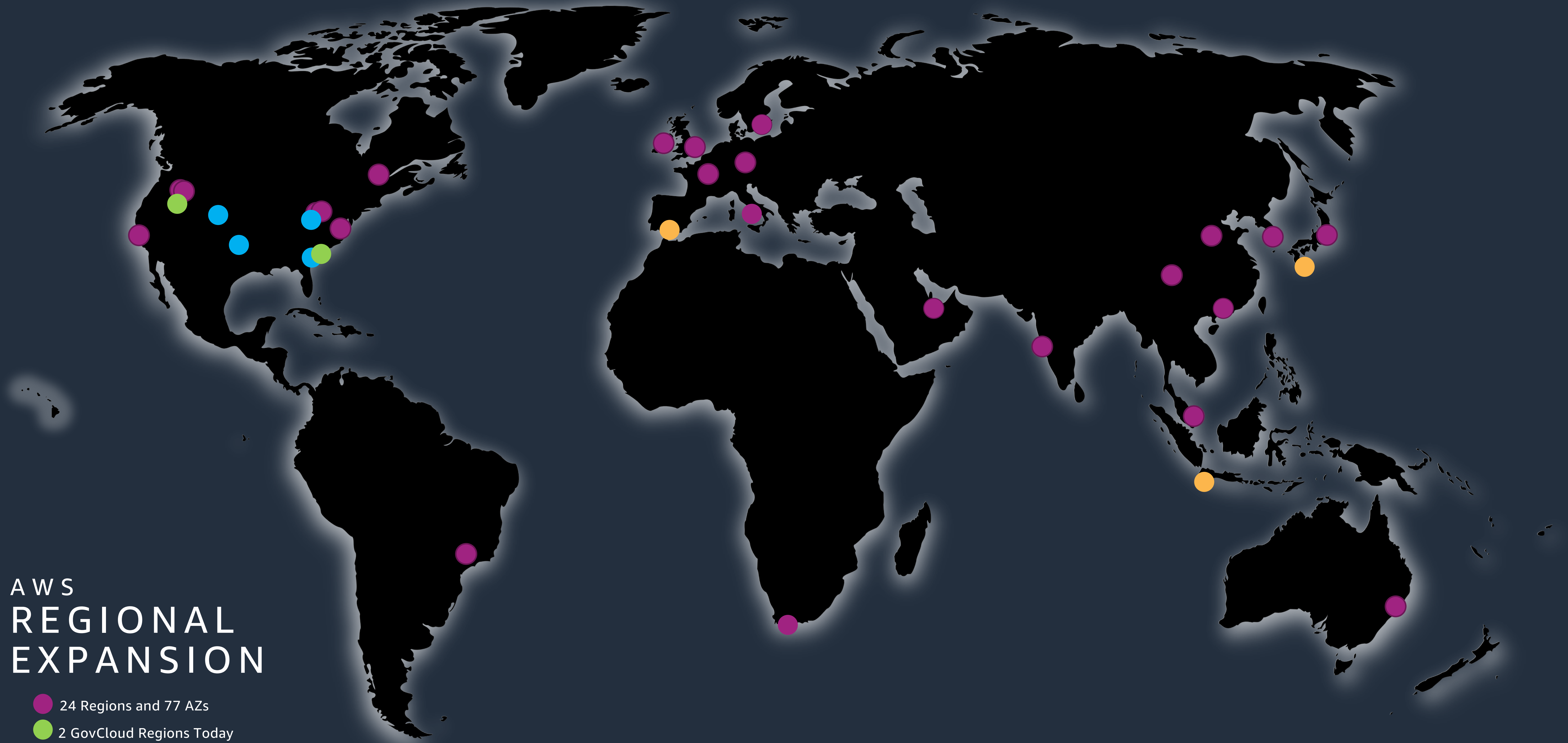
Amazon Web Services

Security Overview

Doug Pardue, Sr. Solutions Architect
wdpardue@amazon.com

Global Infrastructure

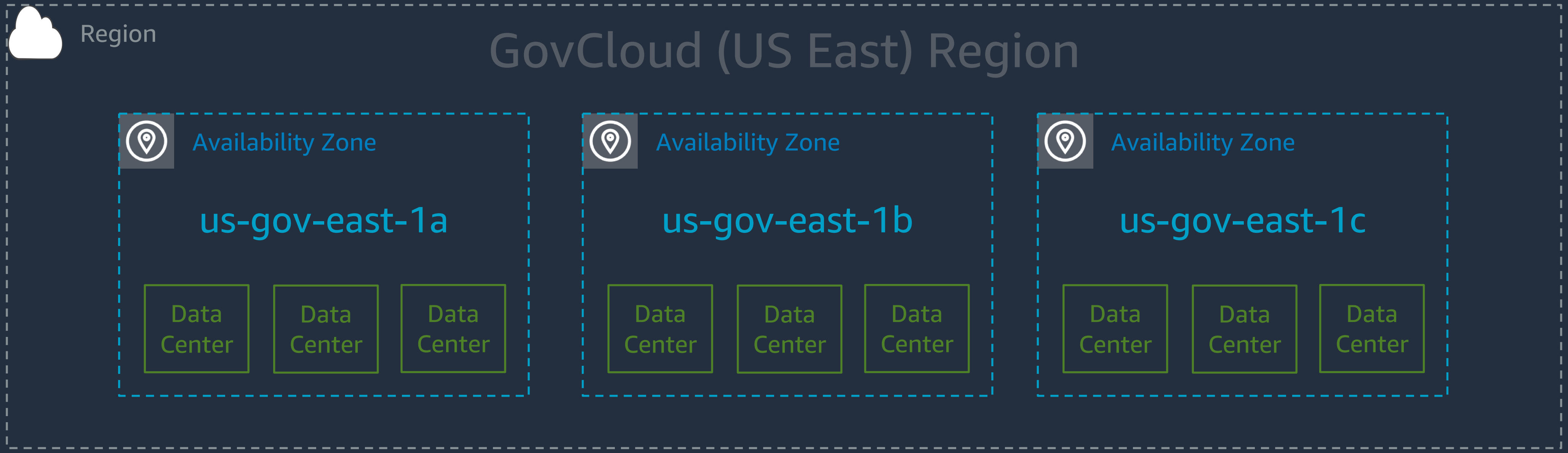


