
AWS
re:Invent

SEC303

Zero Trust: An AWS perspective

Quint Van Deman
Principal Identity Specialist
AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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

Zooming in

KEY DIMENSIONS

First dimension → Network

- Microperimeters?
- Security above network?
- Gateways or proxies?
- More dynamic VPNs?
- Combinations?



Zooming in

KEY DIMENSIONS

Second dimension → Identity

- Humans?
- Machines?
- Software components?
- Combinations?



Zooming in

MOUNTING TENSION



Potential for confusion



Opportunities to build

Guiding principles for Zero Trust



AWS re:Invent

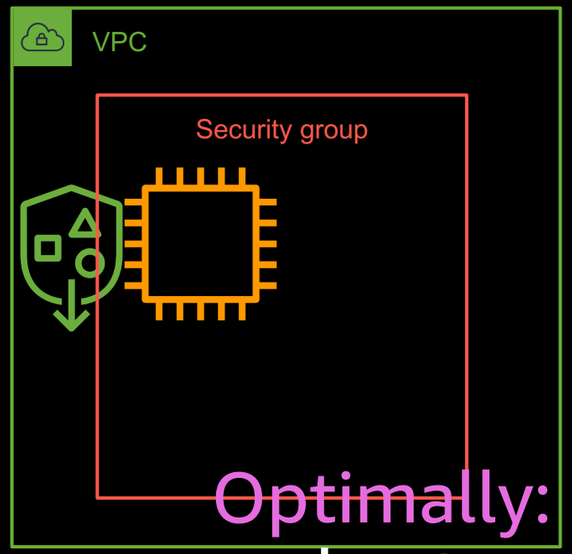
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Avoid a binary choice

GUIDING PRINCIPLE #1

Identity-centric AND Network-centric

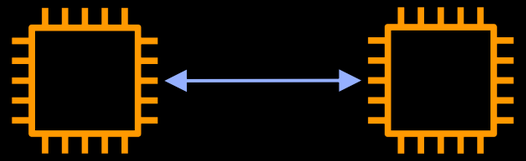




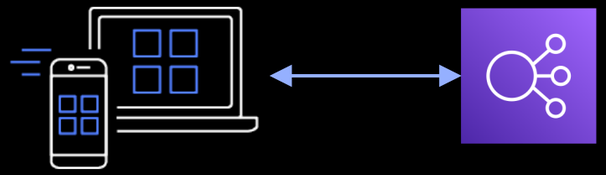
Optimally: Identity-centric and network-centric controls aware of each other

