Zero Trust:
An AWS Perspective

Sandip Samanta (He/Him)

Technical Account Manager
AWS India

Sameeksha Garg(She/Her)

Technical Account Manager
AWS India

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

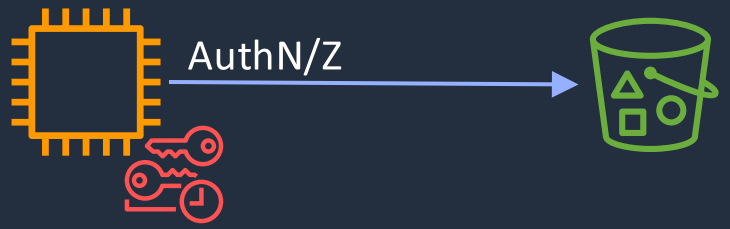
A conceptual security model and associated set of mechanisms that focus on providing security controls around digital assets that do not solely or fundamentally depend on traditional network controls or network perimeters

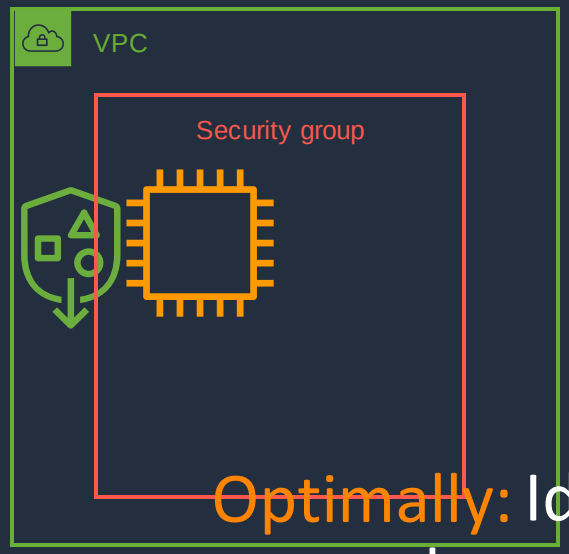
Guiding principles for Zero Trust

Avoid a binary choice

GUIDING PRINCIPLE #1

Identity-centric AND Network-centric

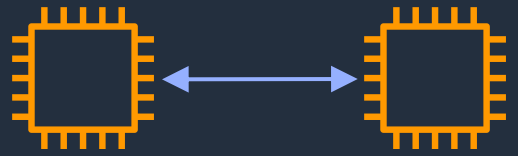




Optimally: Identity-centric and network-centric controls aware of each other

