
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

WPS203

Navigating sovereignty and data protection with AWS

Alex Holmes (he/him)

Senior Manager, Sovereignty and Strategic Infrastructure
AWS

Paul Ahlgren (he/him)

Principal Security Strategist
AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Introduction – sovereignty and data protection

Security baselines

Common questions

Resources available

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Digital sovereignty and data protection

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Digital sovereignty



Data residency

I want to know where all my data is, and control where that data is stored and transferred to at all times.



Operator Access Restriction

I want to be sure that neither AWS nor a foreign government can access my data in the cloud.



Resiliency

I want to be sure that I can sustain operations despite any kind of instability.



Operational Autonomy

I want to be sure that I can operate autonomously despite significant foreign disruption or influence.

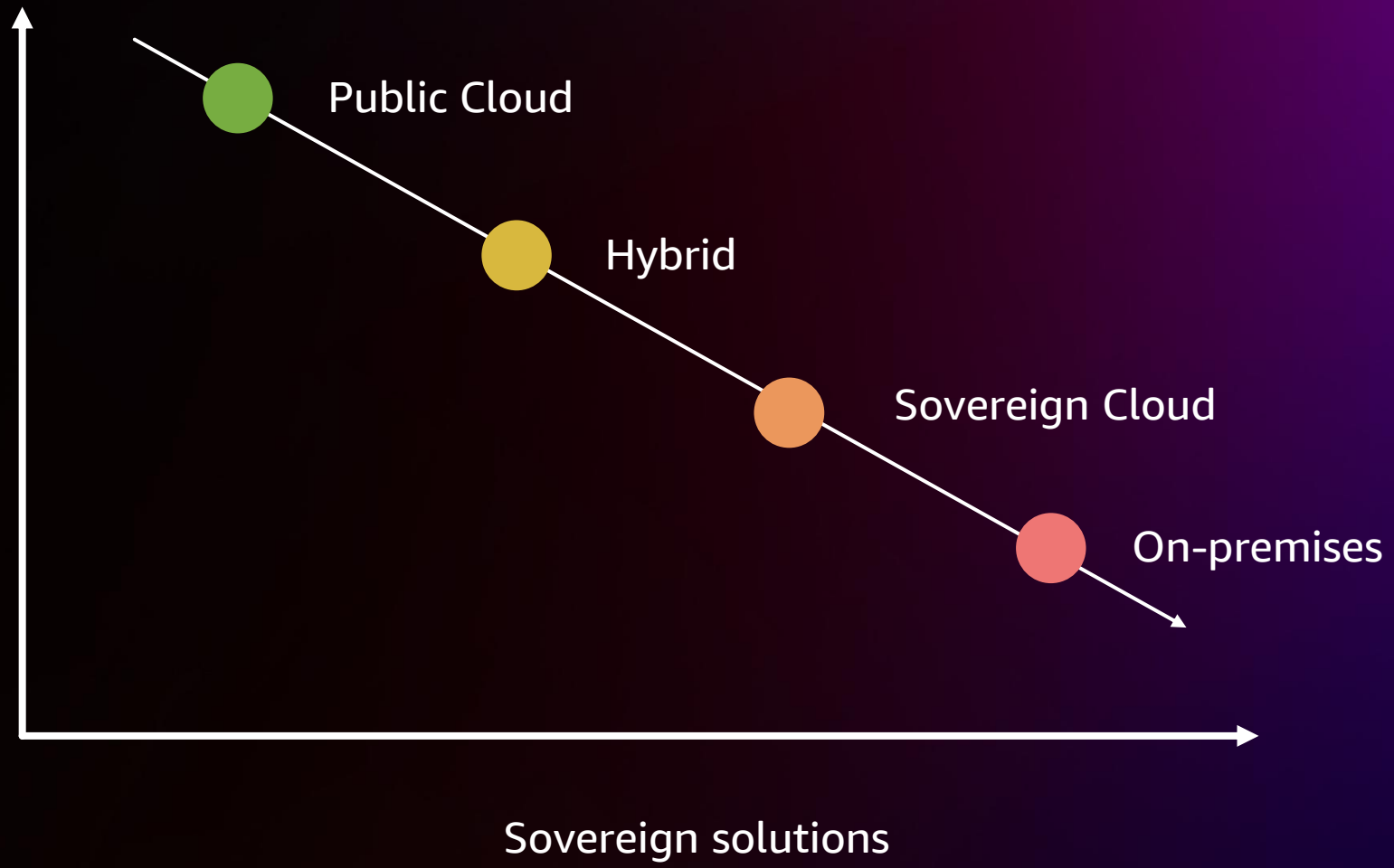
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cloud benefits vs. sovereignty solutions

