



AWS's infrastructure provides operational resilience

- Ability to provide continuous service
- Compartmentalization
- Cell based architecture
- Software deployment in a staggered Fashion



Data center – Perimeter layer

- Access is on a “needs to know” basis and regularly
- Security Guards and CCTV
- Multi-factor authentication required
- Intrusion detection systems
- Access Log Monitoring systems and alarms
- 24/7 monitoring, triage and incident response by Security Operations Centers globally

Data center – Infrastructure layer

- Teams regularly run diagnostics on machines, network and backup equipment
- Electrical power systems are designed to be fully redundant
- Temperature and humidity controls to prevent overheating

Data center – Data layer

- AWS servers can warn employees of any attempts to remove data. In the unlikely event of a breach, the server is automatically disabled
- When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88
- Media that stored customer data is not removed from AWS control until it has been securely decommissioned

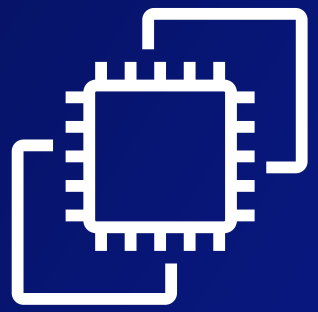
Data center – Environmental layer

- Prior to choosing a location, AWS performs initial environmental and geographic assessments
- Automatic sensors to detect environmental threats like natural disasters and fire
- AWS tests the Business Continuity Plan regularly with drills that simulate different scenarios

Enhance security with the AWS Nitro System

Today, over **60 million** new instances are spun up every day on Amazon EC2

AWS Nitro System



AWS Nitro System

After a decade of Amazon EC2 experience, if we applied all of our learnings, how would we change our server platforms?

Improve throughput

Simplify hypervisor

Reduce latency and jitter

Bare-metal instances

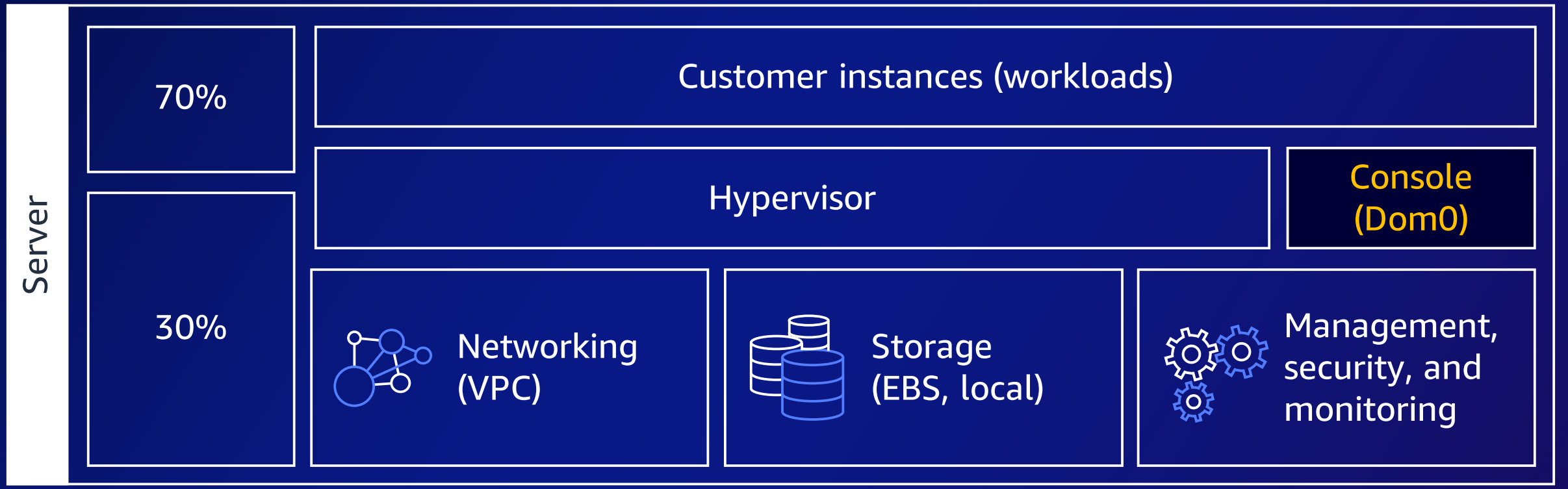
Transparent encryption

Hardware root of trust

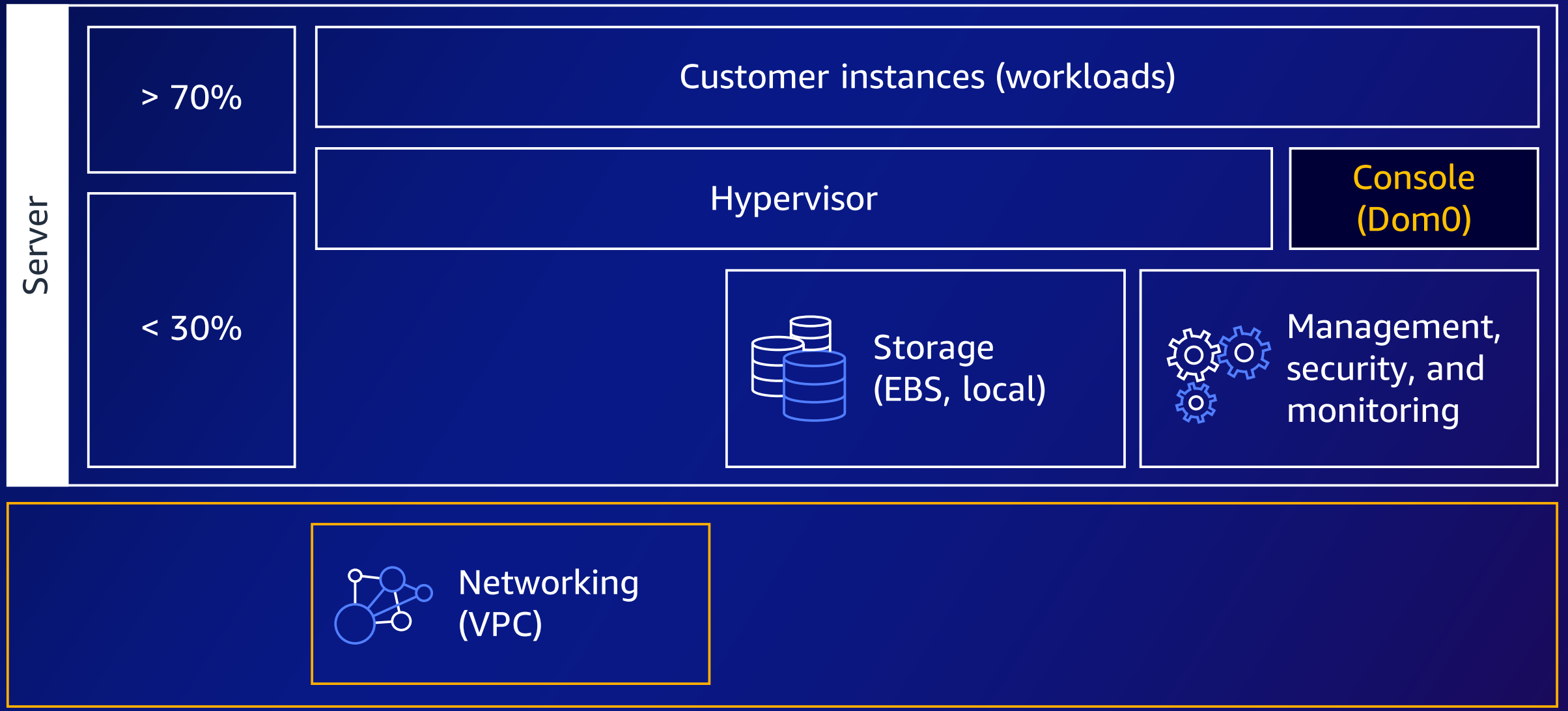
No operator access

Narrow auditable APIs

Original EC2 “instance” host architecture



2013 EC2 “instance” host architecture



2014 EC2 “instance” host architecture

Server

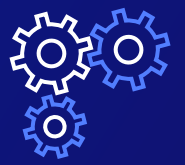
> 70%

< 30%

Customer instances (workloads)

