Microsoft Azure

Azure whitepaper

# Deploying Private Mobile Networks on Azure

## Bringing the power of hyperscale to operator-enabled private mobile networks

# Table of contents

# Introduction

The fourth industrial revolution, Industry 4.0, is upon us, ushering in a wave of new industrial applications that will transform the way businesses operate. Driven by improved processing power and connectivity, these applications collect and process data from across the organization to help businesses run more strategically and more efficiently. As enterprises scale, they need solutions that can handle these mission-critical workloads.

To meet these demands, modern enterprises need both private mobile networks and multi-access edge computing (MEC). Private LTE/5G networks give businesses the speed, security, mobility, and quality of service they need to process data efficiently, while edge compute supports latency-sensitive industrial applications, data localization, and data processing at the edge.

To realize the benefits of private LTE/5G networks, some key challenges need to be addressed. These include operational and engineering complexity, absence of end-to-end visibility and security, and lack of automated, software-based solutions.

To address these challenges, Microsoft has introduced an innovative approach combining first and third-party capabilities for a fully integrated private mobile network service for mobile operators and managed service providers. It combines Azure cloud, Azure Stack Edge, Affirmed (now a Microsoft company) LTE/5G mobile core, and end-to-end orchestration and management. Microsoft's unique approach solves the cost and complexity challenges faced by mobile operators and enterprises in the deployment of private mobile networks and is expected to drive their adoption by enterprises globally.

This white paper explains how mobile operators can build private networks for enterprises using Azure services and leverage the benefits of a hyperscale cloud and integrated MEC architecture to significantly lower CapEx/OpEx, accelerate the pace of innovation, and open up new revenue opportunities.

# Private mobile networks

## Private mobile networks, powered by 5G

There is little doubt that private networks, accelerated and enhanced by 5G, will transform the landscape of telecommunications services. Key features in 5G, such as the cloud-friendly Service Based Architecture (SBA) and network slicing, will enable low-latency communications (uRLLC), massive machine type communications (mmTC), and time-sensitive networking (TSN), which will allow operators to offer new services oriented to the developers of high-performance, industrial applications and empower the introduction of new, disruptive commercial models.

While consumer-based offerings such as voice, text, data, and video will remain an integral part of the telco operator service portfolio, new enterprise-based offerings such as LTE/5G private networks, IoT applications, and augmented/virtual reality (AR/VR) experiences will drive unprecedented revenue opportunities for operators. Yet, to deliver these next-generation enterprise services, telco operators will need to look beyond the traditional telco network architecture to cloud and multi-access edge computing (MEC).

We believe that private mobile networks represent a strong use case for 5G enterprise services, as these capabilities will underpin the more sophisticated services, such as smart cities and Industry 4.0 applications. The demand for private enterprise networks is already here, as evidenced by the fact that 4G private networks are emerging in enterprises worldwide.

A confluence of factors is driving the practicality of private enterprise mobile networks. The limitations of current in-building wireless systems, the rising amount of generated data, the increased need for mobility, security, and the demand for real-time data processing are evidence that a new approach is required. The convergence of 5G, MEC, and the cloud now makes it possible to create private wireless networks that are ultra-fast, secure, scalable, and can take advantage of powerful cloud applications for analytics.

Yet, for all the advantages of a 5G private network, challenges remain for operators and enterprises. First and foremost is the complexity of deploying and managing a 5G network within the enterprise environment. 5G networks have many considerations that lie outside the traditional enterprise skill set, from RF design to 5G mobile core architectures. Simultaneously, telco operators may lack the technology portfolio to deploy 5G networks and cloud edge computing within the enterprise environment.

Microsoft proposes a simplified approach that combines a hyperscale cloud platform, integrated MEC components, a rich ecosystem of cloud applications, and a cloud-native 5G mobile core. Our approach enables the enterprise to collect data from across their network, process it efficiently at the edge, and leverage Azure's robust suite of IoT, analytics, AI, and machine-learning tools to deliver much greater value.

# Benefits of private mobile networks

The arrival of 4G changed private mobile network economics by allowing enterprises to deploy a dedicated network using small cell technology and virtualized network functions. With 5G comes faster speeds, lower latencies, improved cost efficiencies, and richer capabilities. These features are desirable to industries such as manufacturing and transportation, where geographic challenges and expanding IoT applications require the enhanced network characteristics (e.g., high bandwidth capacity, real-time processing) that 5G can provide.

At Microsoft, we see the demand for 5G private networks driven by several key benefits: low latency, deterministic access support, higher throughput, greater coverage, data localization/privacy, operational simplicity, backhaul savings, and legal and regulatory compliance improvements.

**Low latency**
5G networks offer much lower latency than 4G networks—around an order of magnitude less. This is important for time-sensitive applications such as robotic control systems, which typically have round-trip latency budgets of 10 ms or less. 5G networks, with applications deployed in local edge compute facilities, can comfortably support such latency requirements.

**Deterministic access support**
5G radio, by design, supports deterministic access. This places a guaranteed upper limit on latency and jitter, which is important for many kinds of applications. In this dimension, 5G is far closer to the performance of wired Ethernet. Applications that would have required wired connections in the past can now be untethered, thanks to 5G.

**Higher throughput**
While 4G technology is capable of delivering the throughput demanded by many private network applications, 5G can deliver 10-20x the throughput of 4G, expanding the range of applications that can be supported wirelessly, resulting in a truly future-proof network.

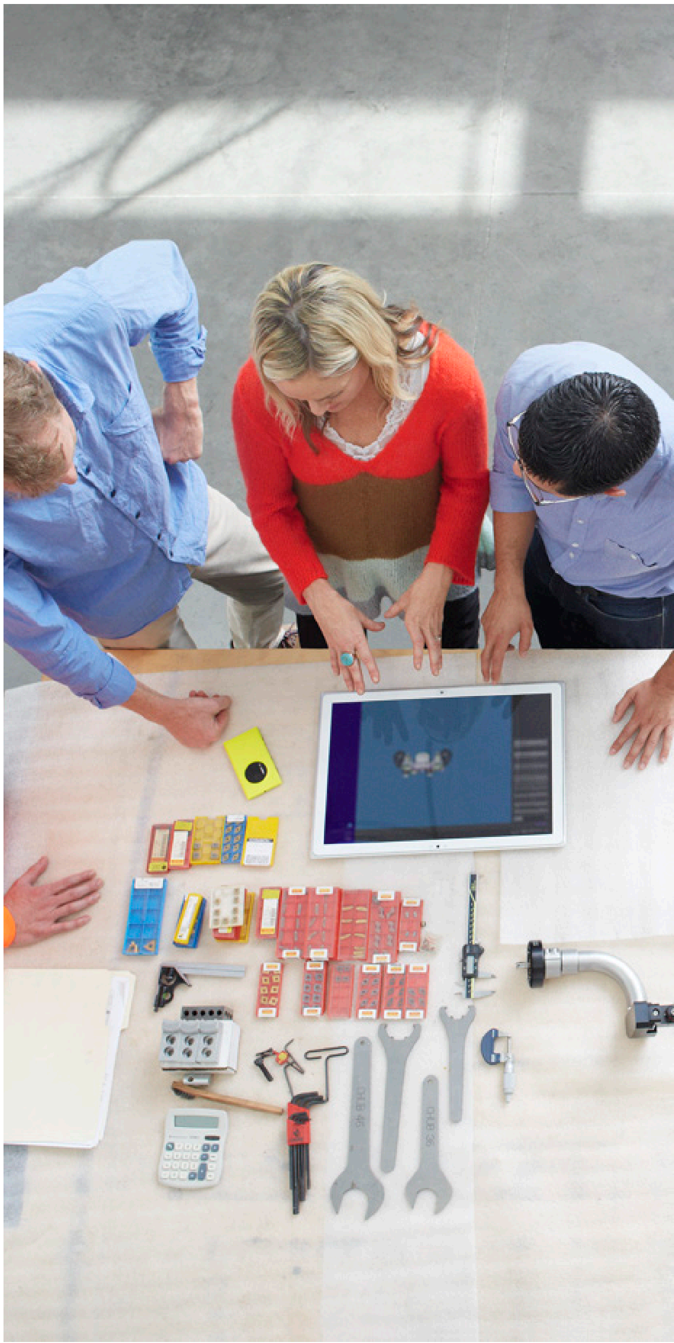
**Greater coverage**
Many industrial and enterprise applications demand wireless connectivity that exceeds the range limitations of Wi-Fi technology. 5G radio access networks provide high-performance and cost-effective wireless connectivity over large sites, including airports, seaports, open-cast mines, distribution centers, campuses, and construction sites.