Cloud benefits:

- Price
- Scalability
- Resiliency
- Elasticity
- Pace of innovation
- Security



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Customers want sovereignty without compromising the full breadth and depth of the cloud

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sovereign-by-design

An AWS Approach

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

1. Control over the location of your data

2. Verifiable control over data access



3. The ability to encrypt everything everywhere

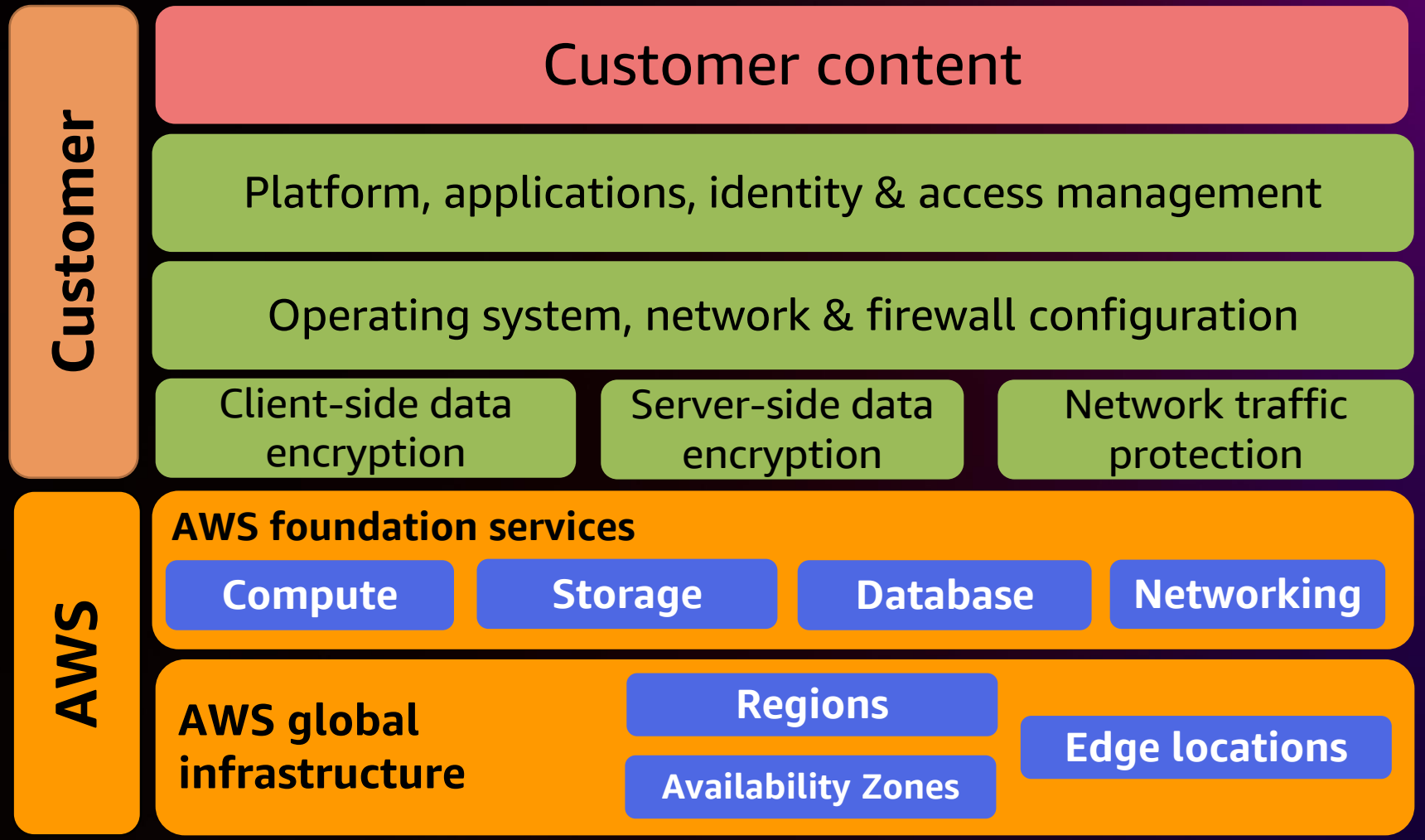
4. Resilience of the cloud

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Shared responsibility model

Customers are responsible for **their** security and compliance **IN** the cloud

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



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Technical tools and services

