
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SEC405

Zero Trust: Enough talk, let's build better security

Quint Van Deman

Principal, Office of the CISO
Amazon Web Services

Pritesh Parekh

VP of Engineering and
Chief Trust & Security Officer
Delphix, Inc.

Jeff Dutra

Director of Engineering
Delphix, Inc.

Our next 60 minutes together

A (quick) grounding in Zero Trust fundamentals

Examples of Zero Trust within AWS

Building Zero Trust on AWS

Customer success: Delphix, Inc.

Additional real world examples

The fundamental underlying question

"What are the optimal patterns to ensure the right levels of security and availability for my systems and data?"

Zero Trust Defined

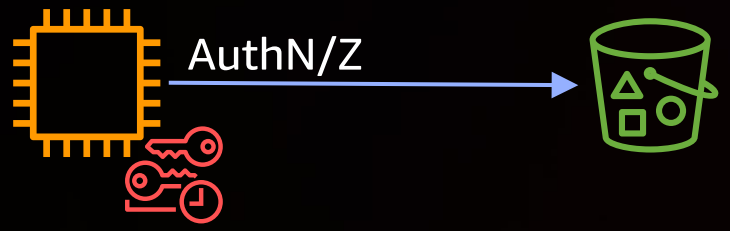
A conceptual security model and associated set of mechanisms that focus on providing security controls around digital assets that do not solely or fundamentally depend on traditional network controls or network perimeters

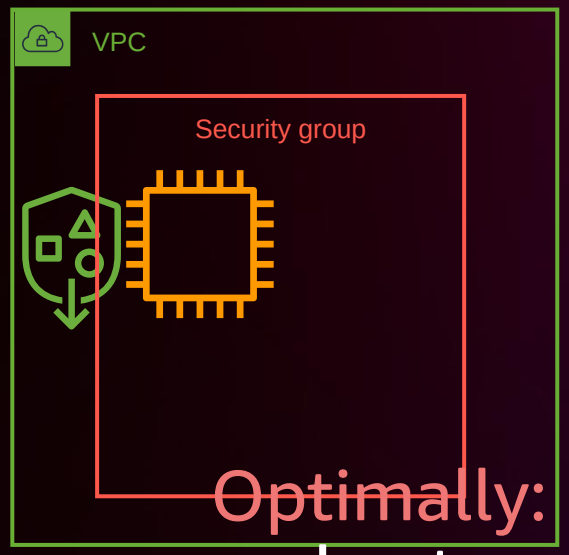
Guiding principles for Zero Trust

Avoid a binary choice

GUIDING PRINCIPLE #1

Identity-centric AND Network-centric

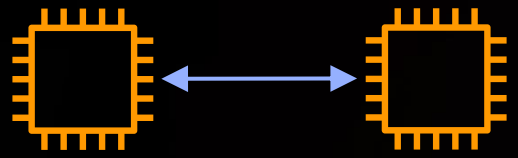




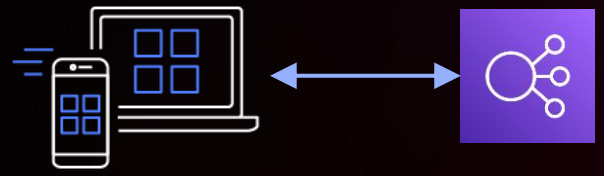
~~Optimally:~~ Identity-centric and network-centric controls aware of each other

Focus on use cases

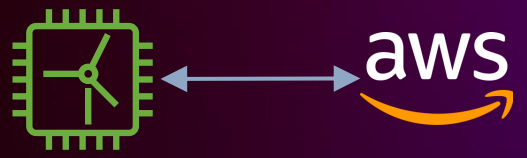
GUIDING PRINCIPLE #2



Machine-to-machine



Human-to-application



Digital transformation

Same: Technical principles

Different: Organizational objectives

Focus: Problems we're trying to solve

Avoid: Getting mired in low value discussions

One size doesn’t fit all

GUIDING PRINCIPLE #3

Do: Apply in accordance with the value of the systems being protected

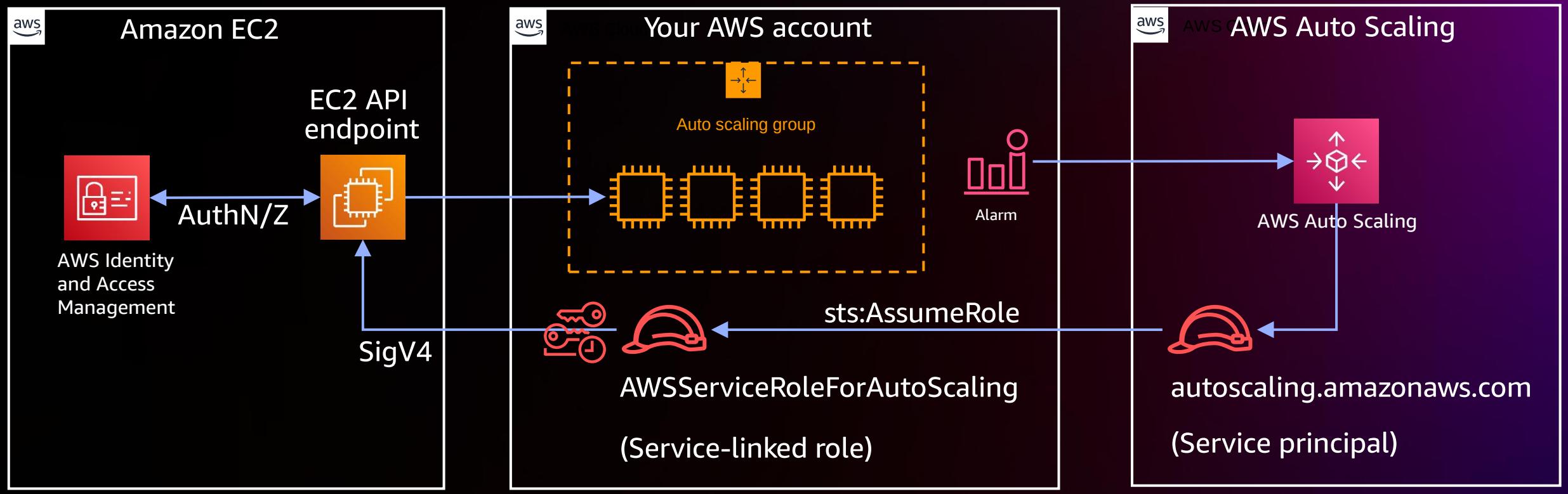
Don’t: Issue inflexible mandates

Examples of Zero Trust within AWS

Interacting with AWS APIs

Use case 0 for Zero Trust?