Focus on use cases

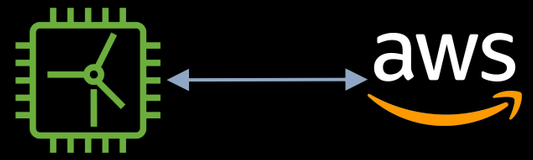
GUIDING PRINCIPLE #2



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

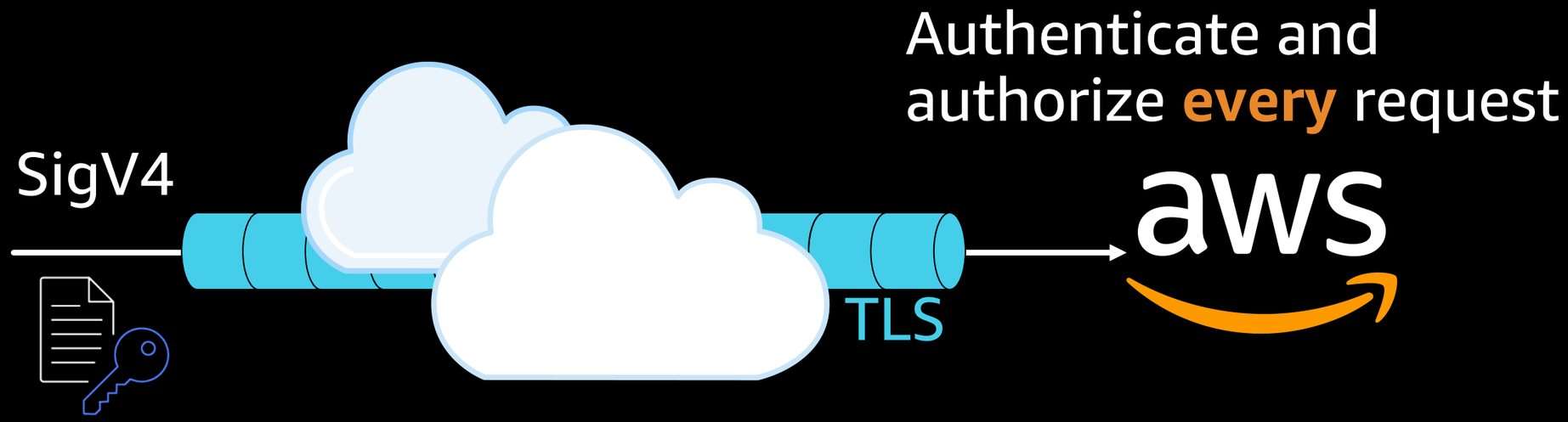


AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Interacting with AWS Application Programming Interfaces (APIs)

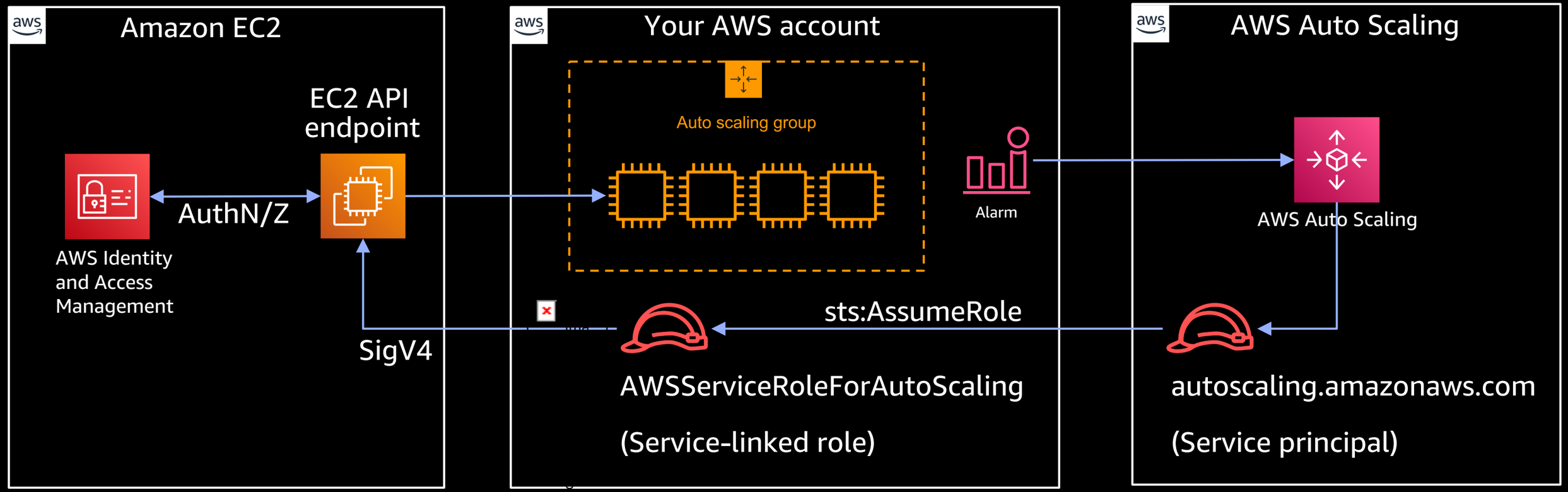
ZERO TRUST WITHIN AWS



Use case 0 for Zero Trust?

