AWS Denver Learning Days

Building Zero Trust Architecture on AWS

Grant Joslyn

Sr Solutions Architect

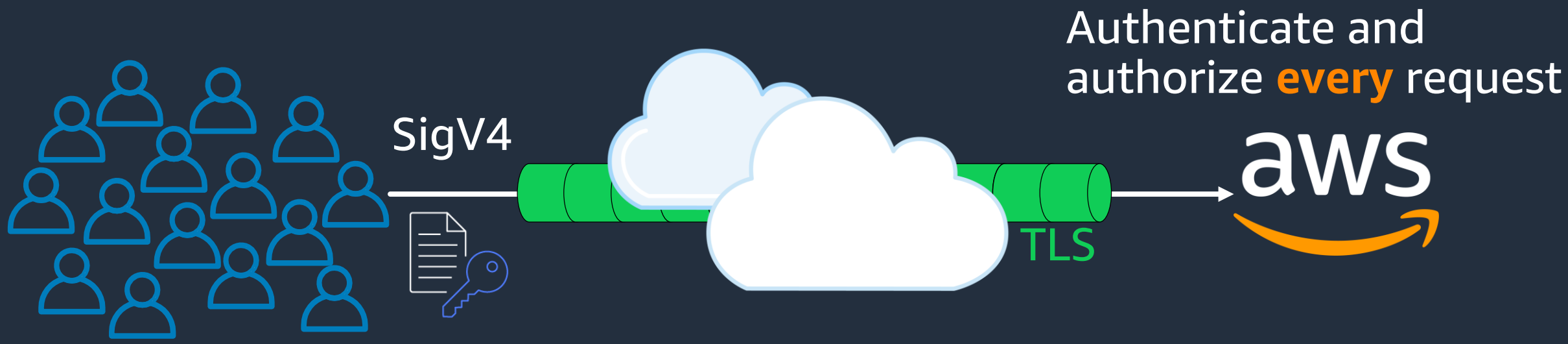
gajoslyn@amazon.com

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

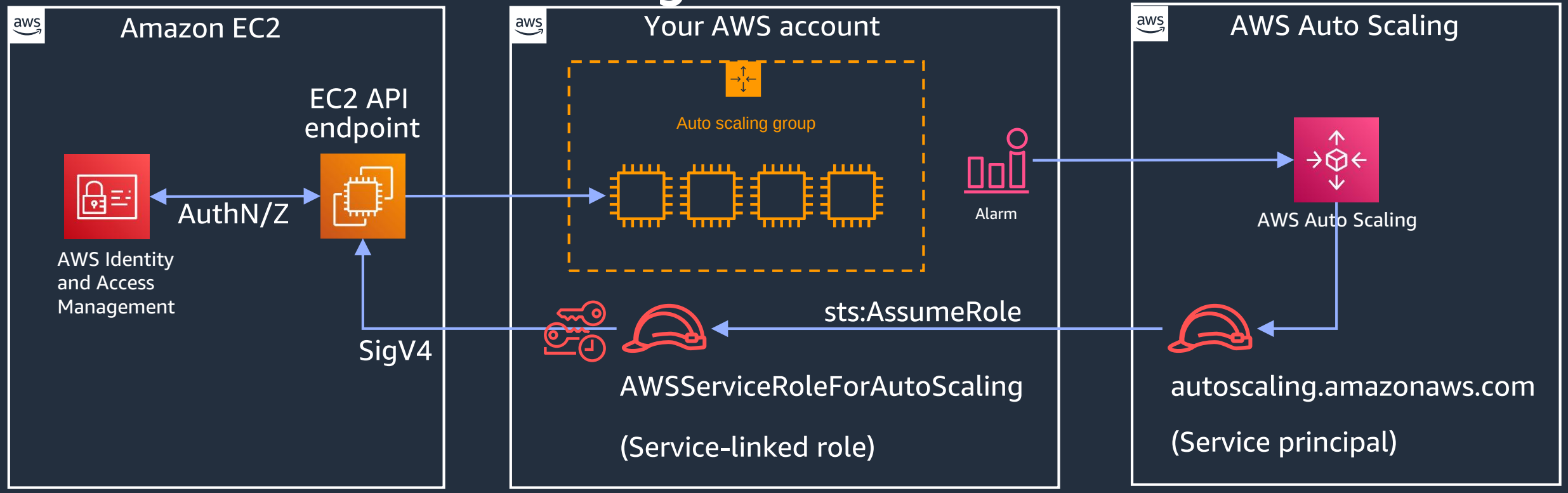
Examples of Zero Trust within AWS

Interacting with AWS APIs



Use case 0 for Zero Trust?