AWS REGIONAL EXPANSION

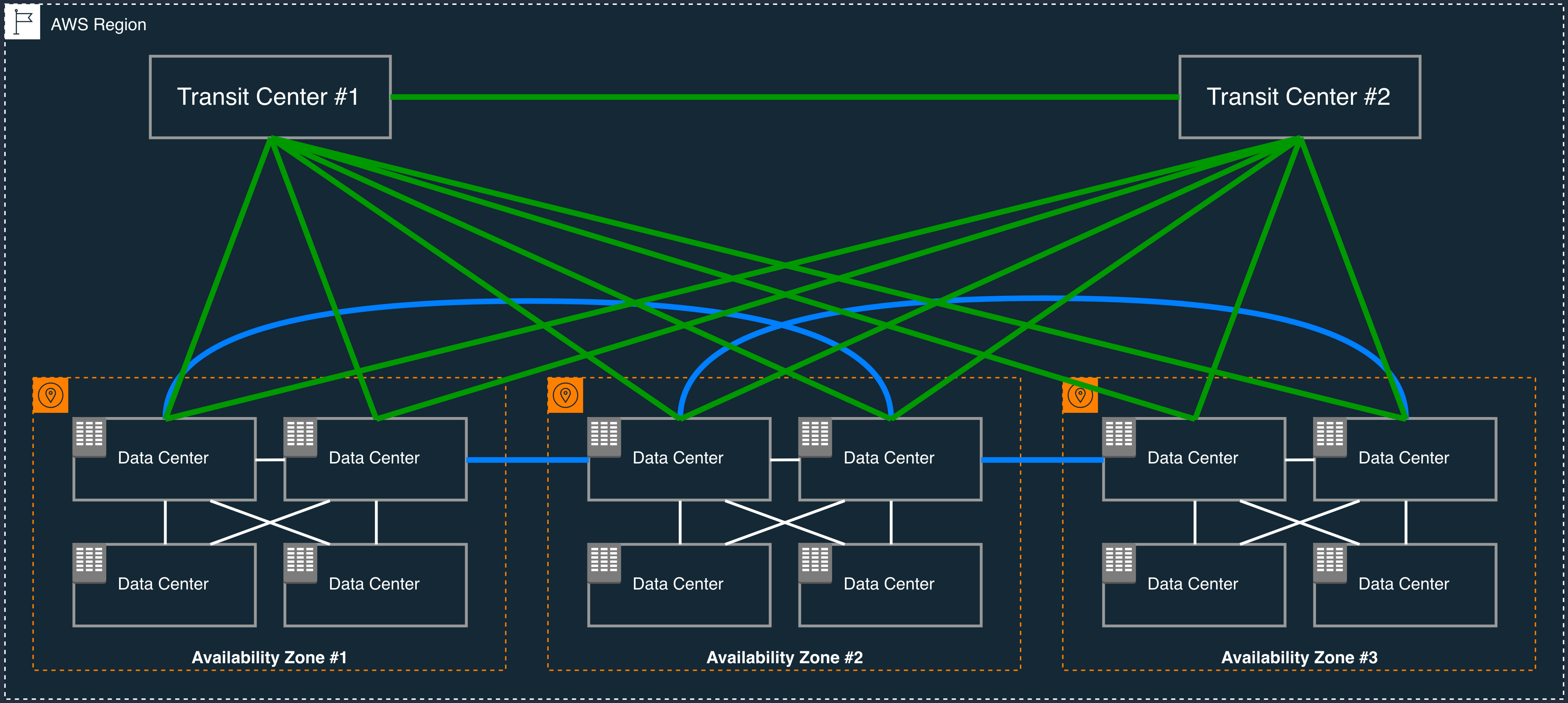
- ● 24 Regions and 77 AZs
- ● 2 GovCloud Regions Today
- ● New Regions Coming Soon
- ● New GovCloud, TS, and Secret Regions Coming Soon