Hypervisor

Console (Dom0)

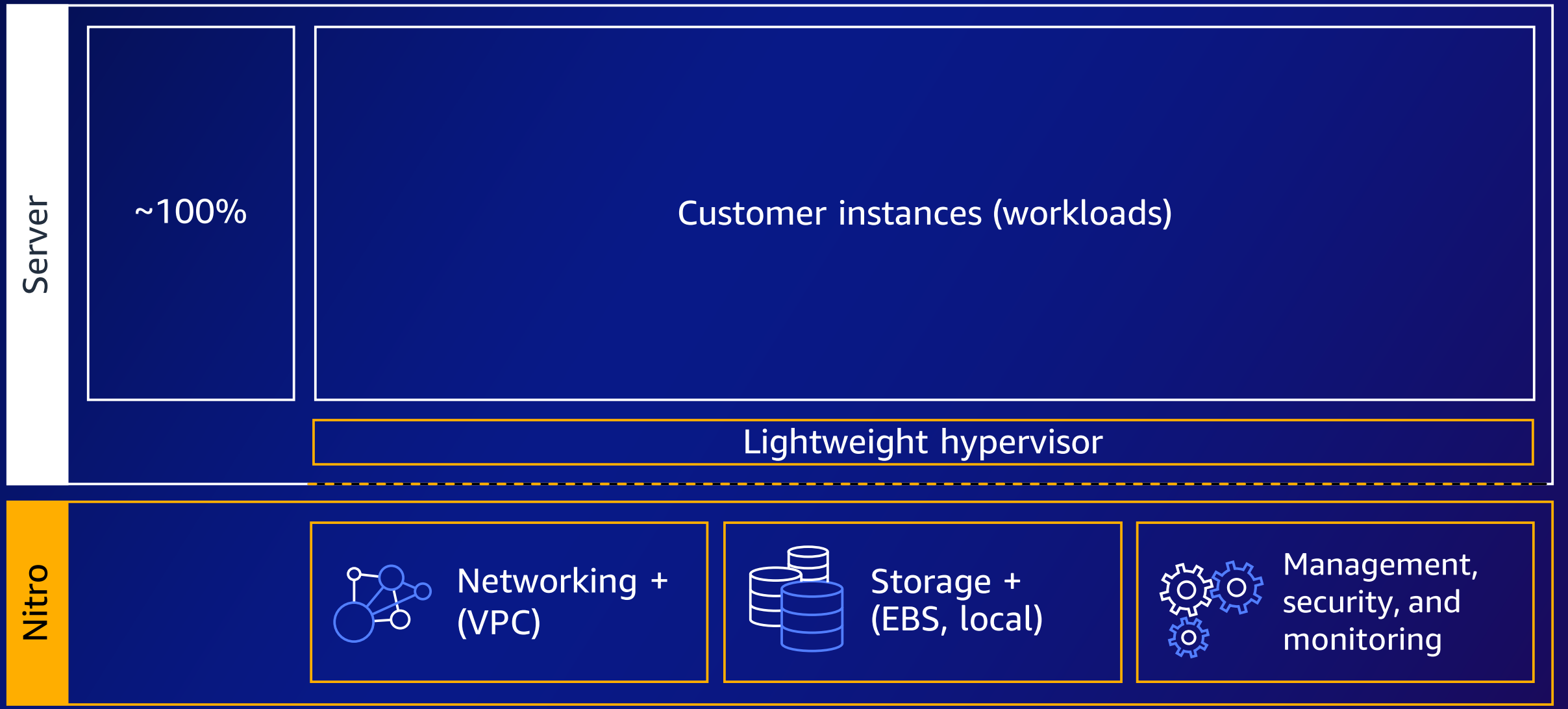


Management, security, and monitoring

Networking + (VPC)

Storage (EBS, local)

Today: The AWS Nitro System architecture

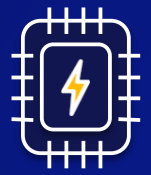


AWS Nitro System

Nitro Cards

VPC networking
Amazon EBS
Instance storage
Nitro SSDs
System controller

Nitro Security Chip



Integrated into motherboard
Traps I/O to nonvolatile storage
Hardware root of trust
Protects hardware resources

Nitro Hypervisor

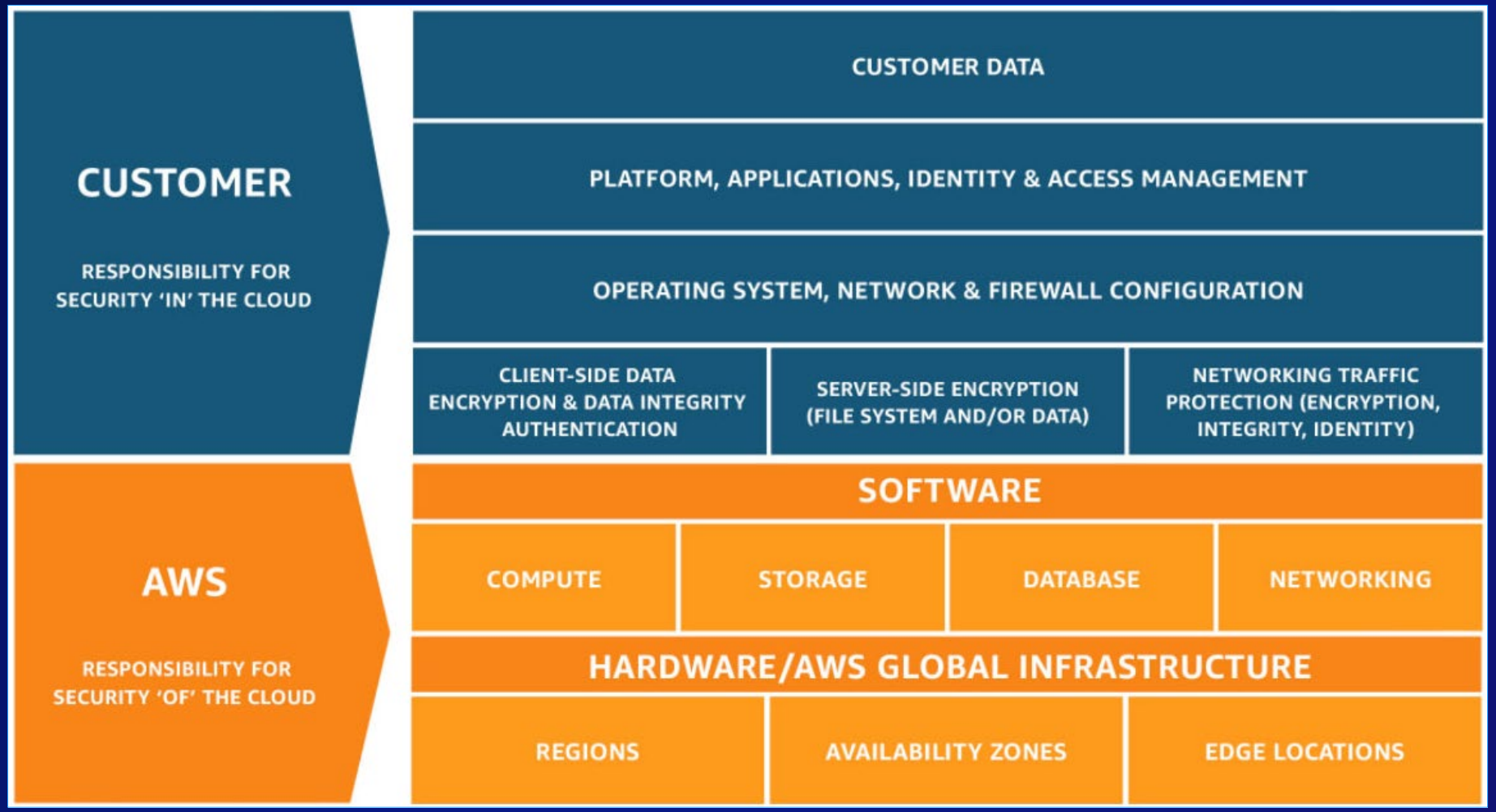
Lightweight hypervisor
Memory and CPU allocation
Bare-metal-like performance

