Microsoft Azure

Deployment of 5G in Cloud: Technology options, Management and Orchestration (MANO)

Uma Mahesh Mudigonda
Microsoft

Microsoft Azure

Evolution of operator virtualization platforms

Appliance Model

Vertically Siloed
Vendor Lock In

Private cloud

Software-based solution
Complex multi-vendor integration
Ongoing certification and integration costs
Limited PaaS services

Hybrid cloud

As-a-service offering
Comprehensive automation / integration
Software agility and innovation
Cloud-based economics

Leverage scale, services, and security features of hyperscale

Microsoft Azure

Key principles of Microsoft's operator strategy

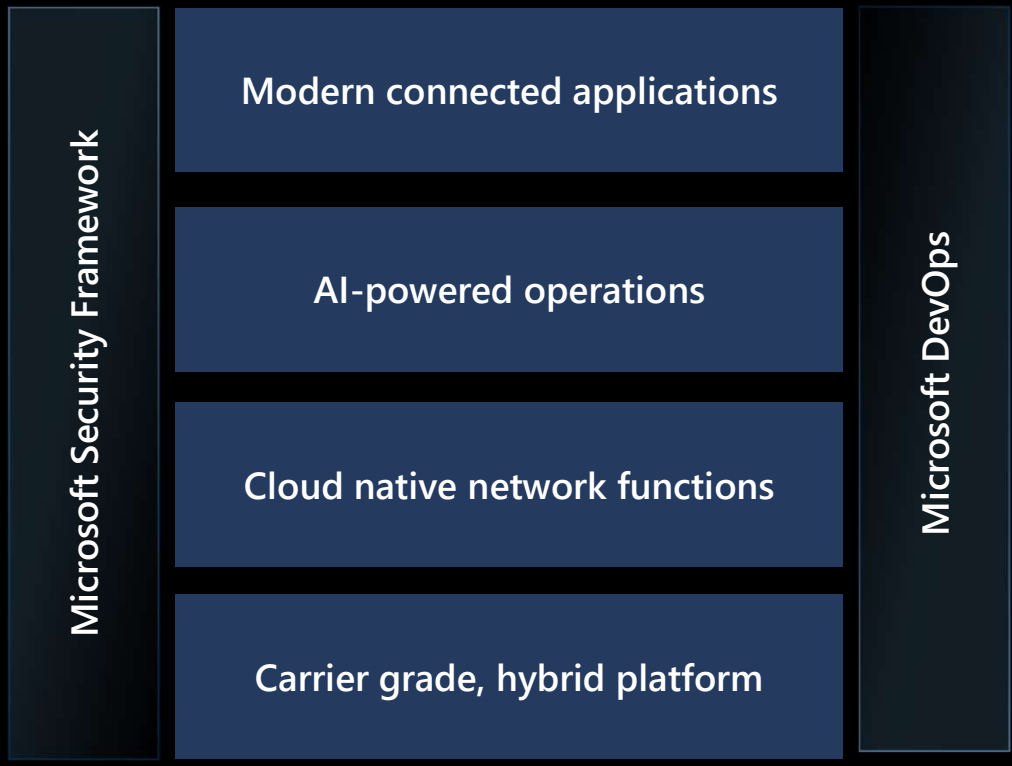
1. We are bringing the power of cloud to future-proof Telco network, driving down costs and opening new revenue streams
2. We partner—Telcos own customer, brand, ideation, experience
3. We remain a platform business—our focus is on moving workloads to a carrier-grade cloud
4. We meet Telcos where they are—on-premises, at the edge or in the cloud
5. Support the ecosystem—we work closely with providers of RAN, Core, CNFs, and OSS/BSS to integrate and innovate
6. It is a journey—we act as a trusted partner to help Telcos transform at a pace that makes sense for their business

Microsoft Azure

Modernize and monetize with Azure for Operators

Outcomes

- Lower total cost of ownership (TCO)
- AIOps for efficiency and resiliency
- Enhance security of distributed networks
- Modern connected apps
- Integrate with industry leading ecosystem



Microsoft Azure

Azure Operator Nexus

A hybrid cloud service that enables operators to run carrier-grade workloads on-prem or on Azure