Availability Zones

- A Region is comprised of multiple Availability Zones (typically 3)
- Fully independent partitions on isolated fault lines, flood plains, and power grids
- Each AZ: redundant power and redundant dedicated network
- Each AZ: typically multiple data centers

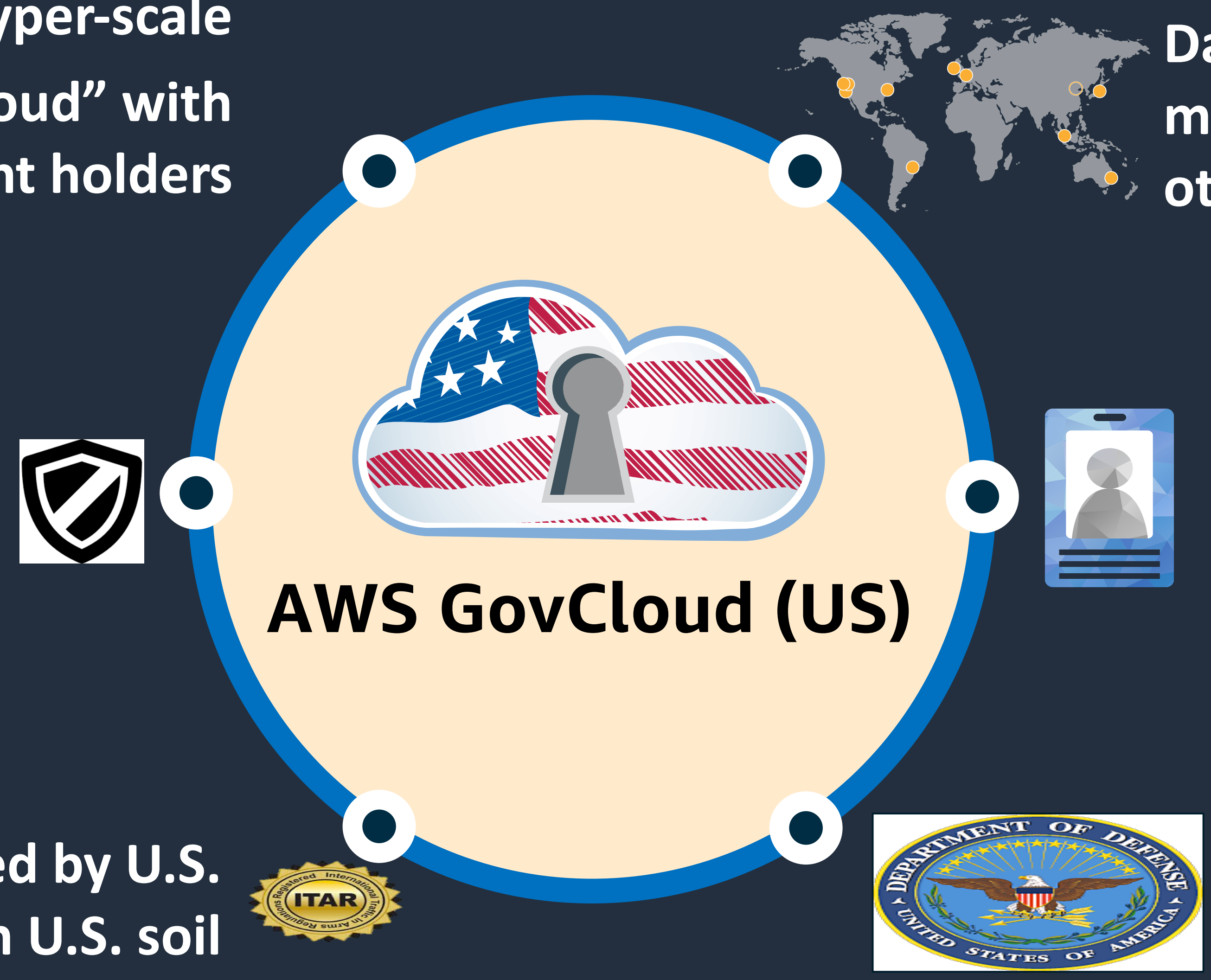