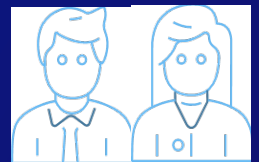
NitroTPM

Trusted Platform Module 2.0
Instance health attestation
Cryptographic offload

Shared Responsibility Model

Security & compliance is a shared responsibility





Customer Compliance Auditors

Third-party Independent Auditors

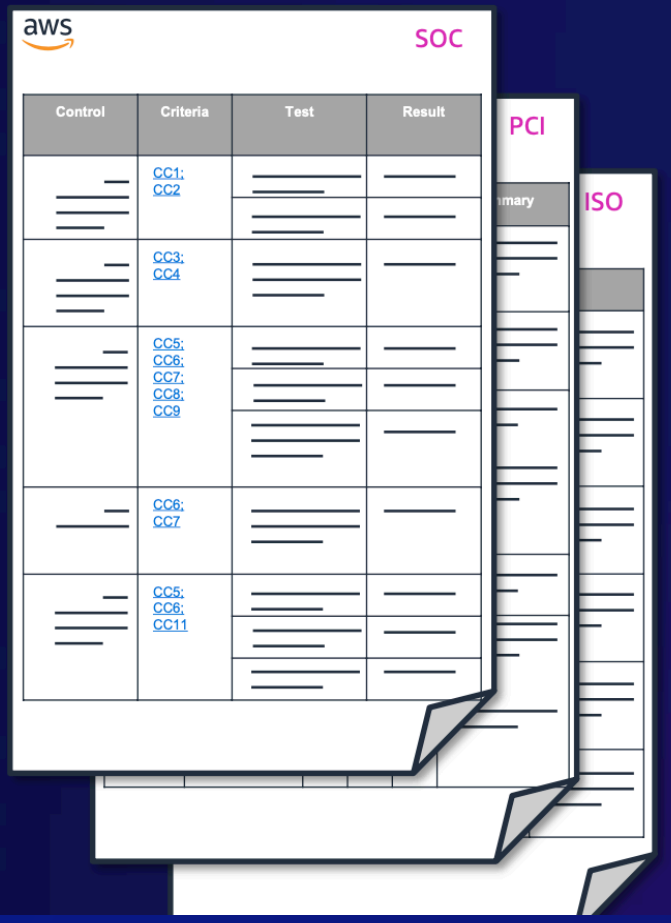
https://aws.amazon.com/compliance/shared-responsibility-model/

Applying Shared responsibility

Customer cloud control framework

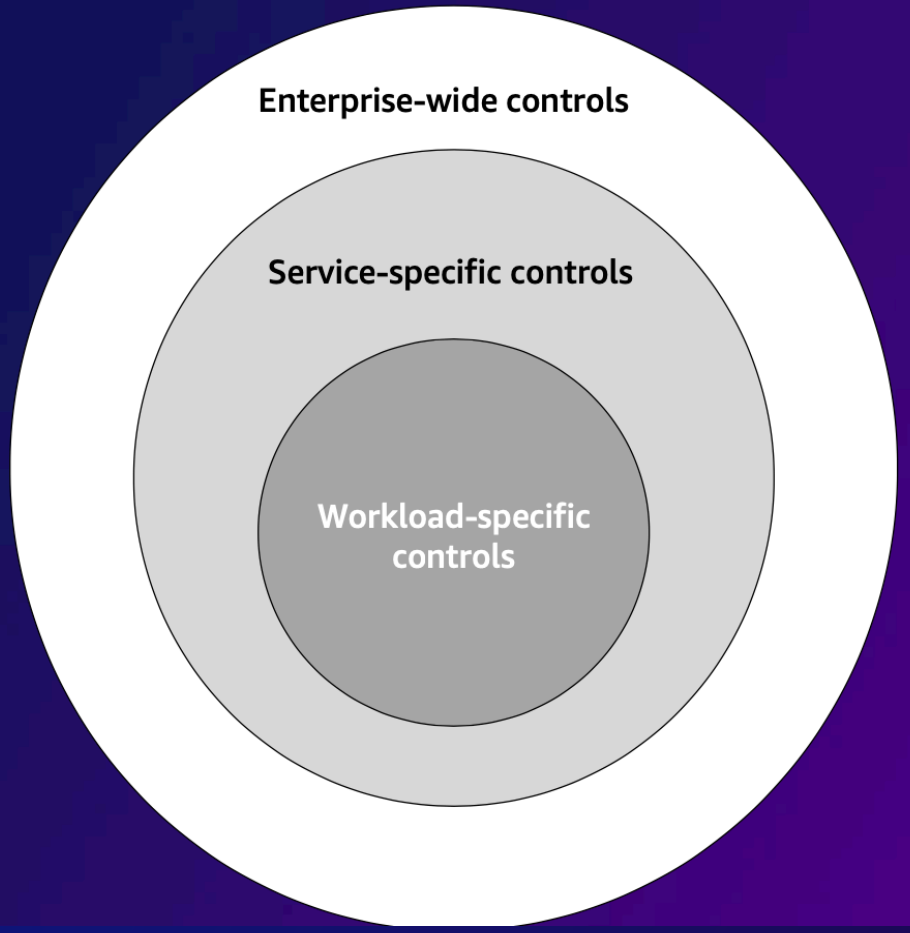
=

Controls inherited from AWS



+

Customer controls in the cloud



Cloud Certifications and Attestations

Service Organization Controls (SOC) & ISO Reports

SOC 1: Information relevant to customer internal controls over financial reporting *(formerly SAS 70, SSAE16)*

SOC 2: Reports on AWS security controls relevant to security, availability, processing integrity, confidentiality, and privacy

SOC 3: Publically-available summary of the AWS SOC 2 report

6 month rolling audit : Apr – Sep & Oct - March

Continued Operations Notice: States that we continue to operate our control environment described in last audit report

ISO 27001: Security management best practices and comprehensive security control guidance

ISO 27017: Cloud-specific security control guidance

ISO 27018: Protection of personal data, Personally Identifiable Information (PII), in the cloud

ISO 9001: Quality management and quality assurance

ISO 20000-1: Service management system (SMS) standard

ISO 27701: Privacy Information Management System (PIMS)

Ministry of Electronics & Information Technology (MeitY) empanelment

AWS Mumbai Region is MeitY Empaneled since 2017, yearly conformance audit. Hyderabad Region is under empanelment with MeitY.