AWS Services interacting with each other

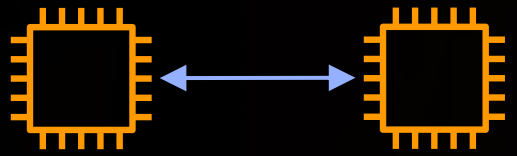


Exact same identity-centric mechanism you use

How AWS can help you on your Zero Trust journey on AWS

Authorizing specific flows between components

USE CASE #1



Machine-to-machine

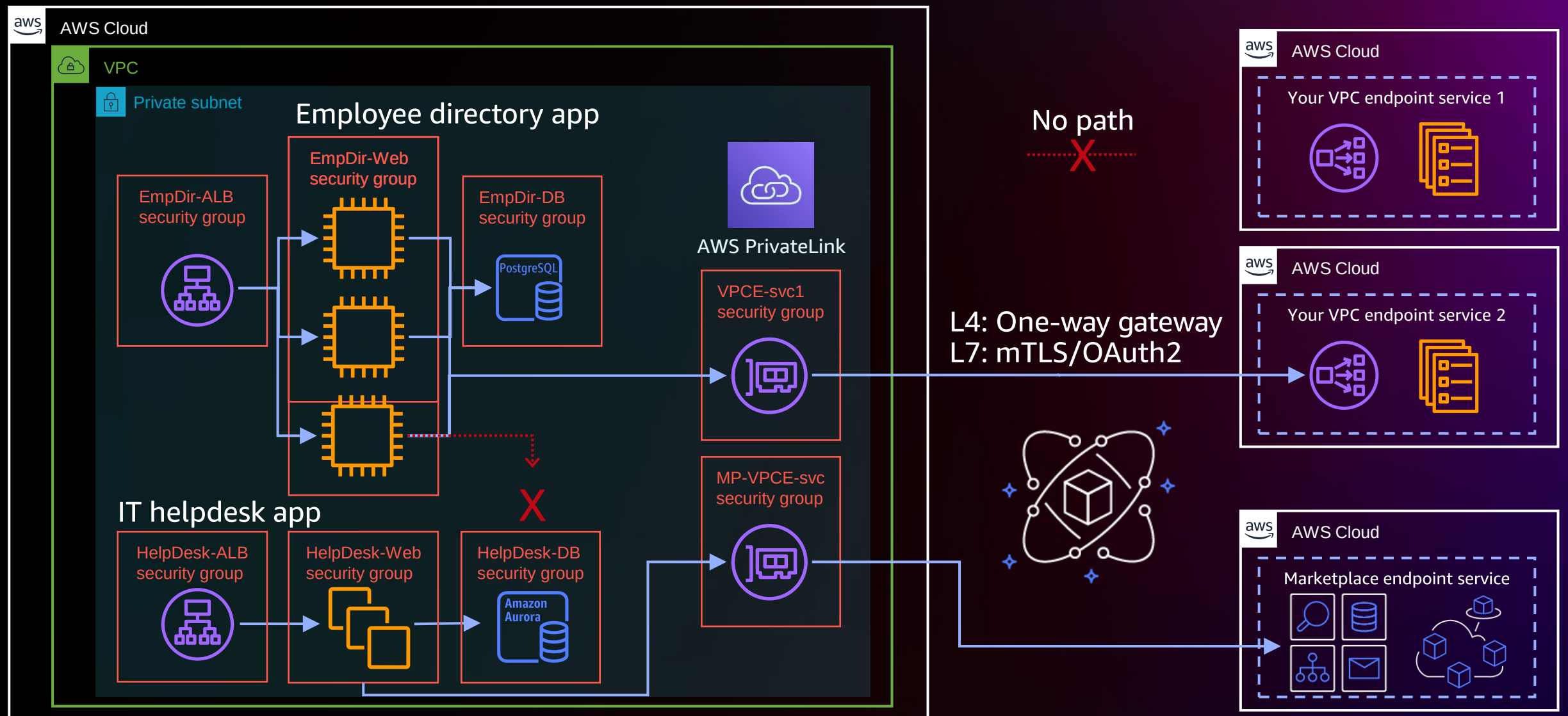
Goal: Eliminate unneeded lateral network mobility

Reduce surface area of systems

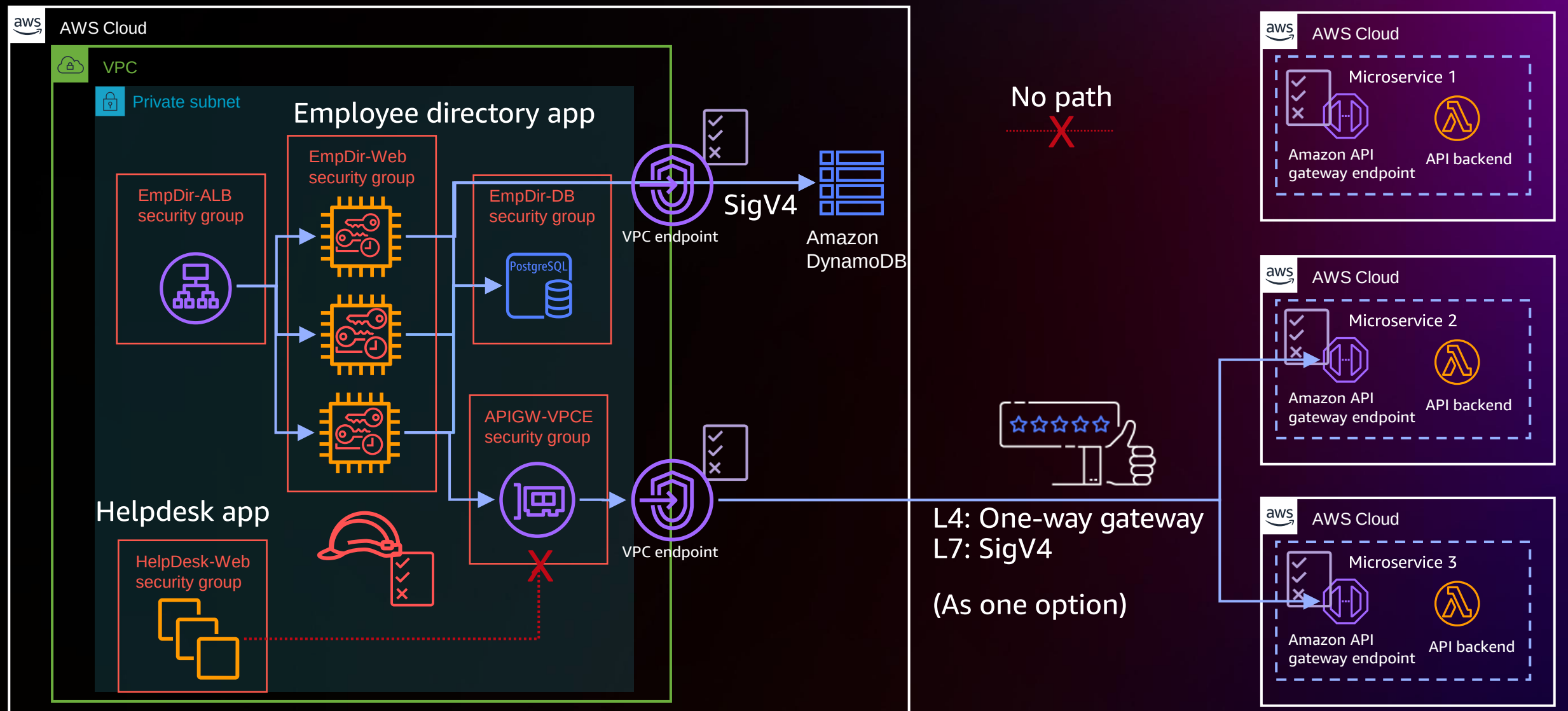
Eliminate unnecessary pathways to data

Consideration: Patterns follow architectures

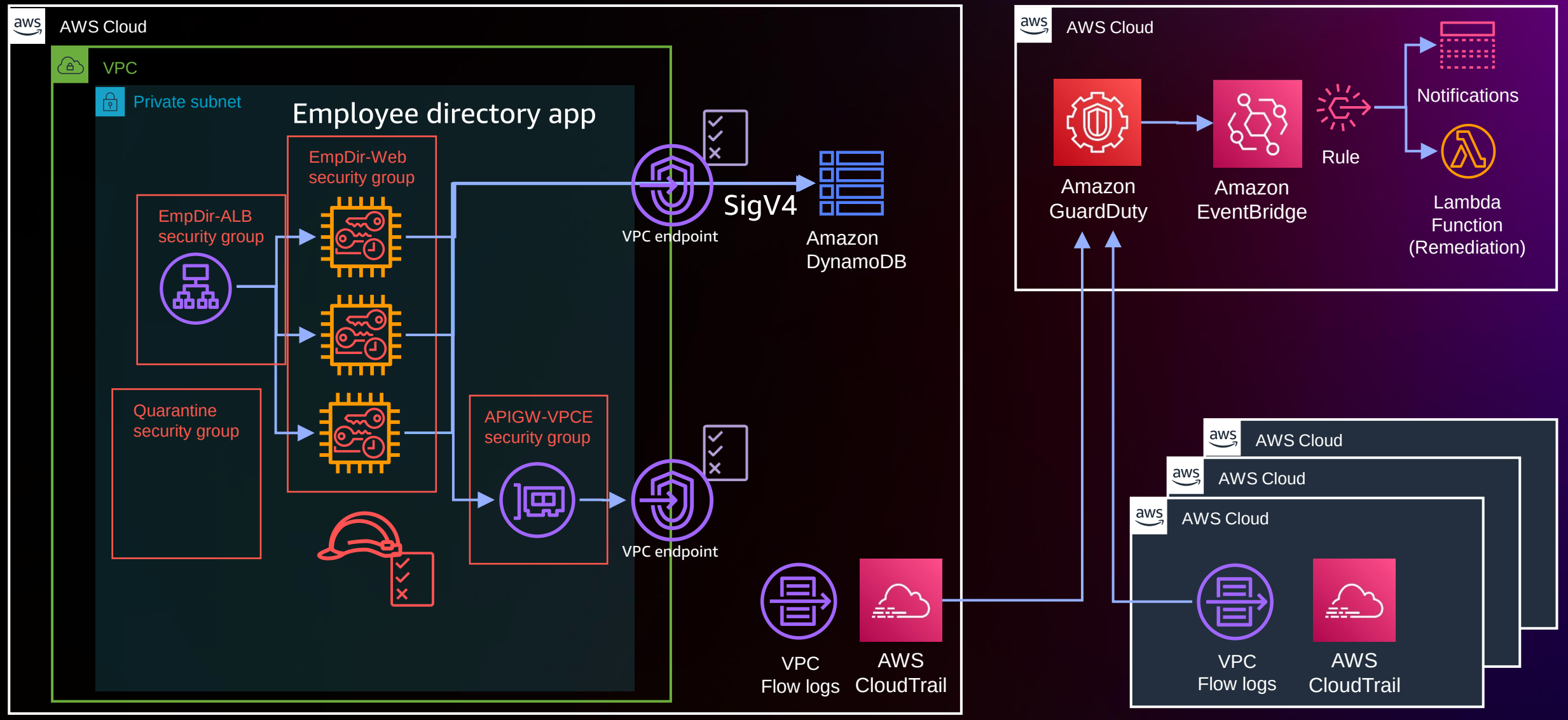
Authorizing specific flows between components



Authorizing specific flows between components



Detective controls for anomalous behavior



Customer Success: Delphix, Inc.

