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

SEC205

Meeting digital sovereignty requirements on AWS

David Woodhouse

Principal Engineer, AWS Digital Sovereignty
AWS

Luis Wang

Sr. Manager, Product Management, EC2
AWS

Agenda

What is digital sovereignty?

Existing approaches in the market

Cloud benefits vs. sovereignty tradeoffs

AWS approach to digital sovereignty

Transparency and Assurance

Local Trusted Partners

Closing

What is digital sovereignty?

80%

of organizations in Europe considered digital sovereignty to be the highest priority for their boards.

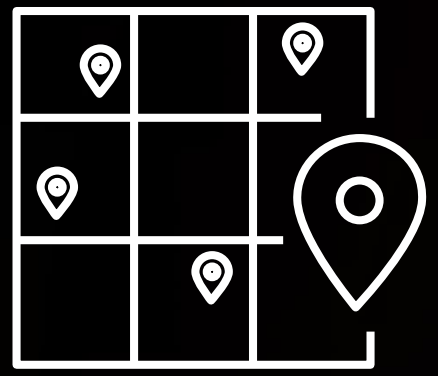
January *2022 IDC worldwide CEO survey*

60%

of organizations in Europe believe digital sovereignty increases the cost of doing business globally.

Europe's Quest for Digital Independence, IDC, May 2022

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 and Survivability

I want to be sure that I can sustain operations despite any kind of foreign disruption and influence.

Independence

We want our digital industries and sectors to thrive and compete at the global level.

Three approaches in the market

On-Premise

Some customers are choosing to hold back innovation on global cloud platforms, stalling projects or deploying internally.

Hybrid

Some customers are splitting workloads across public cloud and on-premises.