Availability Zones



AWS GovCloud

What is GovCloud?



AWS GovCloud (US)

Hyper-scale

"Community Cloud" with vetted account holders

Data, network, and machine isolation from other regions

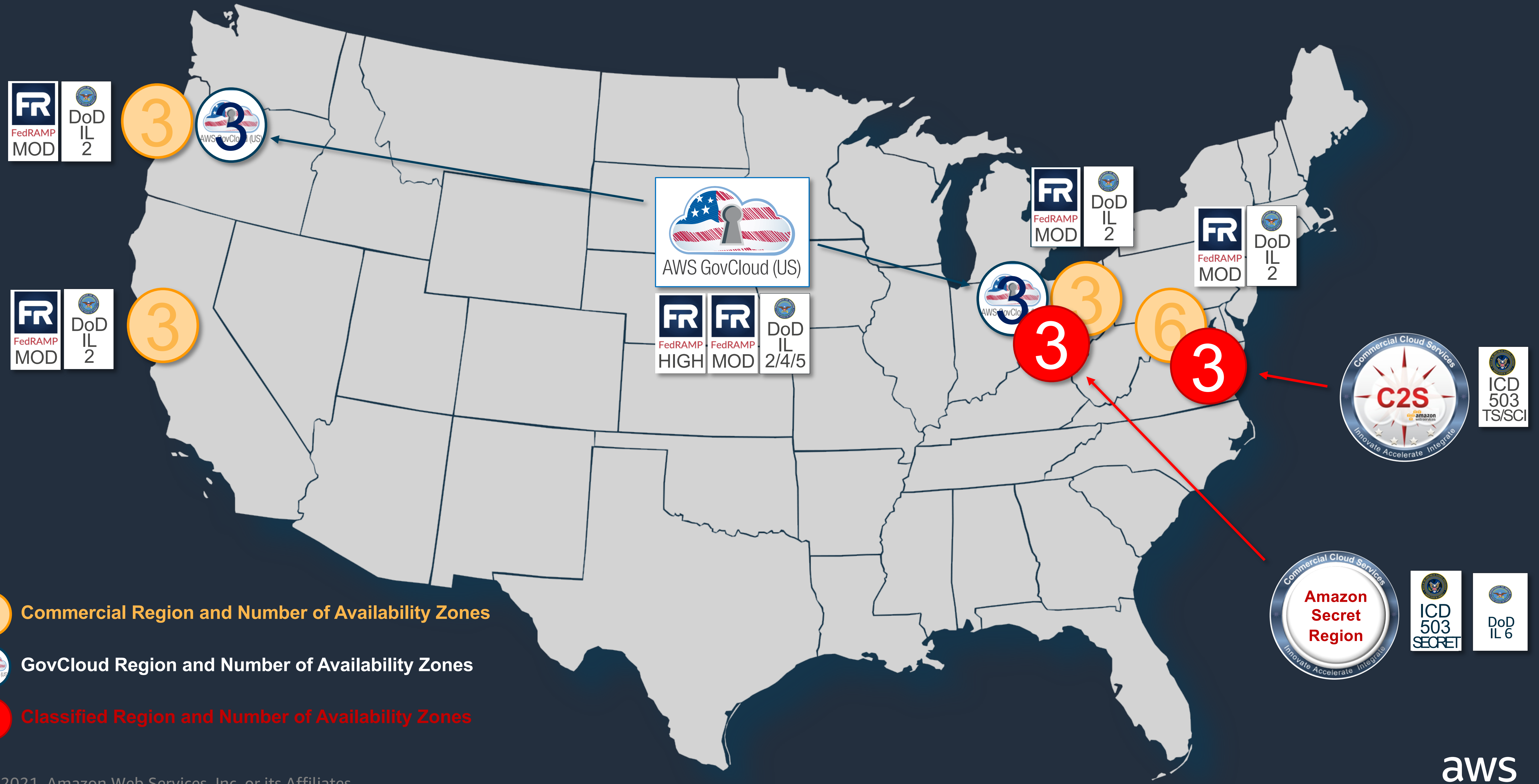
Connectivity to DoD Cloud Access Points (CAPs)