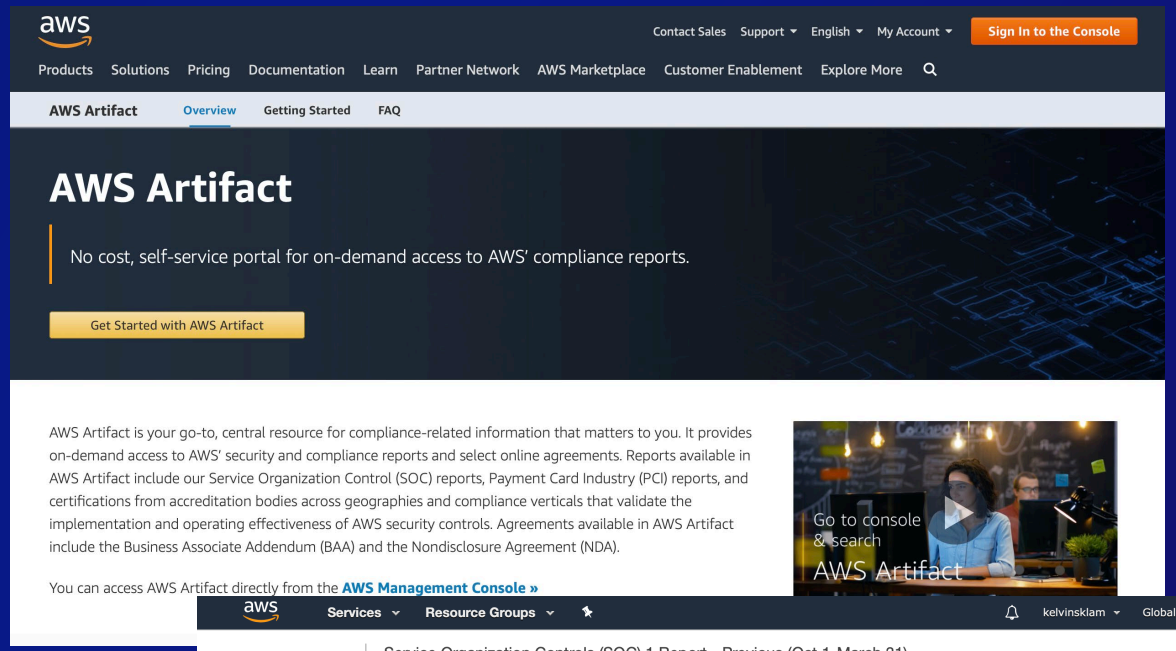
- **TIA-942:** Certificate of Conformance Constructed Facility for Data Centres. In India all AWS data centers are TIA – 942, Level III compliant required as per MeitY

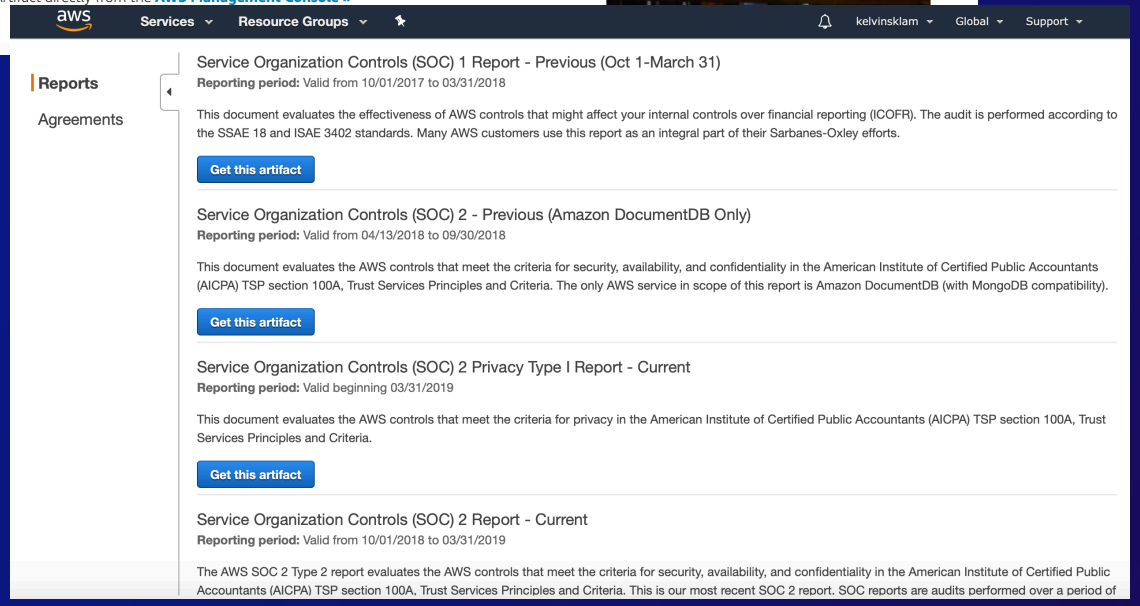
- **ISO 20000-1:** Service management system (SMS) standard

AWS Artifact

AWS Artifact A central resource for compliance-related information for our customer

- **Comprehensive Resources** access all of AWS' auditor issued reports, certifications, accreditations and other third-party attestations
- On-Demand access





https://aws.amazon.com/artifact/

CSP Responsibility – Security of the Cloud

Global Infrastructure

AWS Regions, and Availability Zones (AZs)

AWS Edge Locations and Points of Presence (POPs)

Content Delivery Network (CDN)

Physical & Environmental Security

Physical Security of the Data Centers

Ensure Environmental Monitoring and Protection

Physical Access Control

Equipment Monitoring and Maintenance

Security Operations Centre (SOC)

Infrastructure Security

Security of Compute, Storage, and Database Infrastructure

Hypervisor Security

Infrastructure availability and resiliency

Network Security

Telecommunication Security

Network Security

Network Segregation and Protection

Network availability and resiliency

Compliance & Assurance

Global Standards & Certifications

Regulatory and Compliance Requirements

Customer Audits

SECR002

Security is top priority- How AWS Security operates under the hood

Vikas Sood
Head of Security Assurance
AWS India

Avanish Yadav
Sr. Networking Specialist SA
AWS India

AWS Global Network

AWS Global Infrastructure

AWS REGIONS, LOCAL ZONES, EDGE LOCATIONS, AND GLOBAL BACKBONE

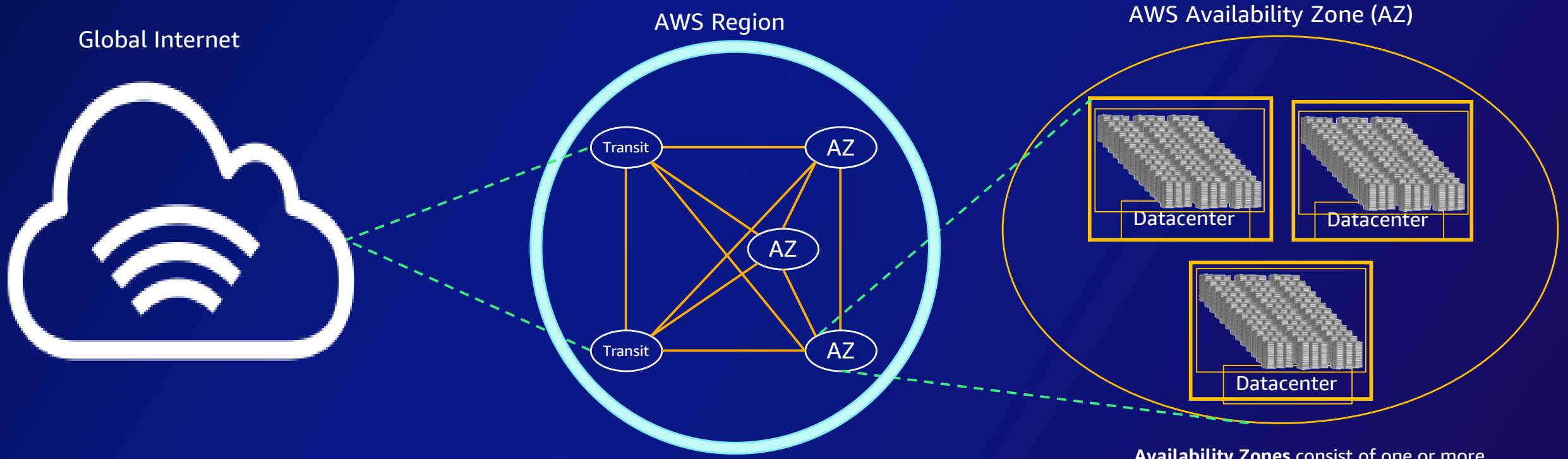
AWS Network Backbone
Redundant 400GbE network and private capacity between all regions except China

Direct Connect:
100+ locations; customers can reach every AWS Region from their local Direct Connect PoP

aws

AWS region connecting to global internet

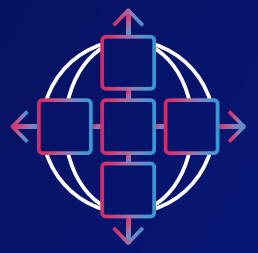
AWS Regions are comprised of multiple AZs for **high availability, high scalability,** and high **fault tolerance.** Applications and data are replicated in real time and consistent in the different AZs.