Data encryption

Services such as AWS CloudHSM and AWS KMS allow you to securely generate and manage encryption keys

AWS Identity and Access Management (IAM) and AWS Control Tower

IAM allows customers to securely manage access to AWS services and resources, including limiting access to services in specific Regions. AWS Control Tower data residency guardrails help ensure no customer data is stored or processed outside a specific AWS Region or Regions.

Monitoring and logging

Services like AWS CloudTrail and Amazon CloudWatch deliver monitoring and logging capabilities for access control

Amazon Macie

Amazon Macie uses pattern matching and machine learning to detect personally identifiable information – including unencrypted information – to discover and protect sensitive data in Amazon S3 buckets

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Certifications and attestations















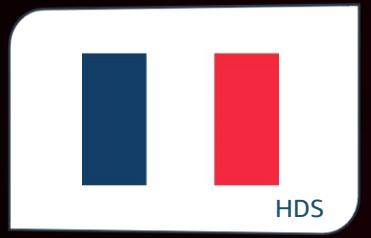


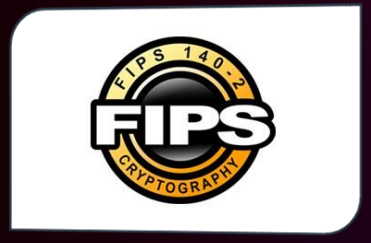












aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Partner Network and Programs

Authority to Operate (ATO)

Helps AWS Partners meet their customers' authorization needs, whether it be architecting, configuring, deploying, or integrating tools and controls

AWS Managed Security Service Providers (MSSP)

Full outsourcing or integrate and join forces with your internal security teams to help you fully operationalize your AWS security

AWS Security Competency Partners

Software and service engagements to help customers elevate their security in the cloud

Data Protection as a Managed Service

In Germany, T-Systems (part of Deutsche Telekom) offers Data Protection as a Managed Service on AWS

AWS ClearStart

In Sweden, AWS ClearStart helps public sector organizations meet their security and regulatory needs through partners such as Atea, Capgemini, Cybercom, Nordcloud, and SecureAppbox

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Frequently asked questions

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

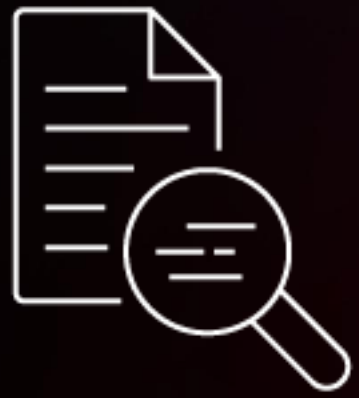
Q1: Can the U.S. government see my data?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Contractual commitments



Challenge law enforcement requests that are overbroad, or where we have any appropriate grounds to do so, including where the request conflicts with EU law



Bi-annual Information Request Report describing the types and number of information requests AWS receives from law enforcement

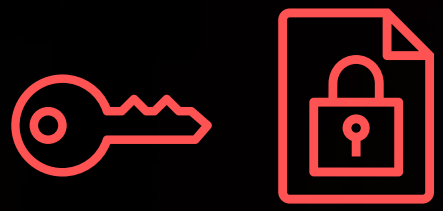
0

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

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Encryption everywhere



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



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



AWS Key Management Service (AWS KMS)



AWS CloudHSM

AWS KMS, CloudHSM, and XKS (NEW!) provide customers the ability to manage their keys and encrypt all their data to meet regulatory requirements

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Can AWS see my keys?