**Data localization/Privacy**
Using traditional corporate networks, enterprises are able to effectively limit the exposure of data to specific geo-fenced regions. However, with the widespread adoption of wireless technologies, the ability to limit data exposure came at the price of restricting access. Private mobile networks, combined with edge computing, can provide better visibility and control over where data is accessed and processed. They enable highly sensitive information to be kept securely and locally while not being exposed over external network connections.

**Operational simplicity**
Today, operators are faced with implementing multiple versions of network technology, along with access control and other security functions based on the need for wired, Wi-Fi, and, increasingly, mobile broadband access to corporate resources. Private wireless networks will offer corporate IT the opportunity to build a simplified access architecture that will work for employees in the office and on the go.

**Backhaul savings**
Some types of industrial and enterprise applications—such as high-resolution video cameras for surveillance or inspection—generate vast volumes of data. These applications usually involve some mix of storage and analysis. While they are typically not highly latency-sensitive, it makes sense to deploy such applications in local compute facilities to avoid the high cost of backhauling very large volumes of data to a centralized cloud. Private mobile networks make this possible. Connectivity to centralized cloud facilities then only has to handle summarized data, for example, information about actionable events detected by local analysis.

**Legal and regulatory compliance improvements**
Private 5G mobile networks help enterprises protect themselves from a constantly evolving set of threats to their information and communications security. 5G radio is inherently more secure than any earlier generation of cellular technology and includes protection from sophisticated attacks, such as IMSI-catcher or Stingray.



# Path to private 5G networks

Private 5G networks exist at the intersection of the traditional enterprise LAN space, specialized industrial networks, and the public mobile network. They offer operators a chance to expand the scope of the 5G services into a market arena in which they have never previously competed.

In considering how to deploy private 5G networks, many enterprises will look favorably on mobile network operators as potential suppliers of the solution. Operators are viewed by enterprises as trusted partners in communications, and commercial relationships between them are already well-established. Operators have a great deal of expertise in successfully deploying and operating secure and reliable mobile networks, and depending on the local situation with regard to spectrum licensing, there may be a regulatory requirement for an enterprise to partner with a mobile operator in order to deploy private 5G.

> "In considering how to deploy private 5G networks, many enterprises will look favorably on mobile network operators as potential suppliers of the solution."

Some network operators may view private 5G networks as a natural extension of their public mobile networks. They could leverage their existing network assets, including the mobile packet core and the radio access network, and use network slicing to securely partition enterprise mobile traffic from public networks. The architecture of 5G networks and, in particular, the separation of control plane and user plane makes it possible to use an existing centralized mobile packet core to provide the control plane for private 5G networks while keeping user plane traffic local to the enterprise.

While this approach may be suitable as an initial offering or for relatively simple services, such as a dedicated network for a particular industry vertical with limited management options, enterprises may require more control than is possible with this approach. Today's solutions for public networks were not designed for multi-tenancy or managed services. It would require an enormous amount of work to enhance the traditional 4G mobile packet core control and management plane so that the necessary management capabilities can be delegated to enterprise customers. Furthermore, public networks have been built out primarily to serve the mobile broadband market, and they are highly optimized for this purpose. Enterprise applications will place all sorts of new and different demands on the network, which simply won't offer the flexibility needed to meet these demands.

To take full advantage of the control offered by the network slicing features of 5G, operators and enterprises should take advantage of the programmability and disaggregation offered by 5G.

# Critical attributes of a private mobile network

So, what does an effective private mobile network solution—one that operators and enterprises alike can feel confident in deploying—look like? The answer can be summarized in three key solution attributes:

1. **Managed connectivity.** While many enterprises have experience with managing their Wi-Fi network and mobile access points, few have experience with 4G/5G radio network design and deployment. This presents an opportunity for the operator to bring a managed radio and spectrum solution to meet the enterprise's needs.

2. **Managed services.** A private mobile network partner that can provide managed services adds significant value to the customer. These managed services would ideally address the RAN, core, and edge components in the solution. Moving the total solution management into a centralized, cloud-based environment allows operators and managed service providers (MSPs) to deliver end-to-end managed services from a single pane of glass. Leveraging automation and a software-based architecture—rather than hardware-based architecture—is essential to providing a compelling service experience and creating a clear ROI model for enterprises to adopt private mobile networks.

3. **Self-management options.** Use cases for private mobile networks are as unique as the businesses they serve. For example, a remote oil-drilling platform will have very different mobile network considerations than an automotive manufacturer. To address these varied use cases, there must be flexibility and simplicity in how these networks are configured, deployed, and managed. Where possible, portals and dashboards can simplify service customization. Service level assurance must also be customizable and visible to the enterprise. To achieve broad adoption, the installation and management of private wireless networks must be greatly simplified for both the operator and the enterprise.

> "There must be flexibility and simplicity in how these networks are configured, deployed, and managed."

# Building a private mobile network

## An integrated approach with Azure

There are four critical components to a private mobile network: the local radio resources, the edge compute platform, the application ecosystem, and the cloud. Today's private mobile network solutions are often built as a collection of loosely integrated components. While this loose integration approach may make sense in terms of physical and organizational demarcation points, it has several critical drawbacks: it is challenging to deploy, complex to manage, costly to scale, and inherently insecure.

Microsoft offers operators a different approach: a fully integrated, yet open, private mobile network solution that features cloud-native mobile core technology, advanced edge computing, and a hyperscale cloud environment that is designed for enterprises but delivered by operators/MSPs. Microsoft's architectural approach to private mobile network provides unique advantages to both operators and enterprises while integrating with multiple radio access technologies. The advanced edge computing not only provides a platform to host mobile core, but the same platform can be leveraged to host O-RAN components like vCU and vDU from Microsoft's partner ecosystem.

**Azure Stack Edge: the edge, simplified**

An operator needs to provide both the local radio infrastructure and the managed compute in a private mobile network service. A cloud edge computing component is also required to process the cloud services and applications. Some solutions propose splitting the compute functions into two boxes: one managed by the operator and the other by the cloud service provider. But this solution architecture introduces a myriad of management and security issues for the operator and the enterprise.

For example, consider the scenario where the enterprise customer is a national retail chain with hundreds of stores. To deploy a private mobile network across these stores would require two distinct compute platforms at every location: one for the mobile network functions (managed by the operator) and another to run distributed cloud and enterprise-developed applications. The management complexity issues are self-evident.

> " Azure Zero Trust security model ensures that every application and all traffic are secure from end to end."

Microsoft proposes a different approach: a shared, secure edge where both the mobile network functions and local edge applications run side-by-side in a common zero-trust security framework provided by Azure Stack Edge. This approach offers seamless integration between the 5G network, edge computing, and the cloud and significantly reduces CapEx and OpEx. Azure Zero Trust security model ensures that every application and all traffic is secure from end to end.

**Single-pane-of-glass management**
With Microsoft, the mobile core, edge, and cloud services are all managed from the Azure portal, which is a starkly different approach than other vendors. A single, centralized management environment makes it much easier for operators and the enterprise to manage and control the network experience. The single-pane-of-glass approach not only allows operators to deploy the service but quickly instantiate the private mobile network service at scale for its enterprises. This portal can then be used for full-service assurance and automation, including configuration, fault, and performance management.

### Integration with Azure Services

Microsoft's approach opens up a rich ecosystem of applications to operators and enterprise customers, including business intelligence/analytics, artificial intelligence, and machine-learning applications from Microsoft and many others. Affirmed Networks, now part of Microsoft, provides the cloud-native mobile core on the single architecture, allowing enterprises to quickly move data in and out of their mobile network for processing in the cloud while intelligently choosing which data should be processed on-site and which should be sent to the cloud.

