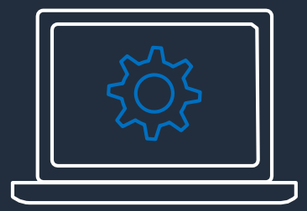
AWS Outposts

AWS Services On-Premises

Mohammad Mizanur Rahman

CTO, Brain Station 23 Ltd.

Applications that need to remain on-premises



Latency sensitive

Equipment and processes sensitive to compute latency

Interactive workloads such as AR/VR, design, and visualization

Complex workloads that span a variety of host and storage systems

Local data processing

In hybrid workflows, transcoding, filtering, caching, and alerting applied at the edge

Bringing AWS compute to large datasets that can't be easily moved

Residency

Where regulations dictate that data and infrastructure reside in specific countries

Where contracts specify where applications are deployed

Where enterprises are not ready to move to AWS regions for Infosec or other reasons

aws

Customers want the same experience across on-premises and 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

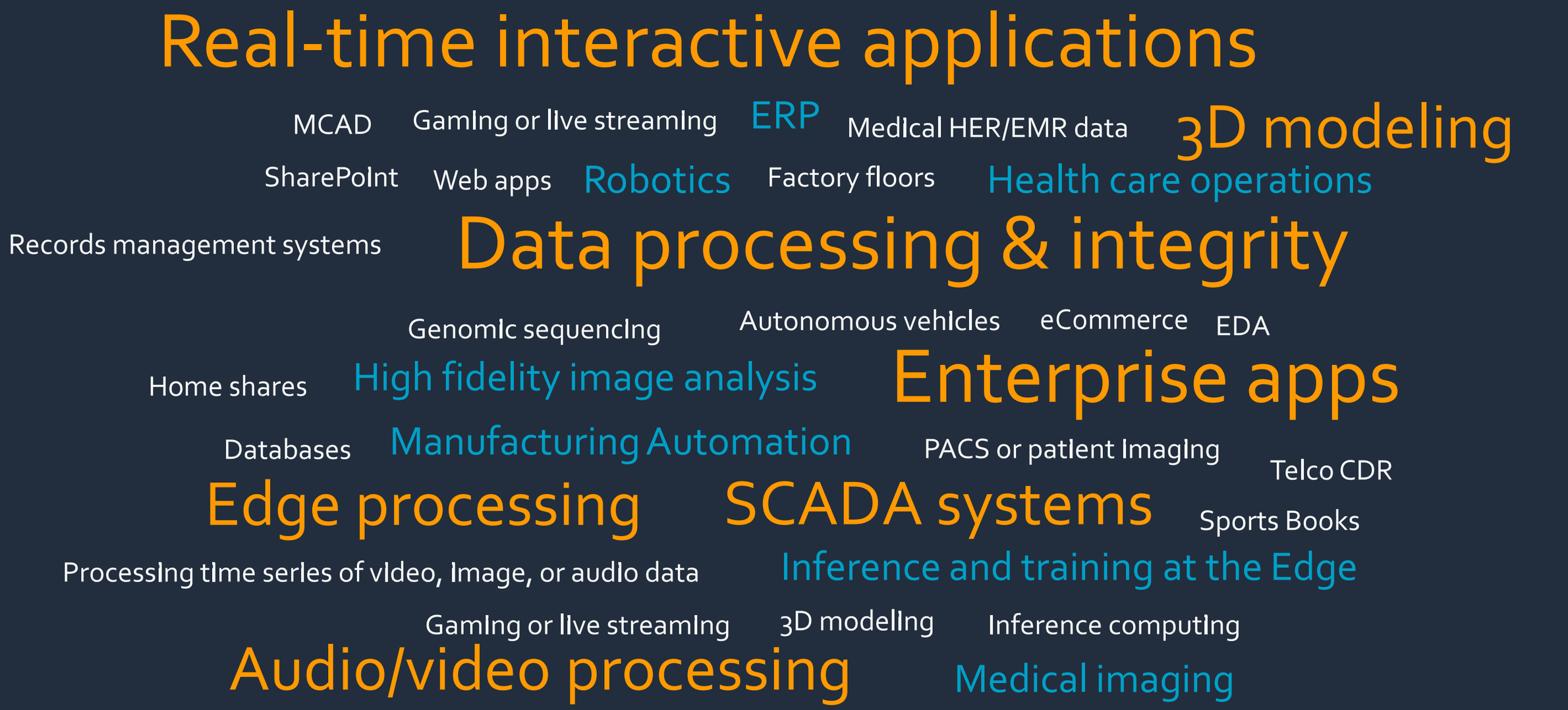
AWS Outposts

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


Real-time interactive applications
MCAD
Gaming or live streaming
ERP
Medical HER/EMR data
3D modeling
SharePoint
Web apps
Robotics
Factory floors
Health care operations
Records management systems
Data processing & integrity
Genomic sequencing
Autonomous vehicles
eCommerce
EDA
Home shares
High fidelity image analysis
Enterprise apps
Databases
Manufacturing Automation
PACS or patient imaging
Telco CDR
Edge processing
SCADA systems
Sports Books
Processing time series of video, image, or audio data
Inference and training at the Edge
Gaming or live streaming
3D modelling
Inference computing
Audio/video processing
Medical imaging

