PUBLIC SECTOR SYMPOSIUM

BRUSSELS | MARCH 28, 2023

BMT104

Meet Digital Sovereignty Requirements on AWS

Alex Meek-Holmes (he/they)
Senior Manager, Sovereignty and Strategic Infrastructure
AWS

Kathy Liu (she/her)
Sr Business Development Manager, Digital Sovereignty
AWS

Agenda

What is digital sovereignty

Our Sovereign-by-Design pillars

- Our capabilities today
- Our forward looking pledge

How we support local economies

Resources for you

What is Digital Sovereignty?

Digital Sovereignty themes

Data residency

Operator Access Restriction

Resiliency and Survivability and Independence

Data sovereignty

Operational sovereignty

Digital Sovereignty

Why is sovereignty important to you?

Do you have to follow regulations?

What other outcomes do you want to achieve in the Cloud?

Where to you want to be in the long term?

Control without Compromise

AWS Security Blog

AWS Digital Sovereignty Pledge: Control without compromise

by Matt Garman | on 27 NOV 2022 | in Announcements, Foundational (100), Security, Identity, & Compliance | Permalink |

Comments | Share

French | German | Indonesian | Italian | Japanese | Korean | Portuguese | Spanish

AWS Cloud is Sovereign-by-Design

We pledge to give our customers

1. Control over the location of your data

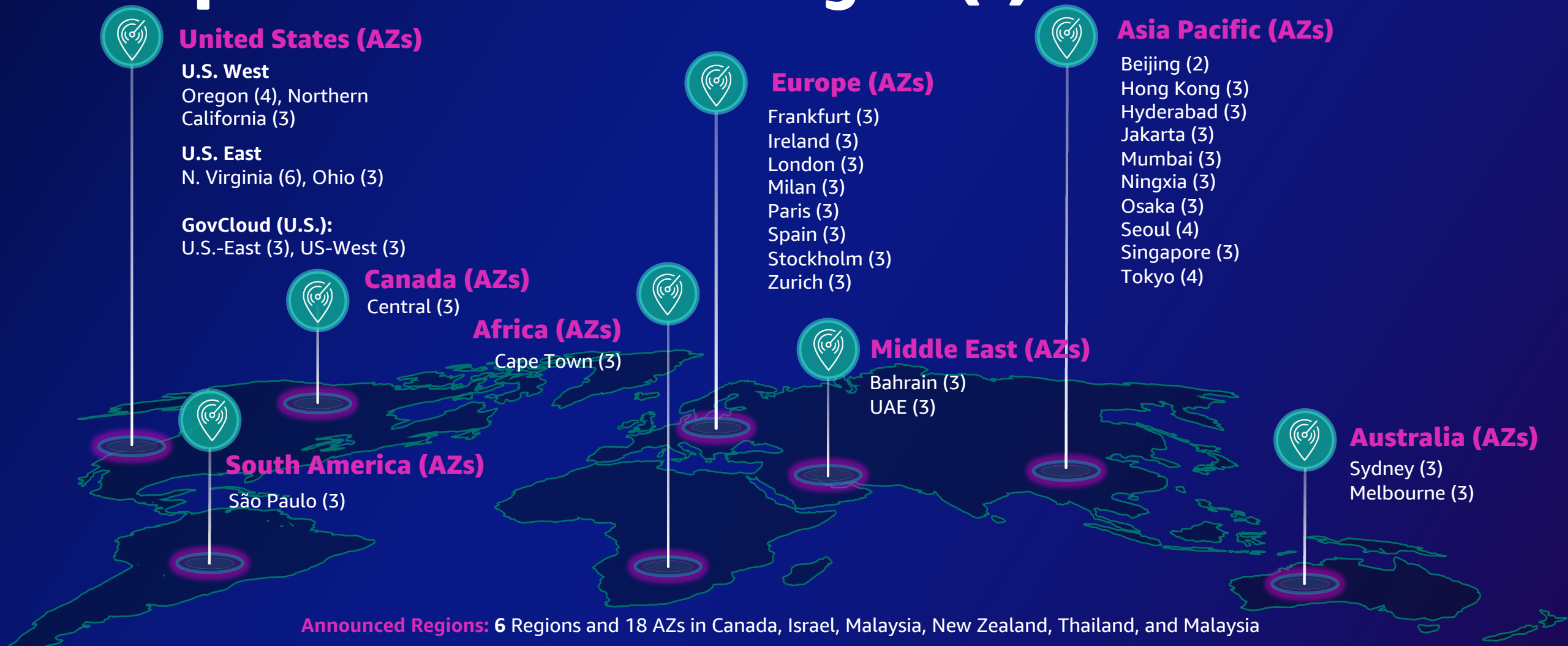
2. Verifiable control over data access

3. The ability to encrypt everything everywhere

4. Resilience of the Cloud

1. Control over the location of your data

Keep data in the AWS Region(s) selected



United States (AZs)

U.S. West
Oregon (4), Northern California (3)

U.S. East
N. Virginia (6), Ohio (3)

GovCloud (U.S.):
U.S.-East (3), US-West (3)

Canada (AZs)

Central (3)

Africa (AZs)

Cape Town (3)

South America (AZs)

São Paulo (3)

Europe (AZs)

Frankfurt (3)
Ireland (3)
London (3)
Milan (3)
Paris (3)
Spain (3)
Stockholm (3)
Zurich (3)

Middle East (AZs)

Bahrain (3)
UAE (3)

Asia Pacific (AZs)

Beijing (2)