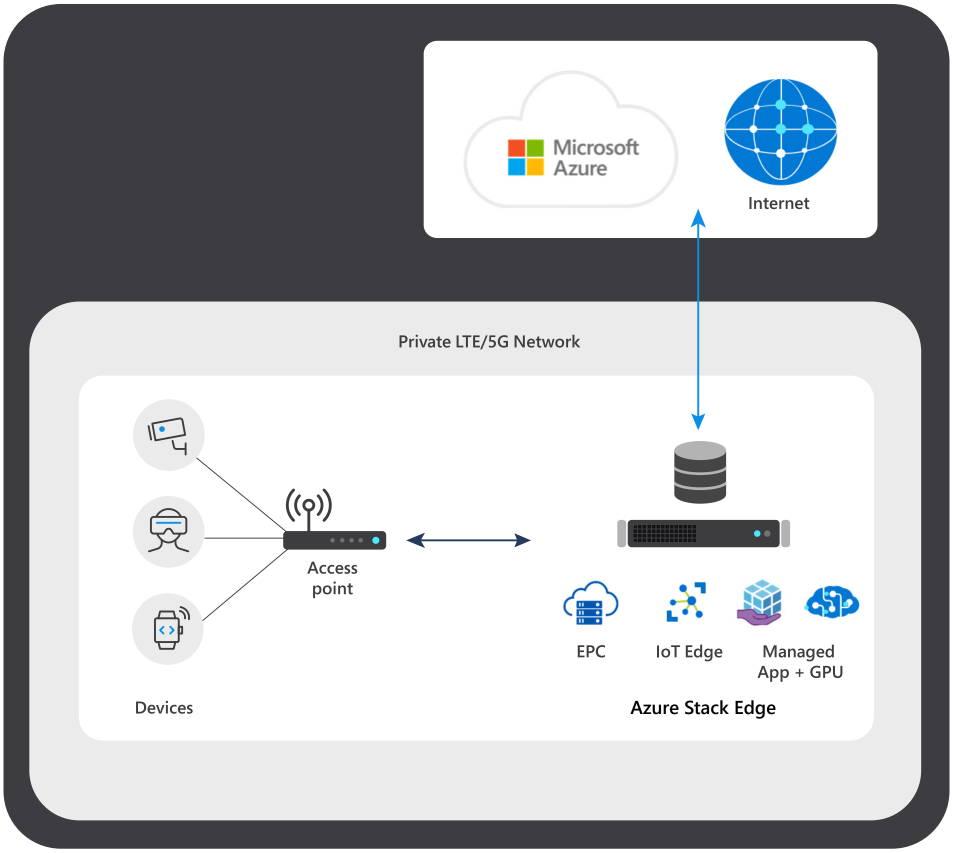


*Figure 1*

## Run applications and network functions side by side

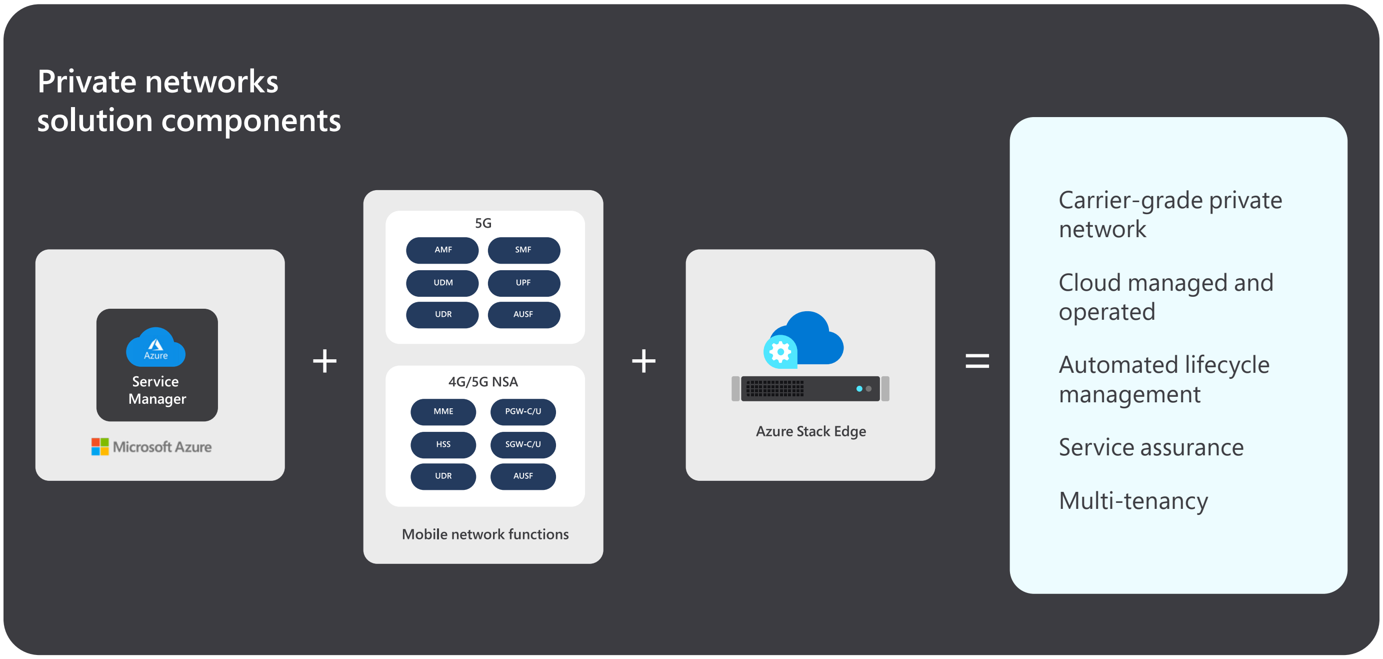
- Run managed applications such as video interferencing using GPU on the device
- Deploy Azure and 3rd-party network functions from an ecosystem of partners that enable private wireless networks
- Cloud-native orchestration, monitoring, configuration, and updates for applications and Virtual Network Functions

### Private mobile network-as-a-service

Affirmed Networks, now part of Microsoft, continues to develop revolutionary core technology that allows operators, for the first time, to deploy a complete CBRS/4G/5G mobile core in the cloud as a service. The private mobile network-as-a-service approach completely changes the way private mobile networks are deployed and managed. Instead of being tied to location-based hardware, operators now have greater flexibility and can provide the mobile core functionality as a hosted and fully-managed service within the Azure for Operators cloud, whether on-premises or in the cloud.

# Solution components

Microsoft's approach to private mobile networks is a completely integrated solution from the mobile core to the edge to the cloud. This solution architecture has four key components: Azure Stack Edge, Affirmed Service Manager, Azure Network Function Manager, and Affirmed Mobile Core.



- Carrier-grade private network
- Cloud managed and operated
- Automated lifecycle management
- Service assurance
- Multi-tenancy

*Figure 2*

**Azure Stack Edge**
Azure Stack Edge provides a single point for processing mobile network data at the edge. Microsoft's edge computing platform acts as an extension of the Azure cloud into the enterprise environment. With the mobile network environment, integration between Azure Stack Edge and Affirmed 4G/5G mobile core technology enables local, intelligent breakout of data processing and seamless data sharing for faster processing and lower bandwidth consumption.

> "This solution architecture has four key components: Azure Stack Edge, Affirmed Service Manager, Azure Network Function Manager, and Affirmed Mobile Core."

**Affirmed Service Manager**
Affirmed Service Manager is the application that operators use to deploy, monitor, and manage private mobile core networks on the Azure platform. Service Manager is the heart of the solution, providing the key speed, agility, and automation required to deploy and manage private mobile networks at scale. It automates the lifecycle management of private network services and is completely open to provide REST APIs to integrate with other operator systems, like Sim Management or OSS/BSS. The Service Manager includes capabilities like device provisioning, policy management, and service assurance. It is designed for operators to become Managed Service Providers; hence, it can operate in a multi-tenant model and support role-based access controls to provide flexible control to enterprise customers.