A Region is a physical location in the world where we have multiple **Availability Zones.**

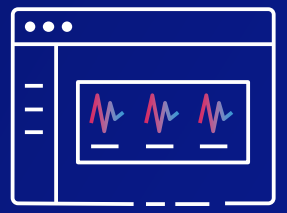
Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in separate facilities.

Why have a global backbone network?



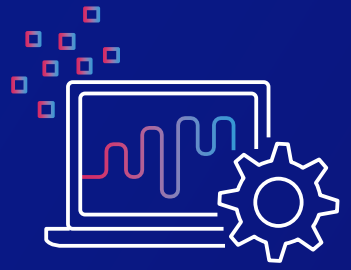
SCALABILITY

Improved scalability by controlling network expansion



AVAILABILITY

Improved availability by controlling network redundancy



PERFORMANCE

Improved performance by controlling paths customer traffic traverses

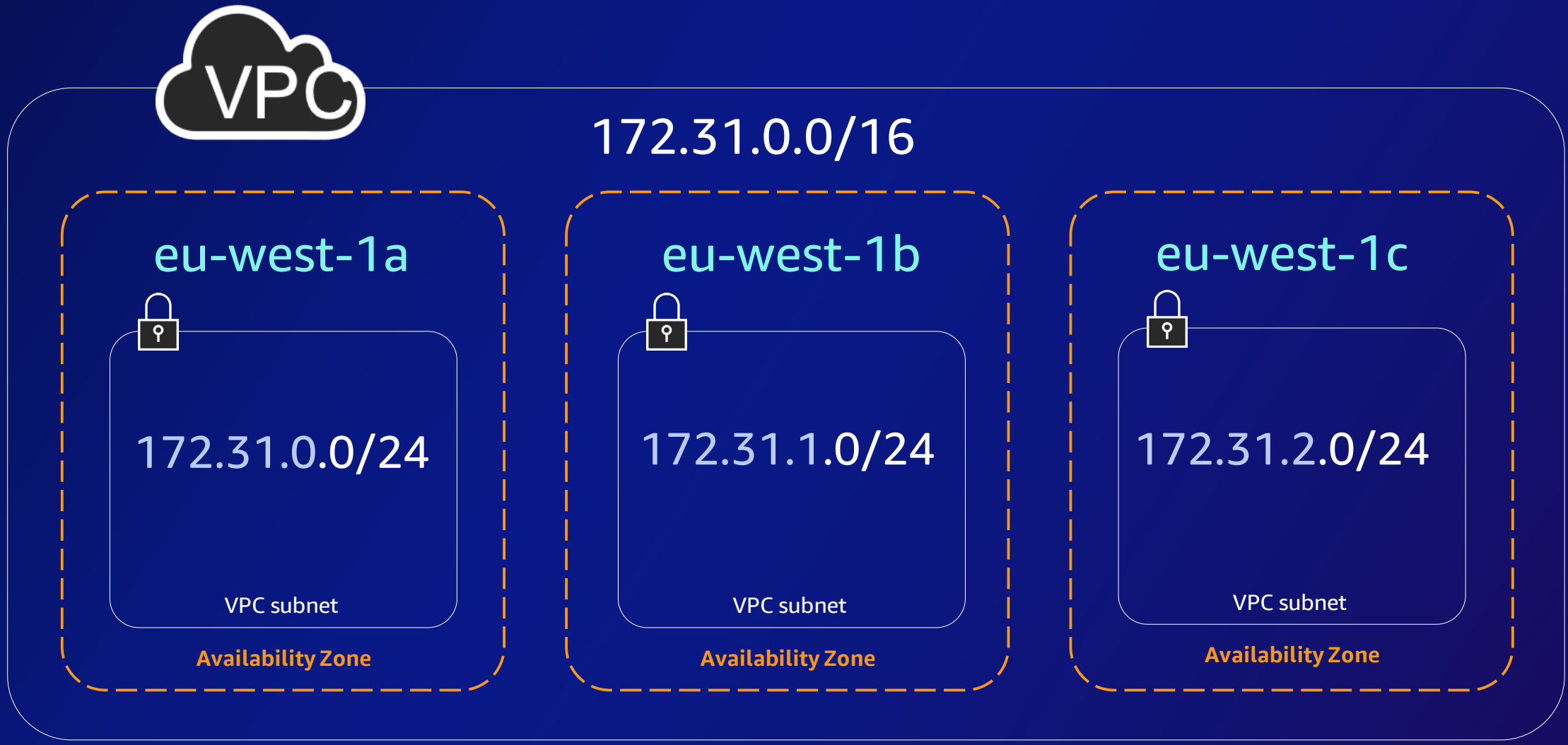
SECURITY

Improved security by ensuring traffic traverses our infrastructure rather than the internet

ALL REGION-TO-REGION TRAFFIC TRAVERSES THE AWS BACKBONE

How the AWS Backbone is available to you ?

VPC subnets and availability zones



Network Level Encryption

Protecting data using encryption

WE PUT SECURITY AT THE CENTER OF EVERYTHING WE DO

CROSS-REGION

Traffic sent between Regions with VPC peering or TGW peering is encrypted by default

BETWEEN INSTANCES

Majority of instance types use the offload capabilities of the Nitro System hardware to automatically encrypt in-transit traffic between instances

TO YOUR DATA CENTER

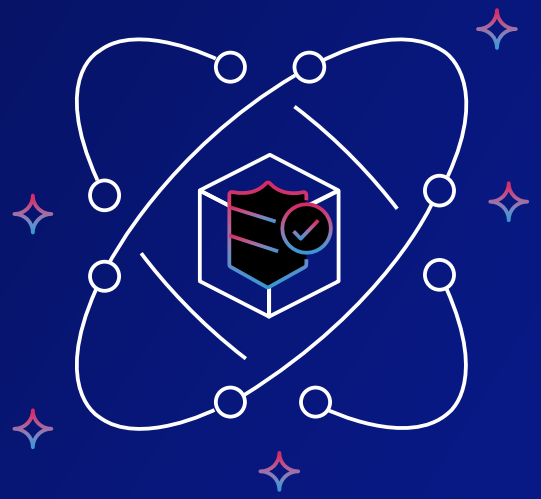
Use IPsec VPN tunnels or Direct Connect MACsec support to ensure that traffic between AWS and your locations remains protected