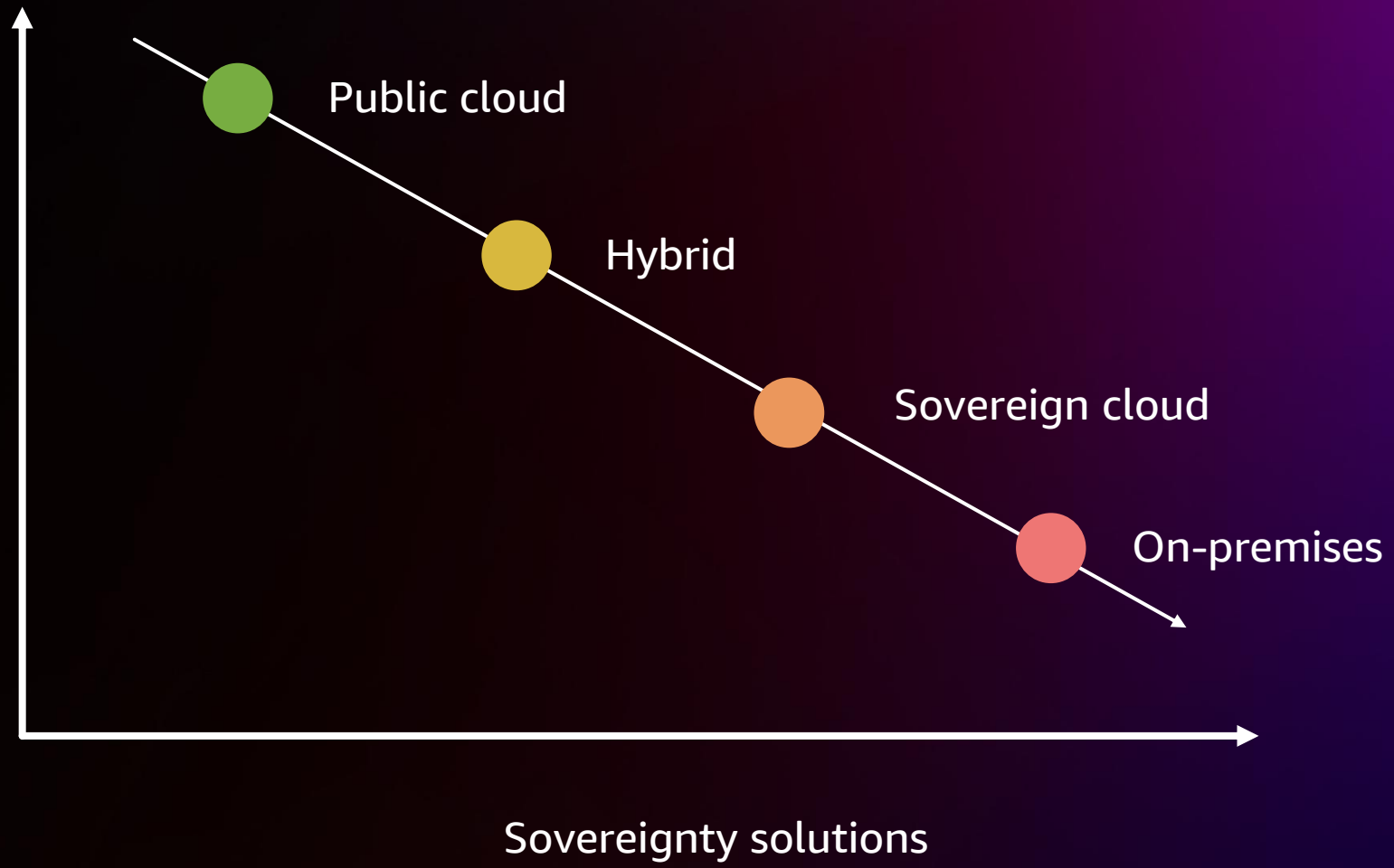
Sovereign Cloud

Some public cloud providers promise to deliver dedicated sovereign clouds in the future.

Cloud benefits vs. sovereignty solutions

Cloud benefits:

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



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

AWS Cloud is sovereign by design

Data Residency Controls

Transparency & Assurances

Operator Access Restriction

Trusted Local Partners

Encryption Everywhere

Resiliency in the Cloud

Data residency

Largest global infrastructure footprint

410+

400+ Edge Locations and 13 Regional Edge Caches

96

Availability Zones

30

Launched Regions
Each with 3 or more Availability Zones

AWS Control Tower

- **Preventive controls (service control policies)**
  - Ensure that your accounts maintain compliance because controls disallow actions that lead to policy violations
- **Detective controls (now powered by AWS Security Hub)**
  - Detect noncompliance and security risks in existing resources in line with AWS Foundational Security Best Practices
- **NEW! Proactive controls (CloudFormation Guard)**
  - Policies are automatically enforced on all CloudFormation deployments