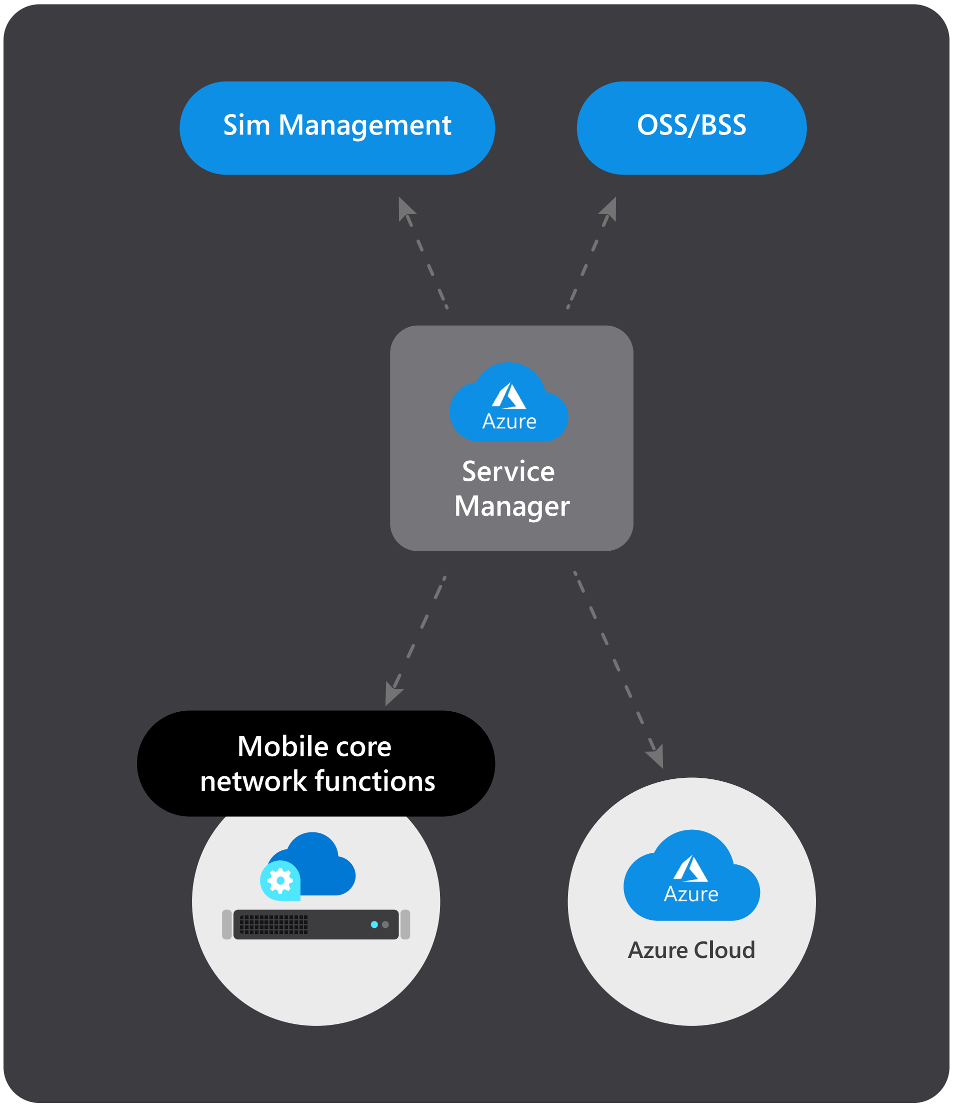


*Figure 3*

## Azure Cloud Hosted and Cloud Managed

**Automated private network service lifecycle management**

- Automation
- Network orchestration
- Service orchestration
- Service management

**Device provisioning and integration to SIM management**

- Bulk production, activate, deactivate, and delete devices

**Policy management**

- Device profiles, QoS policies, and traffic management

**Rest APIs for northbound OSS/ BSS integration service assurance**

- Observability
- Topology view and aggregation
- Customizable enterprise dashboards
- Monitoring

**Multi-tenancy with role-based access control**

- Provides limited control to enterprise customers

### Network Function Manager

Azure Network Function Manager (NFM) is a fully managed cloud-native orchestration service that enables customers to deploy and provision network functions on Azure Stack Edge Pro with GPU for a consistent hybrid experience using the Azure portal.

When used with Azure Stack Edge, NFM provides deployment, provisioning, and secure cloud-based management of your on-premises network functions or apps directly from the Azure portal. A managed service means that an Azure-managed service provider handles updates, lifecycle management, and support for your network functions and applications running on the edge device. The platform supports virtual machines and containerized workloads, along with one or two GPUs for acceleration.

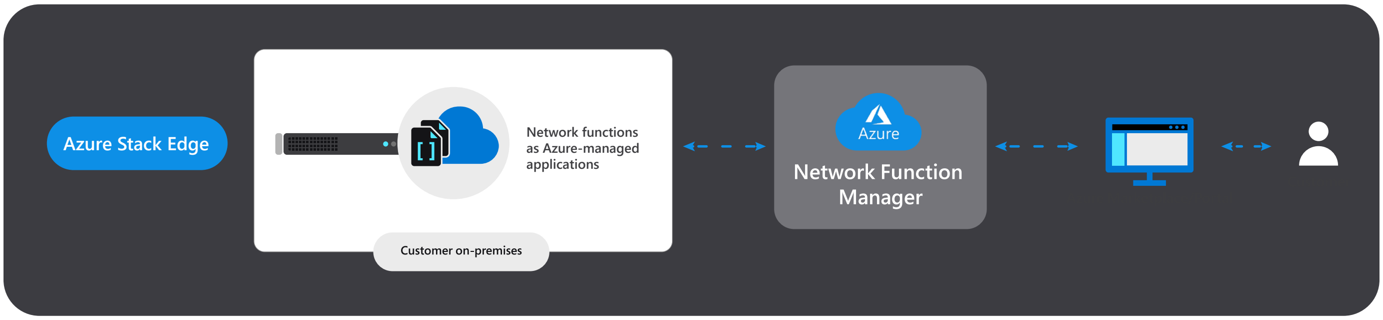


*Figure 4*

### Affirmed Mobile Core

The final component of Microsoft's architectural approach to private mobile networks is the 4G/5G mobile core, which can be deployed as a non-standalone (NSA) 5G core, standalone (SA) 5G core, or 4G virtualized Evolved Packet Core (vEPC) as a single platform. This solution delivers a fully integrated cloud/edge/5G solution to operators. Affirmed's 5G core solution provides a fully virtualized, cloud-native solution that includes all standard 5G core network functions—user plane function (UPF), access and mobility management function (AMF), session management function (SMF), policy control function (PCF), network exposure function (NEF), network slice selection function (NSSF), etc.—plus enhanced functionality (see Figure 5 below), such as virtualized network probes, Wi-Fi interworking, and service automation platform. The 5G core can be deployed on VMs, physical servers, or on an operator's cloud as a mobile-core-as-a-service, eliminating the need for dedicated hardware.

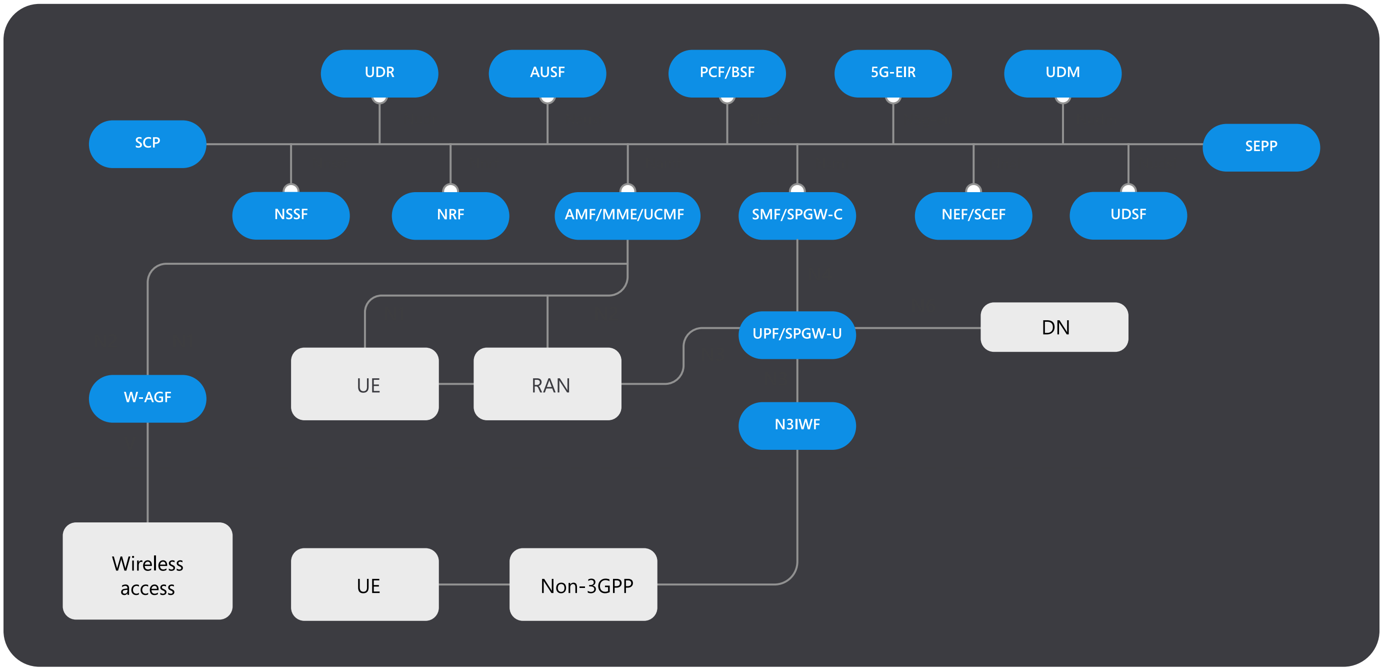


*Figure 5: 3GPP diagram*

# Solution architecture

This solution is fully integrated and cloud-based, which significantly lowers the total cost of ownership of operating a private cellular network. This is achieved through the following key solution attributes:

1. **Automation**
2. **A true cloud-native solution**
3. **Remote management**
4. **A fully integrated solution**
5. **Flexible deployment models**

The Microsoft Azure platform also has built-in features that support the attributes above, including security, five nines of reliability/availability, and mobility.