Separate IAM (unique credentials)

Managed by U.S. Citizens on U.S. soil

Dedicated GovCloud Management Console

US AWS Regions for DoD and Federal Use



# Commercial Region and Number of Availability Zones

# GovCloud Region and Number of Availability Zones

# Classified Region and Number of Availability Zones

SRG Impact Levels

SRG Impact Level	Region	Maximum Data Type	Information Characterization
2	US AWS Regions, GovCloud	Non-Controlled Unclassified Information	Unclassified information approved for public release
			Unclassified, not designated as controlled unclassified information (CUI) or critical mission data, but requires some minimal level of access control
4	Gov Cloud	Controlled Unclassified Information	Requires protection from unauthorized disclosure as established by Executive Order 13556 (Nov 2010); Education, Training, SSN, Recruiting (if medical is not included), Credit card information for individuals (i.e., PX or MWR events)
			PII, PHI, SSN, Credit card information for individuals, Export Control, FOUO, Law Enforcement Sensitive, Email
5	Gov Cloud with Dedicated Instances	Controlled Unclassified Information + NSS	National Security Systems and other information requiring a higher level of protection as deemed necessary by the information owner, public law, or other government regulations
6	AWS SECRET Region	Classified up to SECRET	Pursuant to EO 12958 as amended by EO 13292; classified national security information or pursuant to the Atomic Energy Act of 1954, as amended to be Restricted Data (RD)

AWS GovCloud (US) delivers compliance in the Cloud

International Traffic and Arms Regulation

FedRAMP Moderate and High

DOD Cloud Security Requirements Guide IL 2,4 and 5

Criminal Justice Information Service Security Policy

IRS – 1075 (Section 6103 (p))