Pritesh Parekh

VP of Engineering and
Chief Trust & Security Officer
Delphix, Inc.

Jeff Dutra

Director of Engineering
Delphix, Inc.

Who is Delphix?

- Delphix was founded in 2008, based in Redwood City, California
- Over 400+ global enterprises use Delphix
- 600+ employees across 5 offices around the world
  60+ employees in EMEA
  100+ employees in India
  (Regions NA, EMEA , LATAM, and APJ)
- 25% of the Fortune 100 use Delphix

Transforming Application Delivery

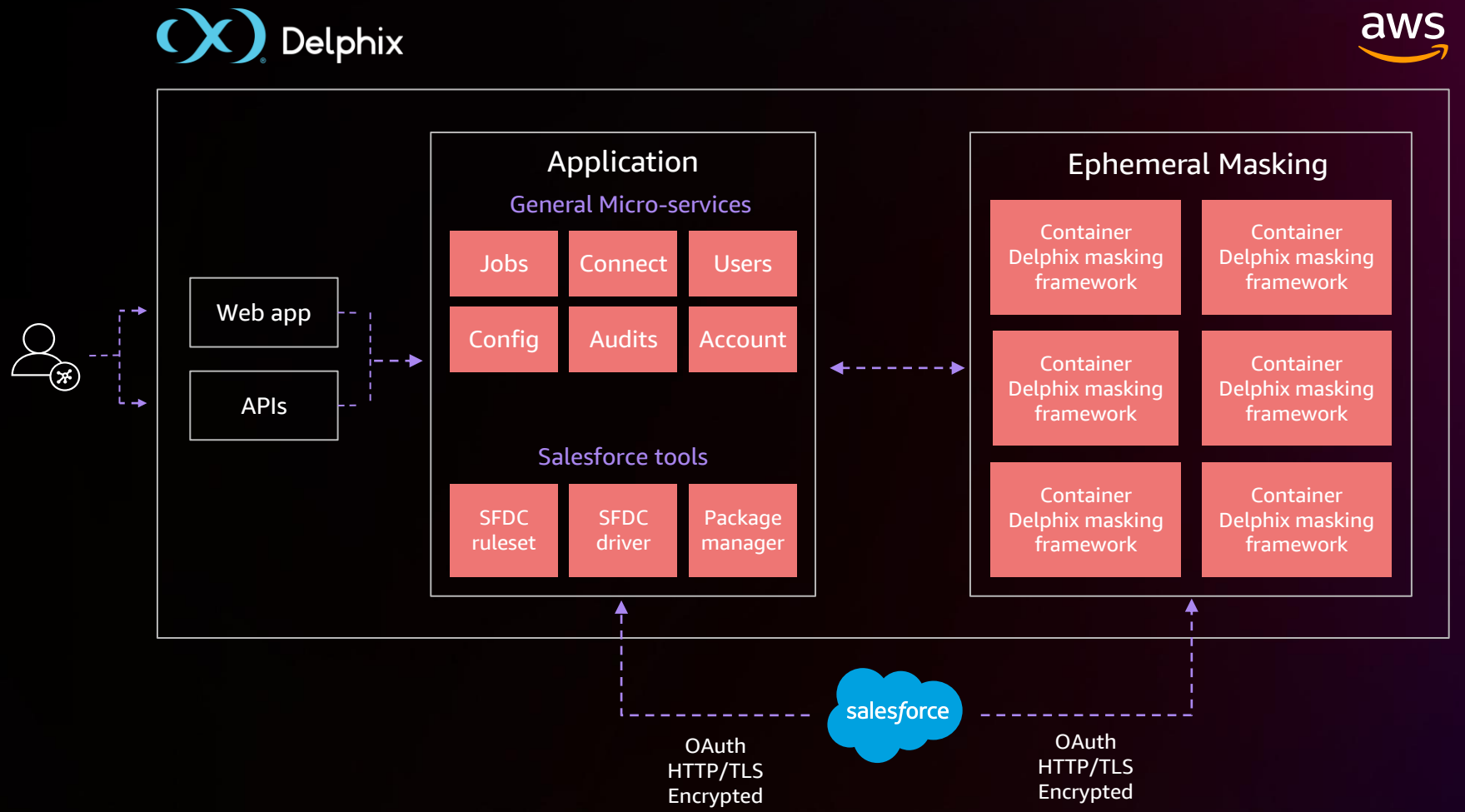
By Enabling DevOps Test Data Management

Our DevOps Data Platform transforms application delivery across the multi-cloud, while protecting data privacy and security

- 10X Faster Application Releases
- 20% Faster Cloud Adoption
- 100% Test Data Compliance

High-level Architecture

DELPHIX AS A SERVICE (DAAS)



Delphix: Zero Trust

Zero Trust is a security discipline that treats every component, service, and user of a system as continuously exposed to security risks and therefore doesn’t make assumptions about their integrity

Delphix: Principles of Zero Trust

Do security fundamentals well

- Layered defense to protect network, system, application and data
- Apply rules of least privilege
- Strong separation of concerns with enforced compartmentalization

Delphix: Principles of Zero Trust

Authenticate and authorize every interaction

- Design choice to validate the user identity and tenant identity with every interaction among every microservice
- User to service interactions authorized using OAuth
- Service to service interactions authenticated using IAM roles and tenant identity via API Gateway (custom authorizer)

Delphix: Principles of Zero Trust

Simplify the security stack

- Fully leverage CSP built-in capabilities
- Proactive enforcement of security controls
- 360 view of the security posture

Zero Trust Outcomes

- Strong foundation for the Security program
- Driving culture of security within the organization
- Building strong trust with customers
- Security compliance as an outcome
- Low friction in the Sales cycle

Delphix Architecture - Our Zero Trust Components

- Cloud Native Architecture
- Serverless and as a Service first design

Network Components

Amazon Virtual Private Cloud (Amazon VPC)

VPC Endpoints

TLS Encryption

Identity Components

AWS Identity and Access Management (IAM)

Amazon Cognito

Delphix Custom Authorizer

Cloud Native Components

Amazon API Gateway

AWS Key Management Service (AWS KMS)