AWS Services interacting with each other

ZERO TRUST WITHIN AWS

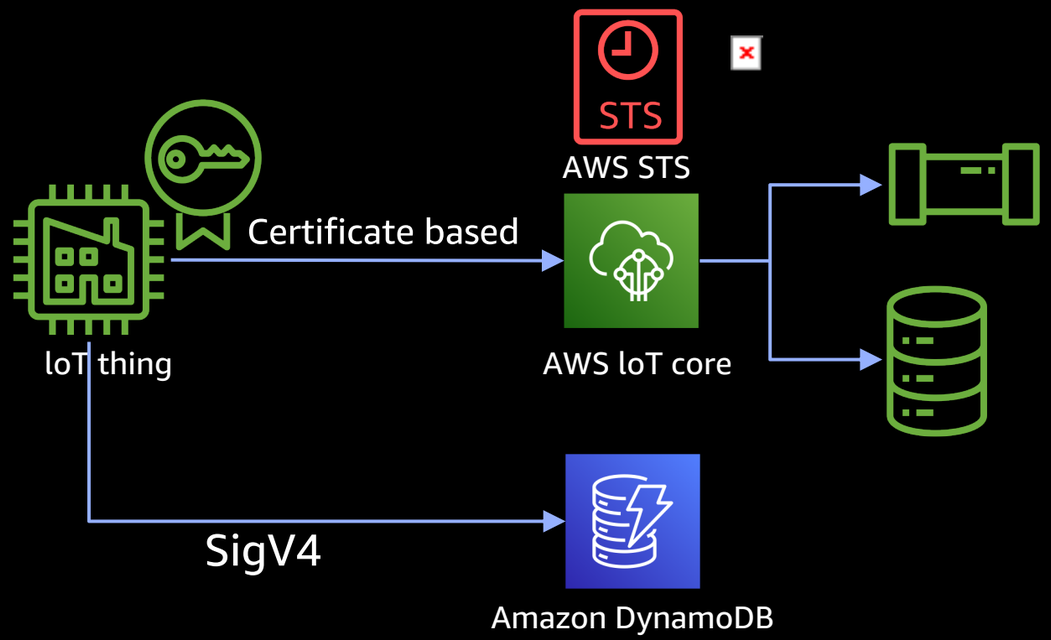


Exact same identity-centric mechanism you use

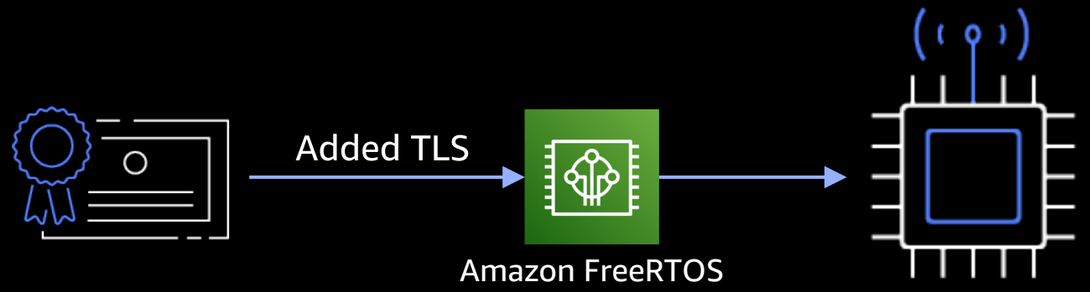
Adherence to AWS security standards

ZERO TRUST WITHIN AWS

Required authentication and encryption at all points



Brought modern secure communication to entire classes



AWS standards brought Zero Trust foundations to the Internet of Things (IoT) domain

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

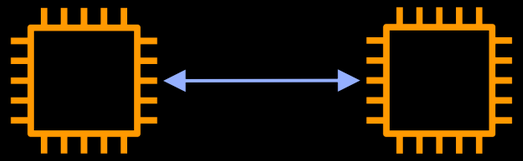


AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Authorizing specific flows between components