On-Premises

Operator Facilities

Operator Owned Hardware

CapEx and OpEx

Multiple Deployment Models

Public

Azure Regions/PoPs

Azure Infrastructure

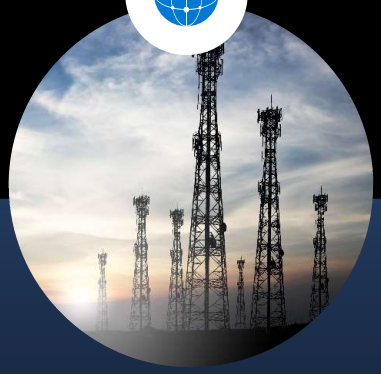
OpEx

Management | Security + Identity | App + Data Services | Dev Tools + DevOps

Use cases from Labs as a Service to Cloud Bursting to 5G SA Core

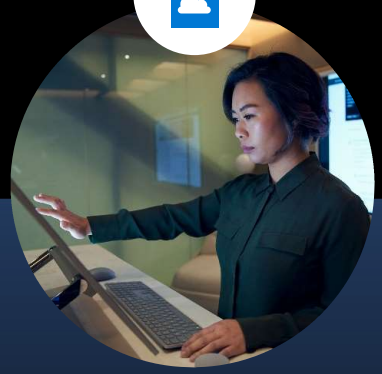
Microsoft Azure

Azure Operator Nexus

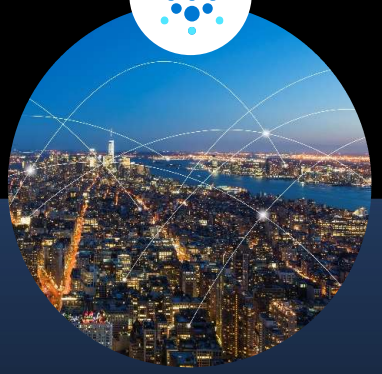


Optimize next-gen networks with unified platform

Run smarter with connected operations & insights



Secure and govern across environments



Harness the power of Azure

Microsoft Azure

Azure uniquely meets operators' business needs

36% OpEx savings compared to private cloud option

58% operation efficiency improvement thru automation

90+
compliance certifications – more than any other public cloud provider

68,000+
partners, largest in the industry

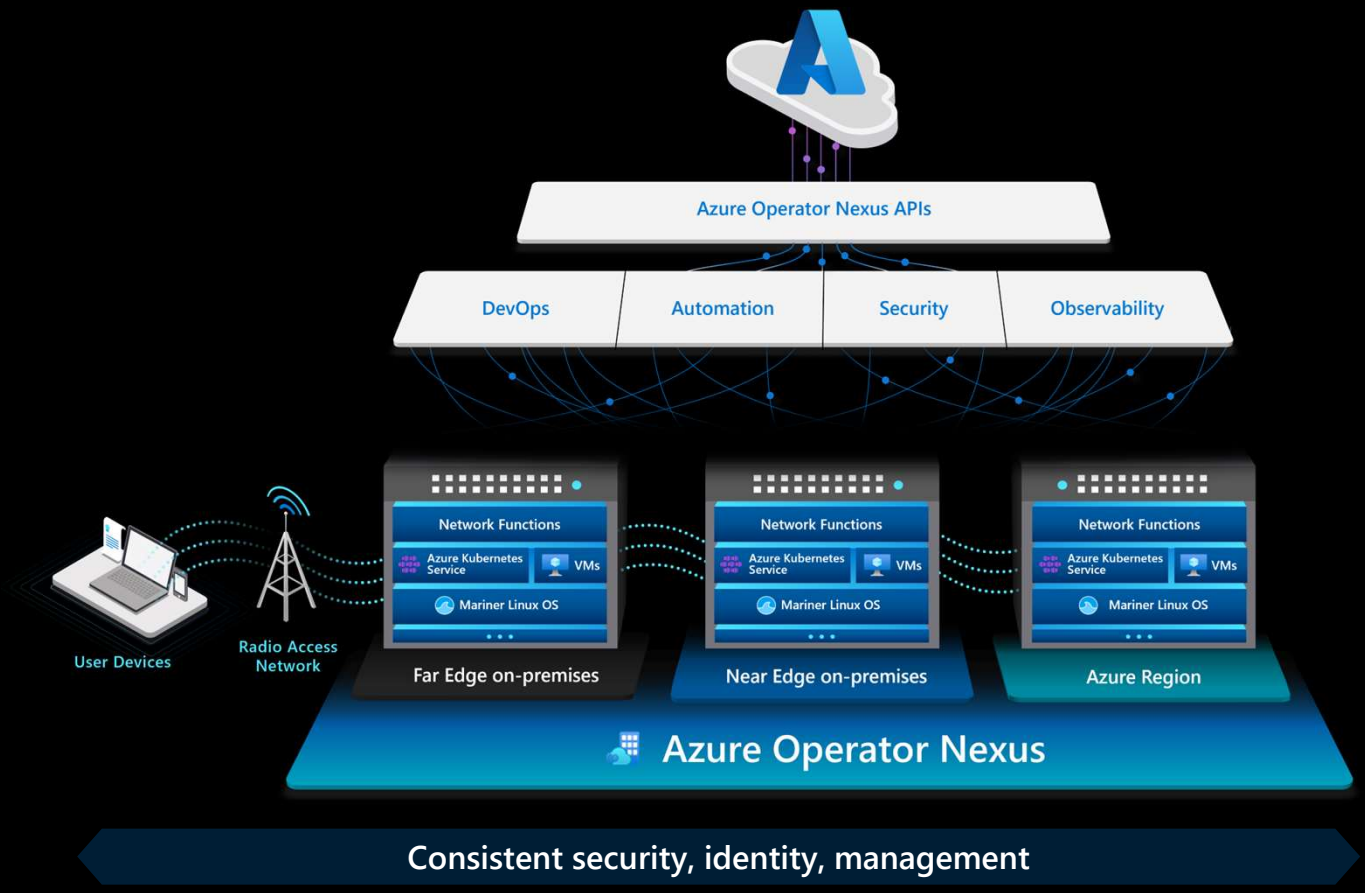
10s of millions
of subscribers on platform