AWS Systems Manager Parameter Store

AWS Lambda

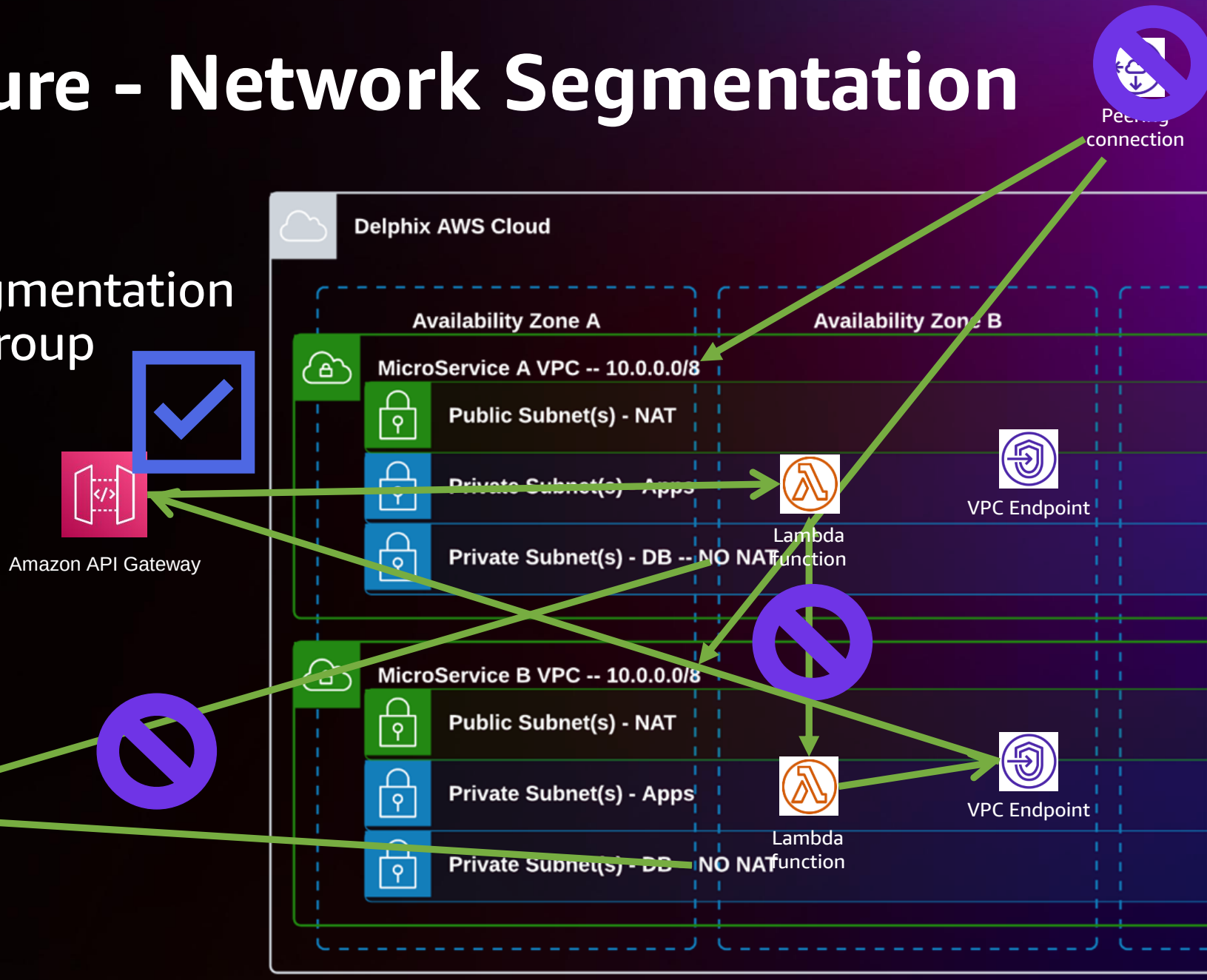
AWS Secrets Manager

AWS Batch

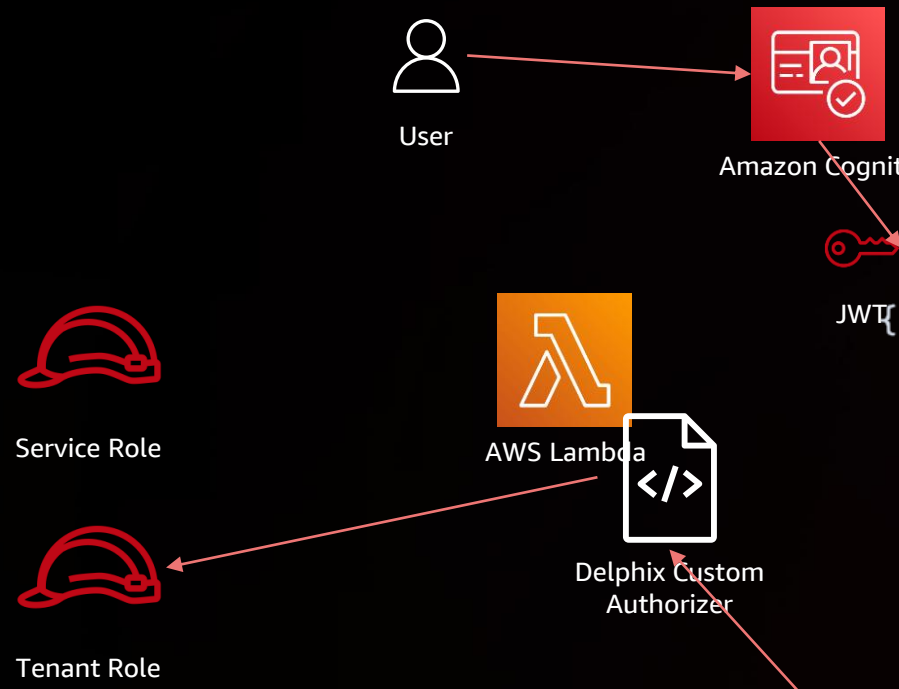
AWS Certificate Manager (ACM)

Delphix Architecture - Network Segmentation

- Service level network segmentation
- Least privilege security group configurations