- **Keys never exist in plaintext outside the HSM**
- **When operational with keys provisioned**
  - No AWS operator can access the HSM (no human interfaces)
  - No software updates allowed (must tear down HSM to blank)
- **After reboot and in a non-operational state**
- No key material on host
- Software can only be updated after multiple AWS employees have reviewed the code
  - Under quorum of multiple AWS KMS operators with valid credentials
- Third-party evidence
- SOC 1 – Control 4.5: *Customer master keys used for cryptographic operations in AWS KMS are logically secured so that no single AWS employee can gain access to the key material*



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS 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.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Q2: Can I be compliant with data protection laws and other regulations if I use AWS?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security standards and compliance certifications

AWS supports more security standards and compliance certifications than any other offering, including FedRAMP, GDPR, C5, CISPE, and NIST 800-171, helping customers satisfy compliance requirements for virtually every regulatory agency around the globe

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Sovereignty Pledge:

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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Q3: Can AWS access customer data?

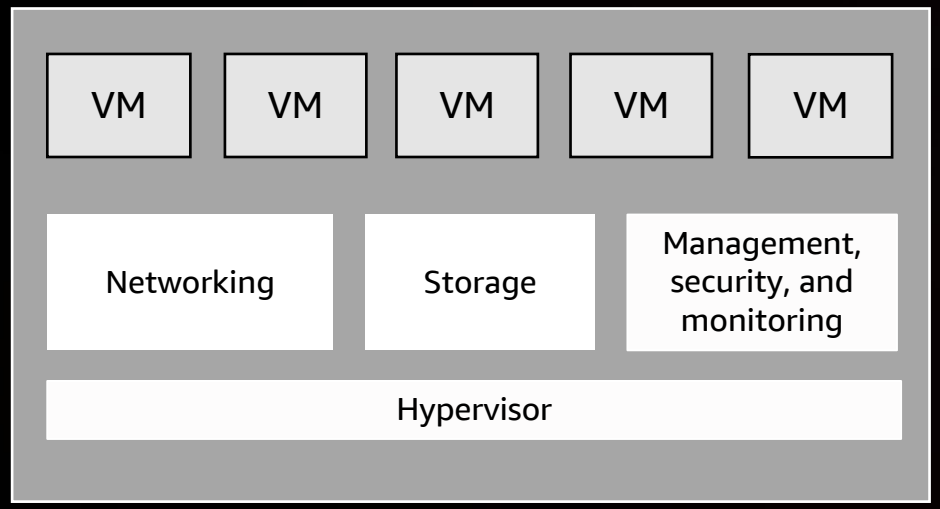
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Access to data

AWS prohibits – and its systems are designed to prevent – remote access by AWS personnel to customer data for any purpose, including service maintenance, unless access is requested by customers, is required to prevent fraud and abuse, or to comply with law

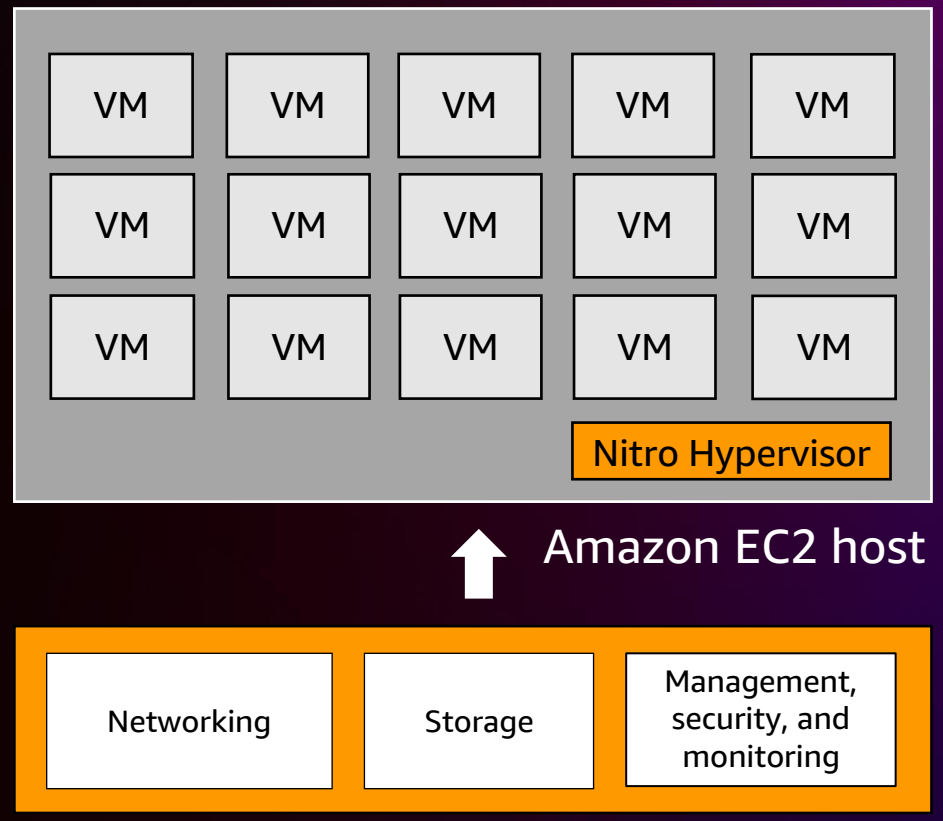
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Reinventing virtualization for the cloud