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

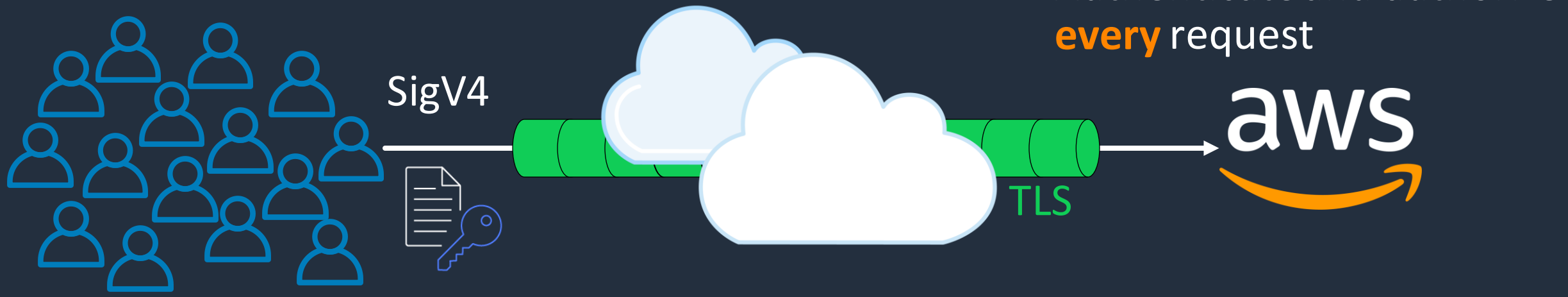
GUIDING PRINCIPLE #3

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

Don’t: Issue inflexible mandates

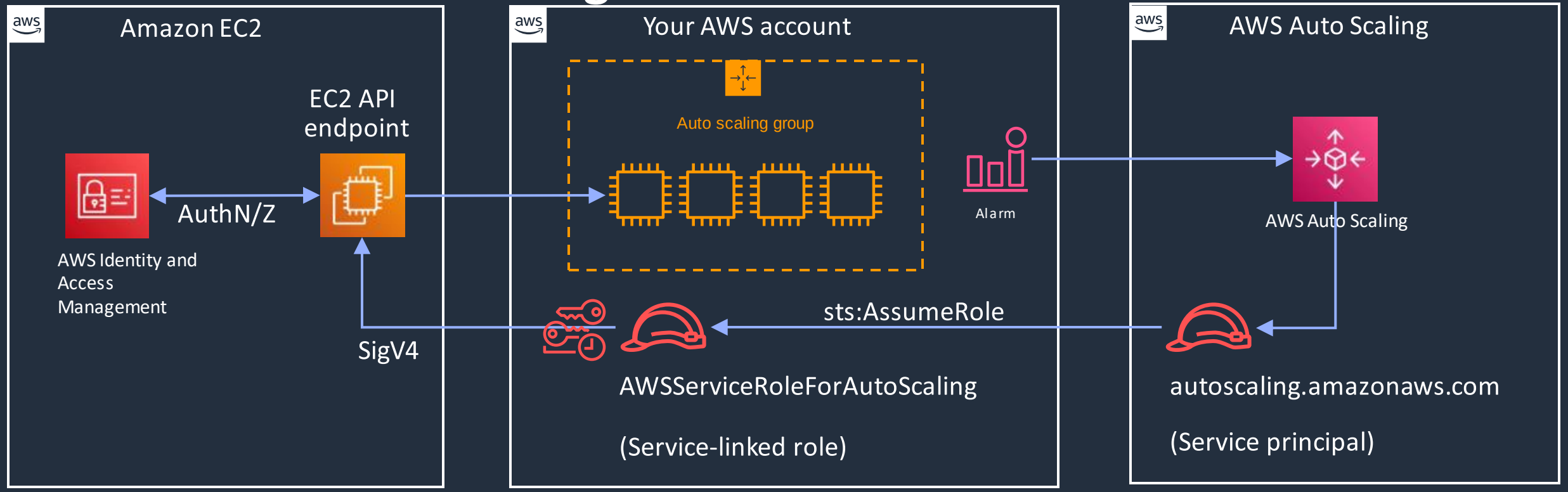
Examples of Zero Trust within AWS

Interacting with AWS APIs



Use case 0 for Zero Trust?

AWS Services interacting with each other

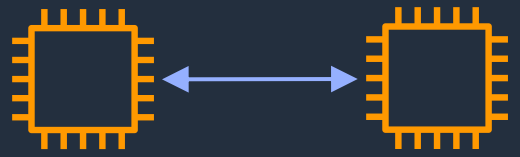


Exact same identity-centric mechanism you use

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

Authorizing specific flows between components

USE CASE #1



Machine-to-machine

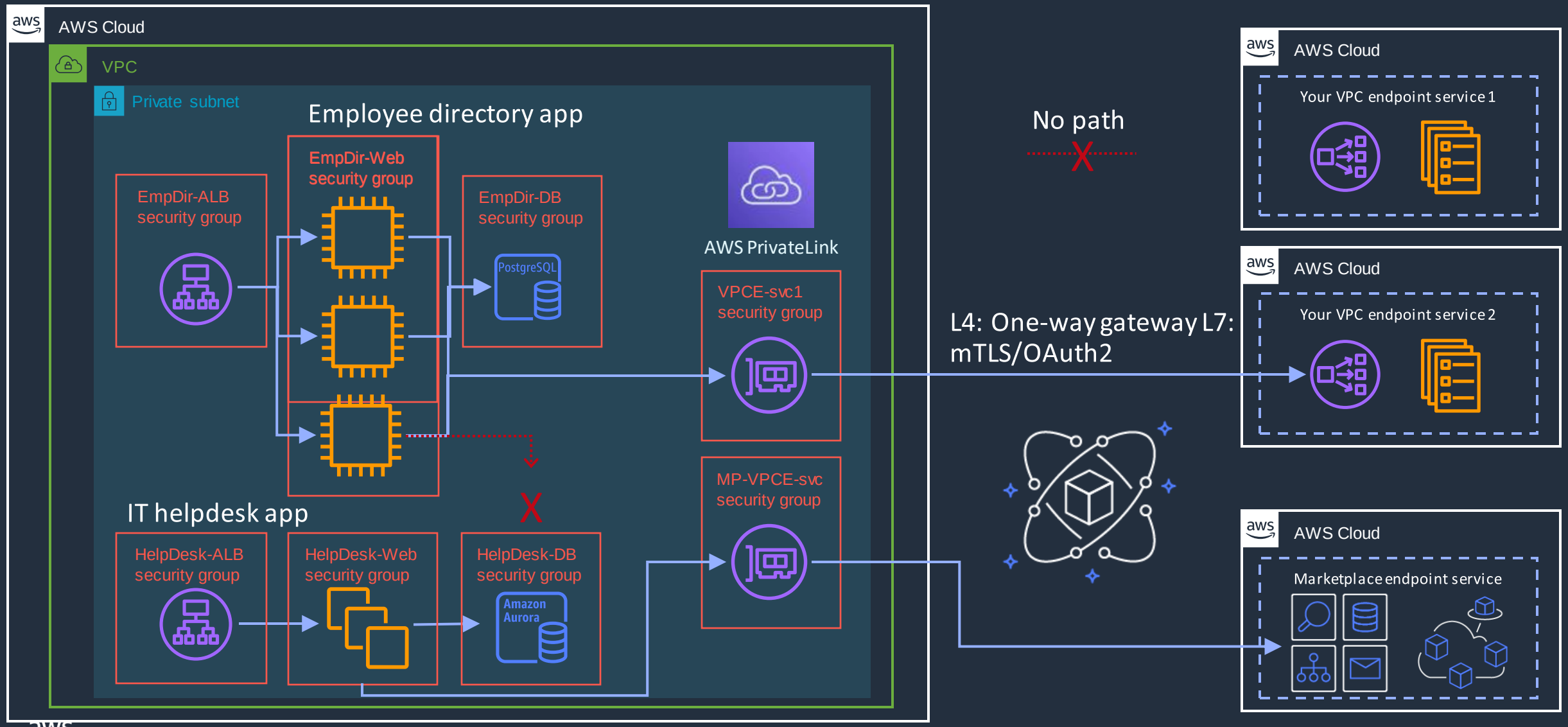
Goal: Eliminate unneeded lateral network mobility