### 1. Automation

Automation delivers a better user experience and simplifies deployment. Solution deployment can be reduced from weeks to days through automation, whether the deployment is managed by the operator, a managed services provider (MSP), or a Systems Integrator (SI). This is extremely important; otherwise, the scale needed to deploy the solution to thousands of enterprises and consumers is unattainable.

The Service Manager is hosted on and leverages the Azure cloud to fully automate the deployment and configuration of the Private Networks Edge Stack on Azure Stack Edge. The Service Manager automates one of the most complex and challenging Day 0 tasks: orchestrating multiple network functions for 4G LTE (MME, SGW, PGW, HSS, SAS) or 5G (AMF, SMF, UPF, AUSF, UDM, UDR, UDSF). It also automates the Day 1 task of service creation across these network functions with minimal input from the customer.

Affirmed 5G core has an integrated vProbe function that can be leveraged to create network insights. These insights can be leveraged for closed-loop automation and providing service assurance to the customers. Beyond network insights, this data can provide useful business intelligence and network monetization to enterprise customers.

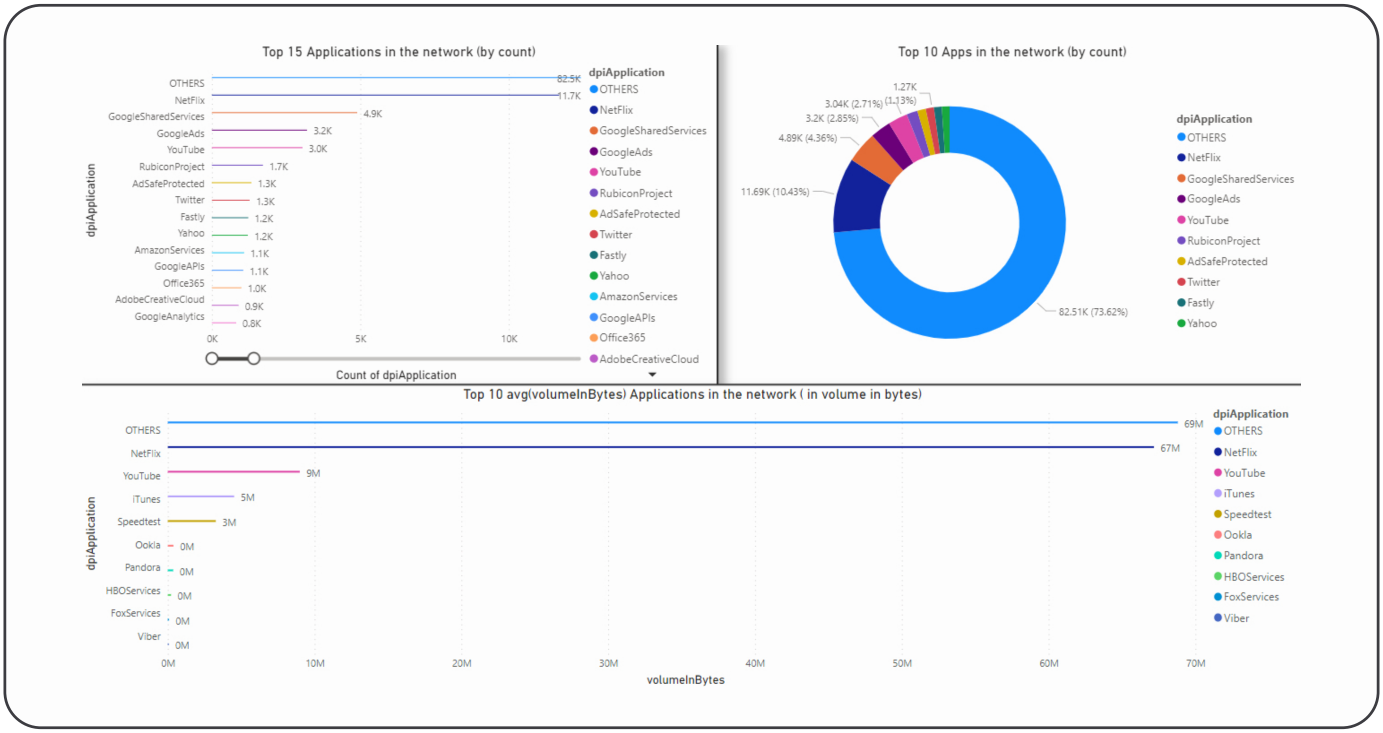


*Figure 6*

### 2. True cloud-native solution on Azure

By leveraging both the Azure cloud and Azure Stack Edge, the solution architecture brings the benefits of cloud economics and a pay-as-you-go consumption model. This allows customers to size and deploy the solution for their current workload and avoid the risk of underestimating or overestimating resource requirements. Another benefit the Azure cloud brings is built-in security and privacy compliance. Customers can confidently deploy the solution for verticals that require stringent data privacy laws, such as healthcare, government, public safety, and defense. Deploying an edge-based solution with Azure Stack Edge provides both connectivity services and the ability to deploy edge applications. This helps customers deploy edge applications that require low-latency and edge-compute processing.

### 3. Remote management

The solution is fully managed remotely through the Affirmed Service Manager on the Azure cloud. This is a multi-tenanted solution that gives role-based access control to end-users via personal dashboards that allow them to view, manage, and control adds/removals and activate/deactivate devices on the private mobile network. Remote management provides big cost savings to customers for several reasons. First, it doesn't require truck rolls to service the solution. Second, it eliminates the need for a bulky OSS solution because it can be completely managed through Service Manager, and third, exposed northbound APIs can be easily integrated with existing subscriber identity management (SIM) and OSS/BSS solutions.

### 4. Fully integrated solution

The end-to-end solution can be integrated with a variety of other RAN and SIM systems through the Microsoft partner ecosystem. In addition to broad integration with other applications on Azure, such as AI/ML and IoT hub, the solution has many built-in features that enterprises require for service integrations. These features typically incur separate cost, compute, and complex operations, but with Microsoft's approach, these essential functions are integrated and included as part of the solution with no additional need for hardware. Services include support for IPsec, GRE, DPI, vProbe, vRouter, and CG-NAT. The solution also offers integrated, advanced local policy to allow differentiated traffic treatment, shaping, and management based on the configured user policies.

### 5. Flexible deployment models

Private networks require the solution to be deployed in different environments with diverse needs. Hence, flexibility in deployment models becomes critical. The Affirmed mobile core ensures that the solution can be deployed in several different ways: as a standalone edge in an isolated environment, in distributed mode by centralizing the control plane on Azure cloud and distributing the user plane on Azure Stack Edge, and fully-hosted on Azure cloud. This flexibility allows the solution to be deployed in various configurations and address all possible mobility, roaming, and operator network integration scenarios.

> " Flexibility allows the solution to be deployed in various configurations and address all possible mobility, roaming, and operator network integration scenarios."

**A. Standalone Edge Model:** The RAN, 5G core, including both Control Plane and User Plane, are on the edge on Azure Stack Edge while the management layer is in the centralized cloud. This model is suited for deployments where chances of cloud connectivity disruption are high due to reduced bandwidth between the cloud and the edge. In such cases, a completely isolated standalone private network on-premises is preferred. Such use cases include mining, remote offshore oil rigs/platforms, and large agriculture farms.