AWS Services interacting with each other

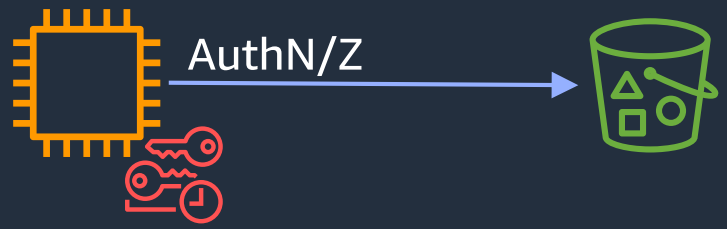


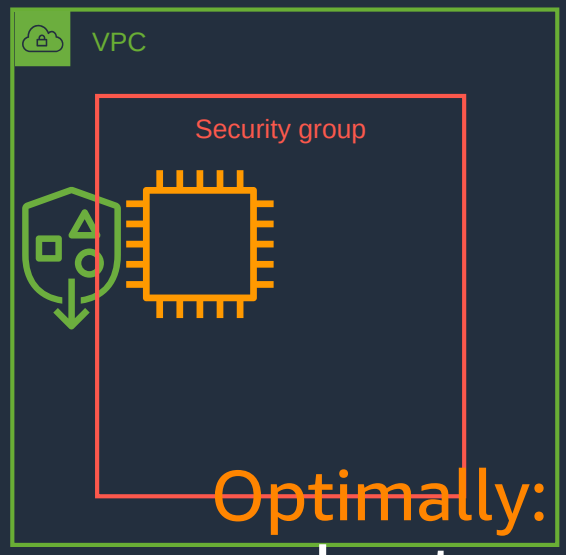
Exact same identity-centric mechanism you use