APPLICATION TRAFFIC

We make it easy for you to encrypt your application traffic with TLS

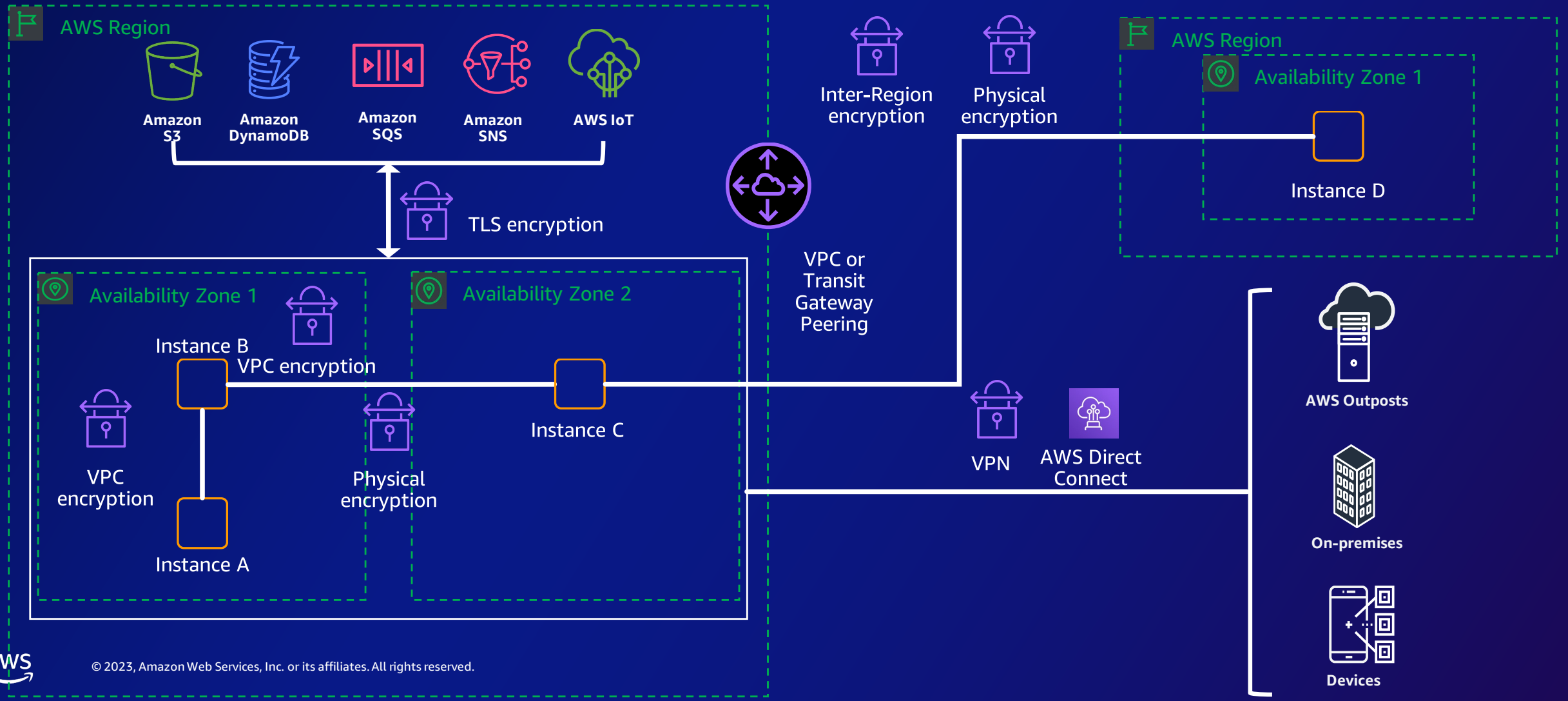
Quantum Safe Encryption

PROTECT YOUR DATA IN TRANSIT WITH QUANTUM SAFE CRYPTOGRAPHY



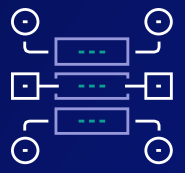
- All physical links leaving Amazon-controlled facility encrypted with AES-256 encryption
- AES-256 VPC encryption with quantum safe key exchange
- Hybrid post-quantum key exchange with AWS KMS

How Encryption is available to you ?



Enhancing security of the Cloud – Edge/Perimeter Protection

Edge/Perimeter protection with AWS Security



Scales automatically, AWS managed infrastructure

Highly flexible customizable rules or AWS Managed rules

AWS Firewall Manager

Centrally configure and manage AWS WAF rules across accounts and applications

AWS Network Firewall

Deploy network security across your Amazon VPCs with just a few clicks

AWS Shield

Managed DDoS protection service that safeguards web applications running on AWS

AWS WAF Web Application Firewall

Protects your web applications from common web exploits ensuring availability and security

Amazon Route 53 Resolver DNS Firewall

Provides protection for outbound DNS requests from your Amazon VPCs

PayU helps customers make secure online payments faster by streamlining firewall management on AWS

PayU offers payment gateway solutions to online businesses worldwide and serves more than 4.5 million merchants across India with over 100 payment methods.

PayU

50% performance improvement

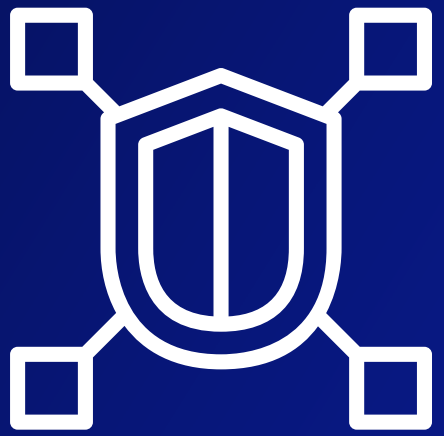
1.2M payments processed daily

Decreased compliance audits to minutes

aws

What’s new to Perimeter Protection Domain ?

Perimeter Protection – New Services



Amazon VPC Lattice

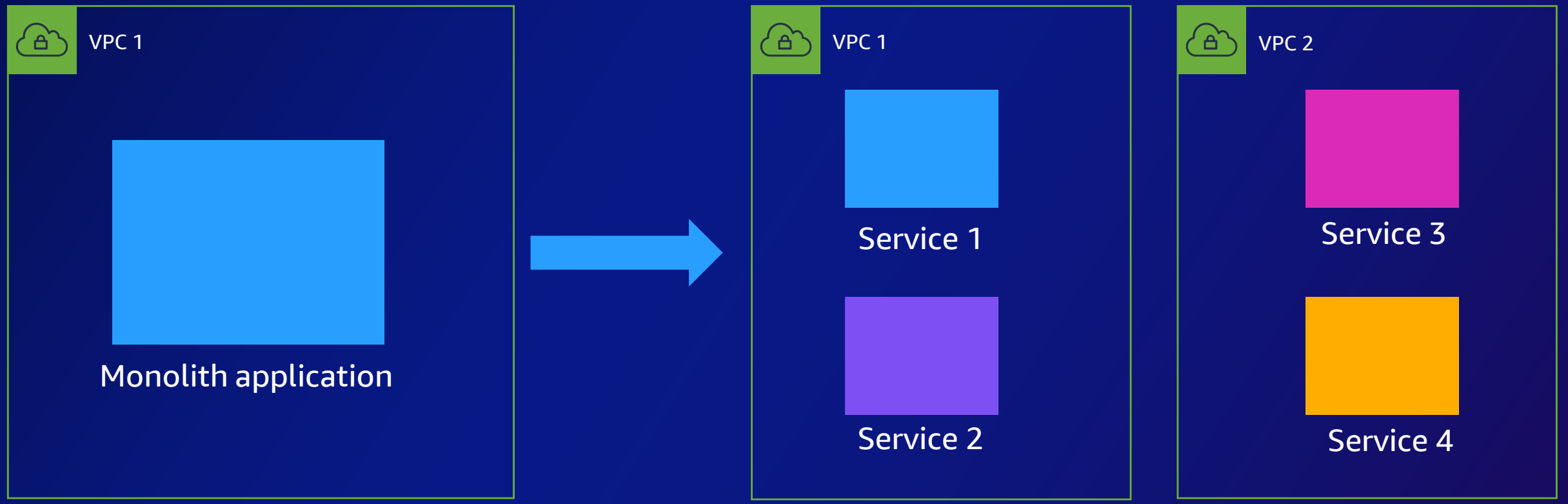
Simplify service-to-service connectivity, security, and monitoring