AWS Control Tower – data residency controls

Four

preventative guardrails

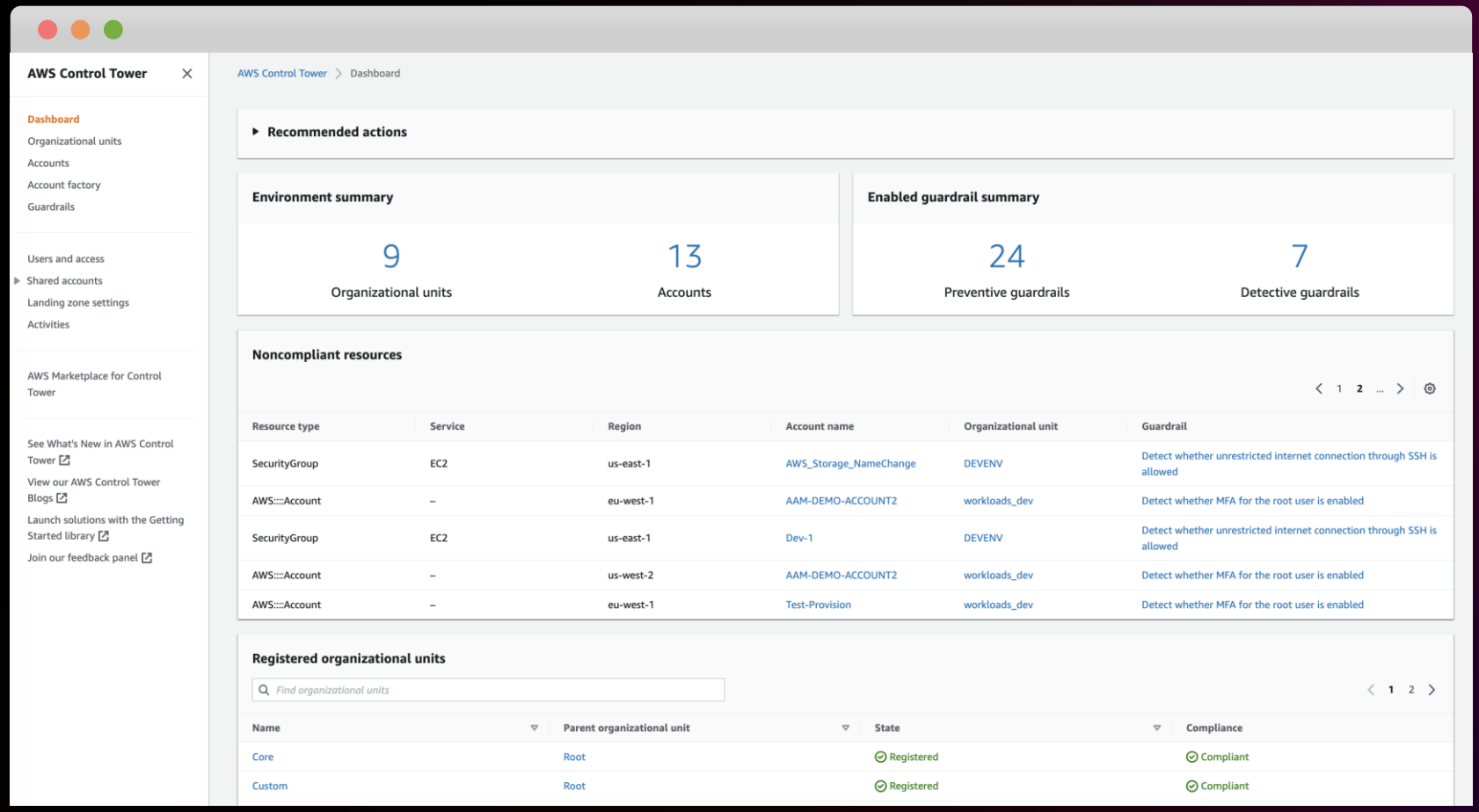
- Deny access to services and operations in selected AWS Regions
- Disallow internet access for an Amazon VPC instance
- Disallow Amazon Virtual Private Network (VPN) connections
- Disallow cross-Region networking for Amazon EC2, Amazon CloudFront, and AWS Global Accelerator

Thirteen

detective guardrails

- Range from detecting whether replication instances for AWS Database Migration Service (AWS DMS) are public to detecting whether any Amazon VPC subnets are assigned a public IP address
- Implemented via AWS Config

Single pane of glass via AWS Control Tower



AWS Digital Sovereignty Pledge

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

Operator access restrictions

Zero privilege operations

Data handling best practices
Categorizing types of data and training employees on secure data handling practices

Always-on accountability
Every action taken by any operator is securely recorded in a manner that cannot be evaded or deleted

Contingent authorization
No one person or system should be a single point of failure for security

Hermetic systems
No general purpose or interactive access, and by design no means to disclose data

