AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

CMP336

Architecting for data residency on AWS Outposts

Manish Gilani
Product Manager – AWS Outposts
AWS

Shweta Joshi
Software Development Manager – Amazon EBS
AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- Data residency
- What is AWS Outposts
- Architecting for data residency
- Customer use case

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is data residency ?



Data residency

The requirement that all customer content be processed and stored in an IT system that remains within a specific locality's borders

AWS Outposts may help you meet data residency needs

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

High standards for privacy and data residency



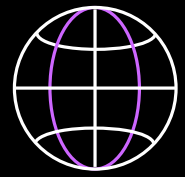
Meet data residency requirements
Choose an AWS Region and AWS will not replicate it elsewhere unless you choose to do so



Encryption at scale with keys managed by our AWS Key Management Service (AWS KMS) or managing your own encryption keys



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



Large network of security partners and solutions

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Application continuum

EASE OF MIGRATION TO CLOUD

AWS Regions

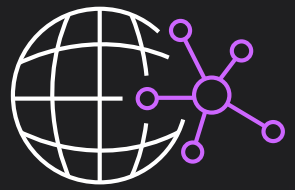
Web and enterprise



Most web and enterprise applications, such as email, collaboration, and intranet applications, are easily migrated to AWS Regions

AWS Regions or on premises

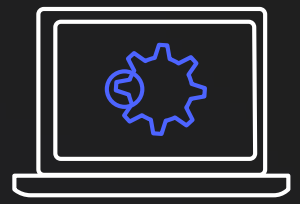
Residency



Regulations or contractual obligations dictate that data and infrastructure reside in specific countries, states, or provinces

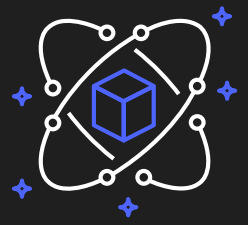
On premises

Local data processing



Transcoding, filtering, caching, and alerting applied at the edge; large datasets that can't be easily moved

Low latency



Equipment and processes sensitive to compute latency; interactive workloads such as AR/VR, design, and visualization; complex workloads that span a variety of local host or storage systems

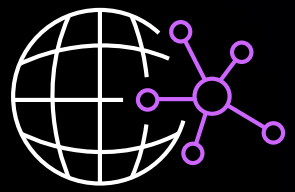
Easier ← Move to cloud → Harder

aws

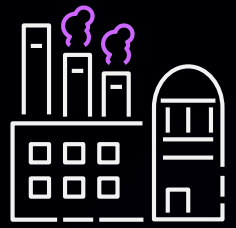
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What if you can’t move your data to an AWS Region?

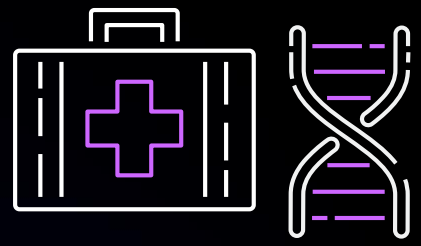
Data residency and local processing requirements of certain countries and highly regulated sectors require both primary data and the backup of the data to be stored locally



Financial



Manufacturing

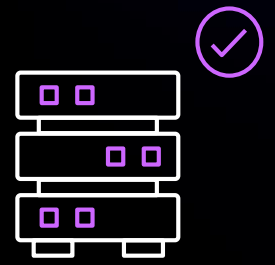


Healthcare

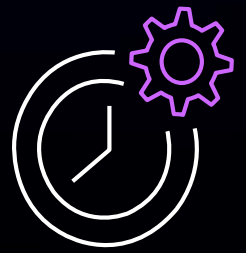
aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

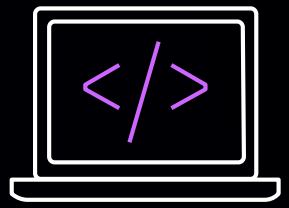
Customers want the same experience on premises and in the cloud