AWS Verified Access

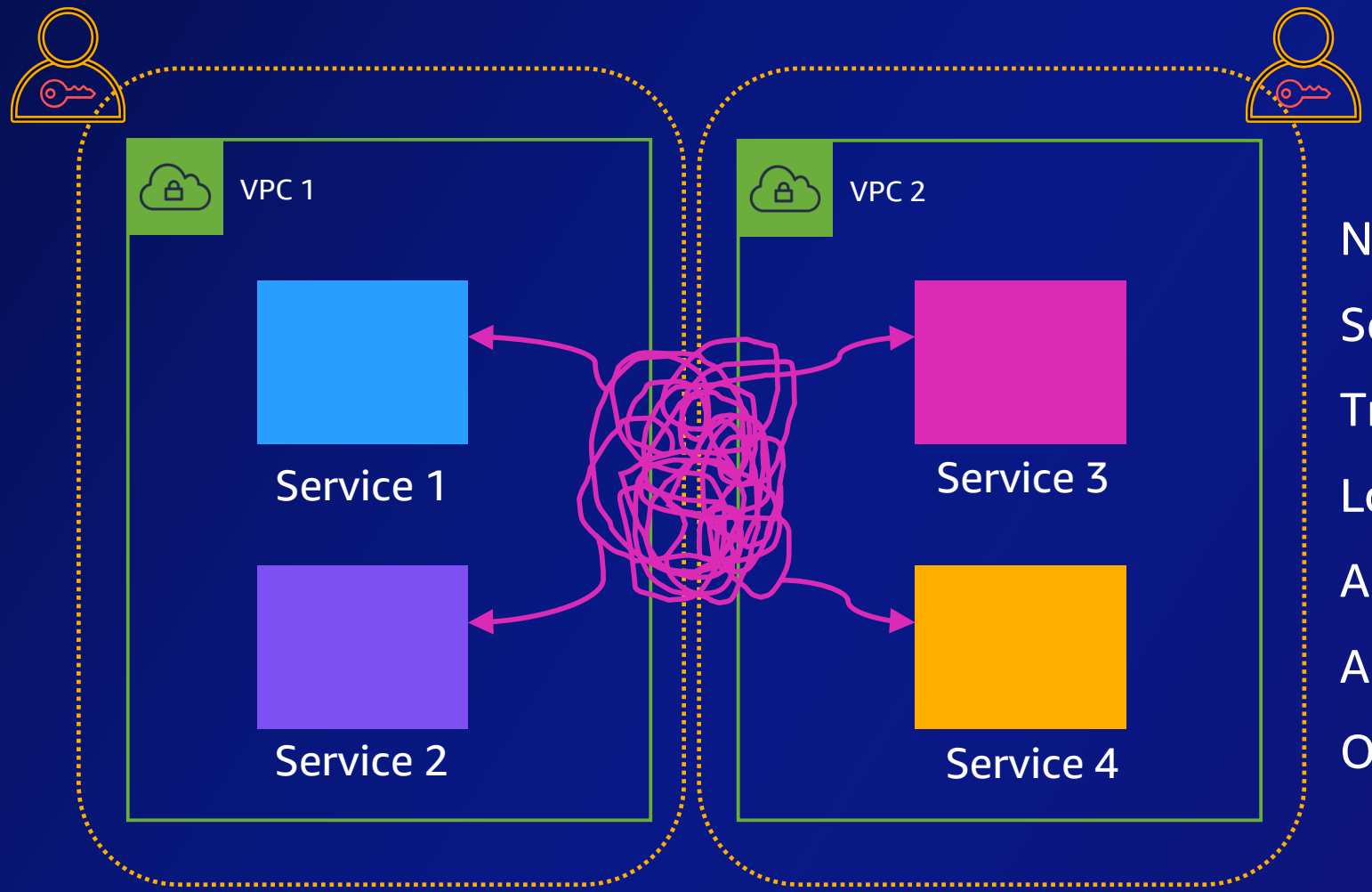
Provide secure access to corporate applications without a VPN

Amazon VPC Lattice

The journey from monolith to microservices



How do you handle . . .



Network connectivity?

Service discovery?

Traffic management?

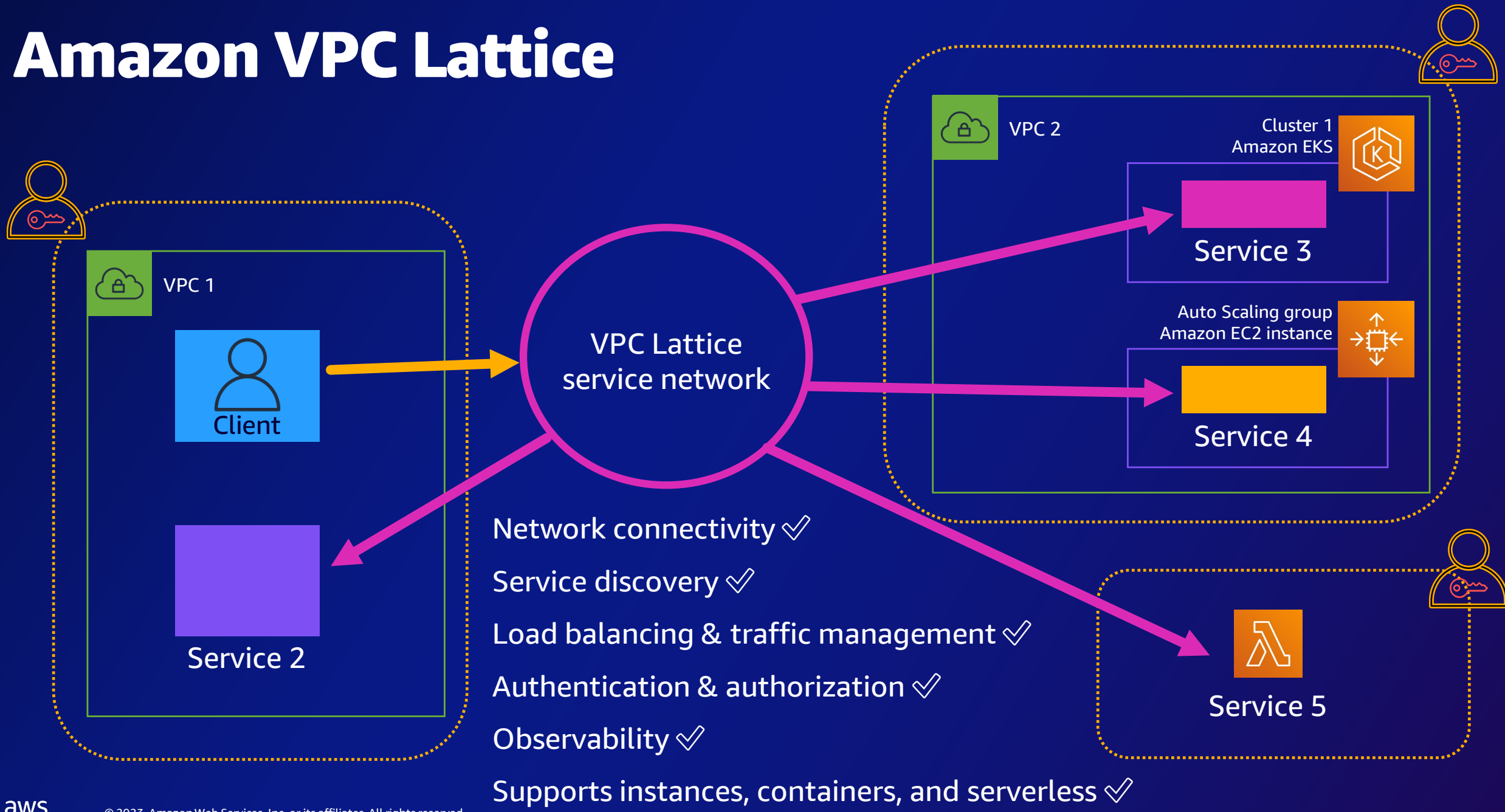
Load balancing?