Investment in Telco DNA

Microsoft Azure

Azure Operator Nexus

Carrier-grade platform for network function



5G

Proven carrier-grade infrastructure

Azure scale and automation

Frictionless integration with APIs

Zero Trust Security Strategy

Secure Technology

Azure Security built into Operator Nexus

Identity and access management

Security posture management

Threat protection

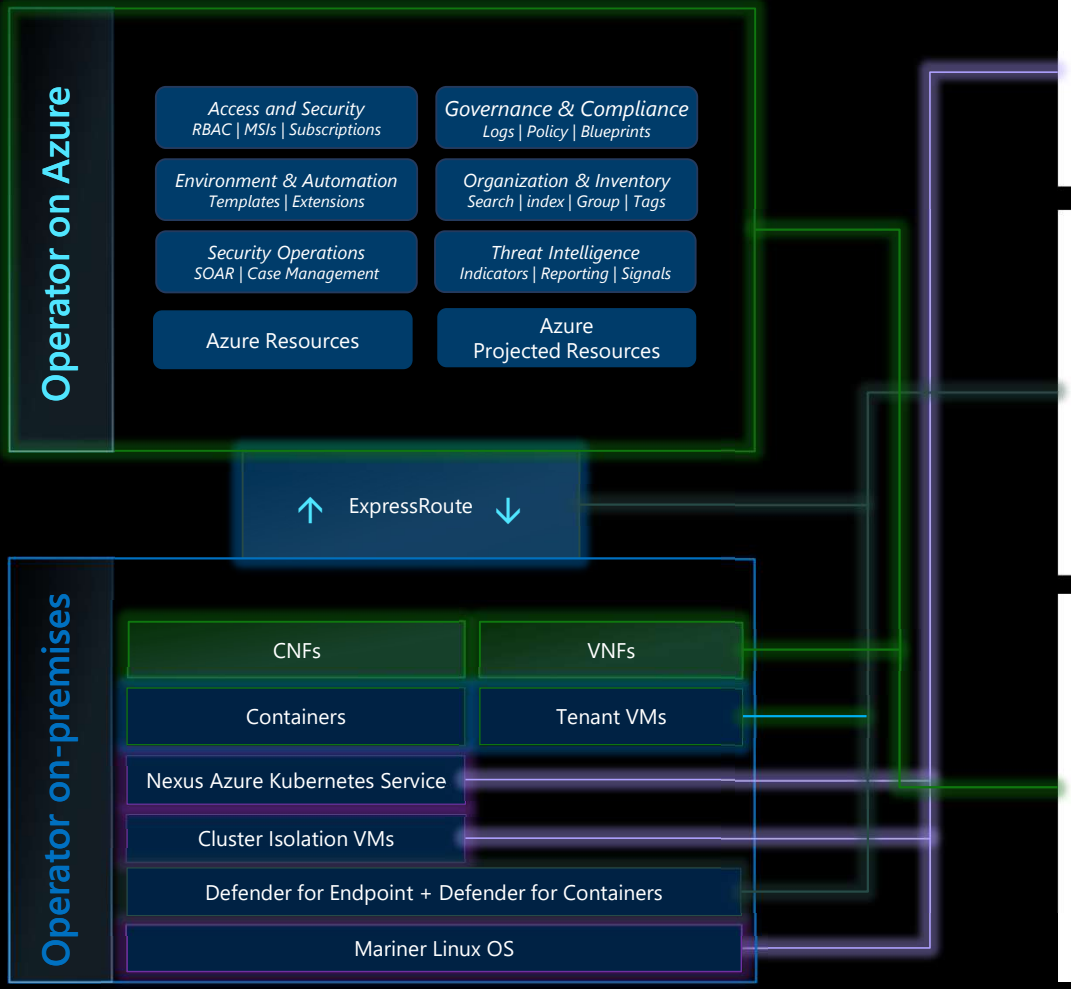
Data security

Network security

Defense in depth

Microsoft Azure

Operator Nexus Security Posture



Reduced Attack Surface

Significantly shortened software supply chain to produce purpose-built Operating System and container images to fit the stringent needs and requirements of Telco Operators.

1. **Reduced exposure** to potential security risks.
2. **Minimization** of unnecessary Operating system packages.
3. **Improved visibility** and traceability.
4. **Built with security and compliance** alignment to industry standards.

Secure by Default Protections

Runtime and network security protections provide default safeguards against common threats and attacks, ensuring that applications and networks are protected from potential vulnerabilities and risks

1. **Microsoft Defender for Endpoint**: deployed by default to prevent, detect, investigate, and respond to advanced threats and attacks and vulnerability analysis.
2. **Microsoft Defender for Containers:** Threat protection for containerized workloads in Kubernetes environments, using behavioral analysis and machine learning to detect and prevent attacks against the supporting infrastructure.
3. **Azure Express Route**: Private and dedicated connections between on-premises infrastructure and Azure datacenters, bypassing the public internet and reducing the attack surface for potential security threats.