ZERO TRUST ON AWS



Machine-to-machine

Goal: Eliminate unneeded lateral network mobility

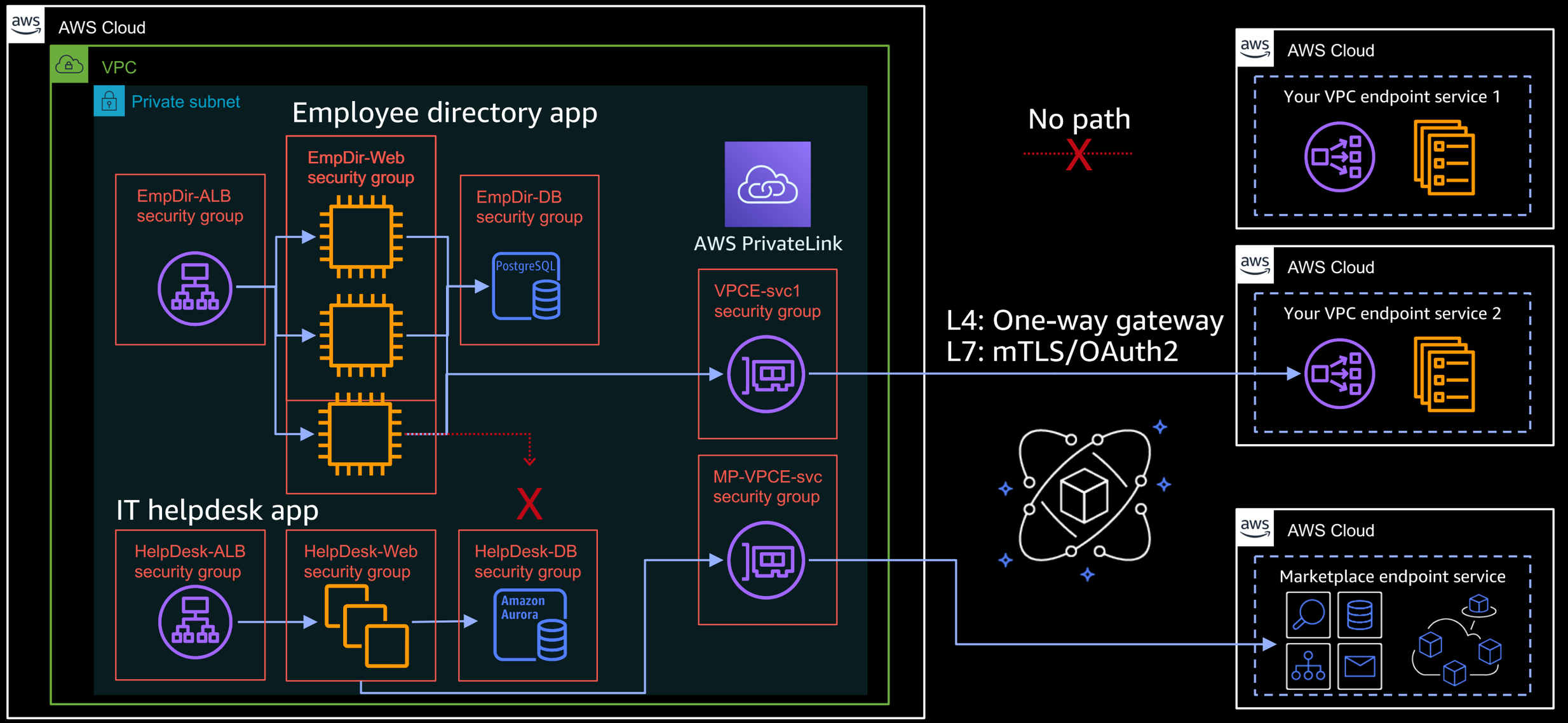
Reduce surface area of systems

Eliminate unnecessary pathways to data