AWS Nitro System

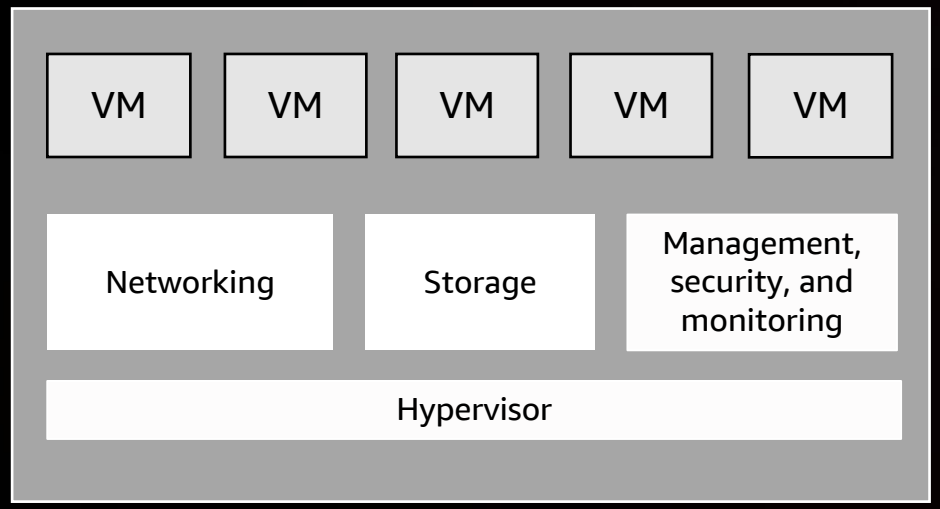
AWS Lambda

AWS KMS

ACM for Nitro Enclaves

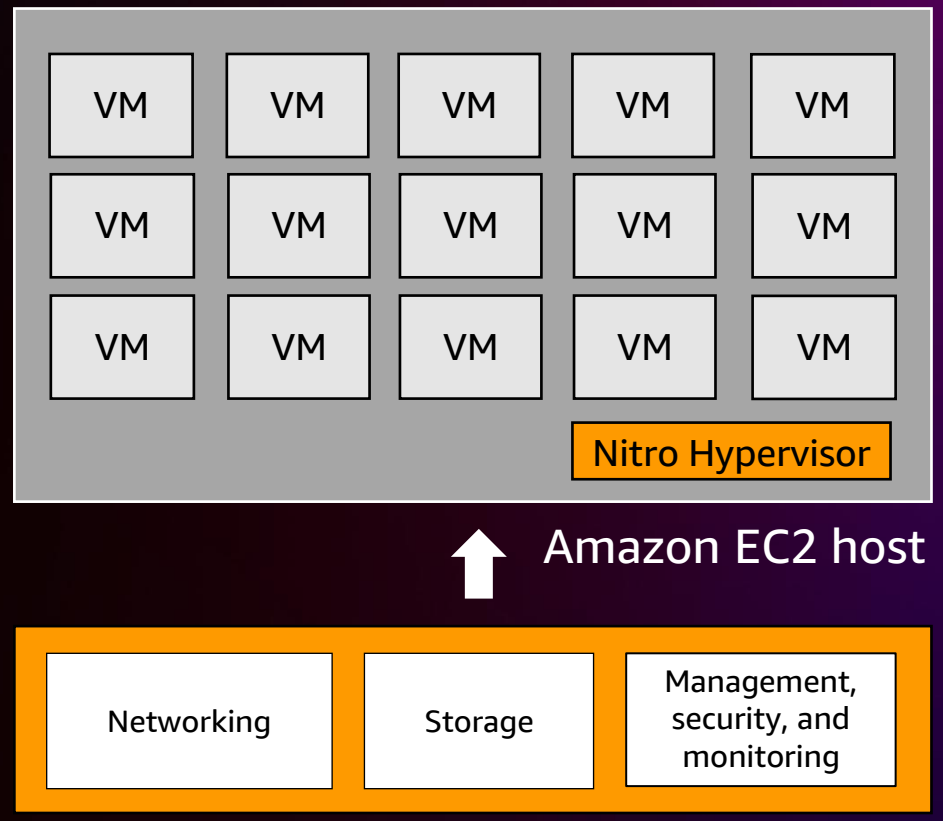
AWS Nitro System

Reinventing virtualization for the cloud



Host

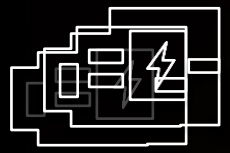
Classical virtualization



AWS Nitro System

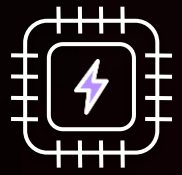
AWS Nitro System

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

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

- Detailed review of the security design 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

What is AWS Nitro Enclaves?