Hong Kong (3)
Hyderabad (3)
Jakarta (3)
Mumbai (3)
Ningxia (3)
Osaka (3)
Seoul (4)
Singapore (3)
Tokyo (4)

Australia (AZs)

Sydney (3)
Melbourne (3)

Announced Regions: **6** Regions and 18 AZs in Canada, Israel, Malaysia, New Zealand, Thailand, and Malaysia

aws

AWS Local Zones – expand your data locality

North America

Atlanta
Boston
Chicago
Dallas
Denver
Houston
Kansas City
Las Vegas
Los Angeles
Miami
Minneapolis
New York City
Philadelphia
Phoenix
Portland
Seattle
Querétaro
Toronto
Vancouver

Europe and Africa

Hamburg
Copenhagen
Helsinki
Warsaw
Lagos
Amsterdam
Athens
Berlin
Brussels
Helsinki
Johannesburg
Lisbon
Munich
Nairobi
Oslo
Prague
Vienna

Asia Pacific

Delhi
Taipei
Bangkok
Kolkata
Bengaluru
Chennai
Delhi
Hanoi
Manila

Available
Announced

South America

Buenos Aires
Santiago
Lima
Bogotá
Rio de Janeiro

Australia and New Zealand

Perth
Auckland
Brisbane

Transparency in Privacy Features of AWS

AWS service	Customer can encrypt	Customer can delete	Customer can monitor processing	No remote access*
Alexa for Business	✓	✓	✓	✓
Amazon API Gateway	✓	✓	✓	✓
Amazon AppFlow	✓	✓	✓	✓
Amazon AppStream 2.0	✓	✓	✓	✓
Amazon AppStream 2.0 User Pools	✓	✓	✓	✓
Amazon Athena	✓	✓	✓	✓
Amazon Augmented AI (A2I)	✓	✓	✓	✓
Amazon Aurora	✓	✓	✓	✓
Amazon Braket	✓	✓	✓	✓
Amazon Chime	✓	✓	✓	✓
Amazon Cloud Directory	✓	✓	✓	✓
Amazon CloudFront	✓	✓	✓	✓
Amazon CloudWatch	✓	✓	✓	✓
Amazon CloudWatch Logs	✓	✓	✓	✓
Amazon CodeGuru Profiler	✓	✓	✓	✓

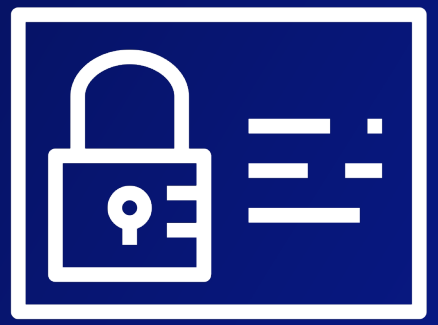
https://aws.amazon.com/compliance/privacy-features/

Assurance on data residency

The CISPE Code requires cloud infrastructure service providers to give customers the **choice** to use services to **store and process customer data exclusively in the European Economic Area (EEA).**

Inherit global security and compliance controls

AWS Control Tower Guardrails



Guardrails to provide more control over the physical location of where customer data is stored and processed.