Same reliable, secure, and high-performance infrastructure



Same operational consistency



Same services and APIs



Same tools for automation, deployments, and security controls



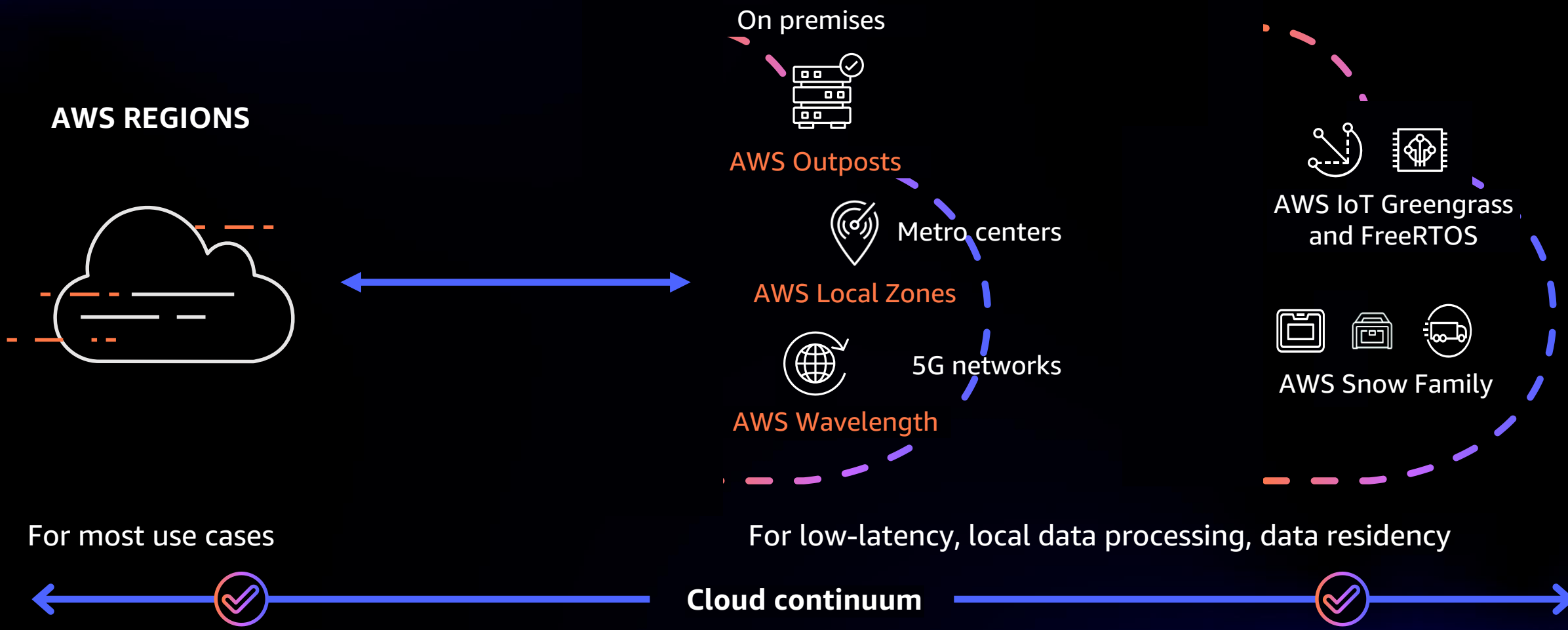
Same pace of innovation as in the cloud

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cloud continuum

AWS: DELIVERING CLOUD WHERE CUSTOMERS NEED IT

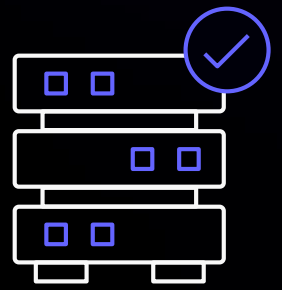


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Outposts

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

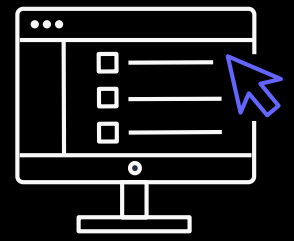
AWS Outposts: Bringing AWS on premises



Same AWS-designed infrastructure as in AWS data centers (built on AWS Nitro System)



Fully managed, monitored, and operated by AWS as if in AWS Regions



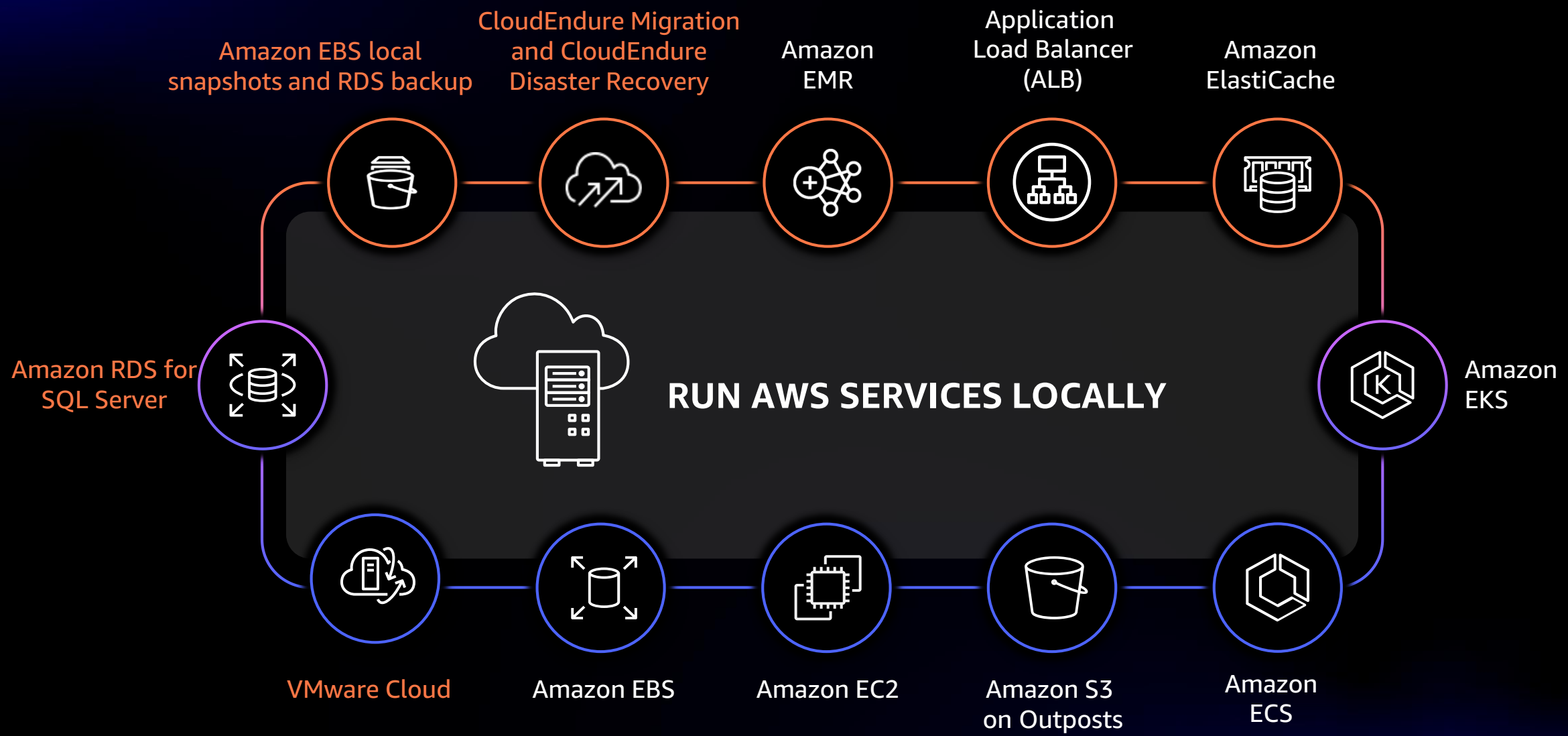
Single pane of management in the cloud providing the **same APIs and tools** as in AWS Regions