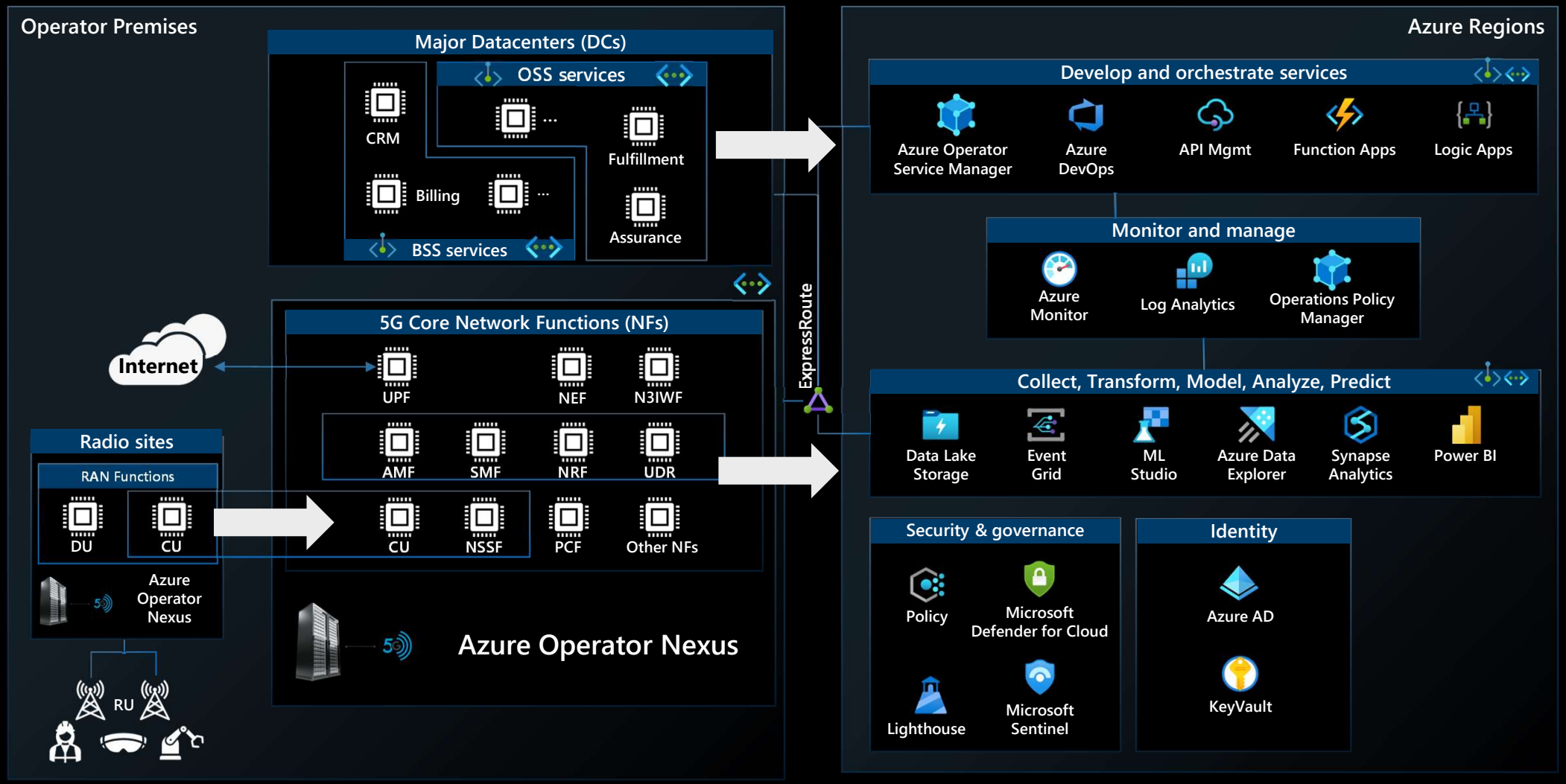
Azure Security Ecosystem Integration

Operator Nexus - connectivity empowers Operators to customize and define their security posture by leveraging a wide range of security solutions and services within the Azure ecosystem.

1. **Azure Activity Directory**: Role-based access control for cloud resources that enables customers to manage permissions and access to resources at scale, reducing the risk of unauthorized access and data breaches.
2. **Azure Sentinel:** Cloud-native SIEM and SOAR solutions that provides intelligent security analytics and threat intelligence, enabling customers to detect, investigate, and respond to security threats and attacks in real time.
3. **Azure Policy**: Centralized management of security policies and controls across hybrid and multi-cloud environments, providing visibility and control over security configurations and reducing the risk of misconfigurations and security breaches.

Microsoft Azure

Sample 5GC Deployment on Azure Operator Nexus



Azure Operator Nexus key features

- Automated, simplified, carrier-grade platform
- Integrated network fabric automation
- Unified observability and network packet broker