Reduce surface area of systems

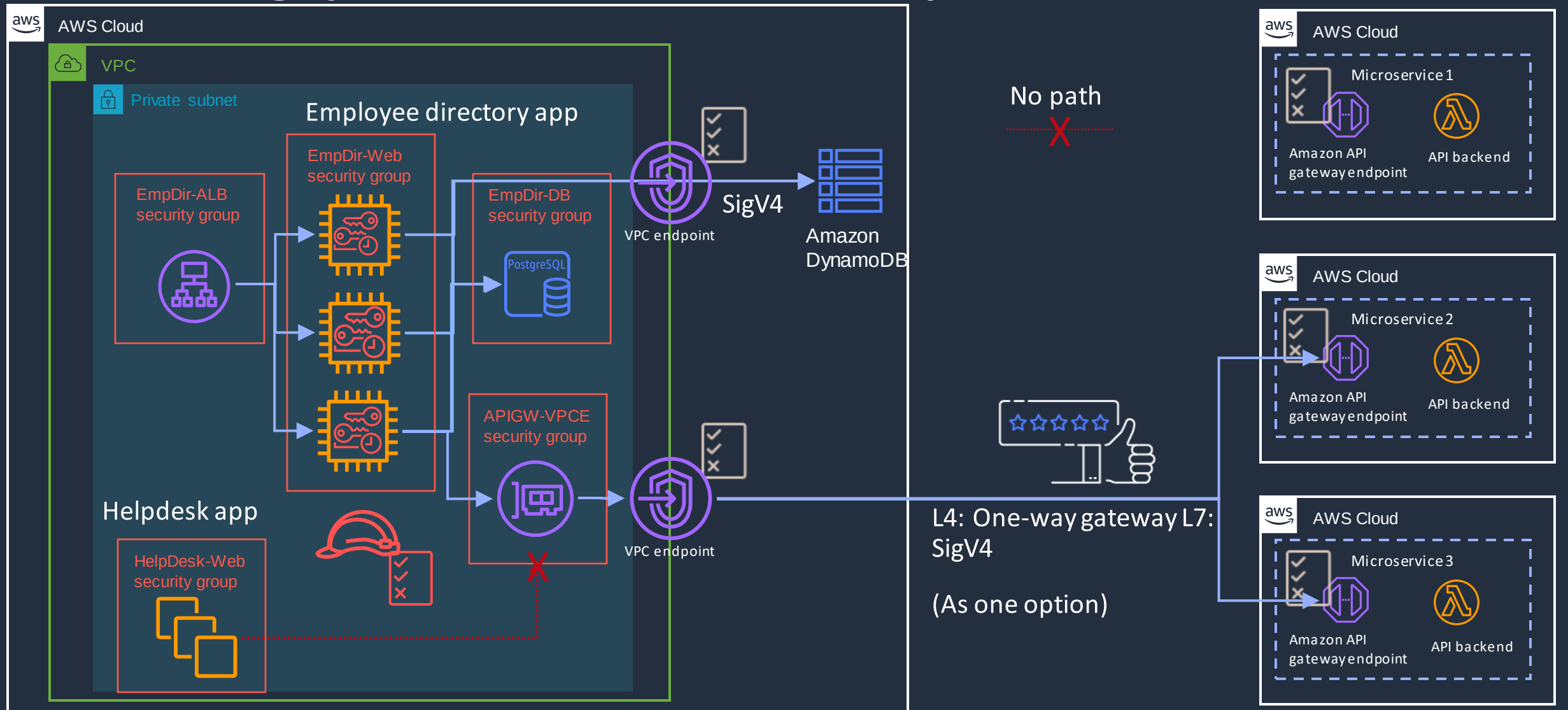
Eliminate unnecessary pathways to data

Consideration: Patterns follow architectures

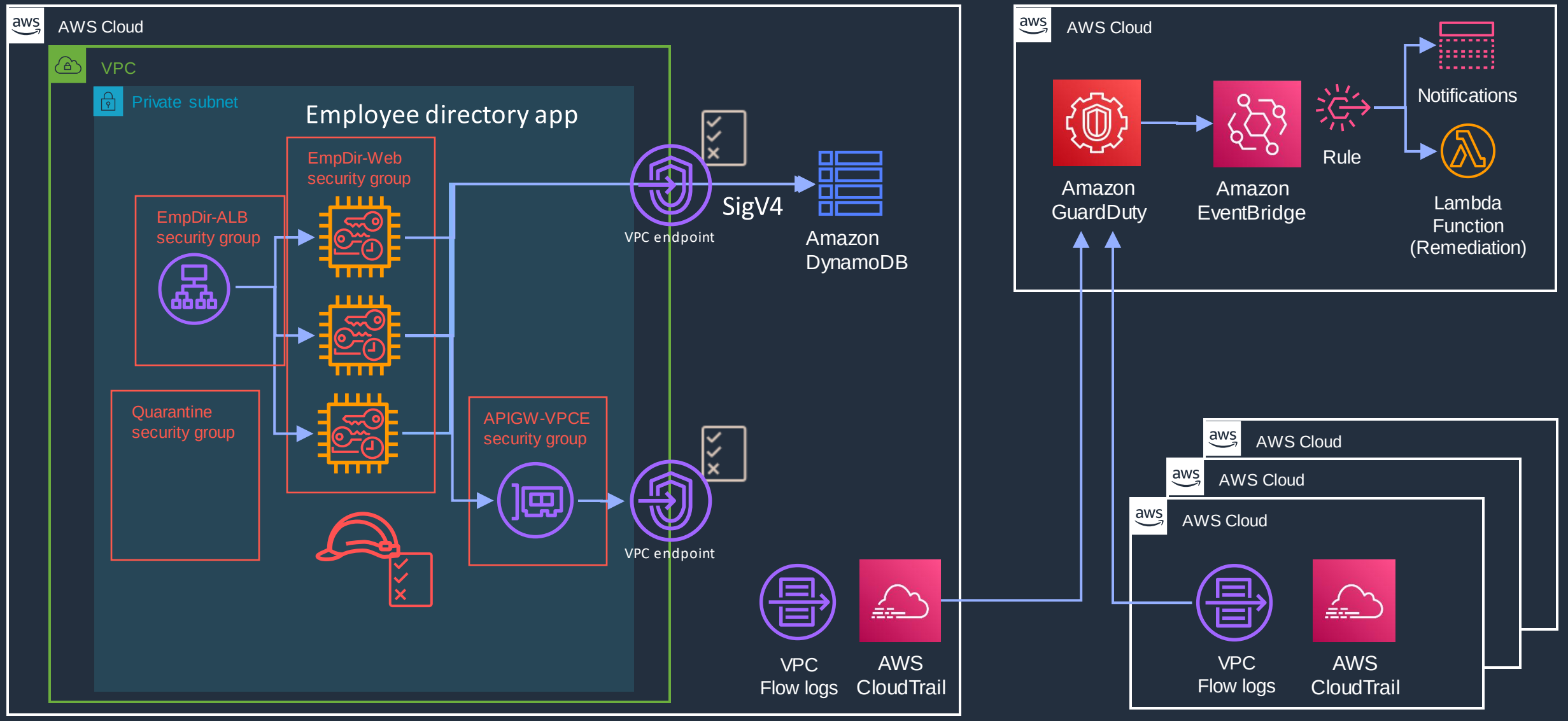
Authorizing specific flows between components