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Outposts rack

- Industry standard **42U rack**
- **Fully assembled,** ready to be rolled into final position
- **Installed by AWS,** simply plugged into power and network
- **Centralized redundant power conversion unit** and DC distribution system for higher reliability, energy efficiency, easier serviceability
- **Redundant active components** including top of rack switches





© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Outposts shared responsibility model

- Customer data
- Platform, applications, AWS Identity and Access Management (IAM)
- Operating system, network, and firewall configuration (security groups)
- Client- and server-side encryption
- Network traffic protection



MANAGED BY AWS CUSTOMERS

- Physical security and access control
- Regional connectivity
- Capacity management

CUSTOMER'S DATA CENTER

- AWS foundation services: compute, storage, database, networking
- AWS global infrastructure: Regions, Availability Zones, edge locations



MANAGED BY AMAZON WEB SERVICES

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data residency using AWS Outposts

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Outposts security

Enclosed rack with a lockable door

Data on Outpost is encrypted

Removable and destroyable hardware security key on each server

Encrypted network connection to the AWS Region

Physical security of the Outpost location is the customer's responsibility



aws

Nitro security key (physical security)

All data is encrypted at rest and in transit in Nitro

Key material is wrapped to external key stored in removable device

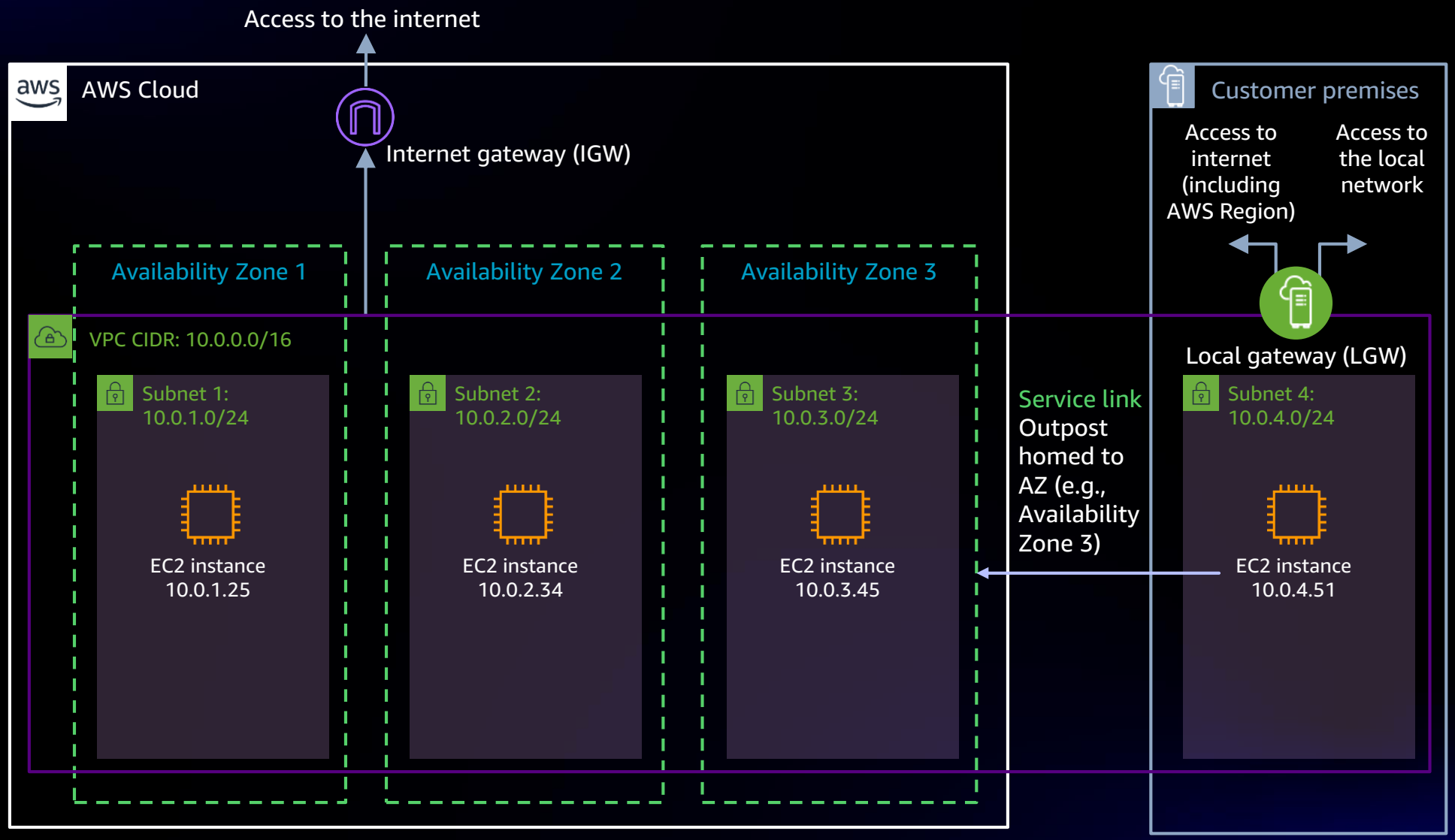
Destroying the device is equivalent to destroying the data