Authentication?

Authorization?

Observability?

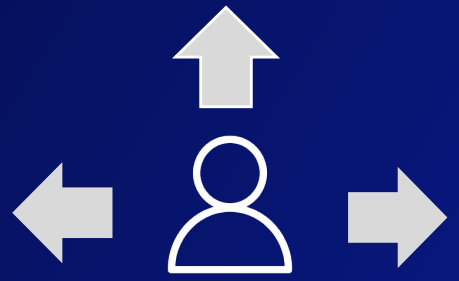
Amazon VPC Lattice



- Network connectivity ✓
- Service discovery ✓
- Load balancing & traffic management ✓
- Authentication & authorization ✓
- Observability ✓
- Supports instances, containers, and serverless ✓

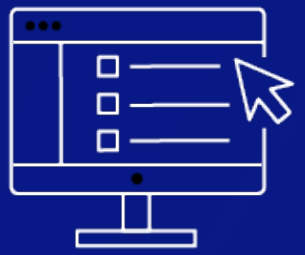
AWS verified access

AWS verified access



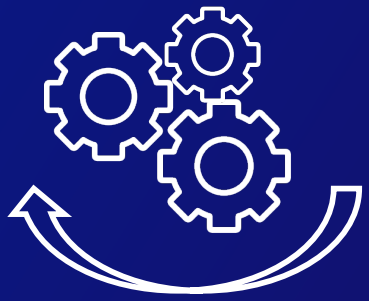
Increase workforce mobility

Users access applications with a web-browser, without any additional agents



Improve security posture

Built using AWS Zero Trust principles, evaluates each user request in real-time using identity and device posture

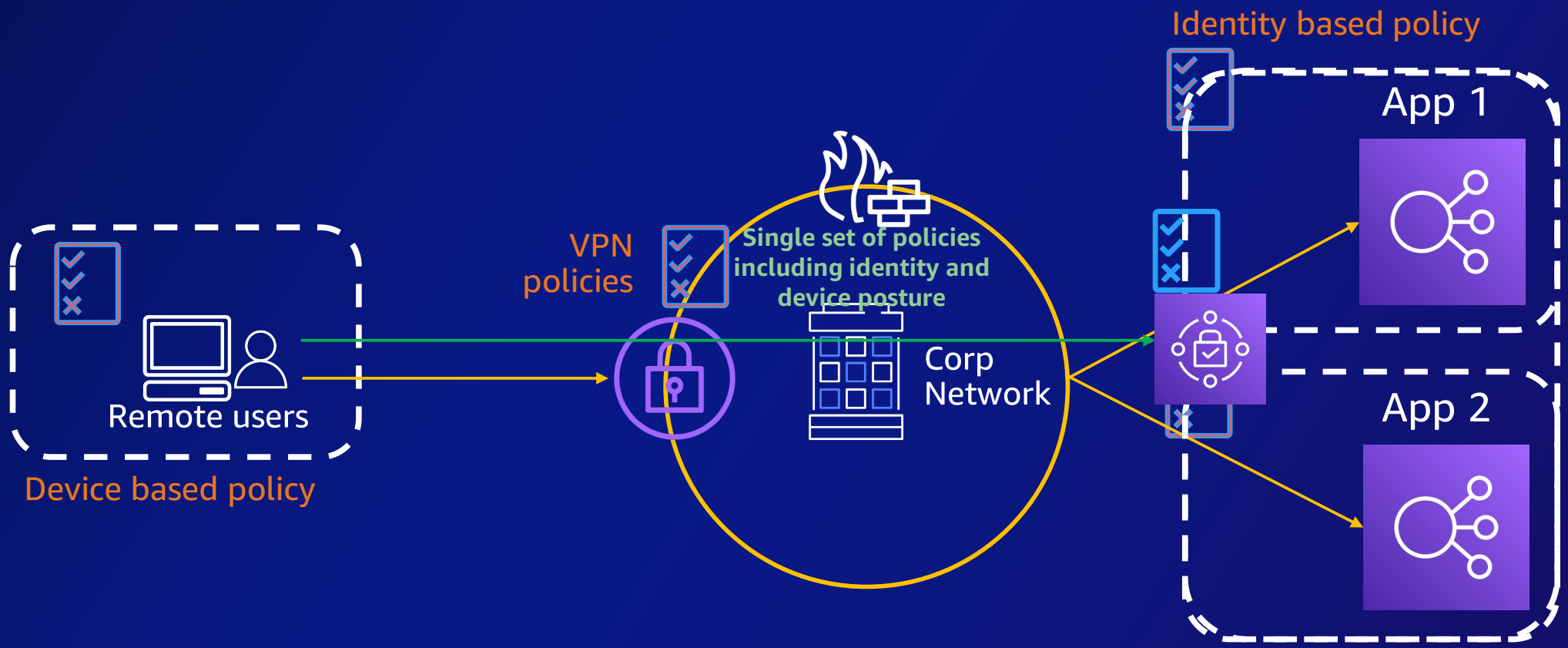


Simplify Security Operation

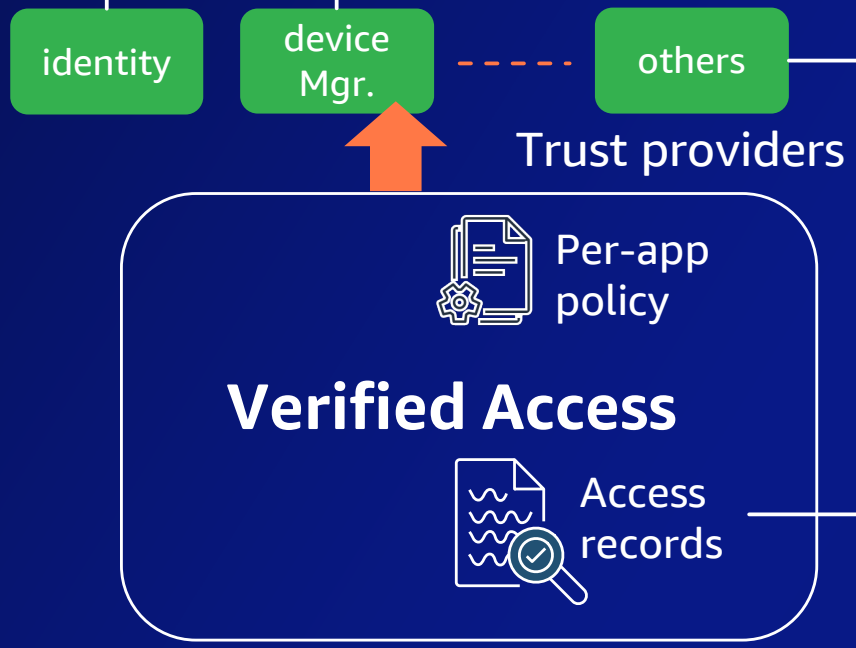
Onboard applications using a few clicks, create and manage all your access using a single set of policies

Work from anywhere with VPN-less secure access

Simplify Zero Trust Implementation



Verified Access – Partners



Trust Providers

IdP partners– provide users identity

Device security partners– provide device context

Contextual data partners – provide behavioral analytics & geolocation, and many more

SIEM/Observability Providers

Analyze Risk & Generate insights

Managed Connectivity providers

Build a managed Connectivity solution

Summary

- Security of the cloud
- AWS global connectivity and its need
- Different levels of physical encryption
- Additional services to perimeter protection domain – Amazon Lattice, AWS verified access

Thank you!

Please complete the session survey

Vikas Sood
Head of Security Assurance
AWS India

Avanish Yadav
Sr. Networking Specialist SA
AWS India