Authorizing specific flows between components



Detective controls for anomalous behavior



What if instead of eliminating unnecessary paths through the network…

We could stop worrying about the network entirely…

Amazon VPC Lattice

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

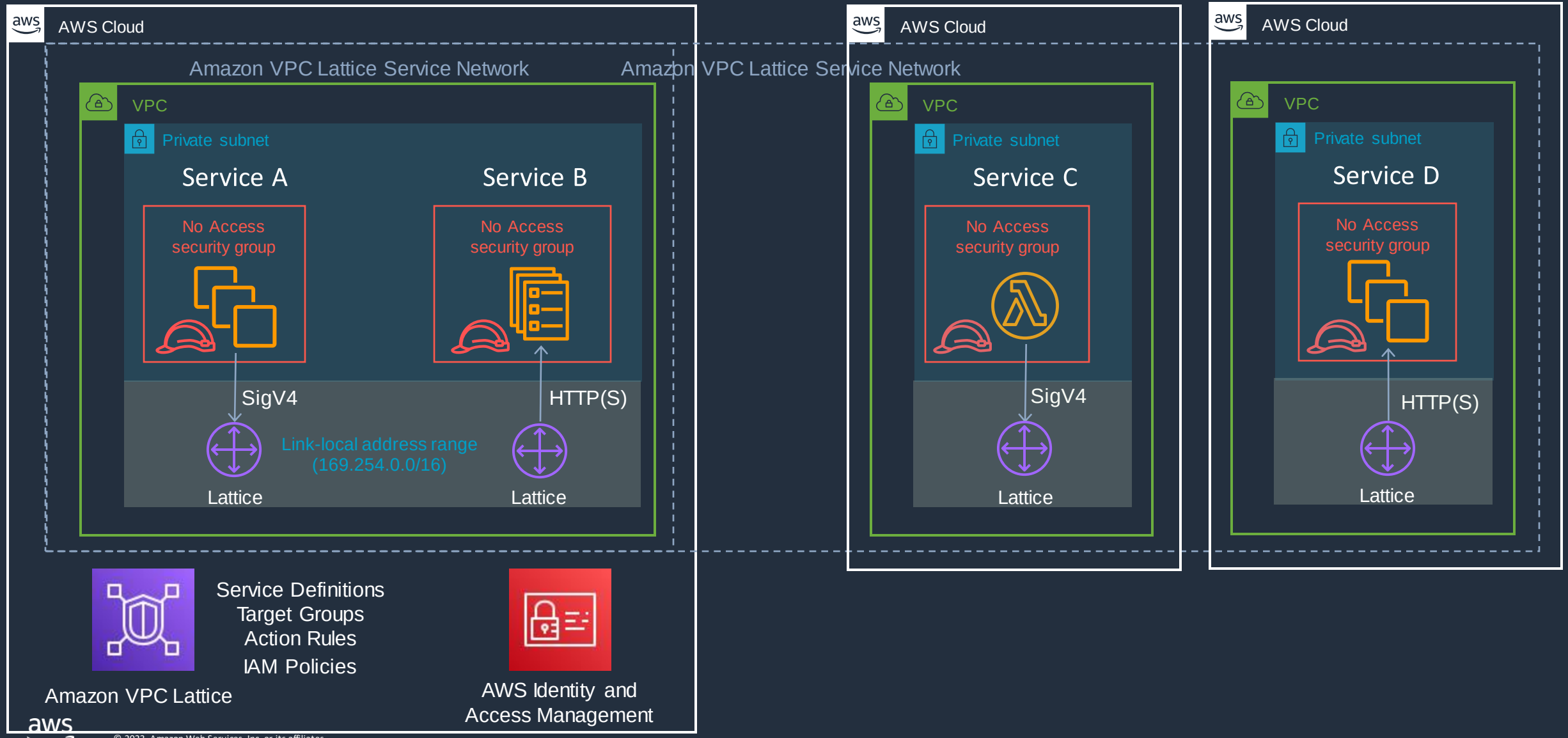
STREAMLINE SERVICE-TO-SERVICE INTERACTIONS

Monitor and troubleshoot communication with detailed access logs and metrics

PREVIEW

aws