To learn more about Nitro on Outposts: Attend AWS re:Invent 2021 – CMP311

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Networking with Outposts racks



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

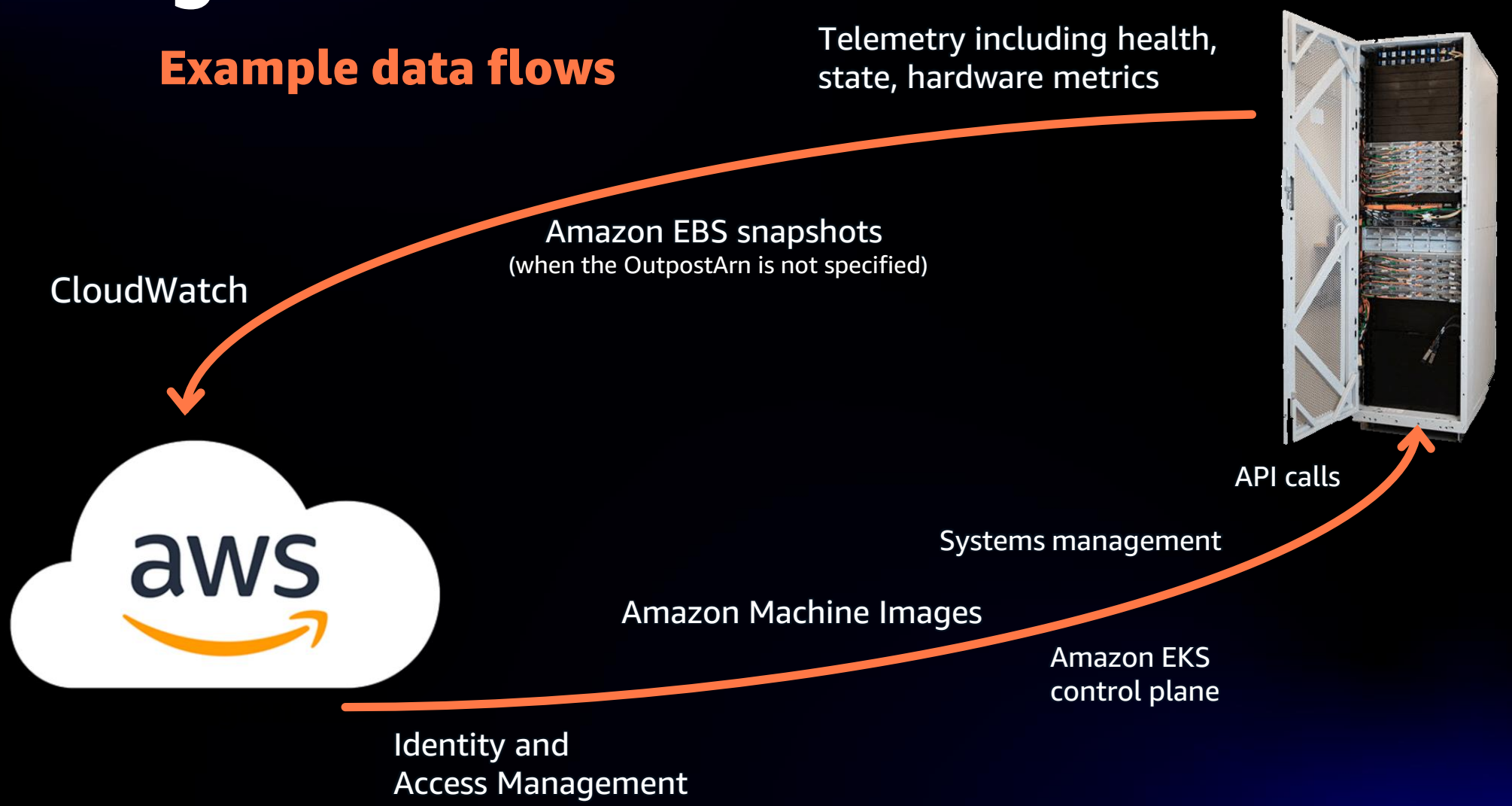
You can keep your VPCs contained within Outposts