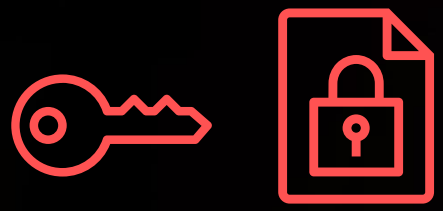
Nitro Enclaves provides additional isolation for data in use

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.

Encryption everywhere

Encryption everywhere



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

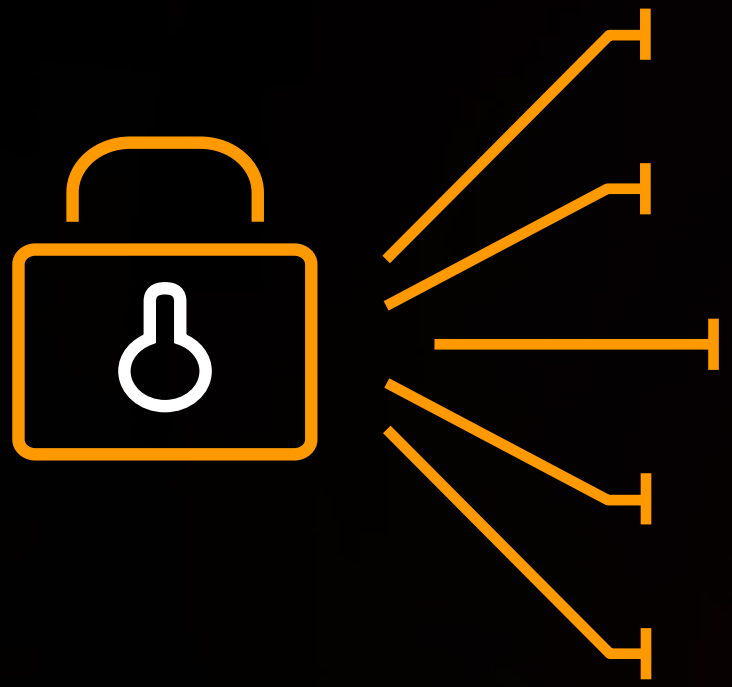
All services support encryption. Most services support encryption with customer managed keys that are inaccessible to AWS

AWS Key Management Service (AWS KMS)

AWS CloudHSM

AWS KMS, CloudHSM and the new XKS feature in KMS provide customers the ability to manage their keys and encrypt all their data to meet regulatory requirements

AWS Cryptography Stack



Physical layer	Secure facilities and optical encryption using AES-256
Data link layer	MACsec AES-256 (IEEE 802.1AE)
Network layer	VPC Encryption | Cross-Region Peering | Amazon VPN
Transport layer	Amazon s2n | NLB-TLS | ALB | CloudFront | ACM integration
Application layer	AWS Crypto SDK | Server-side encryption with KMS integration | Memory encryption

Customer selects these options

What is AWS KMS?

- AWS KMS lets you create, manage, and control cryptographic keys across your applications
- Scales to any workload (50,000 TPS) with low latency and 99.999% public SLA
- All sensitive key operations protected inside FIPS 140 certified fleet of HSMs
- AWS KMS is incorporated in over 100 AWS services to encrypt sensitive data and create digital signatures