AWS Digital Sovereignty Pledge:

We will expand data residency controls for operational data, such as identity and billing information.

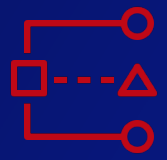
2. Verifiable control over data access

"We prohibit -- and our systems are designed to prevent -- remote access by AWS personnel to customer data for any purpose, including service maintenance, unless that access is requested by you or unless access is required to prevent fraud and abuse, or to comply with law."

AWS

Tools and services to help you monitor access

AWS Identity and Access Management (IAM)

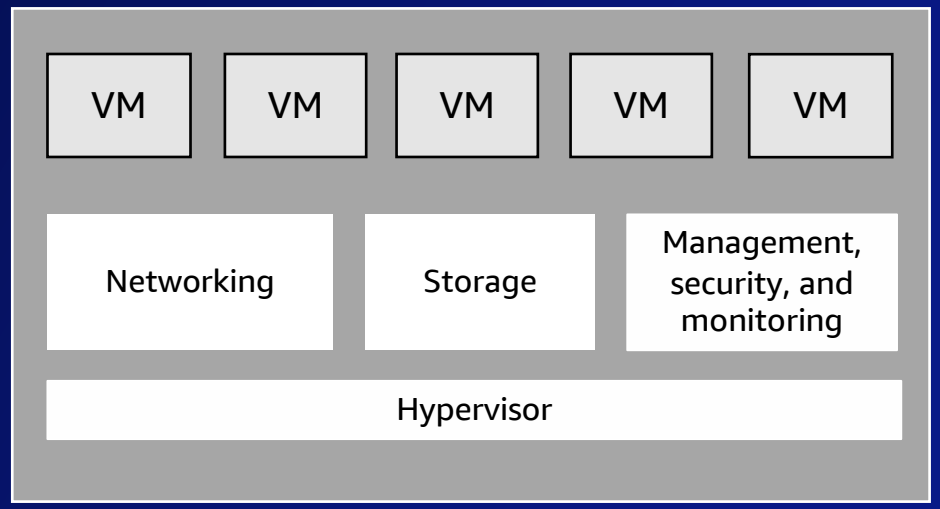


AWS IAM Access Analyzer

AWS CloudTrail

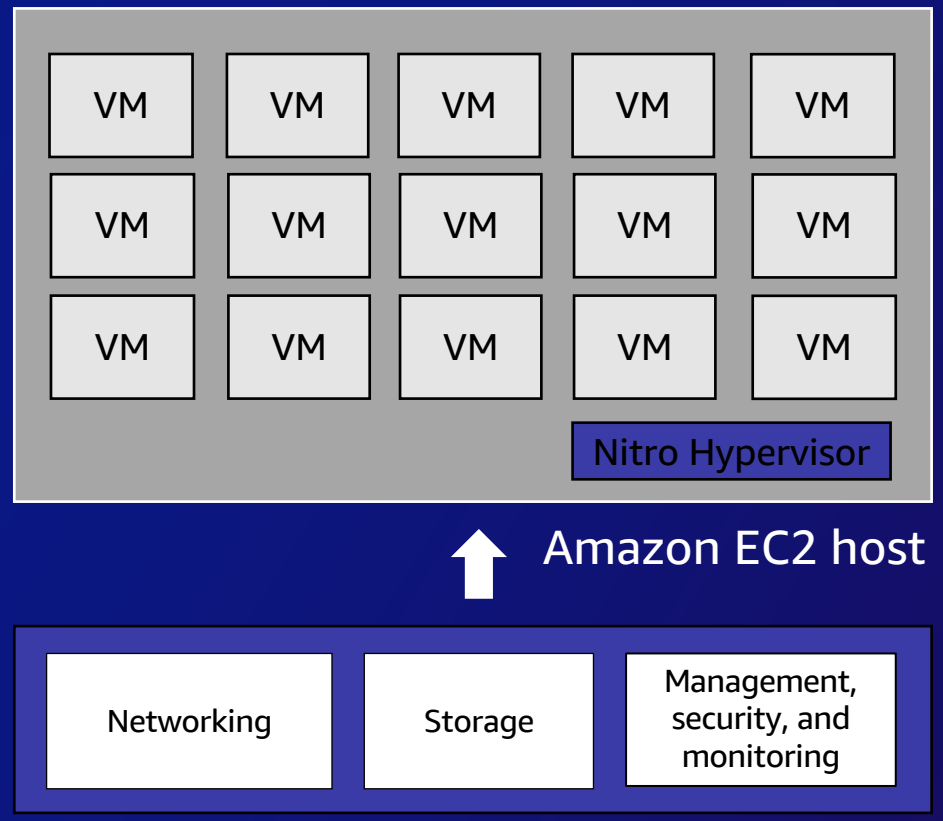
Amazon CloudWatch

Reinventing virtualization with AWS Nitro



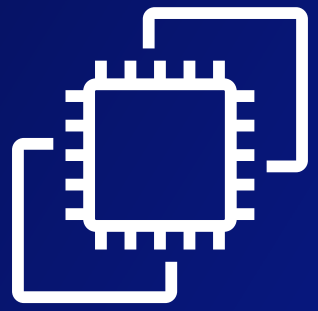
Host

Classical virtualization



AWS Nitro System

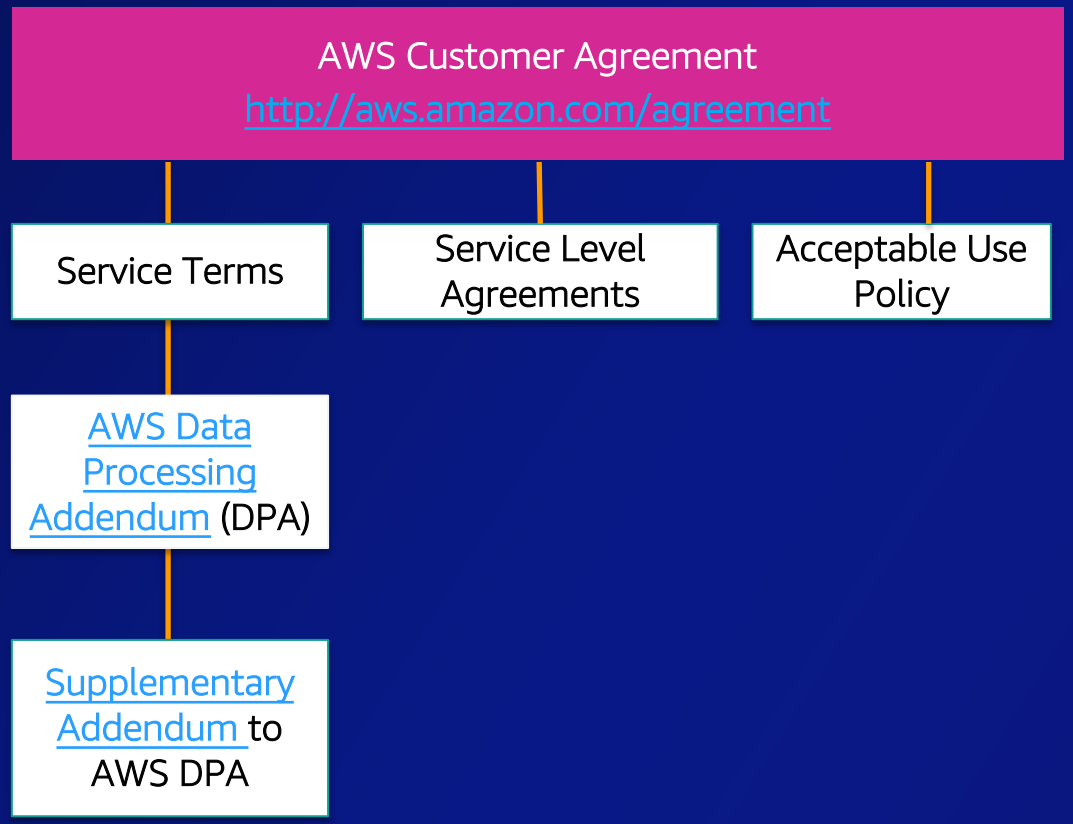
The Nitro Approach: Protection from cloud operators