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

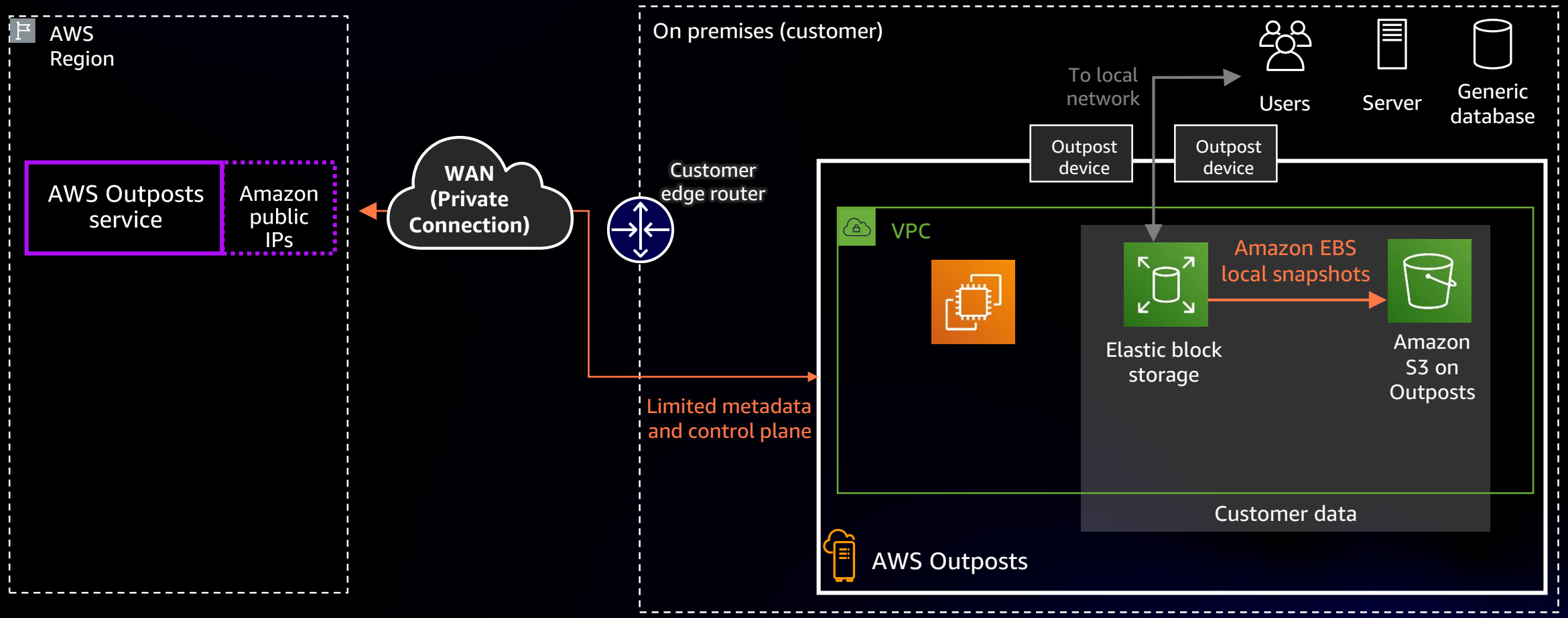
Management and control plane in the AWS Region

Example data flows



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Customer data and processing can stay resident on Outposts



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Architecting for data residency

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon EBS



Persistent block storage

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon S3 on Outposts



Persistent block storage

Persistent object storage

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon S3 on Outposts



Persistent block storage

Persistent object storage

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Where is my object data stored?