Rethinking Service-to-Service communications



We’ve welded the computer shut

Enabling friction-free access to internal apps

USE CASE #2

Human-to-application

Goal: Improve workforce mobility and experience

Make internal applications available anywhere

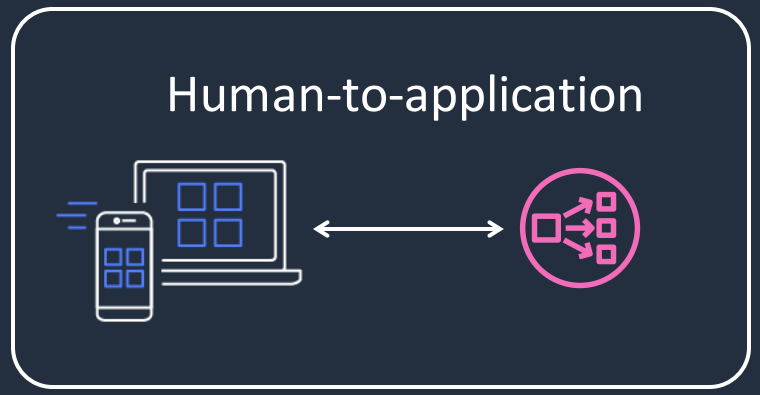
Maintain (or improve) security assurance

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

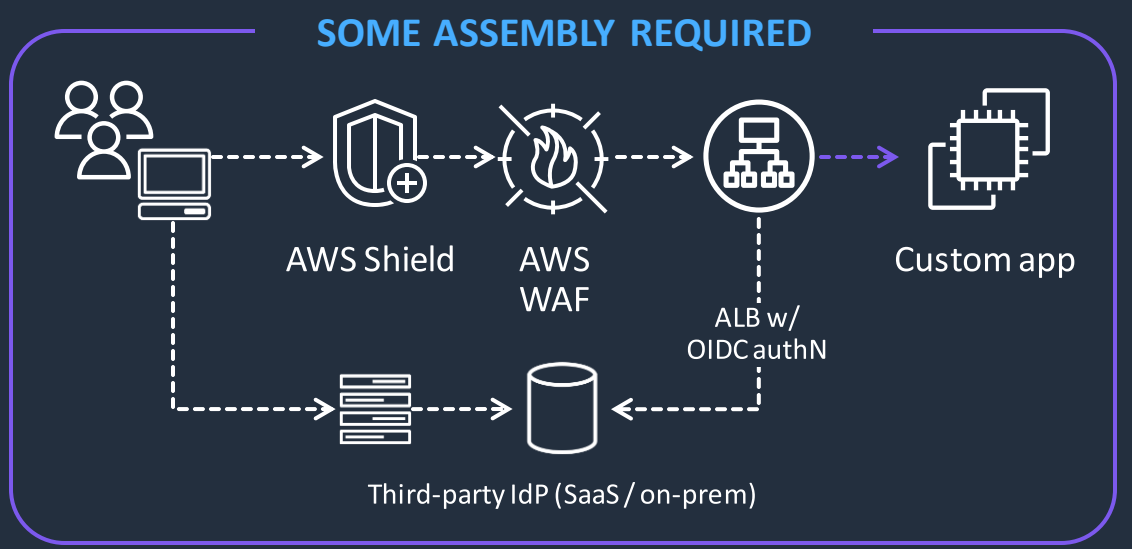
Enabling friction-free access to internal apps