AWS Nitro System

- No operator access
- No ability to read the memory of EC2 instances
- No access to any data stored on instance storage and encrypted EBS volumes.
- Maintenance carried out using a strictly limited set of authenticated, authorized, and audited administrative APIs, with cannot access customer data on the EC2 server
- No AWS operator can bypass these controls and protections

Earning trust through contractual commitments



AWS challenges law enforcement requests that are overbroad, or where we have any appropriate grounds to do so.

Earning trust through organizational transparency

AWS published bi-annual Information Request Report (IRR) describing the types and number of information requests AWS receives from law enforcement.

0

Request

Resulted in the disclosure to the U.S. government of enterprise content or government content data located outside the United States since we started to collect this datapoint in July 2020.

AWS Digital Sovereignty Pledge:

We commit to continue to build additional access restrictions that limit all access to customer data unless requested by the customer or a partner they trust.

3. The ability to encrypt everything everywhere

Power of AWS KMS and CloudHSM

AWS Key Management Service (AWS KMS)

AWS CloudHSM

Ability to encrypt all your data, whether in transit, at rest, or in memory.

All services support encryption with customer managed keys that are inaccessible to AWS.

SOC 1 - Control 4.5: *Customer master keys used for cryptographic operations in AWS KMS are logically secure so that no single AWS employee can gain access to the key material.*

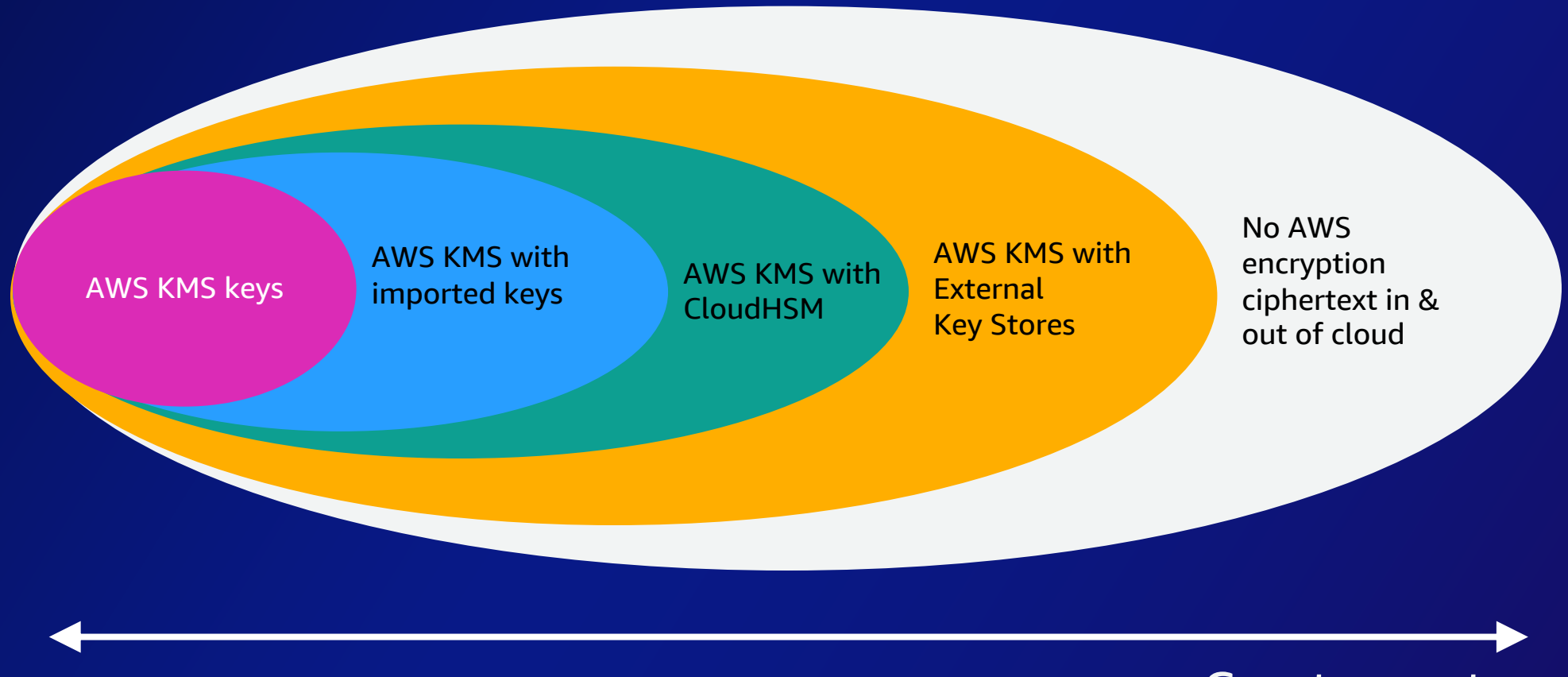
AWS Digital Sovereignty Pledge:

We commit to continue to innovate and invest in additional controls for sovereignty and encryption features so that our customers can encrypt everything everywhere with encryption keys managed inside or outside the AWS Cloud.

More options to control the key: AWS KMS External Key Store (XKS)

- Full removal of root of trust from AWS KMS
- Transparent to AWS services and client apps
- Flexibility on which keys you choose to store in external key manager
- Customer owns the key in meaningful ways Serves as “kill switch”: Turn off XKS & AWS data becomes unreadable

Control without compromising on performance



Working with partners

Vendor support for AWS KMS XKS

Navigating change as a team

Our trusted partners play a prominent role in bringing solutions to customers.

AWS Partner Programs
- Authority to Operate (ATO) on AWS
- AWS ClearStart

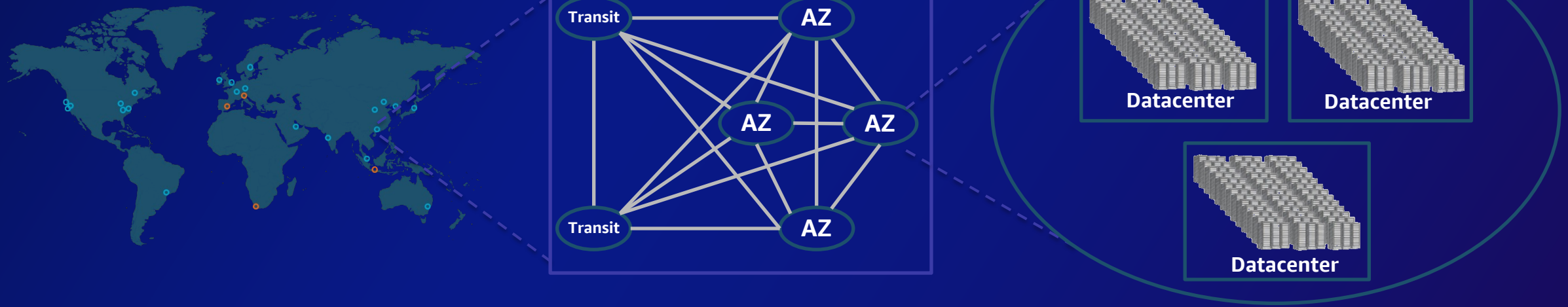
AWS Partner Competencies
- AWS Managed Security Service Provider
- AWS Security Competency

Partnership Examples
- T-Systems (part of Deutsche Telekom) Data Protection as a Managed Service

4. Resilience of the cloud

Designed for resilience

AWS Regions are comprised of multiple AZs for **high availability, high scalability**, and high **fault tolerance.** Applications and data are replicated in real time and consistent in the different AZs. We use **statically stable** designs



A Region is a physical location in the world where we have multiple **Availability Zones.**

Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in separate facilities.