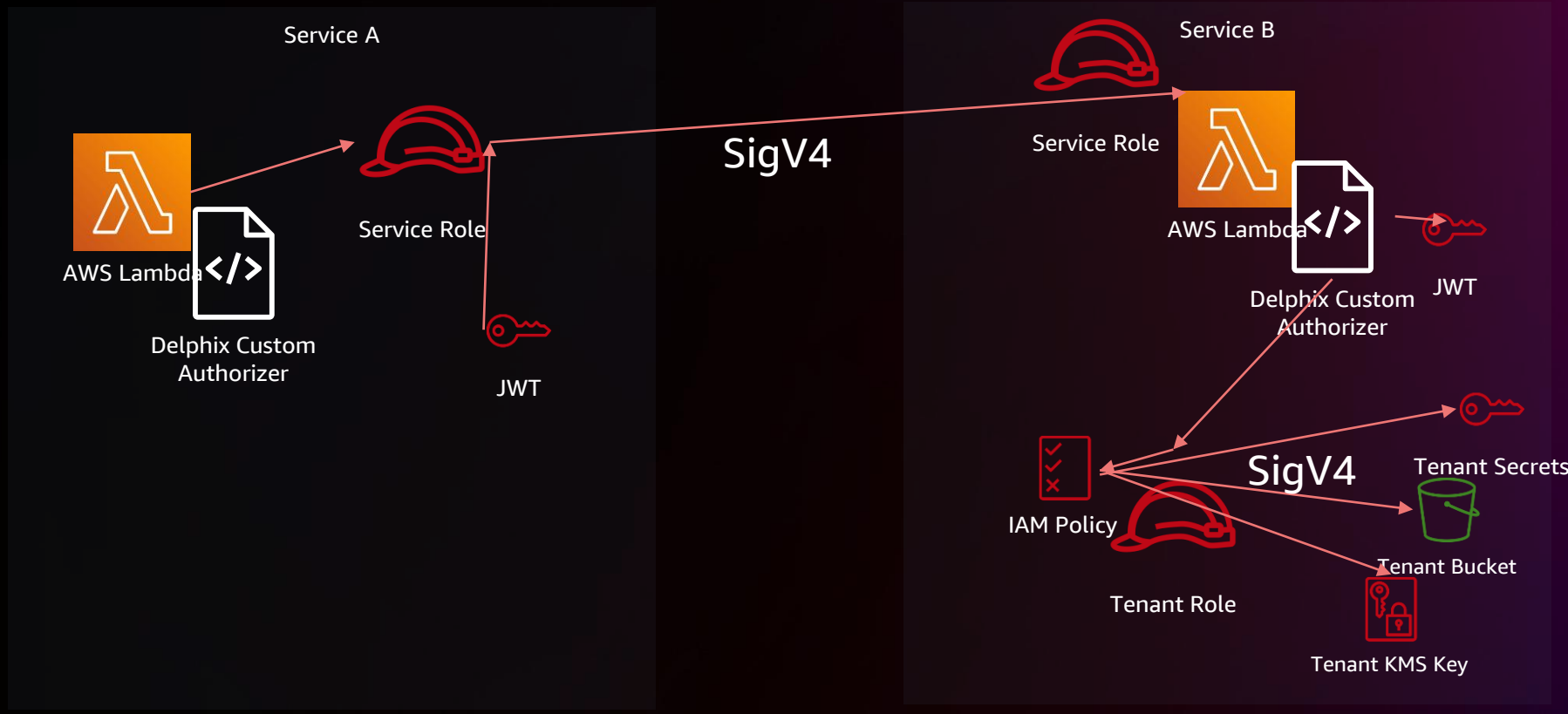


Zero Trust Identity for Tenants

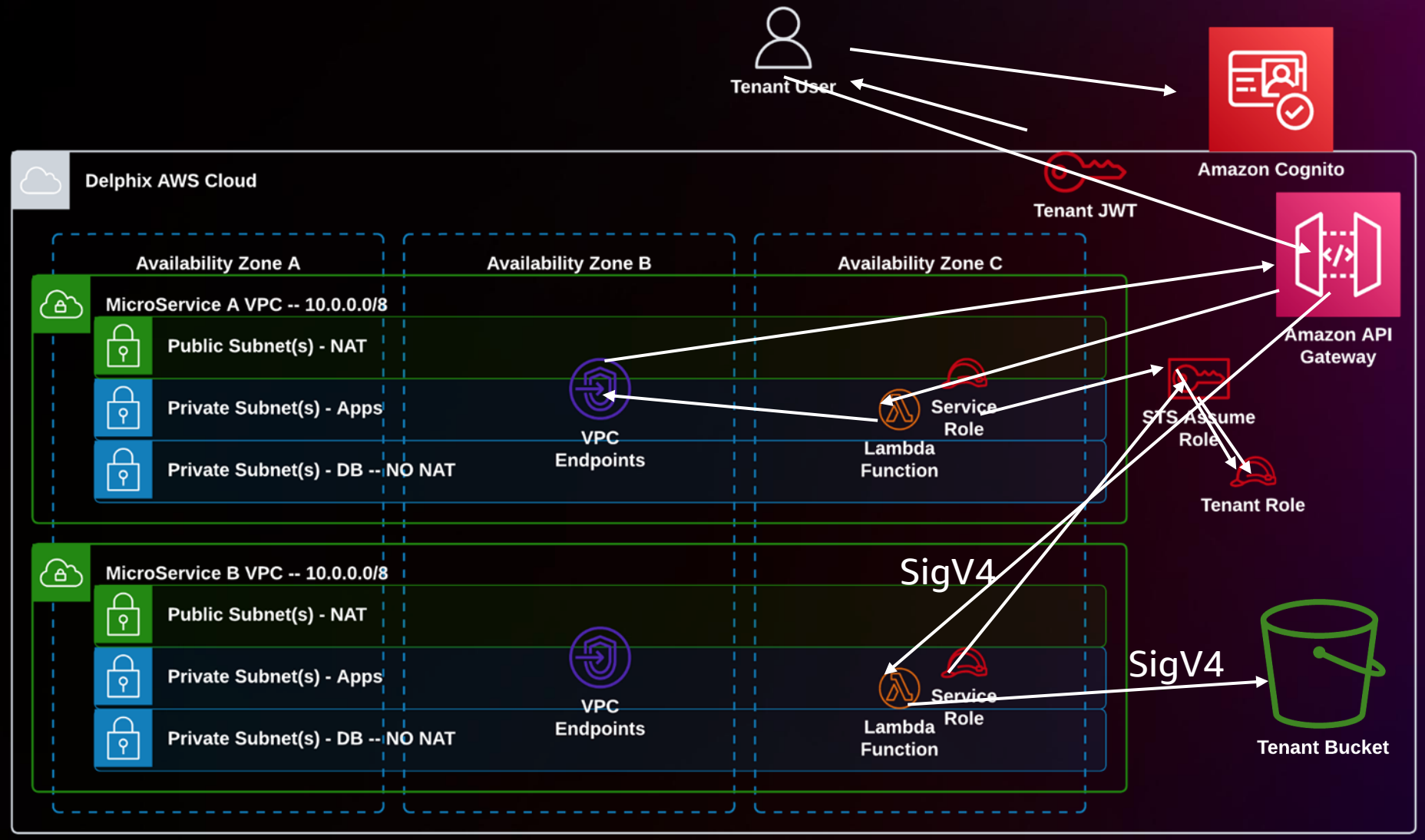



```
{
    "sub": "00000000-0000-0000-0000-000000000000",
    "iss": "https://cognito-idp.us-west-2.amazonaws.com/us-west-2_000000000",
    "cognito:username": "00000000-0000-0000-0000-000000000000",
    "custom:trial_end_date": "0000-00-00 00:00:00.000000",
    "origin_jti": "00000000-0000-0000-0000-000000000000",
    "aud": "00000000000000000000",
    "custom:organization_uuid": "00000000-0000-0000-0000-000000000000",
    "custom:account_type": "FULL",
    "event_id": "00000000-0000-0000-0000-000000000000",
    "token_use": "id",
    "auth_time": 0000000000,
    "exp": 0000000000,
    "custom:user_type": "ORGANIZATION_ADMIN",
    "iat": 0000000000,
    "custom:user_uuid": "00000000-0000-0000-0000-000000000000",
    "jti": "00000000-0000-0000-0000-000000000000",
    "email": "myemail@mydomain.com",
    "custom:tenant_uuid": "00000000-0000-0000-0000-000000000000"
}
```

Zero Trust Identity for Services



Delphix Architecture - Service Auth Flow



Delphix Architecture - Considerations

- CICD
- Account quota limits

Delphix Architecture - Cloud Native Benefits

- Serverless allows for very **granular segmentation** both in Network and Identity
- Serverless and cloud-native services mean **we don’t need to do some common maintenance tasks** like system patching
- Cognito Handles Authentication natively for us
- KMS for encryption and ACM for Certificates
- Native AWS services offer **direct integration with all other zero trust components** for ease of implementation

</Delphix>

What if instead of eliminating unnecessary paths through the network…

NEW

We could stop worrying about the network entirely…

Amazon VPC Lattice

NEW

Amazon VPC Lattice

Simplify connecting, monitoring, and securing your application networks

CONNECT SERVICES AT SCALE

Easily connect your services across multiple VPCs and accounts

APPLY GRANULAR ACCESS CONTROLS

Improve security posture and support zero-trust architectures

IMPLEMENT ADVANCED TRAFFIC CONTROLS

Apply rich traffic controls, such as policy-based routing and weighted targets

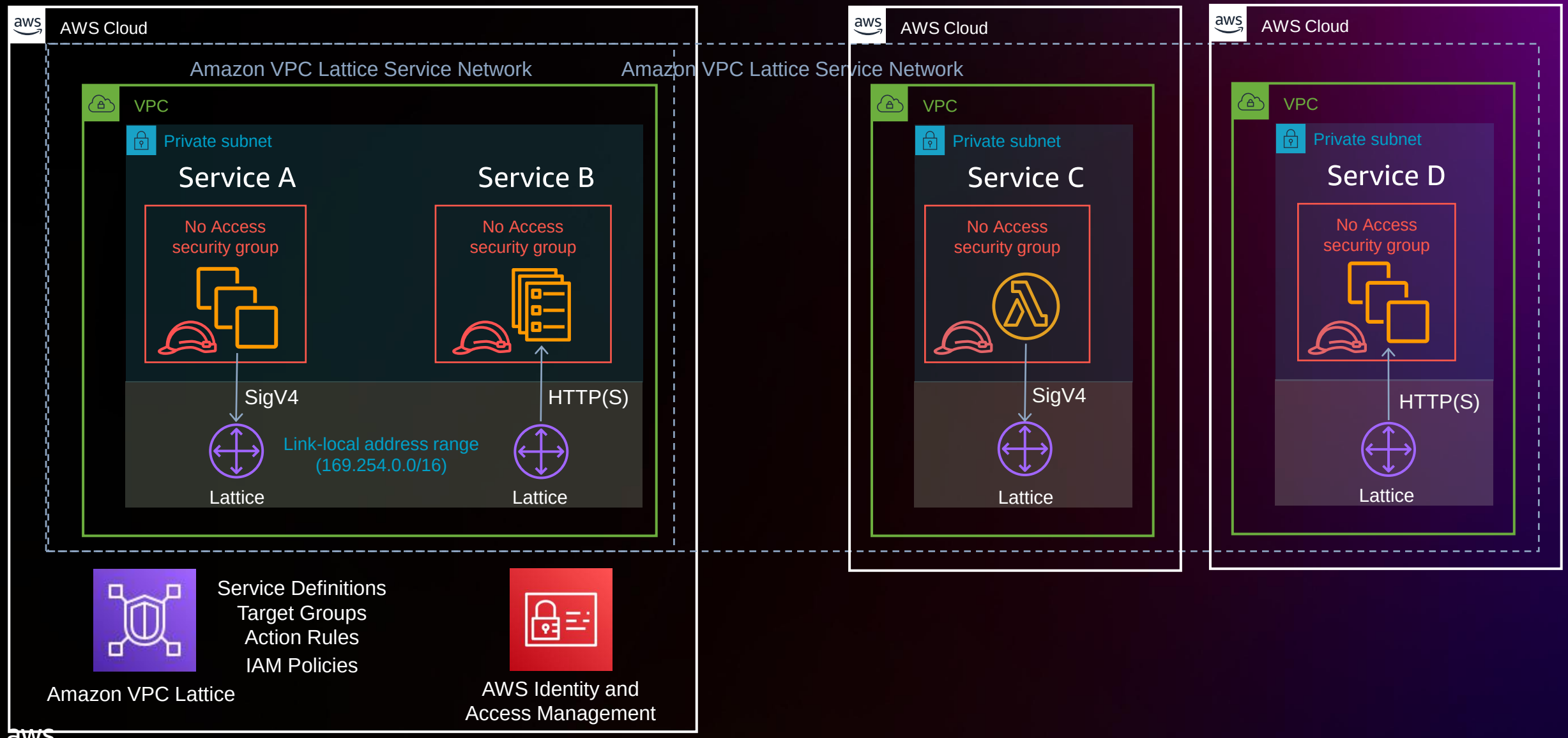
STREAMLINE SERVICE-TO-SERVICE INTERACTIONS