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

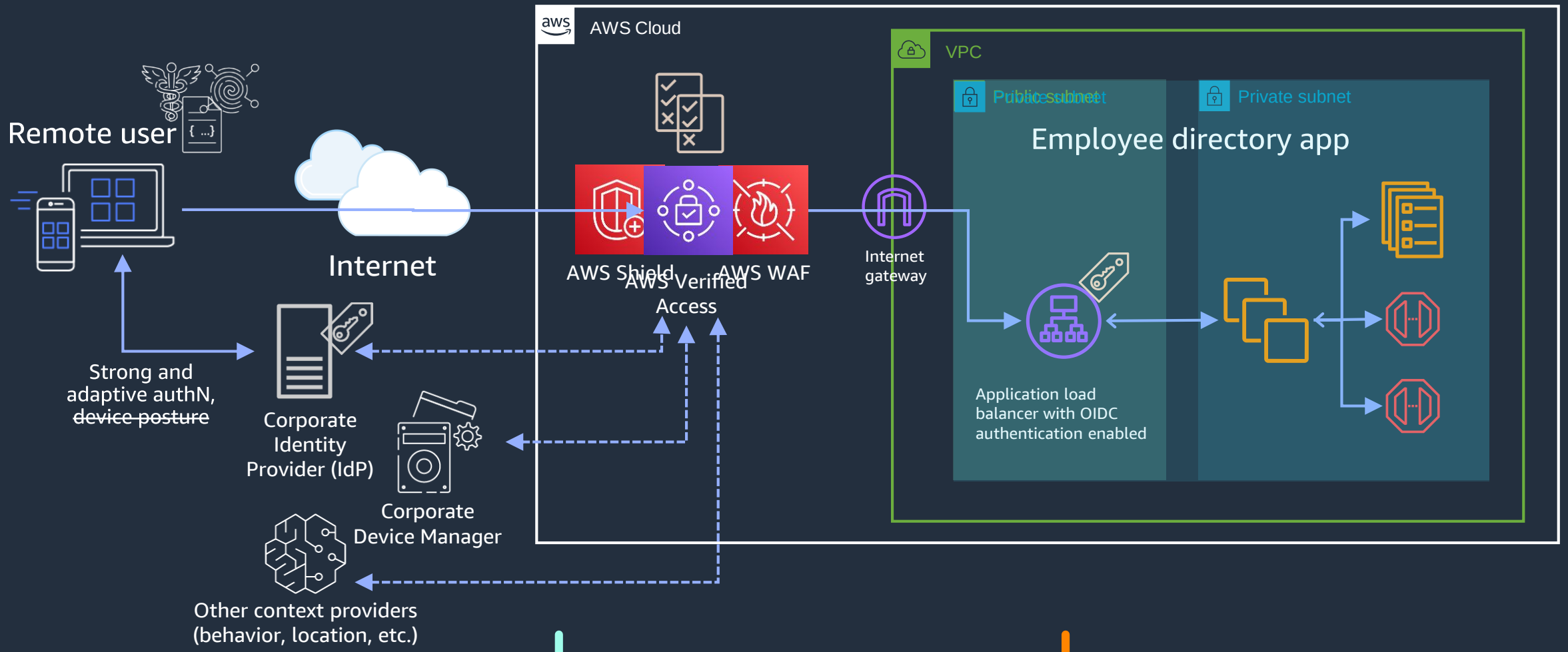
Same: Technical principles

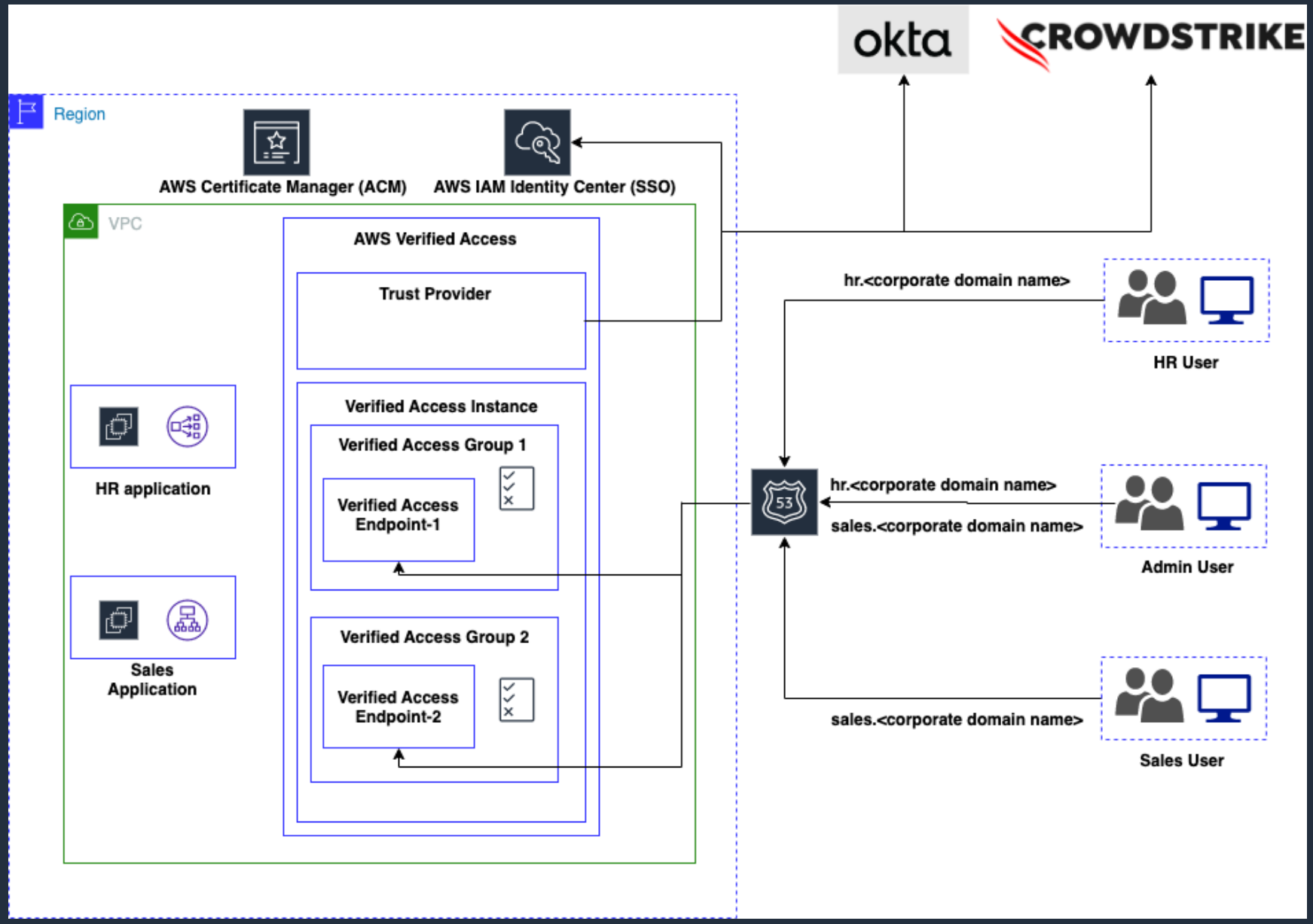
Different: Organizational objectives

Focus: Problems we're trying to solve

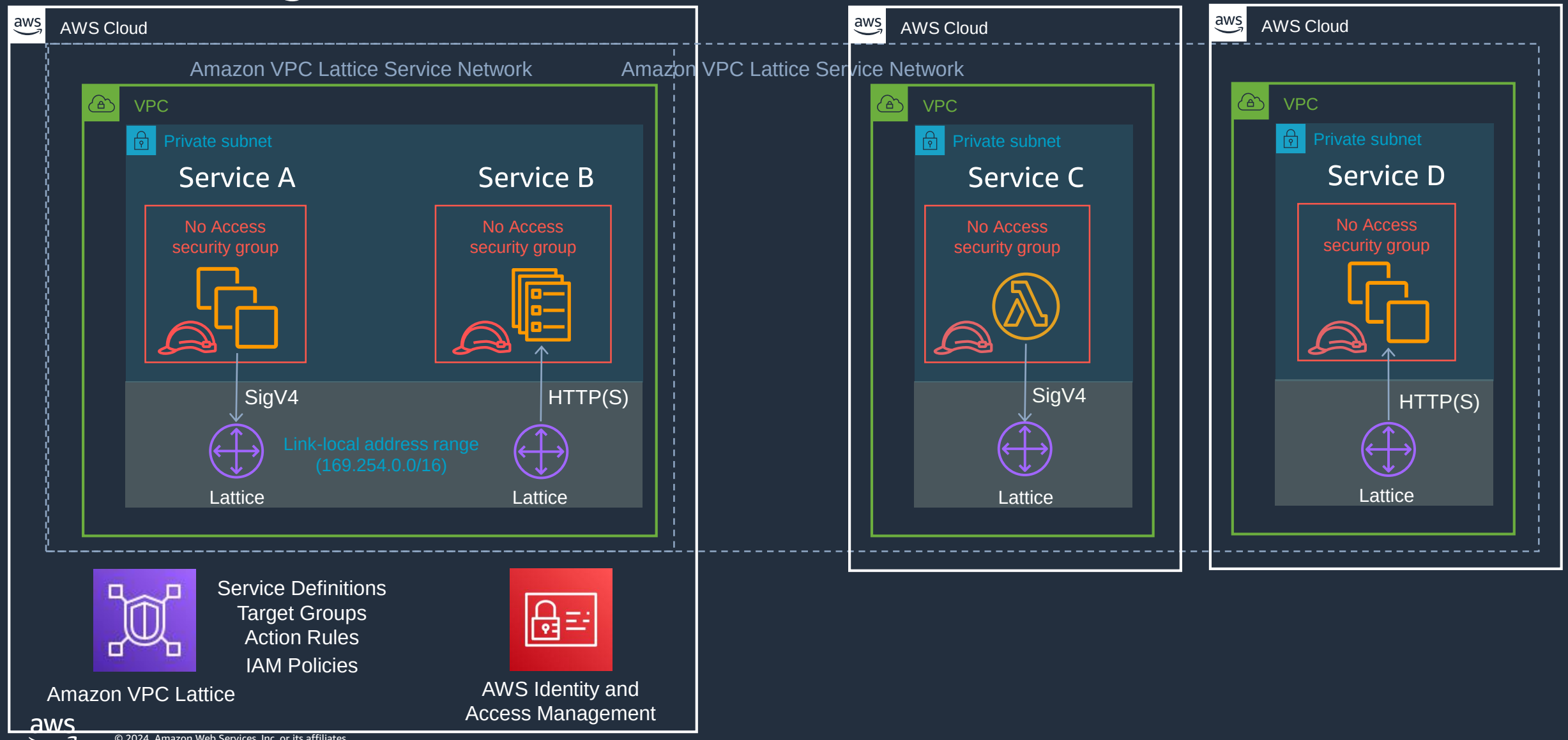
Avoid: Getting mired in low value discussions

Enabling friction-free access to internal apps





Rethinking Service-to-Service communications



Inherent capabilities of AWS

SINCE THE DAWN OF THE CLOUD

- Software defined dynamic microperimeters
- Request level authentication and authorization
- Perfectly accurate, maintenance free inventory and state data
- Machine identity with cryptographically verifiable hardware root of trust
- Credential distribution and rotation at hyperscale
- Many more…

Please complete the session survey by scanning the QR code

Grant Joslyn
Senior Solutions Architect
gajoslyn@amazon.com

Mission Track
Zero trust workshop