Data is always stored on the Outposts

- Object data
- Object system and user metadata
- Object tags



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon S3 security and access control features



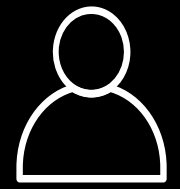
IAM policies



S3 Block Public Access
(always enabled)



S3 Access Points
(VPC restricted)



S3 Object Ownership
(always enabled)

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon EBS Local Snapshots



Persistent block storage

Persistent object storage

Local data backup on Outposts

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon EBS Local Snapshots



Persistent block storage

Persistent object storage

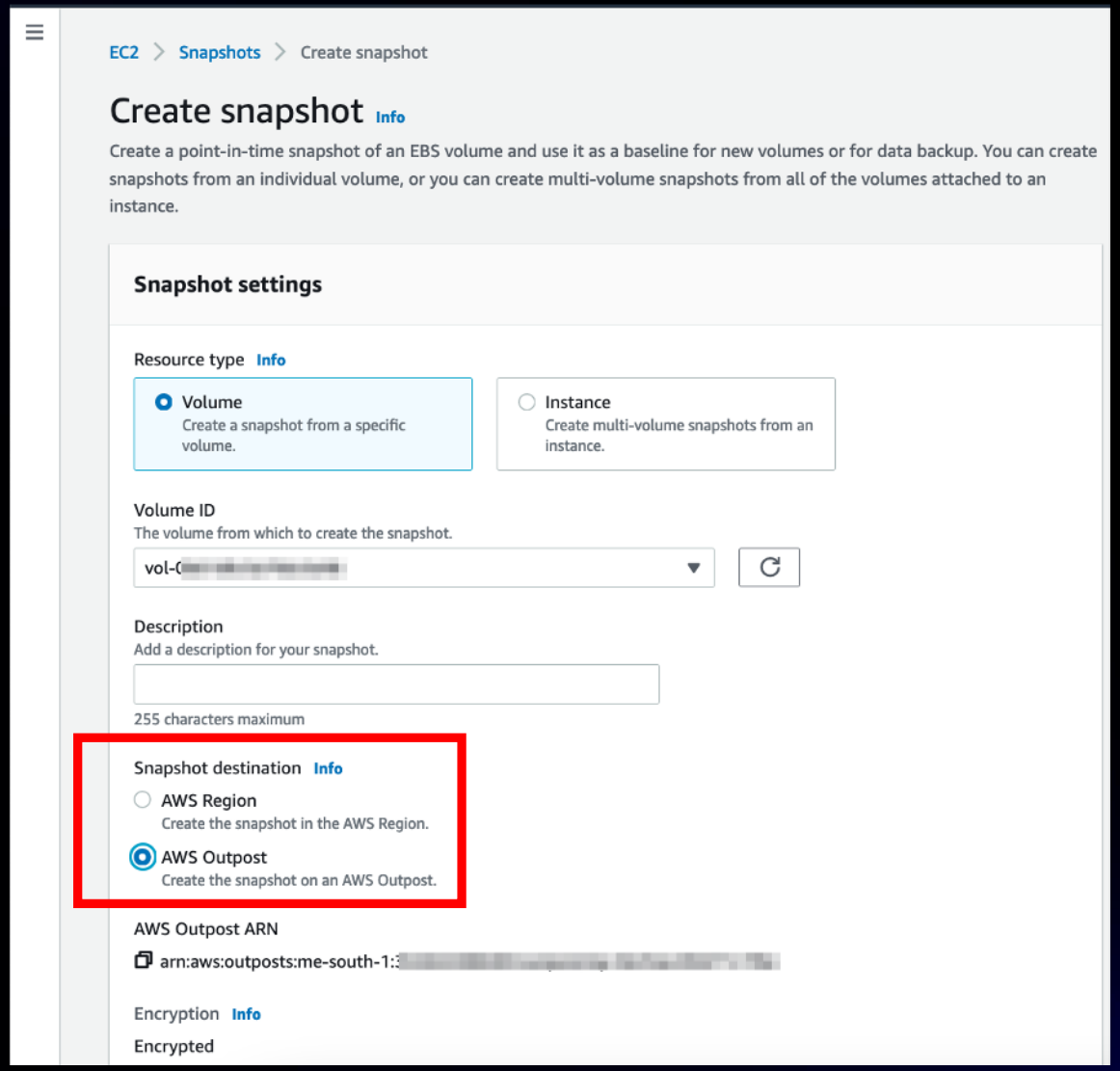
Local data backup on Outposts

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Using Outposts storage for data residency