Monitor and troubleshoot communication with detailed access logs and metrics

PREVIEW

aws

Rethinking Service-to-Service communications



Lattice policy example

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":{ "AWS":[ "arn:aws:iam::111111111111:role/serviceA“ ] },
      "Action":"vpc-lattice-svcs:Invoke",
      "Resource":[
        "arn:aws:vpc-lattice-svcs:us-west-2:222222222222:service/svc-xxxxx/jobs"
      ],
      "Condition":{
        "StringEquals": { "vpc-lattice-svcs:Method": "GET“ },
        "StringEquals": { "aws:PrincipalOrgID": "o-xxxxxxxxxxx“ }

      }
    }
  ]
}
```

We’ve welded the computer shut

Learn more

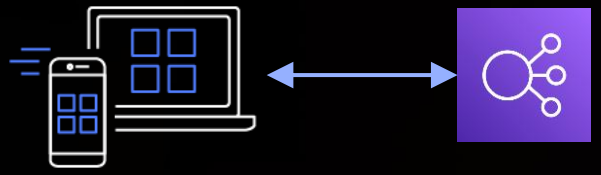
AMAZON VPC LATTICE

Breakout – NET215 – Introducing Amazon VPC Lattice: Simplifying application networking, Friday 12:30-1:30pm

Chalk Talk – NET212 – Application networking best practices, Thursday 3:30-4:30pm

Enabling friction-free access to internal apps

USE CASE #2



Human-to-application

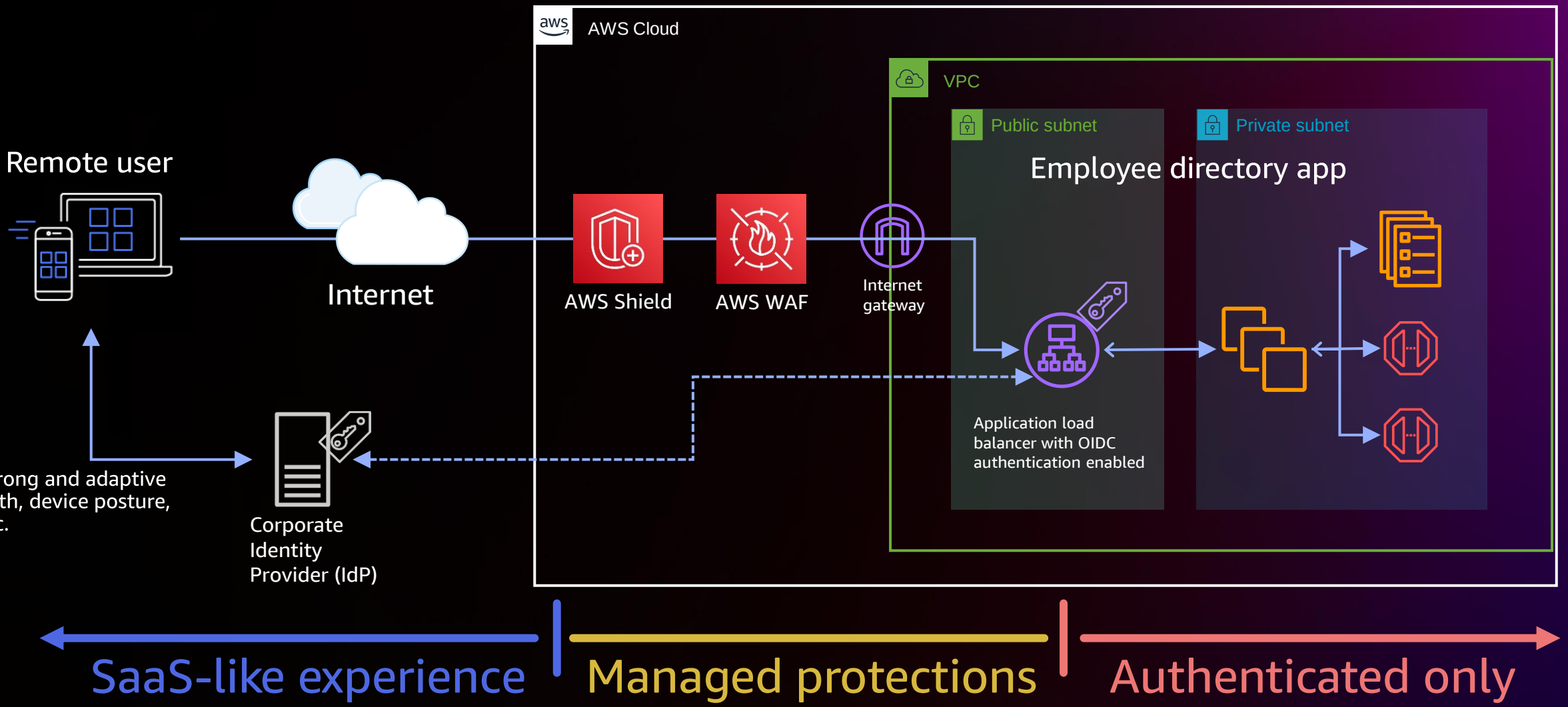
Goal: Improve workforce mobility and experience

Make internal applications available anywhere

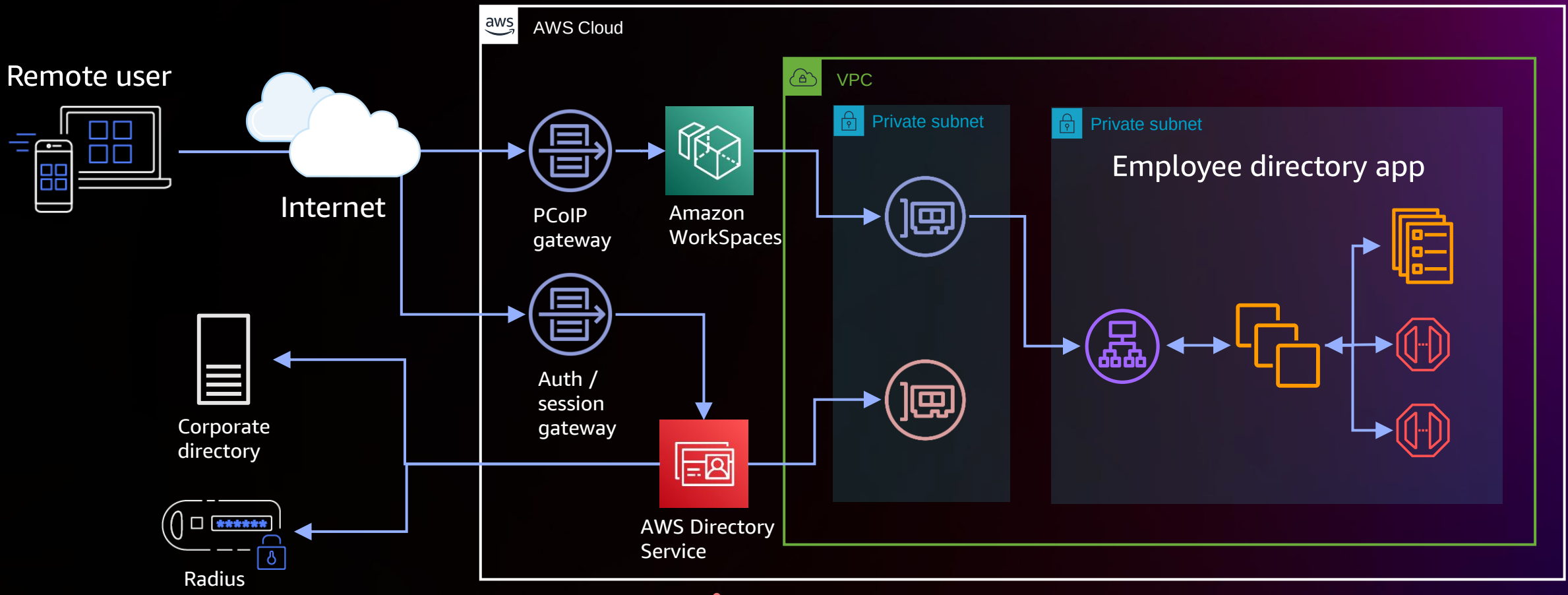