- Simplified NF deployment automation & pre-certified VNF/CNFs
- APIs to integrate with OSS/BSS
- Common Azure PaaS and data fabric

Microsoft Azure

Operator Nexus partner ecosystem

System Integrators

accenture

amdocs

Capgemini

DELL Technologies

Hewlett Packard Enterprise

NEC

TECH mahindra

Network Function Partners

ERICSSON

NOKIA

amdocs

COMTECH

ENEA

f5

Hewlett Packard Enterprise

JUNIPER NETWORKS

MAVENIR

Spirent

Microsoft Azure

Tier-1 Telco case study

Highlights

Bootstrapping

- Remotely bootstrapped Nexus instances from multiple Azure regions
- Bootstrapped Network and Compute Fabric in **4 hours vs months**
- Supported different SKUs with different devices models

Deploying NFs

- SMF deployed in **45mins vs 3 days** via MOPs,
- Onboarding all 5G NFs used by the Telco, from 7 vendors

Observability

- Integrated Observability with Azure Monitor

Learning

Disconnected Operations

- Ability to access network devices from Telco NoC in disconnected mode
- IAM alternative to TACACS

Break-glass capabilities

- Ability to long-in to the devices for troubleshooting

Integrating with legacy infrastructure and solutions

- Integrating legacy active monitoring solutions e.g. TWAMP

Microsoft Azure

Thank you!