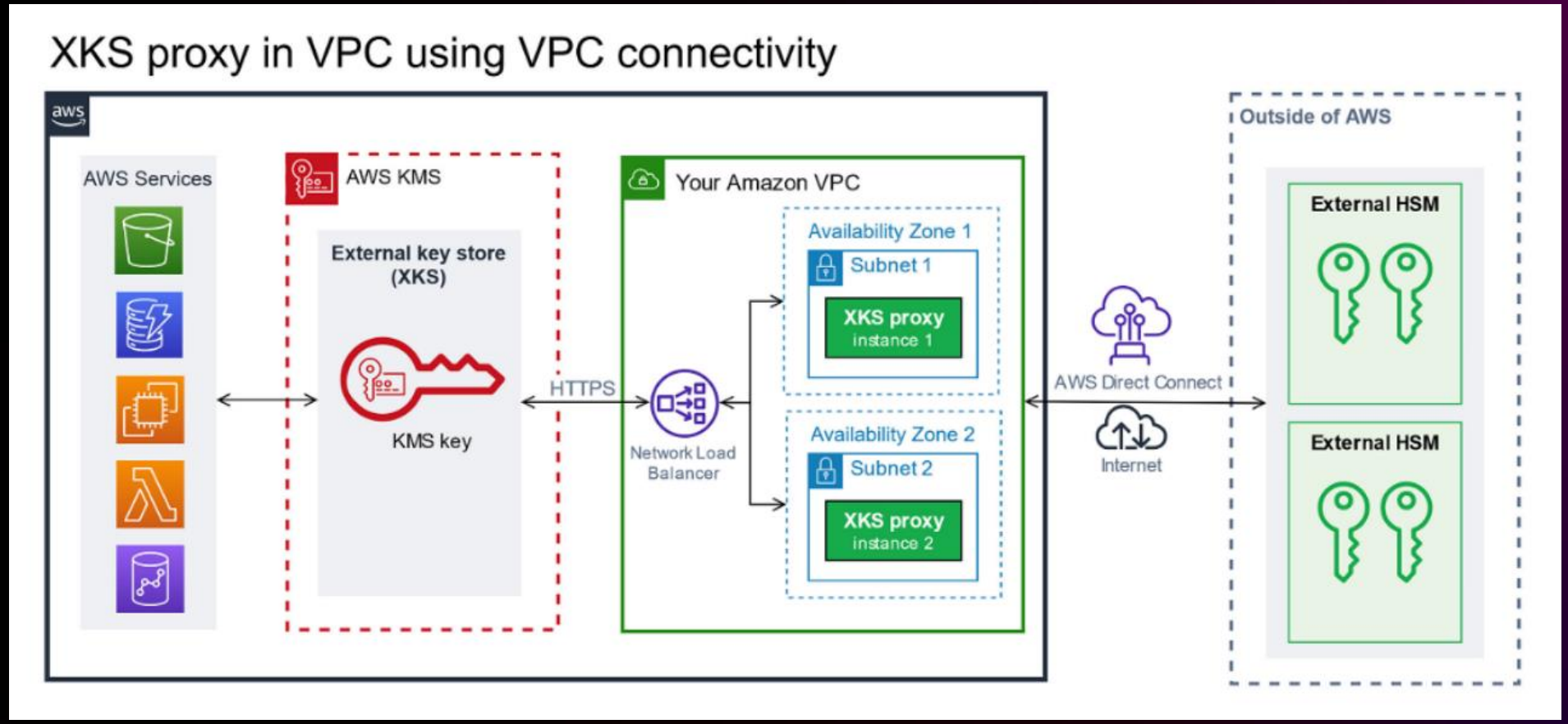
Can AWS see my keys?

- **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*

What is AWS CloudHSM?

- Standalone, dedicated HSM cluster that you own and operate in your VPC
- Extensive support to help “lift and shift” on-premise HSM workloads
- Offers more specialized cryptographic algorithms and legacy ciphers than KMS
- Certified at FIPS 140-2 Security Level 3
- Can become the backend HSM for KMS using the KMS custom key store feature

New! External Key Store (XKS)