Maintain (or improve) security assurance

Consideration: Not a one-size-fits-all scenario

Enabling friction-free access to internal apps



Enabling friction-free access to internal apps

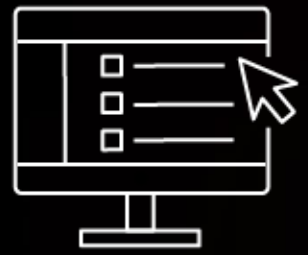


NEW

We knew we could do better:
Less assembly…
Continuous verification…
More context…

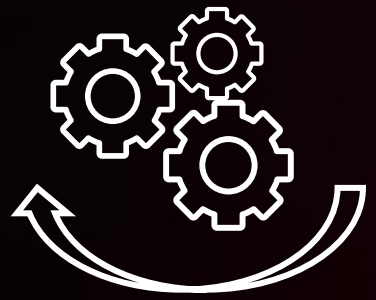
AWS Verified Access

Introducing AWS Verified Access



Improve security posture

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



Simplify security operation

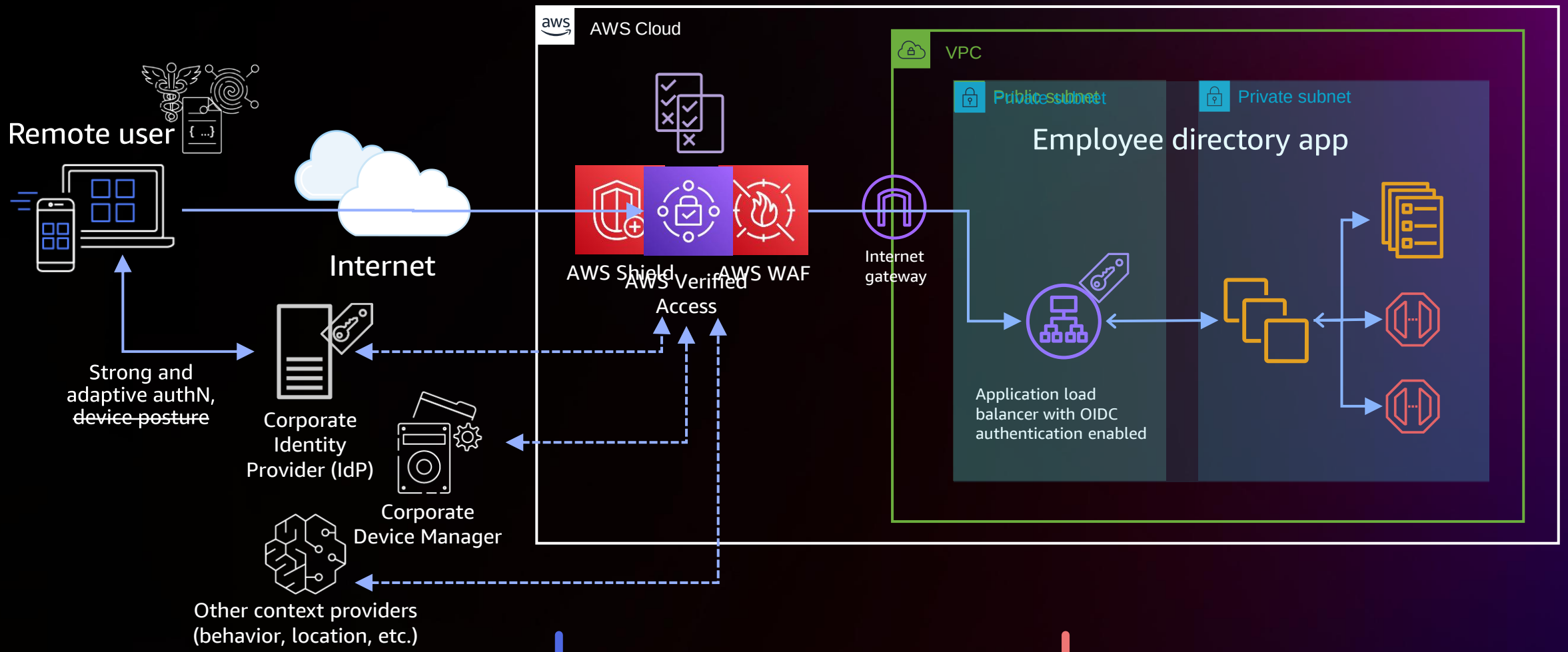
Onboard applications using a few clicks, create and manage all your access using a single set of policies

Increase workforce mobility

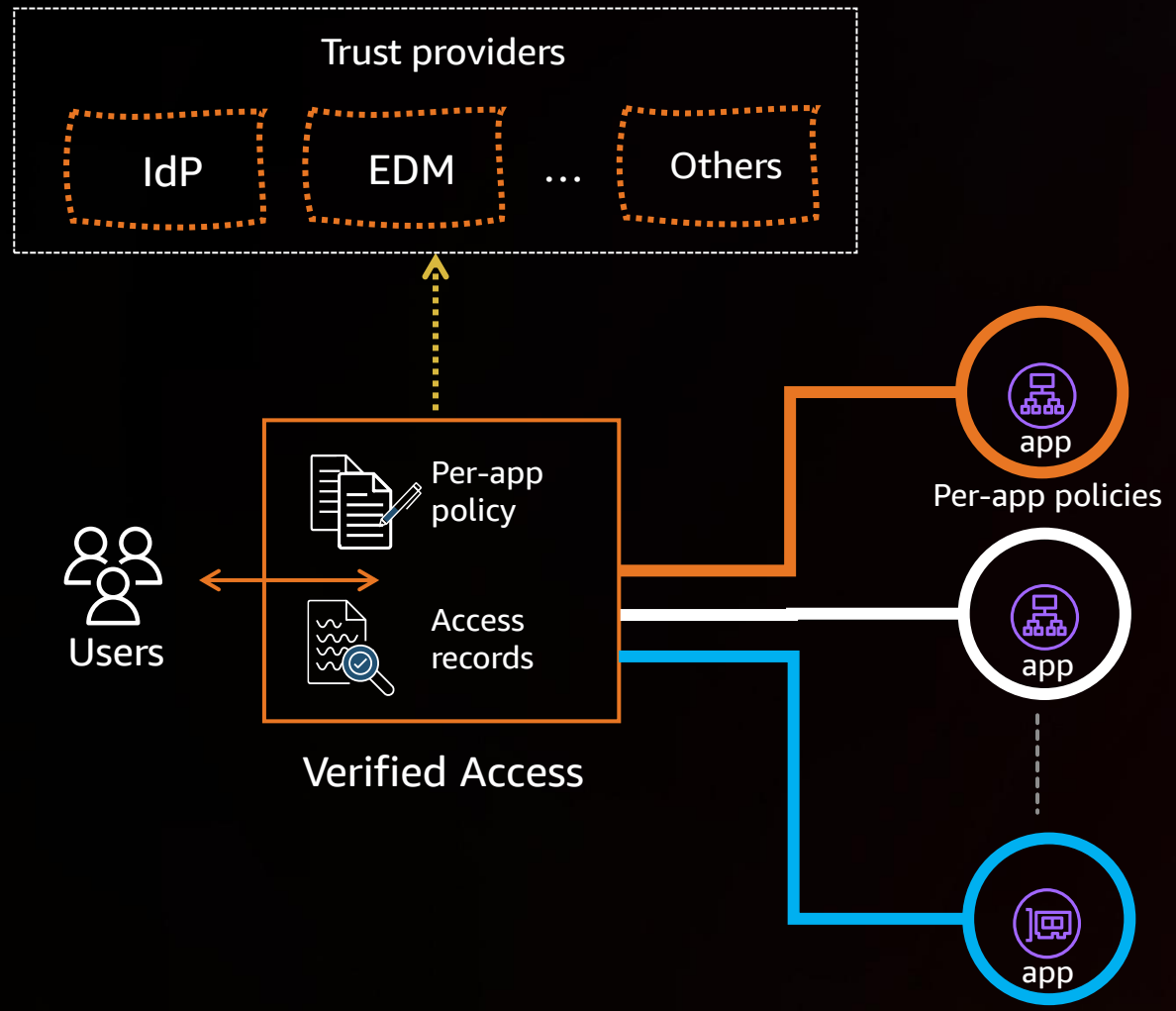
Users access applications with a web browser without any additional agents

Work from anywhere with VPN-less secure remote access

Enabling friction-free access to internal apps



Secure access to corporate applications



- **Fine-grained, dynamic authorization**
  Per-app policy evaluated with every request
- **Improve observability**
  Faster incidence response, auditability, meet compliance
- **Use your existing security services**