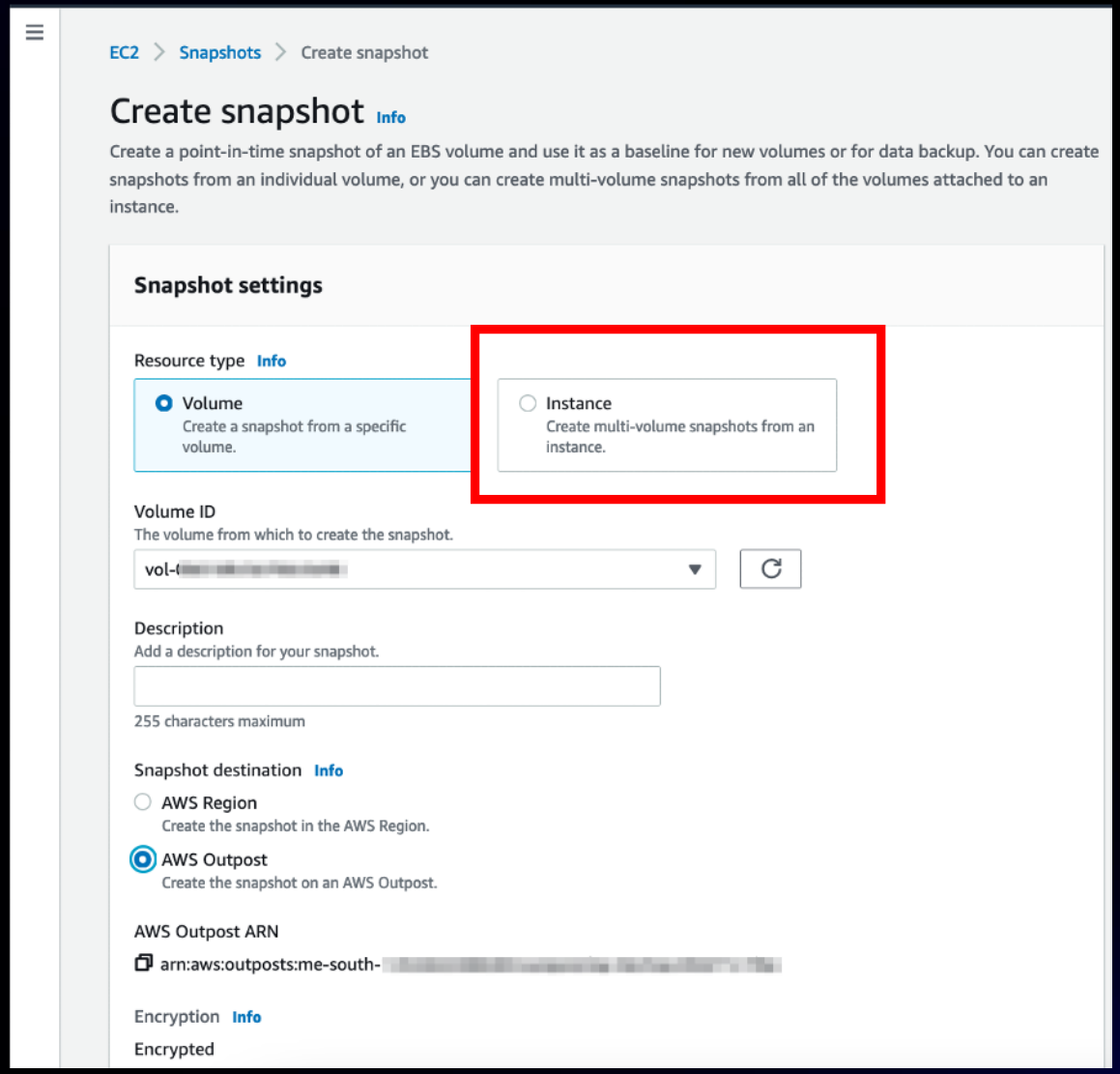
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Creating local snapshots on Outposts



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Creating local snapshots on Outposts



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Operations using Amazon EBS local snapshots

- Create AMIs from local snapshots
- Copy snapshots from an AWS Region to an Outpost
- Copy AMIs from AWS Region to AWS Outposts
- Launch instances from AMIs backed by local snapshots

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data residency enforcement using IAM policies

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Deny Create Snapshots in Region

```
  "Effect": "Deny",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots"
            ],
            "Resource": "arn:aws:ec2:<outpost-region>::snapshot/*",
            "Condition": [
                "StringEquals": [
                    "ec2:SourceOutpostArn": "arn:aws:outposts:<outpost-
region>:<account-id>:outpost/<outpost-id>”
                ],
                "Null": [
                    "ec2:OutpostArn": "true"
                ]
```

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

FANDUEL



The challenge

Accelerate business expansion while meeting data residency requirements

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The solution

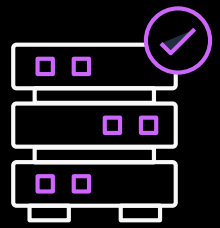
FANDUEL

Migrated betting platforms from OpenStack and VMware to AWS

Pre-stage environments in test and development, and quickly deploy production-ready instances with Outposts

Offloaded day-to-day infrastructure and hardware management to AWS

Worked with regulators to understand data residency requirements and deliver responsible gaming



AWS Outposts: Same AWS-designed infrastructure as in AWS data centers

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

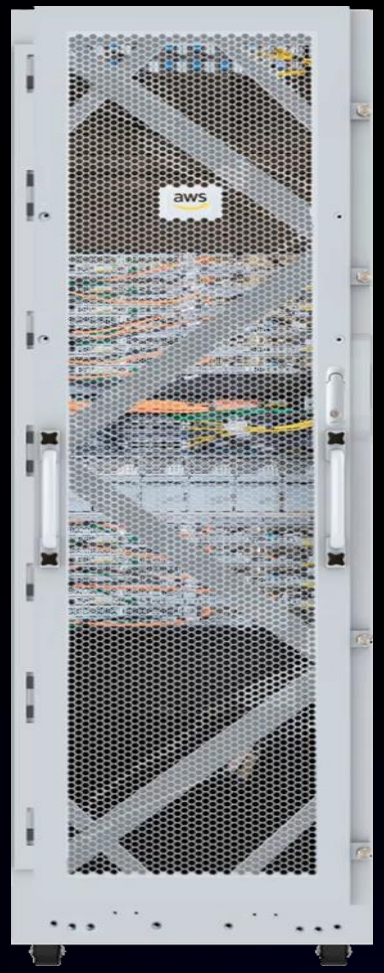
Business outcomes

FANDUEL

Faster time to market: from 15–16 weeks to less than 20 days

30%–40% improvement in application performance

OpEx savings by spending less time managing infrastructure



aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

FANDUEL



“Work with AWS to ensure that you're using their best practices because, in reality, they know how to do infrastructure at scale, and they have the experience of managing these types of environments. Create that partnership with AWS and work together to achieve your business outcomes.”