Host

Classical virtualization

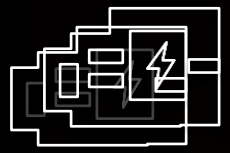


AWS Nitro System

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

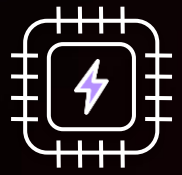
AWS Nitro System

Nitro Cards



- Local NVMe storage
- Elastic block storage
- Networking, monitoring, and security

Nitro Security Chip



- Integrated into motherboard
- Protects hardware resources

Nitro Hypervisor



- Lightweight hypervisor
- Memory and CPU allocation
- Bare metal-like performance

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

New! *The Security Overview of the AWS Nitro System* whitepaper

- Detailed review of the security design of the three primary components of the AWS Nitro System:
  - Nitro Cards,
  - Nitro Security Chip
  - Nitro Hypervisor
- Deep dive on the AWS Nitro System integrity protections, tenant isolation model, and no operator access design



https://a.co/hYWhsH9

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Sovereignty Pledge:

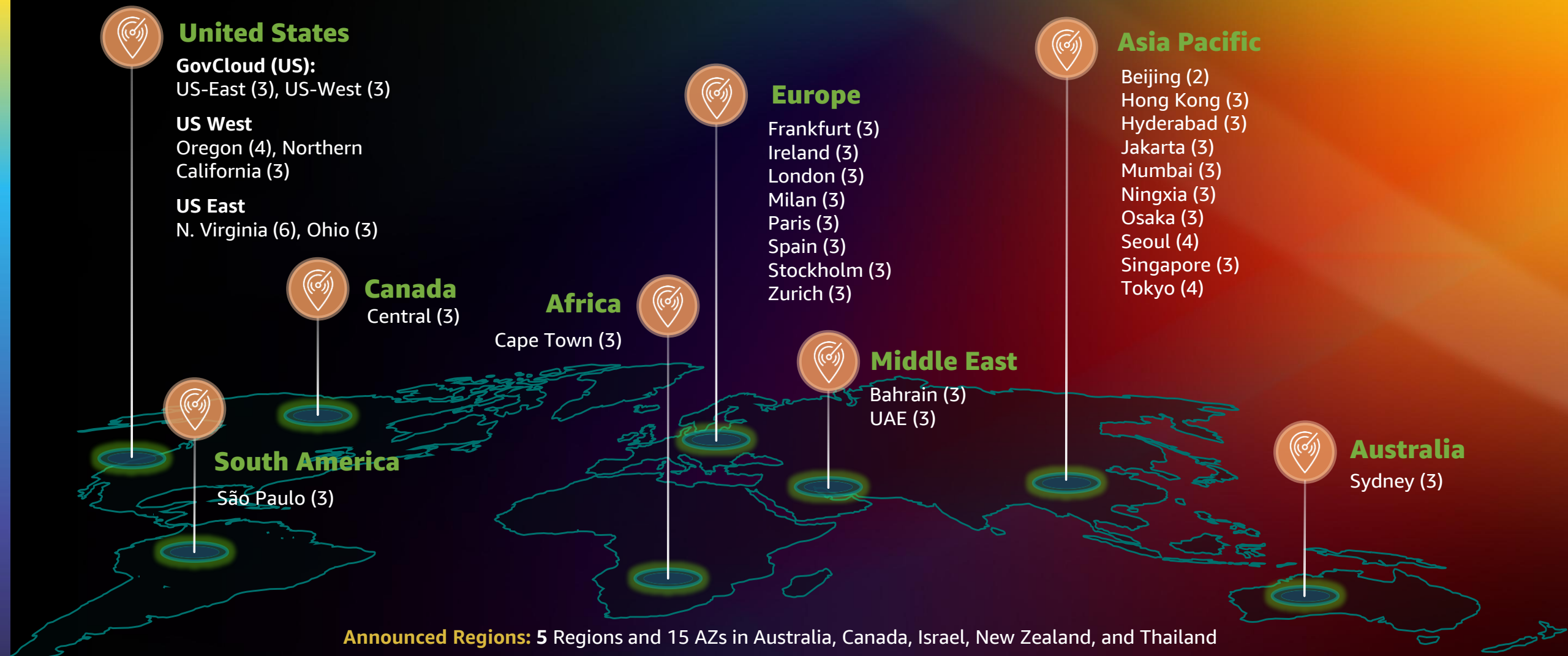
We commit to continue to build additional access restrictions that limit all access to customer data unless requested by the customer or a partner they trust.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Q4: Where is my data and who can move it?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Global AWS Regions and Availability Zones