Consideration: Patterns follow architectures

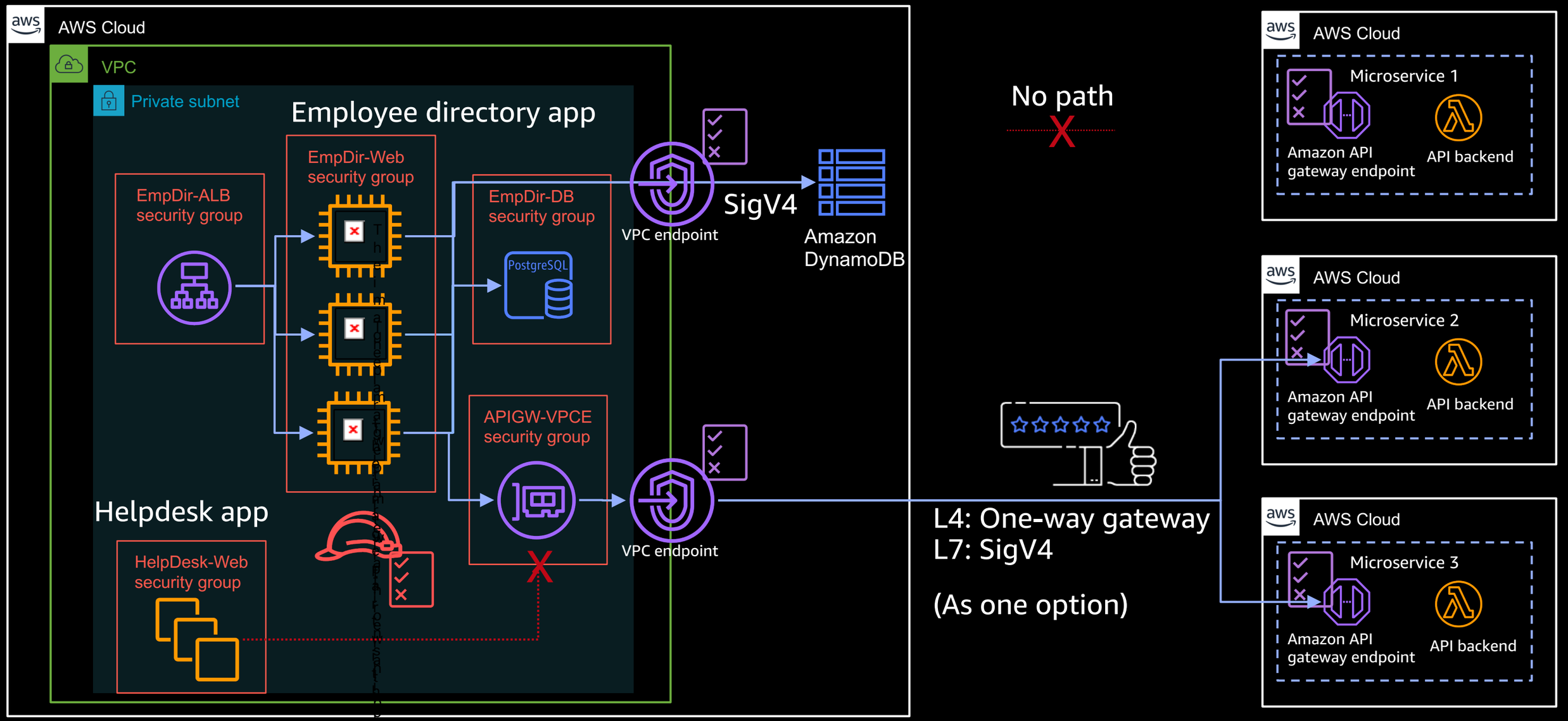
Authorizing specific flows between components

ZERO TRUST ON AWS



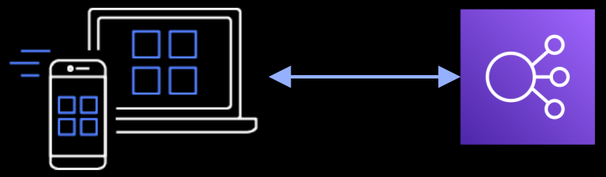
Authorizing specific flows between components