USE CASE #2

Originally



Then



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

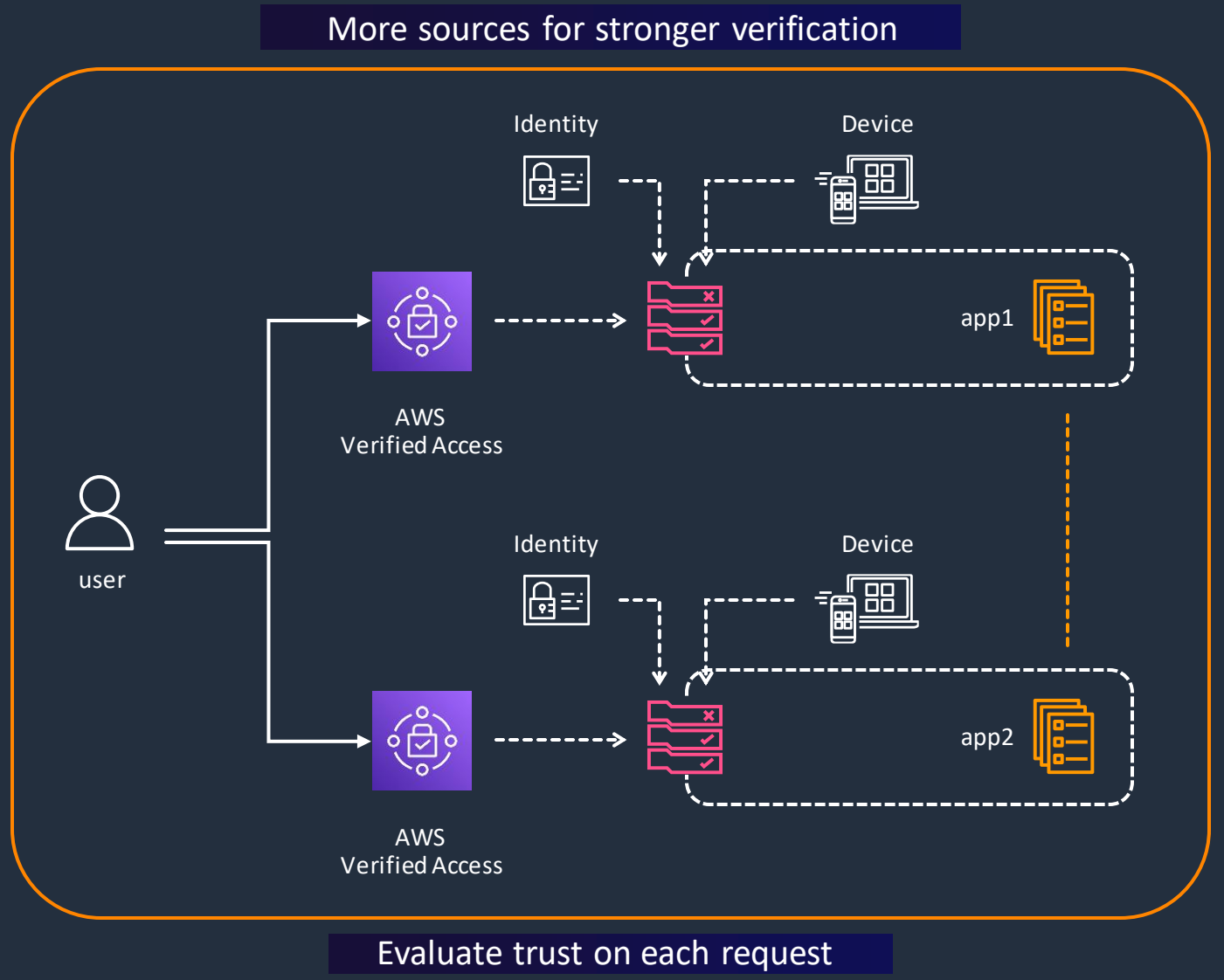
Users access applications with a web browser without any additional agents