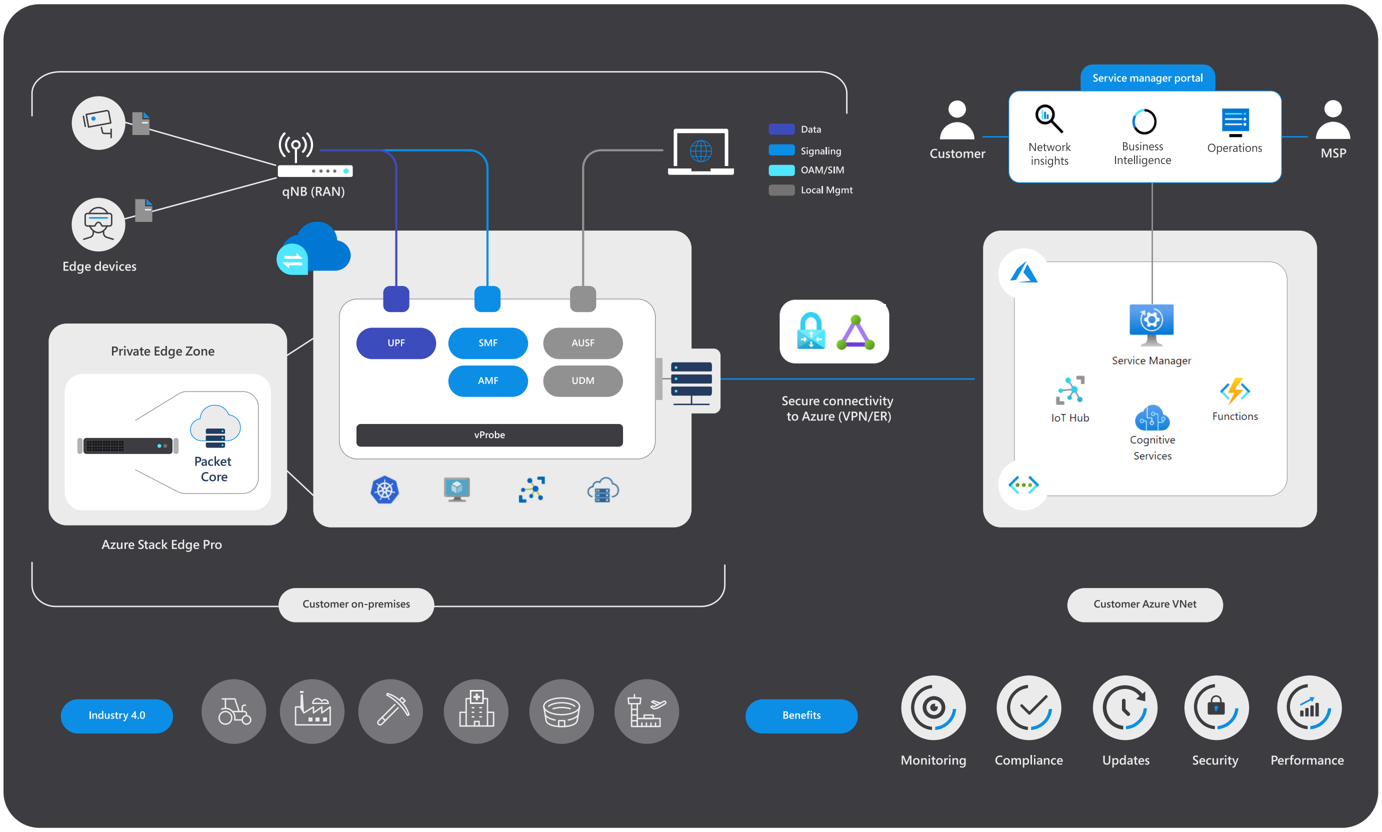


*Figure 7*

**B. Distributed Edge Model:** The 5G Core Control Plane is on Azure cloud while User Plane is on Azure Stack Edge. This model is well suited for deployments in urban industrial areas where there are many manufacturing units well-connected with the cloud but needs local edge processing and breakout for tight industrial control, robotics, or AGVs. This solution offers simplified management of control plans from a centralized location and fewer touchpoints to integrate the control plane with other network functions.

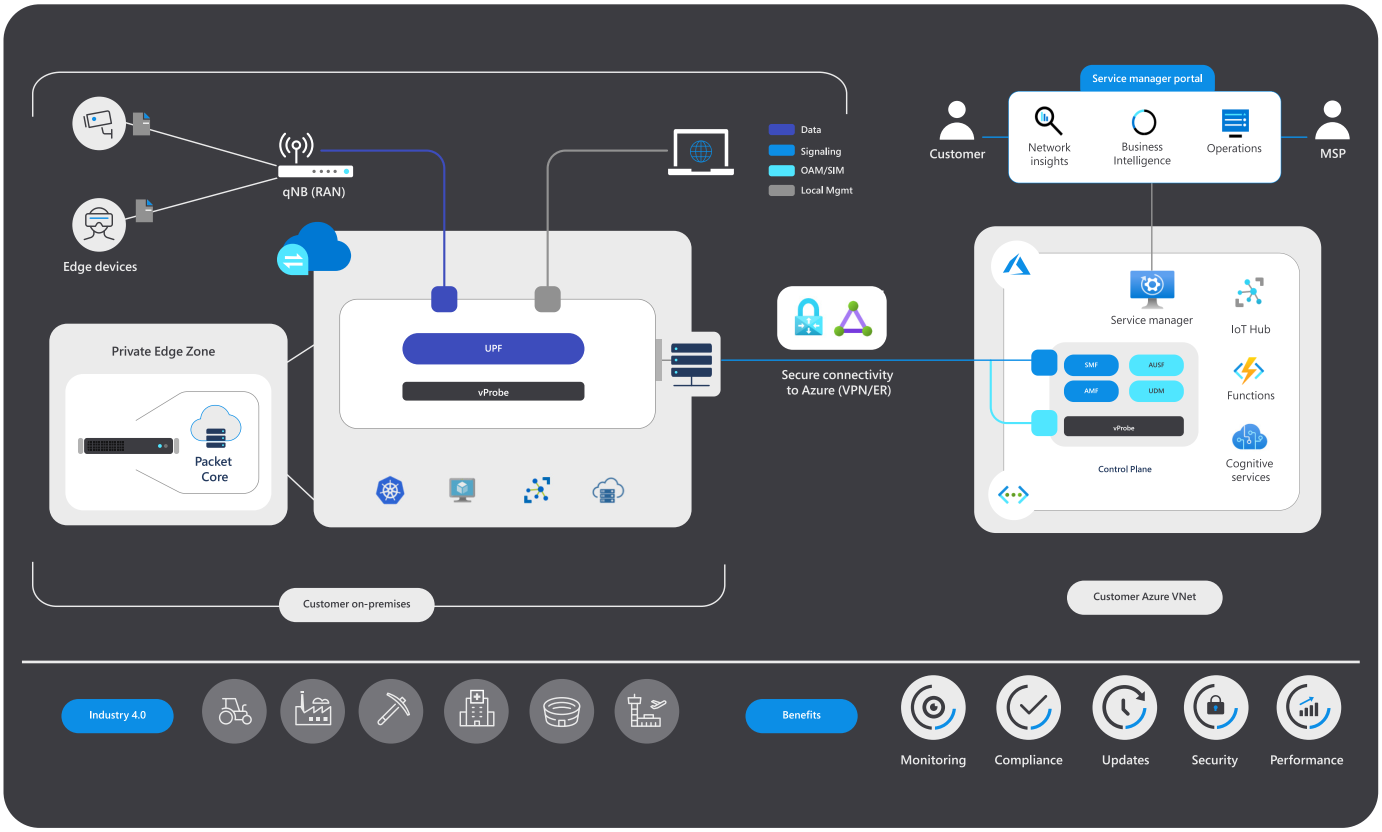
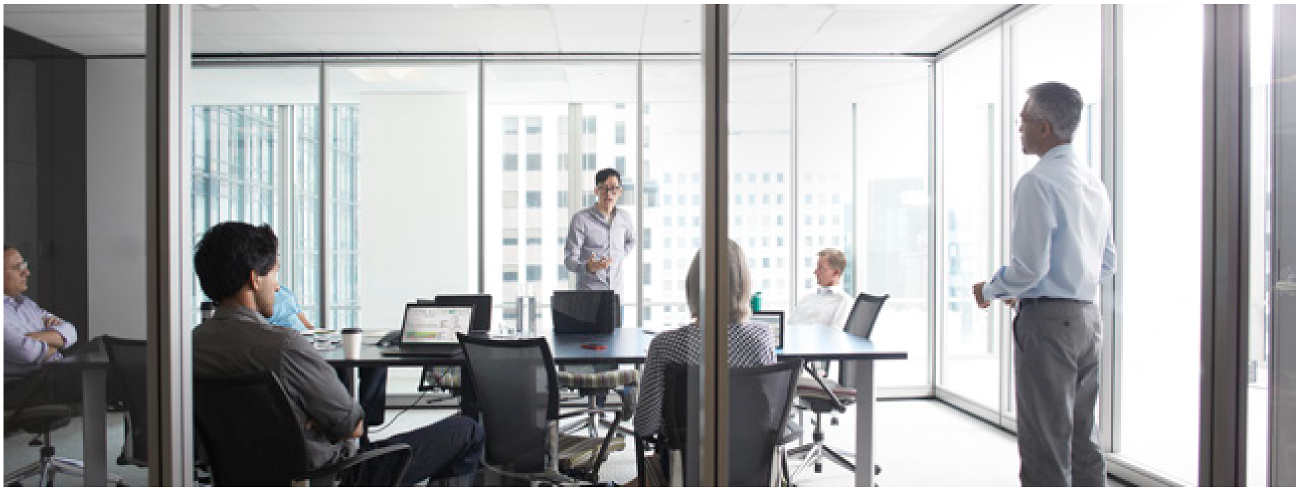


*Figure 8*



**C. All on Cloud:** The entire 5G core is on the cloud with just the RAN on the edge. This is well-suited for applications with a higher latency budget and low throughput requirements. The elastic nature of the workload allows most cost benefits to dynamically scale in and scale out cloud resources with shrinking or growing workload demand.