ZERO TRUST ON AWS



Enabling friction-free access to internal apps

ZERO TRUST ON AWS



Human-to-application

Goal: Improve workforce mobility and experience

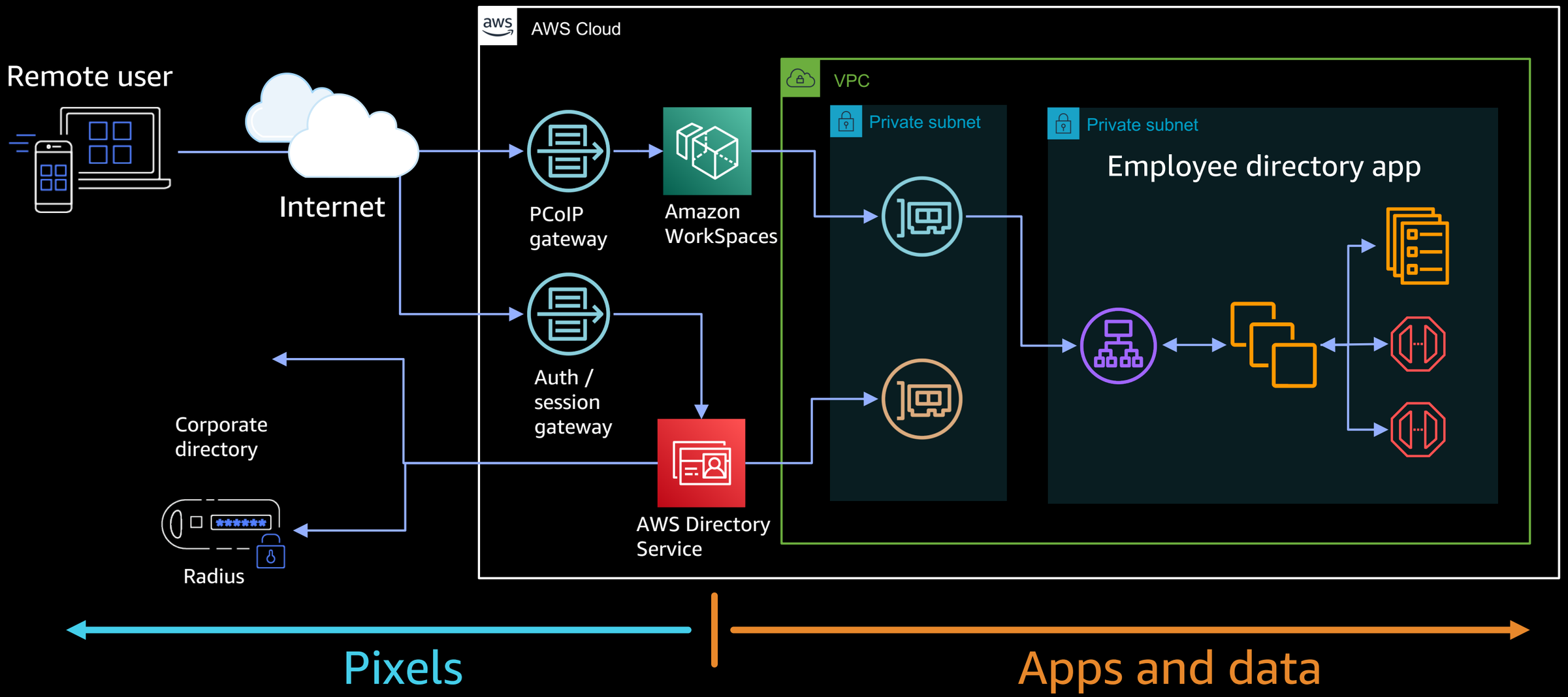
Make internal applications available anywhere