Work from anywhere with VPN-less secure remote access

AWS Verified Access for zero trust architectures

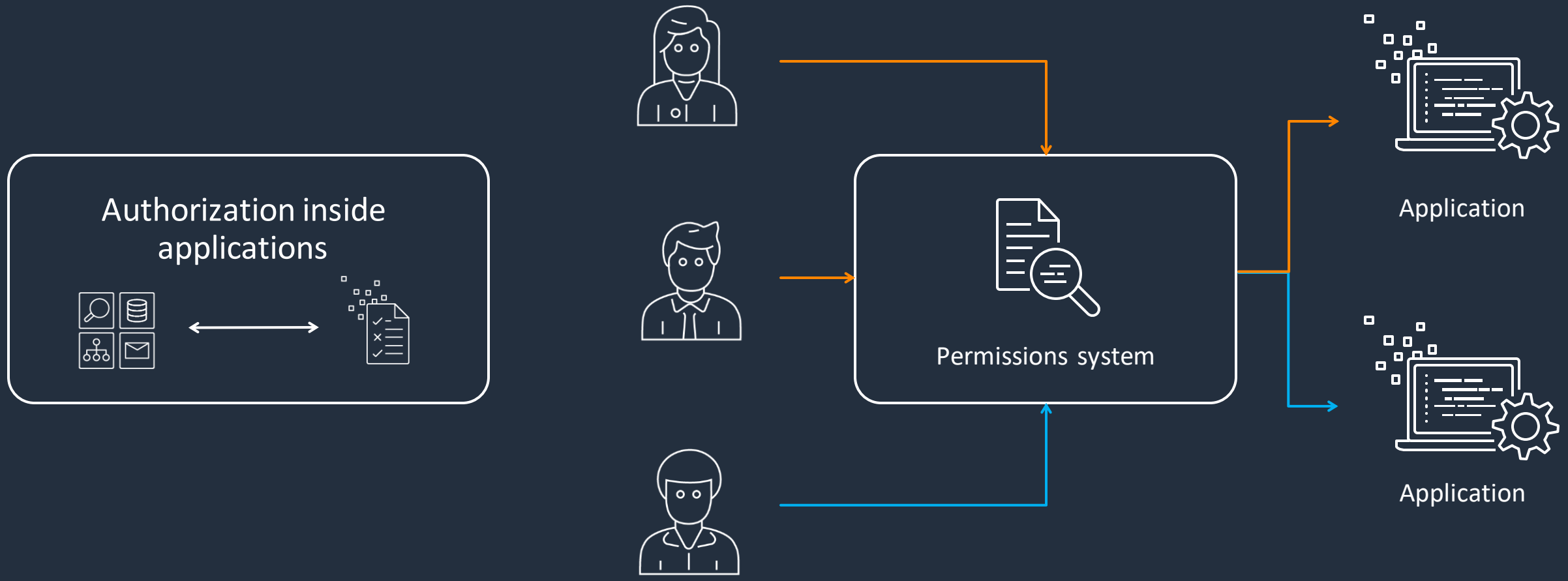
01 Multiple security signals to strongly verify access

02 Continuous verification



Consistent authorization across your applications

USE CASE #3



Amazon Verified Permissions

Scalable permisfine-grained authorization for
applications you buildsions management and

Amazon Verified Permissions for zero trust

01

Centrally create and maintain policies

02

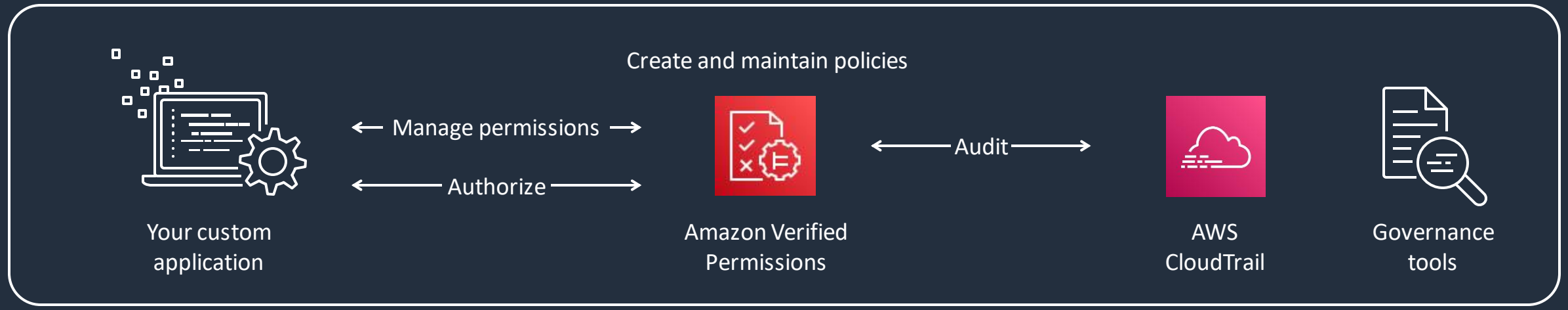
Manage fine-grained permissions across applications