Announced Regions: **5** Regions and 15 AZs in Australia, Canada, Israel, New Zealand, and Thailand

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy features of AWS

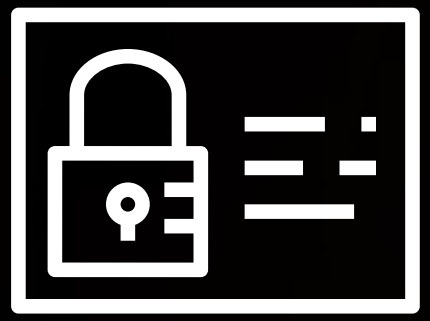
AWS service	Customer can encrypt	Customer can delete	Customer can monitor processing	No remote access*
Alexa for Business	✓	✓	✓	✓
Amazon API Gateway	✓	✓	✓	✓
Amazon AppFlow	✓	✓	✓	✓

AWS services that allow customers to opt-out of transfers of customer data

AWS services that transfer customer data as an essential function of the service

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Control Tower



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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Sovereignty Pledge:

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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

In summary



Technical measures



Process measures



Contractual measures

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resources

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resources

Read our related blogs, whitepapers & other helpful online resources

- **Confidential computing: An AWS perspective**
  - https://aws.amazon.com/blogs/security/confidential-computing-an-aws-perspective/
- **AWS achieves ISO 27701 compliance**
  - https://aws.amazon.com/blogs/security/aws-achieves-iso-iec-27701-2019-certification/
- **AWS Cloud services adhere to CISPE code**
  - https://aws.amazon.com/blogs/security/aws-cloud-services-adhere-to-cispe-data-protection-code-of-conduct/
- **AWS Contractual Agreements**
  - https://aws.amazon.com/blogs/security/aws-and-eu-data-transfers-strengthened-commitments-to-protect-customer-data/
- **AWS Nitro Security Whitepaper**
  - https://a.co/hYWhsH9
- **AWS Control Tower Data Residency Guardrails**
  - https://aws.amazon.com/about-aws/whats-new/2021/11/aws-control-tower-controls-data-residency-requirements/

Visit Data Protection Hub | Data Protection and EU Data Protection webpages

- Data Protection: https://aws.amazon.com/compliance/data-protection/
- EU Data Protection: https://aws.amazon.com/compliance/eu-data-protection/

Visit our updated Data Privacy Center and GDPR Center

- Data Privacy Center: https://aws.amazon.com/compliance/data-privacy/
- GDPR Center: https://aws.amazon.com/compliance/gdpr-center/

Check out the updated Privacy features of AWS services and subprocessor webpages for information on data transfers (customer content)

- Privacy features: https://aws.amazon.com/compliance/privacy-features/
- Sub-processor: https://aws.amazon.com/compliance/sub-processors/
- Bi-annual Amazon Information Requests: https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Read our AWS Digital Sovereignty Pledge

Matt Garman, SVP at AWS

https://aws.amazon.com/blogs/security/aws-digital-sovereignty-pledge-control-without-compromise/

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Alex Meek-Holmes
Twitter: alexholmes24

Paul Ahlgren



Please complete the session survey in the **mobile app**

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.