Maintain (or improve) security assurance

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

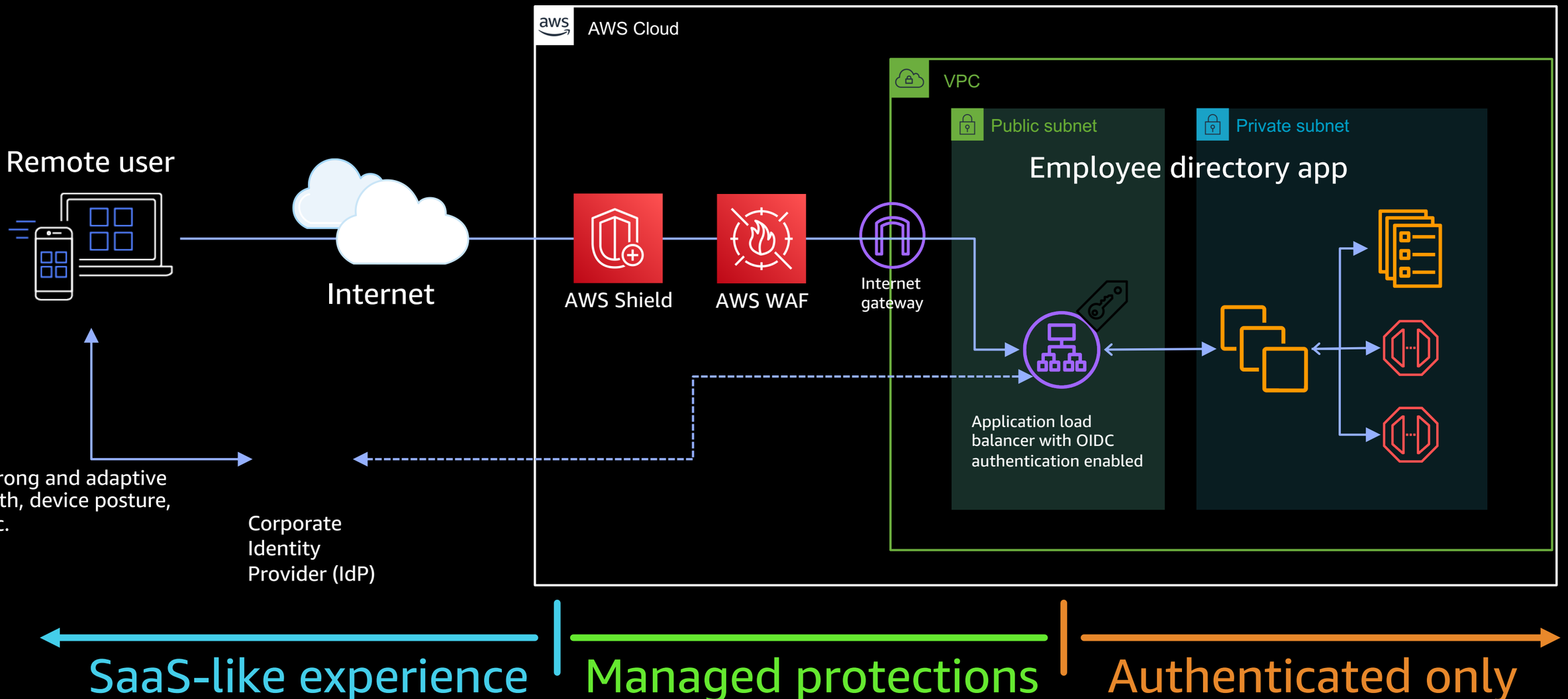
Enabling friction-free access to internal apps

ZERO TRUST ON AWS



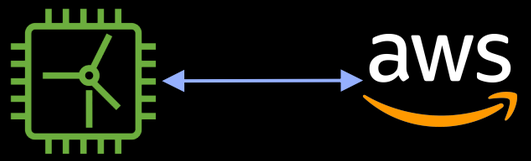
Enabling friction-free access to internal apps

ZERO TRUST ON AWS



Securing digital transformation projects

ZERO TRUST ON AWS



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


“It’s still Day 1.”

Thank you!

Quint Van Deman

@AWSIdentity
LinkedIn.com/in/quint-van-deman

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.