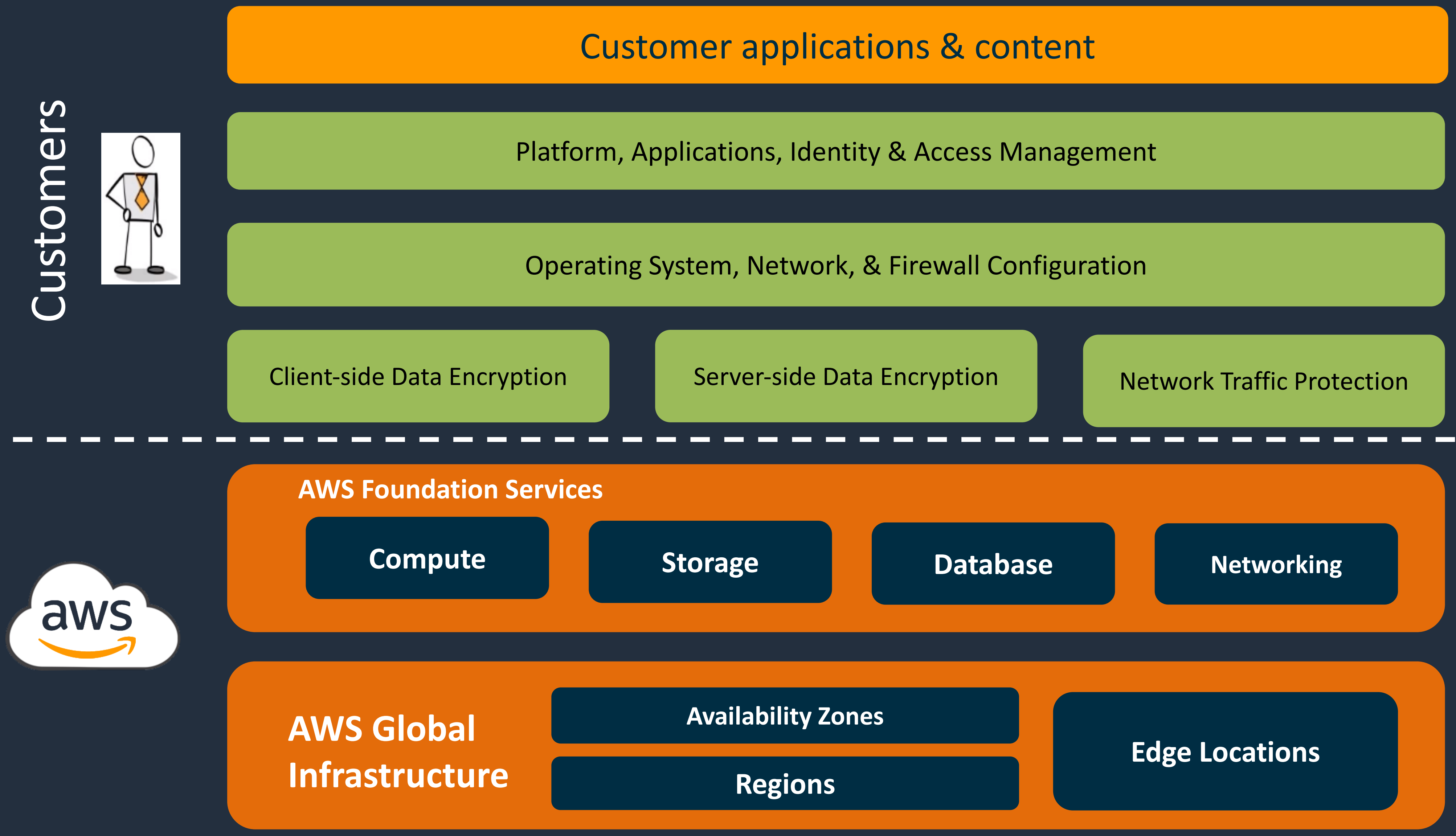
Federal Information Processing Standard

SP 800-53 (rev 4)
SP 800-171

Defense Federal Acquisition Regulation Supplement

Shared Responsibility Model

Security & compliance is a shared responsibility



Customers

Customer applications & content

Platform, Applications, Identity & Access Management

Operating System, Network, & Firewall Configuration

Client-side Data Encryption

Server-side Data Encryption

Network Traffic Protection

aws

AWS Foundation Services

Compute

Storage

Database

Networking

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

Customers have their choice of security configurations **IN** the Cloud

AWS is responsible for the security **OF** the Cloud

Highest standards for privacy and data security

Meet data residency requirements
Choose an AWS Region and AWS will not replicate it elsewhere unless you choose to do so