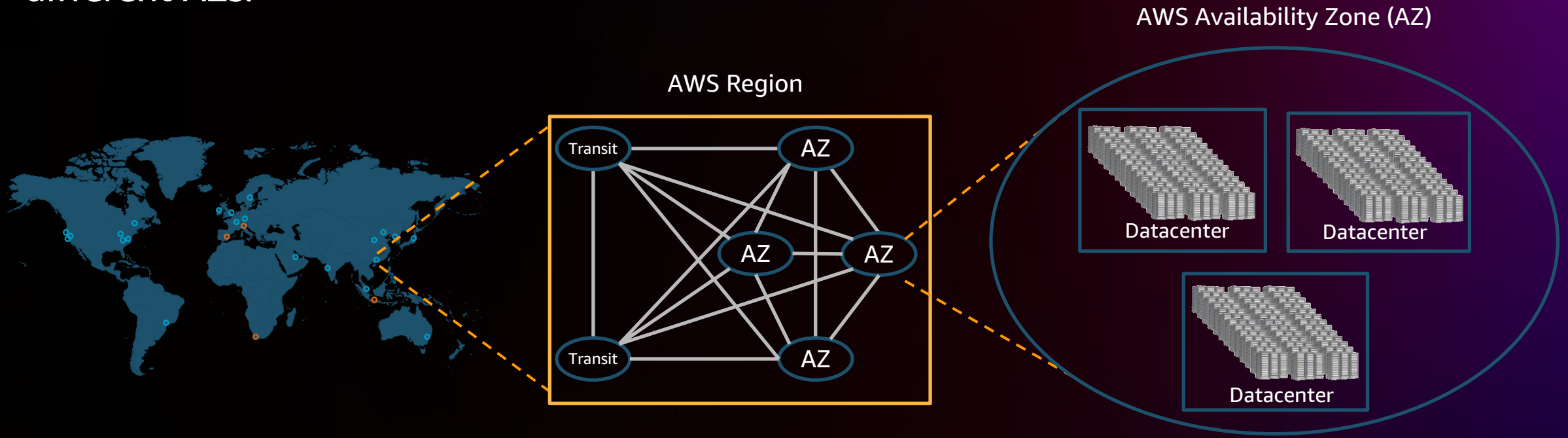
AWS Digital Sovereignty Pledge

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.

Resilience in the cloud

AWS Region design

AWS Regions comprise 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.



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.

Pushing the boundaries from the cloud to the edge

DELIVERING THE CLOUD ANYWHERE CUSTOMERS NEED IT

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

SAME INFRASTRUCTURE, SERVICES, APIS, AND TOOLS FOR A CONSISTENT EXPERIENCE

AWS Regional Services

- 180+ AWS services are fully regionalized
  - They work autonomously in-region
  - Some services are intentionally global (CloudFront, Route 53, etc.)
- If you do not want to use specific regions:
  - Use AWS Organizations to deny access*
  - Regions introduced after March 20, 2019 are disabled by default and must be enabled manually**

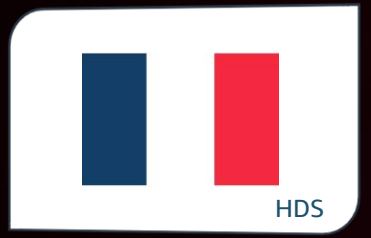
*https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_general.html
**https://docs.aws.amazon.com/general/latest/gr/rande-manage.html

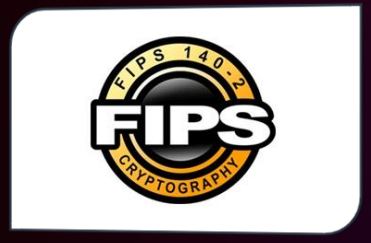
AWS Digital Sovereignty Pledge

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

Transparency and assurance

Certifications and attestations





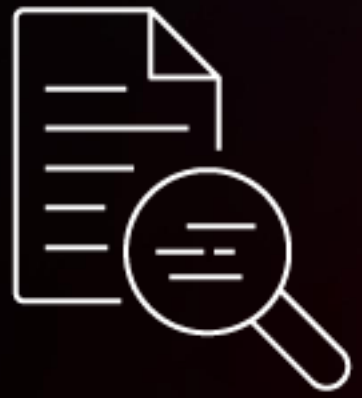
Privacy features of AWS

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/

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

No 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 Digital Sovereignty Pledge

We commit to continuing to provide the transparency and business flexibility needed to meet evolving privacy and sovereignty laws.

Local Trusted Partners

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 to meet their security and regulatory needs through partners such as Atea, Capgemini, Cybercom, Nordcloud and SecureAppbox

AWS Digital Sovereignty Pledge

We are doubling down with local partners that our customers trust to help address digital sovereignty requirements.

Read our AWS Digital Sovereignty Pledge

Matt Garman, SVP at AWS

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

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 ISO27701 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 sub-processor 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

Thank you!

David Woodhouse
dwmw@amazon.co.uk

Luis Wang
wangluis@amazon.com

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