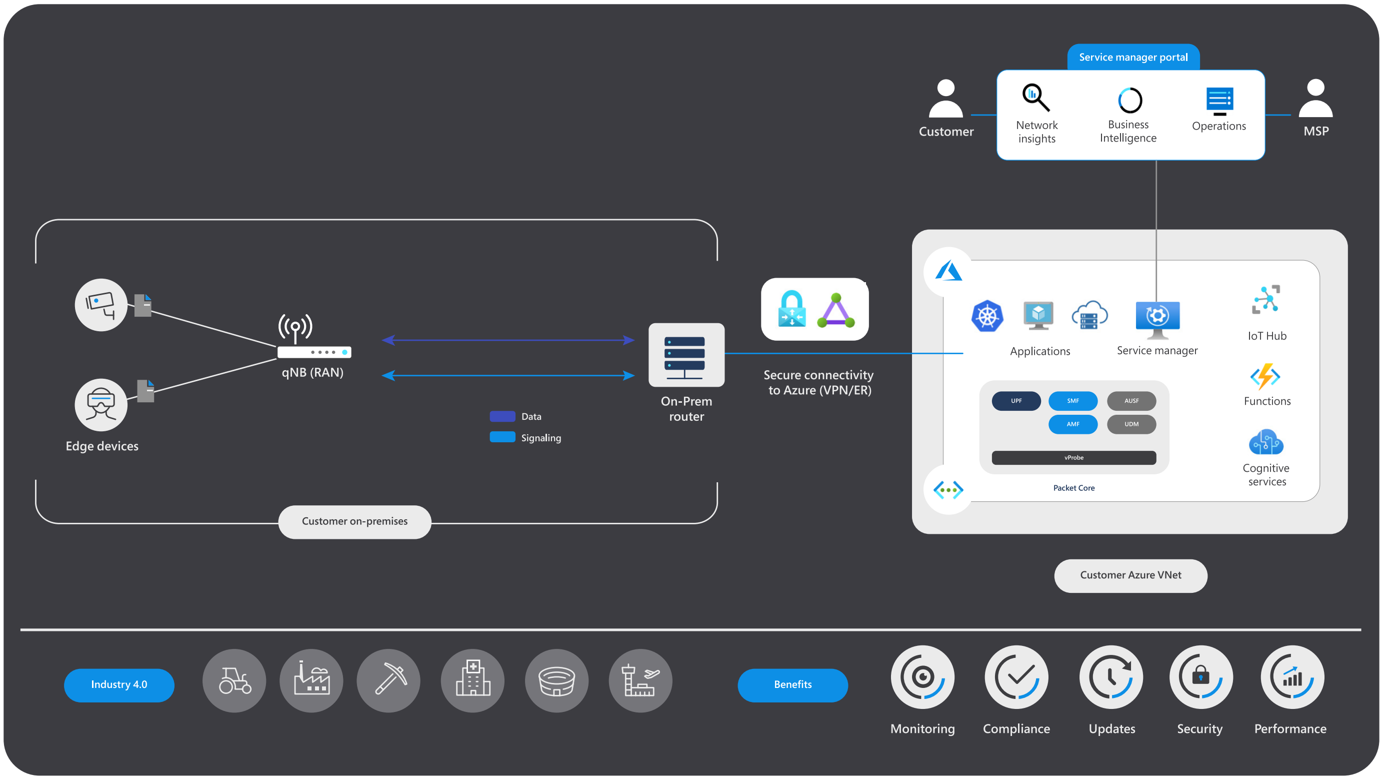
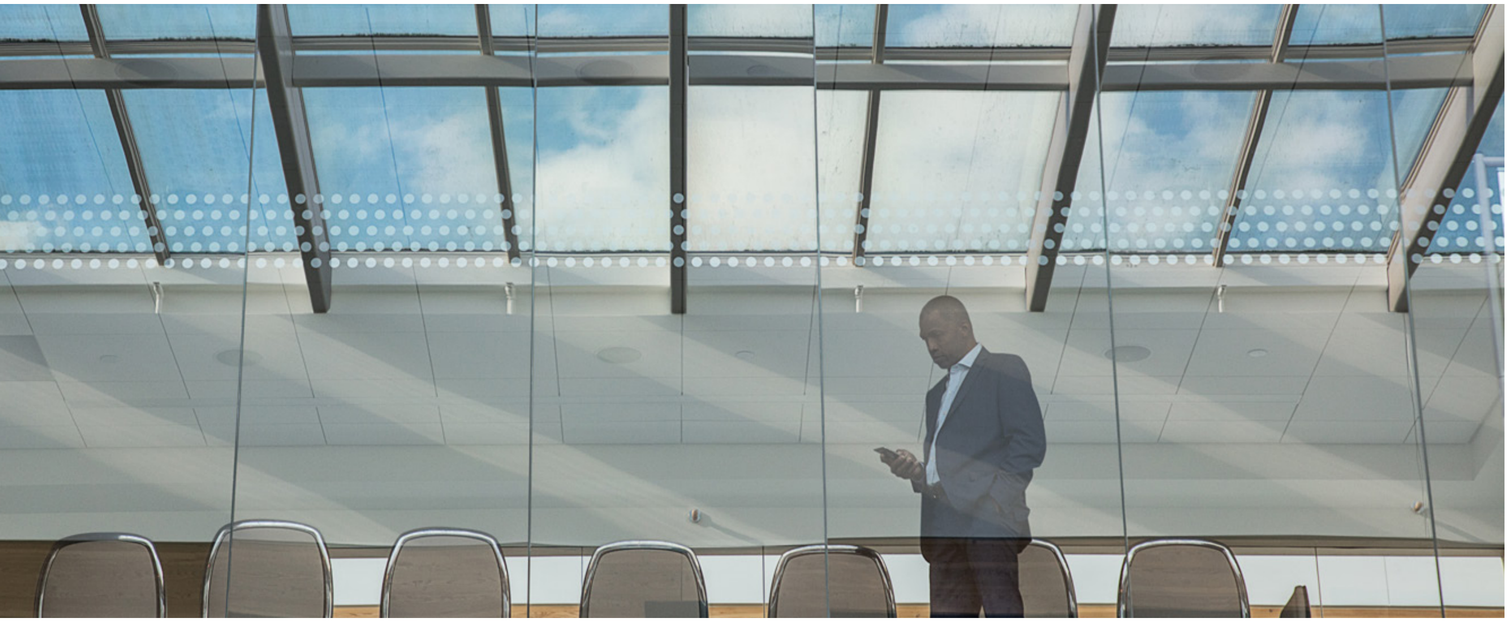


*Figure 9*



# Key benefits

Microsoft's cloud-based, MEC-enabled, fully integrated approach has clear benefits to operators looking to deploy private mobile networks, including:

- A carrier-grade network experience built on a visionary, proven 5G mobile core architecture that runs in many of the world's leading mobile service provider networks.
- A cloud-managed and operated solution hosted in a global, hyperscale cloud environment explicitly designed for tier one (and smaller) carriers.
- Automated lifecycle management that simplifies the administration, security, and operation of private mobile networks.
- Service assurance that meets five nines of reliability and availability to support mission-critical applications.
- A multi-tenant model that allows operators to cost-effectively manage private network services through a single management console, including full integration with existing billing and customer care systems.
- The ability to tap into powerful cloud and IoT applications, including Azure's built-in AI and machine-learning capabilities.

**4G and 5G deployment flexibility**
Operators don't have to deploy 5G to realize the value of a cloud-enabled private mobile network. With Microsoft's approach, enterprise customers and operators can deploy private mobile network in a 4G only, 5G only, or hybrid 4G/5G environment. Affirmed's fully virtualized mobile core technology supports a seamless transition from 4G to a 5G non-standalone or 5G standalone core. This flexibility allows enterprises to start with a 4G implementation and migrate seamlessly to 5G or deploy a hybrid 4G/5G private mobile network solution.