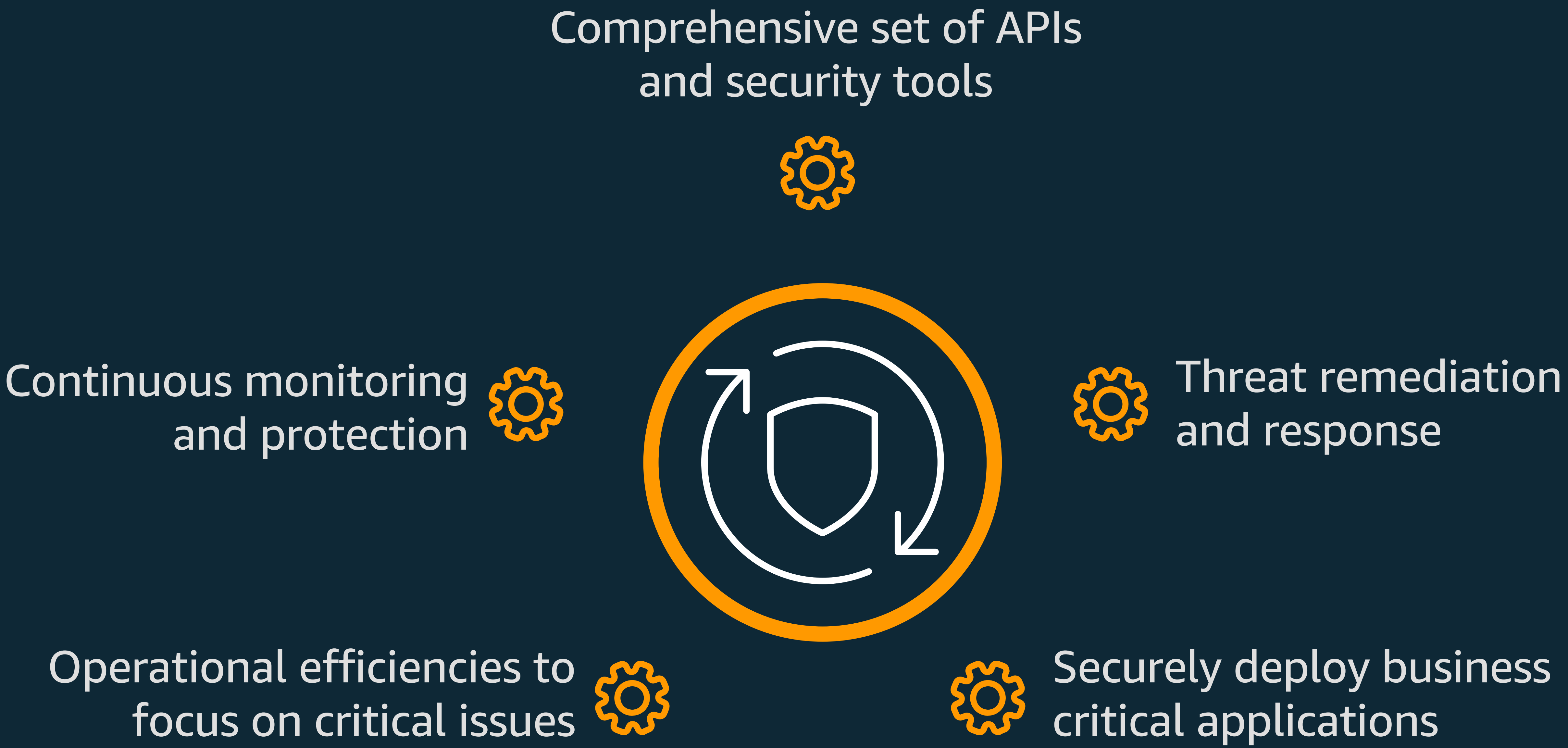
Encryption at scale
with keys managed by our AWS Key Management Service (KMS) or managing your own encryption keys with AWS CloudHSM using FIPS 140-2 Level 3 validated HSMs

Comply with local data privacy laws
by controlling who can access content, its lifecycle, and disposal

Access services and tools that enable you to **build compliant infrastructure** on top of AWS

Security Services

Automate and reduce risk with integrated services



Comprehensive set of APIs and security tools

Continuous monitoring and protection

Threat remediation and response

Operational efficiencies to focus on critical issues

Securely deploy business critical applications

AWS security, identity, and compliance solutions

Identity & access management

- AWS Identity & Access Management (IAM)
- AWS Single Sign-On
- AWS Organizations
- AWS Directory Service
- Amazon Cognito
- AWS Resource Access Manager