  Integrates with popular identity and device trust providers

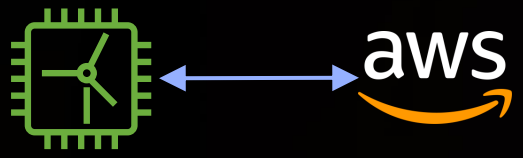
Learn more

AWS VERIFIED ACCESS

Breakout – NET214 – Introducing AWS Verified Access: Secure connections to your applications, Thursday 12:30-1:30pm

Securing digital transformation projects

USE CASE #3



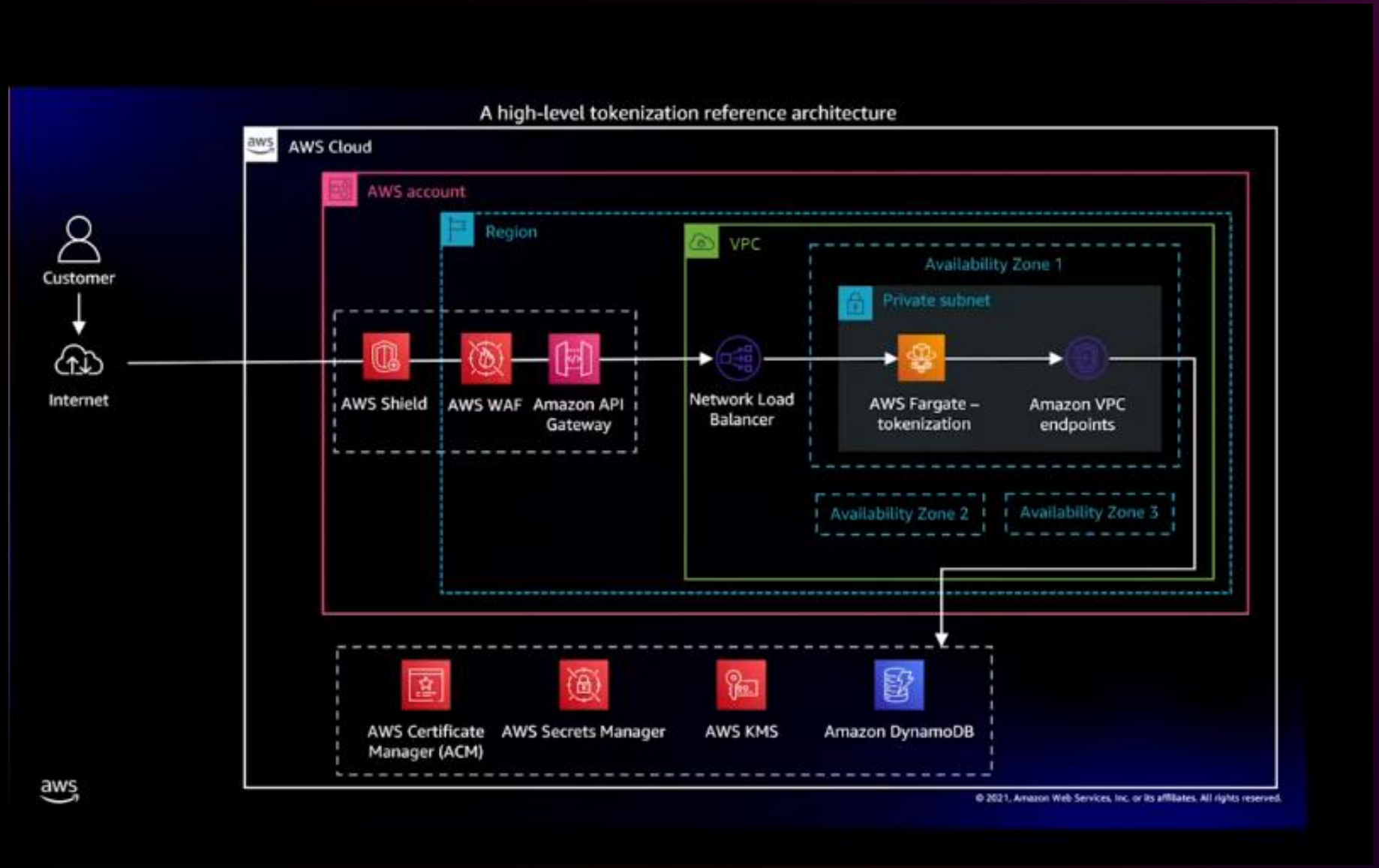
Digital transformation

Goal: Deliver a security model that works when the entire workload often exists outside of the traditional network perimeter

Support essential business and product innovation

Additional real-world examples

Amazon Lumos



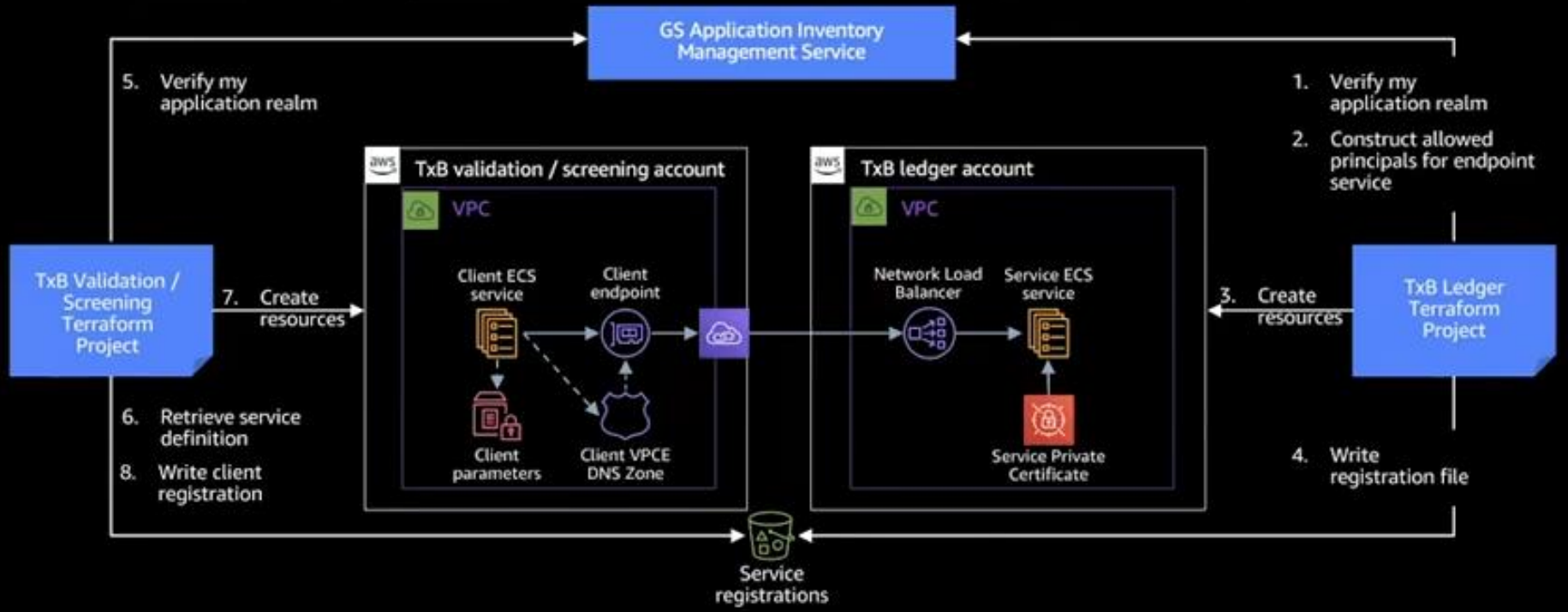
Details here:

Goldman Sachs TxB

VPC endpoint management in TxB

Amazon Simple Storage Service (Amazon S3)–based service registry maps logical service name to AWS service name

Ensures connections only between TxB accounts within same application realm



Details here:

Opportunities to Build

Thank you!

Quint Van Deman
LinkedIn/quint-van-deman/
vandeman@amazon.com

Pritesh Parekh
LinkedIn/priteshp/
pritesh.parekh@delphix.com

Jeff Dutra
LinkedIn/jeffdutra
Jeff.dutra@delphix.com

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