03

Authorize end user actions based on roles/attributes

04

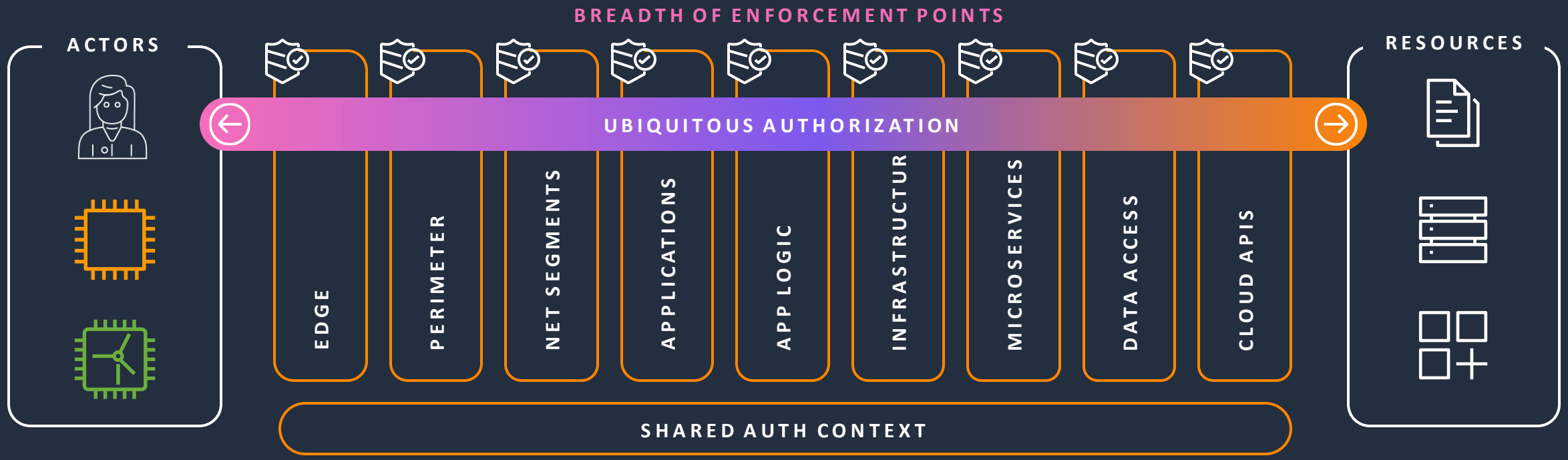
Audit permissions at scale



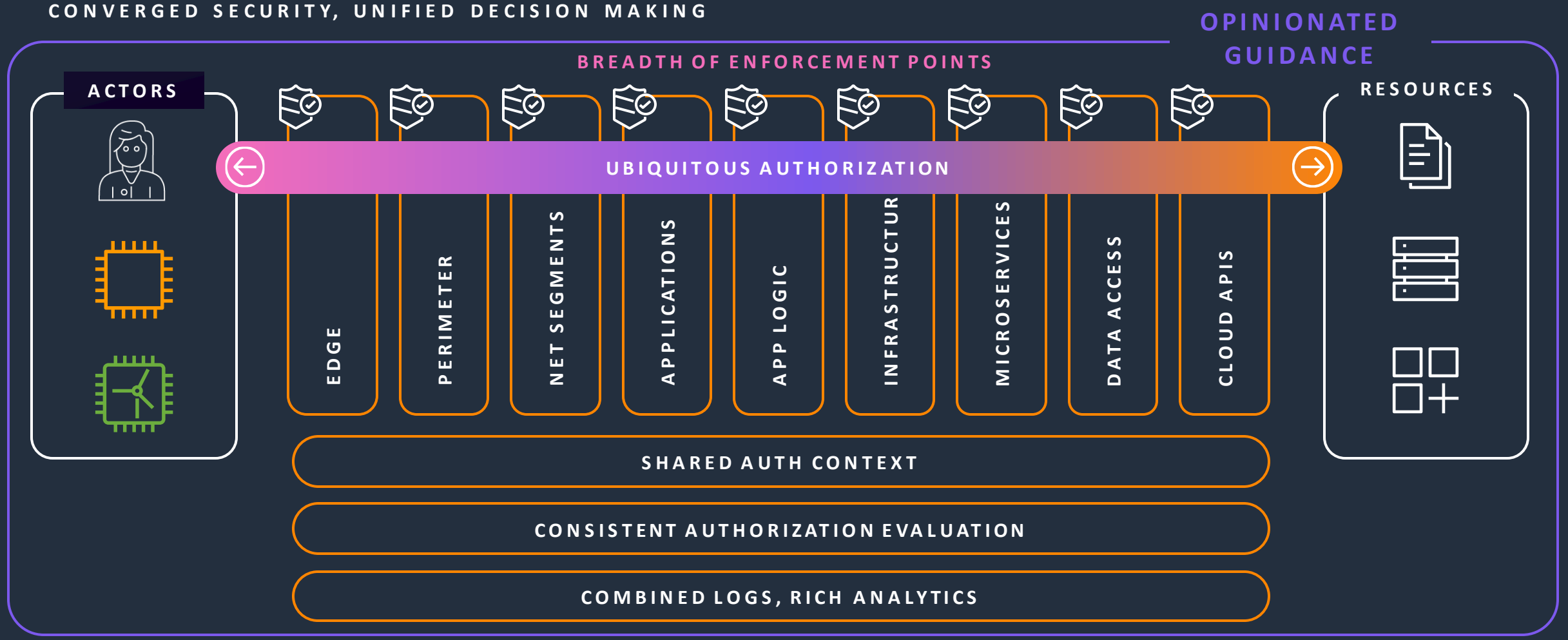
Demo – AWS Verified Permissions

AWS Zero Trust Vision: Ubiquitous Authorization

CONVERGED SECURITY, UNIFIED DECISION MAKING



AWS Zero Trust Vision: Ubiquitous Authorization



Q&A

Thank you!

https://www.pulse.aws/survey/H5OETD1D