Detection

- AWS Security Hub
- Amazon GuardDuty
- Amazon Inspector
- Amazon CloudWatch
- AWS Config
- AWS CloudTrail
- VPC Flow Logs

Infrastructure protection

- AWS Firewall Manager
- AWS Shield
- AWS WAF – Web application firewall
- Amazon Virtual Private Cloud (VPC)
- AWS PrivateLink
- AWS Systems Manager

Data protection

- Amazon Macie
- AWS Key Management Service (KMS)
- AWS CloudHSM
- AWS Certificate Manager
- AWS Secrets Manager
- AWS VPN
- Server-Side Encryption

Incident response

- Amazon Detective
- CloudEndure DR
- AWS Config Rules
- AWS Lambda

Identity & access management

Define, enforce, and audit user permissions across AWS services, actions, and resources

AWS Identity and Access Management (IAM)

Securely manage access to AWS services and resources

AWS Single Sign-On (SSO)

Centrally manage SSO access to multiple AWS accounts & business apps

AWS Directory Service

Managed Microsoft Active Directory in AWS

Amazon Cognito

Add user sign-up, sign-in, and access control to your web/ mobile apps

AWS Organizations

Policy-based management for multiple AWS accounts

AWS Resource Access Manager

Simple, secure service to share AWS resources

Detective controls

Gain the visibility you need to spot issues before they impact the business, improve your security posture, and reduce the risk profile of your environment

AWS Security Hub

Centrally view & manage security alerts & automate compliance checks

Amazon GuardDuty

Intelligent threat detection and continuous monitoring to protect your AWS accounts and workloads

Amazon Inspector

Automates security assessments to help improve the security and compliance of applications deployed on AWS

Amazon CloudWatch

Complete visibility of your cloud resources and applications to collect metrics, monitor log files, set alarms, and automatically react to changes

AWS Config

Record and evaluate configurations of your AWS resources to enable compliance auditing, resource change tracking, & security analysis

AWS CloudTrail

Track user activity and API usage to enable governance, compliance, and operational/risk auditing of your AWS account

VPC Flow Logs

Capture info about the IP traffic going to and from network interfaces in your VPC. Flow log data is stored using Amazon CloudWatch Logs

Infrastructure protection

Reduce surface area to manage and increase privacy for and control of your overall infrastructure on AWS

AWS Firewall Manager

Centrally configure and manage AWS WAF rules across accounts and applications

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 Virtual Private Cloud (VPC)

Provision a logically isolated section of AWS where you can launch AWS resources in a virtual network that you define

AWS PrivateLink

Access services hosted on AWS easily and securely by keeping your network traffic within the AWS network

AWS Systems Manager

Easily configure and manage Amazon EC2 and on-premises systems to apply OS patches, create secure system images, and configure secure operating systems

Data protection

In addition to our automatic data encryption and management services, employ more features for data protection

(including data management, data security, and encryption key storage)

Amazon Macie

Discover and protect your sensitive data at scale

AWS Key Management Service (KMS)

Easily create and control the keys used to encrypt your data

AWS CloudHSM

Managed hardware security module (HSM) on the AWS Cloud

AWS Certificate Manager

Easily provision, manage, and deploy SSL/TLS certificates for use with AWS services

AWS Secrets Manager

Easily rotate, manage, and retrieve database credentials, API keys, and other secrets through their lifecycle

AWS VPN

Extend your on-premises networks to the cloud and securely access them from anywhere

Server-Side Encryption

Flexible data encryption options using AWS service managed keys, AWS managed keys via AWS KMS, or customer managed keys

Incident response

During an incident, containing the event and returning to a known good state are important elements of a response plan. AWS provides the following tools to automate aspects of this best practice

Amazon Detective

Analyze and visualize security data to rapidly get to the root cause of potential security issues

CloudEndure Disaster Recovery

Fast, automated, cost-effective disaster recovery

AWS Config Rules

Create rules that automatically take action in response to changes in your environment, such as isolating resources, enriching events with additional data, or restoring configuration to a known-good state

AWS Lambda

Use our serverless compute service to run code without provisioning or managing servers so you can scale your programmed, automated response to incidents

Thank you!

Doug Pardue, Sr. Solutions Architect
wdpardue@amazon.com