Shane Sweeney
VP of IT
FanDuel

aws

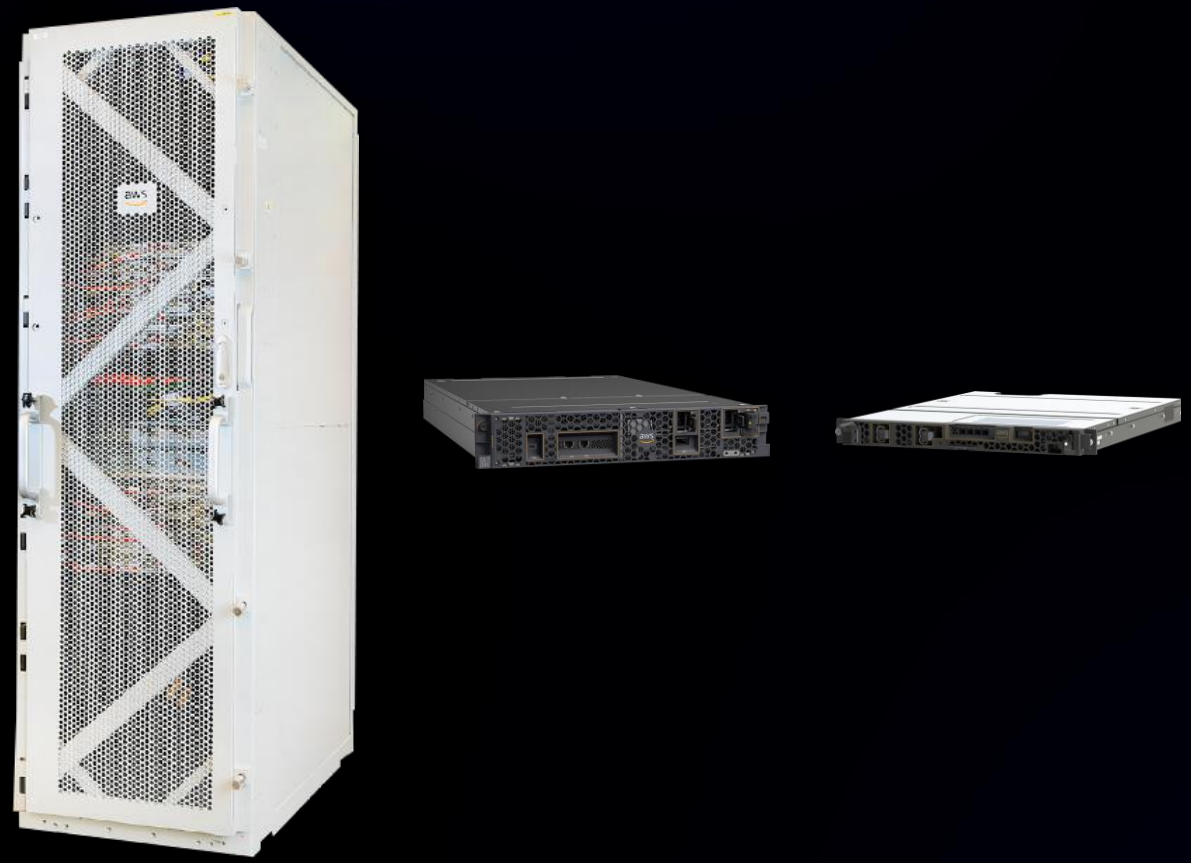
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Takeaways

- AWS Outposts is a fully managed service that offers the same AWS infrastructure, services, APIs, and tools to meet your data residency and local processing requirements
- Store your data on premises on AWS EBS and Amazon S3 on Outposts
- Store snapshots of Data, Boot Volume, and EBS-backed AMIs on Amazon S3 in cloud or now on premises for data residency requirements on Amazon S3 on Outposts
- All data on Outposts are encrypted by default (EBD)
- Control access to data and movement using AWS Identity and Access Management (IAM), monitor using CloudWatch, and audit using AWS CloudTrail

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

See the Outposts rack and servers up close



AWS Hybrid kiosk

AWS Village (Booth #1719)

Venetian | Level 2 | Expo Hall

Automate Quality Inspection kiosk

AWS for Industrial (Booth #1957)

Venetian | Level 2 | Expo Hall

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Additional resources

Visit our website

aws.amazon.com/outposts/

Check out these re:Invent sessions

CMP204
Extending AWS to where organizations need it

CMP320
Dive deep on cloud use cases with AWS Outposts

CMP311
Bringing the AWS experience on premises

CMP319
Architect for highly available applications with AWS Outposts

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.