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

AWS Outposts: addressing customer challenges

Simplifying IT with fully managed infrastructure, growing IT efficiency, and responsiveness to business needs

Amplifying developer productivity with same popular AWS API, console, tools, and broad ecosystem of partner solutions

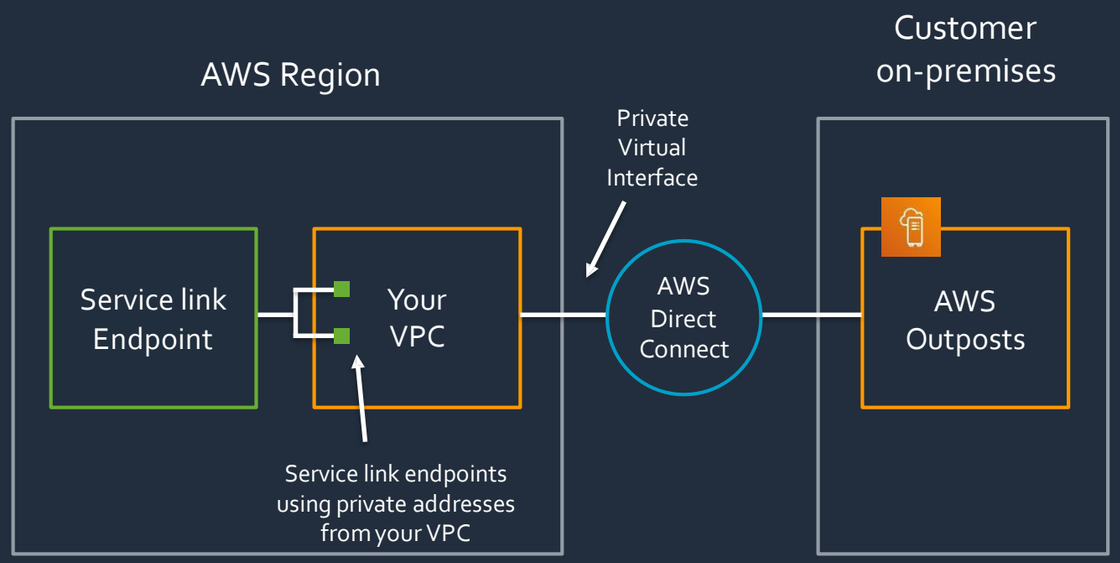
Enabling IT and developers to accelerate pace of business innovation

Delivering cloud infrastructure and services where needed to meet data residency and regulatory requirements

AWS services on-premises


Amazon RDS
Amazon EBS
Amazon EBS Local Snapshots
Amazon EC2
Compliance certifications
Amazon S3
Amazon EMR
RUN AWS SERVICES LOCALLY
Amazon ECS
Application Load Balancer (ALB)
Amazon EKS
Amazon Elasticache

Connect to your AWS Region



Private WAN access

- AWS Service link access: Connects to a VPC that you own, in your AWS Outposts account
- Access from your VPC to your on-premises: Uses an AWS Direct Connect private virtual interface, or other private means such as VPN
- Service link Endpoints use private addressing: Using private addresses in your VPC range, service link endpoints are reachable via VPC routing, no public IP's required
- No public IPs required: Through your AWS Direct Connect, all IP addressing can be private

Getting started

3 steps to get started with AWS Outposts

1. Order

Select your compute and storage capacity

2. Install

AWS delivers and installs the Outpost

3. Launch

Use standard AWS APIs or Management Console to launch and run AWS resources locally

aws

Security, compliance, and responsibility

AWS Outposts: security and compliance

- AWS Outposts have an updated shared responsibility model
- AWS is responsible for protecting Outposts' infrastructure
  similar to securing infrastructure in the cloud today
- Customers are responsible for securing their applications
  running on Outposts as they do in AWS Region
- Customers are also responsible for the physical security of their Outpost racks
- AWS services launched locally on Outposts will go through a separate evaluation for certifications and existing certifications WILL NOT apply
- Compared to certification for other AWS services, with AWS Outposts the customer owns the responsibility for physical security and access controls around the Outpost for compliance certification

Outposts security

- Built-in tamper detection
- 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 customers responsibility

Summary

Emerging need for low-latency, local data processing, and data residency

Customers want the same experience on-premises and the cloud

AWS Outposts delivers the same fully managed infrastructure, services, and APIs as in the cloud

Simplifies IT, grows IT efficiency

Amplifies developer productivity

Accelerates pace of innovation

aws

Thank you!