Meet customers where they are, physically and technologically

GLOBAL

AWS Regions

METRO CENTERS

AWS Local Zones

Amazon CloudFront

5G NETWORKS

AWS Wavelength

ON-PREMISES

AWS Outposts

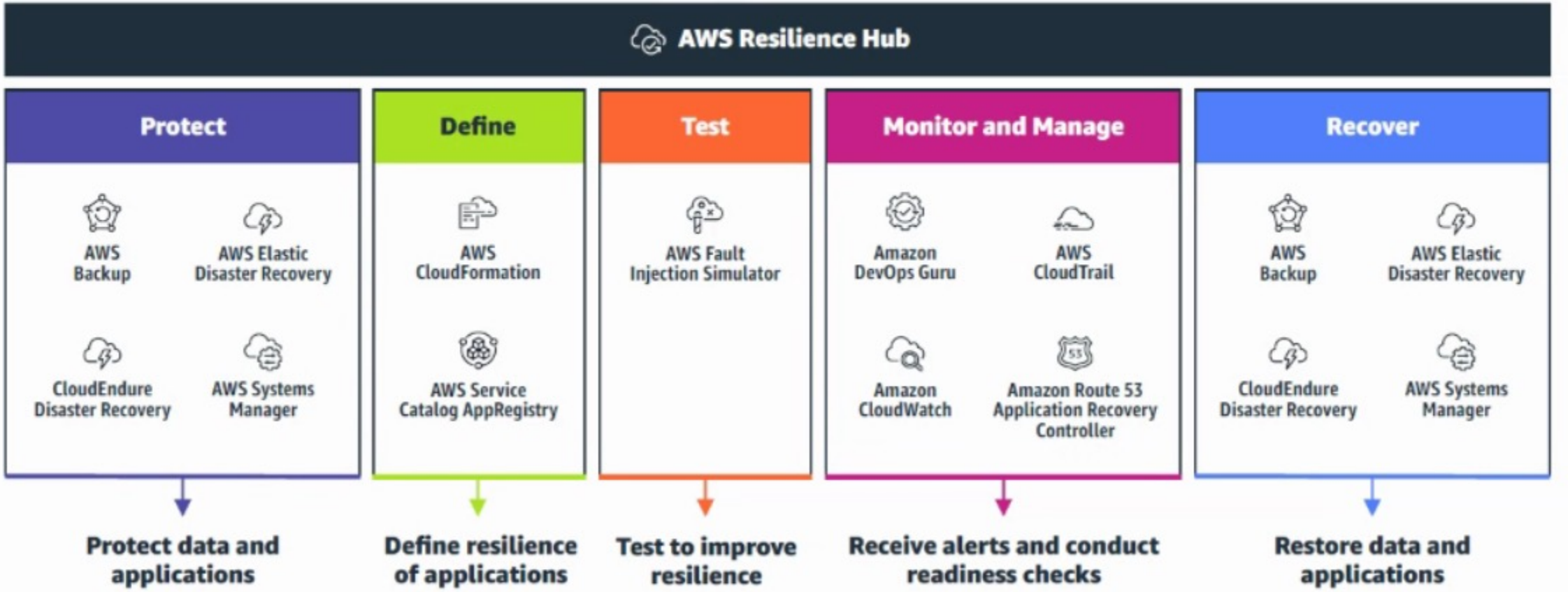
SMART DEVICES

Internet of Things

RUGGED EDGE

AWS Snow Family

How AWS helps you design resilient workloads



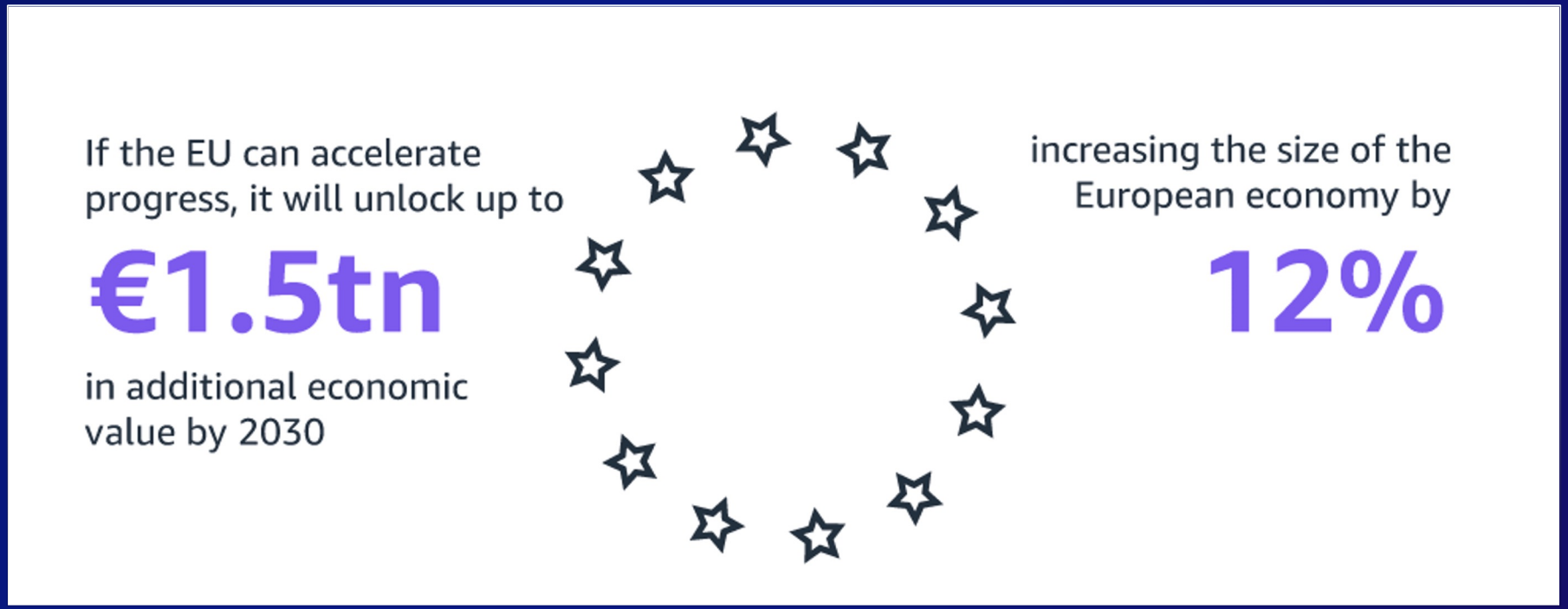
AWS Digital Sovereignty Pledge:

We commit to continue to enhance our range of sovereign and resilient options, allowing customers to sustain operations through disruption or disconnection.

Supporting local economy

Supporting European's Digital Growth

Achieving the Digital Decade goals could unlock **over €2.8 trillion in economic value**. This is equivalent to 21% of the EU's current economy. We estimate that a **majority (55%)** of this potential economic value is reliant on **cloud computing.**



Source: Unlocking Europe's Digital Potential: https://awsdigitaldecade.publicfirst.co.uk/

Supporting European businesses and jobs

Source: The Impact of AWS in the UK in 2020: https://awsimpactreport.publicfirst.co.uk/

Supporting local values and initiatives

Further resources

Learn more:

AWS Digital Sovereignty Pledge: Control Without Compromise [Blog]

AWS landing pages for data protection, GDPR center, and AWS Compliance [Landing page]

The Security Design of the AWS Nitro System [Whitepaper]

Announcing AWS KMS External Key Store (XKS) [Blog]

AWS cloud services adhere to CISPE code [Blog]

AWS Control Tower Data Residency Guardrails [Page]

Navigating Compliance with EU Data Transfer Requirements [Whitepaper]

New Standard Contractual Clauses now part of the AWS GDPR Data Processing Addendum for customers [Blog]

Summary

Summary

- Think long-term
- Do not compromise with temporary solutions
- Ask what outcomes are important to you
- Don’t miscalculate the risk!

Thank you!

Please complete the session survey in the mobile app

Alex Meek-Holmes
alexholmes24

Kathy Liu