**The operator experience**
The offering delivers the high-performance, high-availability, low-latency requirements of telecommunications cloud services that service providers expect. Microsoft's approach to private mobile networks is optimized for operators and MSPs, allowing them to easily manage and control private mobile network services for their enterprise customers. By addressing the infrastructure requirements of private mobile networks in a simple, seamless, and highly scalable platform, the solution allows operators to focus on their strengths and bring the value of Microsoft's industry-leading cloud applications to their customers rapidly and securely.

# Navigating the enterprise network design considerations

As enterprises become better-educated consumers of private mobile network services, they will look for specific features that align with their unique requirements and use cases. Here are some of the questions that mobile operators can expect to hear from prospective enterprise customers.

**How integrated are the mobile core and edge platforms?**
Seamless integration between the core and edge provides reassurance that the private network solution will work as advertised. Multi-vendor solutions can lead to lengthy integrations and challenges when technical issues arise. Because private mobile networks are handling mission-critical applications, disruption is not an option.

**Does the solution offer end-to-end management of the core and edge components?**
Running multiple management tools creates complexity and confusion. A network probe system can provide the end-to-end visibility and management needed for operators to assure service levels and monitor network performance confidently.

**Is the solution carrier-grade?**
Carrier-grade networks deliver five nines of availability and reliability. Enterprises expect the same levels of performance in their networks. A solution that features a proven, integrated architecture from the core to the intelligent edge to the intelligent cloud makes it easier for operators to extend carrier-grade availability into enterprise networks.

**Is the solution simple yet flexible enough to scale dynamically?**
As enterprises realize the benefits of running applications and operations on a private mobile network, the network footprint will expand into other business areas and other sites. Operators will need to scale these solutions quickly and cost-effectively—an area where having a cloud-based mobile core offers a distinct advantage.

**How secure is the network?**
Security is top of mind for enterprises. The effective deployment of a Zero Trust security model within a common architecture ensures the consistent application of security policy across all functions—both operator and enterprise.

**Will the private mobile network integrate with my existing business applications and support my devices?**
Azure’s approach is to provide open and standardized northbound and southbound APIs for seamless connectivity and integration with business applications and devices. Azure’s extensive partnerships with a majority of the network application and device vendors provide out-of-the-box APIs and tool kits for smooth integration. Because Microsoft owns both the cloud and the mobile core components, integration with OSS/BSS systems is streamlined. A unified platform also makes it easier to manage mobile devices’ lifecycle, from onboarding to upgrades.

**How can I see what’s happening in my network?**
A unified Azure solution ensures that enterprises and operators can view, manage, and monitor everything from telemetry data to network traffic through a single pane of glass. Common lifecycle management, security policy, and orchestration provide end-to-end visibility and control to manage the service securely and reliably.

**Does the platform support service automation and orchestration?**
Containers and microservices are the new building blocks for business applications. The ability to automate and orchestrate new mobile services is essential for operators and enterprises as they look to build new applications and services on top of their 5G network. Enterprises also need the option of hosting those applications on-premises or in the cloud. Azure’s unified solution provides end-to-end automation and orchestration across all domains and network functions: physical, virtual, and cloud.

**How do I analyze mobile network data for added value?**
Connected devices generate a wealth of data that can be analyzed for additional business benefits. With Microsoft, enterprises can quickly and securely bring data into the Azure environment for analytics—including third-party business intelligence tools—artificial intelligence, and machine learning.

# Use case

## IoT for Industry 4.0

Smart devices, automation, the cloud, and mobile broadband technology are driving the Industry 4.0 revolution. This, in turn, is fueling demand for private mobile networks in the manufacturing industry. As manufacturers look to connect smart devices and leverage telemetry data to support real-time decisions and improve operational efficiencies, private mobile networks can provide the foundation to achieve these goals.

**Maintenance prediction**

Monitoring and tracking quality

Potential damage, breakdowns, and bottlenecks

Dramatically improve operating efficiencies

**Smart factories**

Connected factory applications

Staff safety applications and air quality management

Access control (security) and smart analytics

**Manufacturing operations**

Includes asset management and intelligent manufacturing

Performance optimization and monitoring

Enables end-to-end operational visibility

The ability to efficiently process network data in the cloud helps manufacturers in a variety of ways:

- Proactively monitor and prevent production issues such as bottlenecks, breakdowns, machine wear, and process inefficiencies.
- Create "smart factories" by connecting business applications, safety and production data from sensors, and analytics in a real-time, secure environment.
- Improve manufacturing operations through end-to-end visibility, performance monitoring and optimization, and secure asset management.

Microsoft's approach to private mobile network is ideally suited to IoT and Industry 4.0 applications. The ability to process data in a single, on-premises platform and intelligently backhaul selective data for processing in the Azure cloud allows for real-time decisions and automation with exceptionally low latencies. A reduction in backhauled traffic also reduces costs, both for the enterprise and the operator.

Azure's Zero Trust model ensures that manufacturing data remains secure as it moves between the mobile network functions, the enterprise, and the cloud, which is critical because manufacturing production information could place a manufacturer in a vulnerable position if it fell into the wrong hands. This built-in security also frees operators from the arduous task of securing customer data themselves.

> " Built-in security also frees operators from the arduous task of securing customer data themselves."

# Looking forward

## To the Edge and beyond

The cloud and multi-access edge computing can unlock the potential of private mobile networks in new and exciting ways. This includes real-time analytics, artificial intelligence, and machine learning—applications that will enable enterprises to harness data from retail stores, manufacturing floors, and warehouses to improve business processes, tighten supply chains, and create better customer experiences. Microsoft is committed to helping telecommunications operators deliver this future by providing an approach that deploys 4G and 5G private mobile networks more effortlessly than ever before.

We believe the path to private mobile networks is clear: a single platform with a fully integrated mobile core, edge, and cloud that supports rapid and repeatable deployment, delivers best-in-class performance, reduces CapEx/OpEx costs, and simplifies management through a single pane of glass. By solving the critical infrastructure challenges to managing and deploying a private mobile network, the barriers to the future have been removed. The only limits that remain are those of the imagination.

To learn more about the cloud-driven private mobile network of tomorrow, visit us online at azure.microsoft.com.

# Glossary of terms and definitions

**AMF**
In the 5G Core Network, the AMF (Access & Mobility Function) is responsible for the Access and Mobility management of the mobile subscribers. It is the point of contact for all mobile users in the core network. It maintains connections with the Radio Access Network (RAN) to transport signaling messages to and from the users.

**AUSF**
Authentication Server Function supports authentication for 3GPP access and untrusted non-3GPP access.

**BSS**
Business Support System.

**Cloud native network function (CNF)**
CNF is a network function designed and implemented to run inside containers. CNFs inherit all cloud-native architectural and operational principles, including K8s lifecycle management, agility, resilience, and observability.

**Control Plane**
The Control Pane is the layer that has the components that are responsible for network traffic paths and for building a picture of the network topology. On traditional networks, this is done by building and sharing network tables. In software-defined networks, this functionality is decoupled from the physical devices and performed by SDN Controllers.

**Control and User Plane Separation (CUPS)**
CUPS stands for Control and User Plane Separation of EPC nodes and provides the architecture enhancements for the separation of functionality in the Evolved Packet Core’s SGW, PGW, and TDF. This enables flexible network deployment and operation by distributed or centralized deployment and the independent scaling between control plane and user plane functions—while not affecting the functionality of the existing nodes subject to this split.

**Data Plane**
The Data Plan is the layer that has the infrastructure to carry network traffic. It is sometimes called the Forwarding Plane, User Plane, Carrier Plane, or Bearer Plane. In traditional networks, the Data Plane functionality is provided by firmware in switches or other network devices. In software-defined networks, the Data Plane functionality is decoupled from hardware and delivered via software-based network elements. These contain SDN Datapath modules that replace the physical devices.

**DevOps**
DevOps is a set of practices that combines software development and IT operations. It aims to shorten the systems’ development life cycle and provide continuous delivery with high software quality.

**DN**
Data Network.

**EPC**
An Evolved Packet Core provides a converged voice and data-networking framework to connect users on a Long-Term Evolution (LTE) network.

**HSS**
A Home Subscriber Server is a database that contains user-related and subscriber-related information.

**Kubernetes**
Kubernetes is an open-source container orchestration platform that enables the operation of an elastic web server framework for cloud applications. Kubernetes can support data center outsourcing to public cloud service providers or can be used for web hosting at scale. Website and mobile applications with complex custom code can be deployed using Kubernetes on commodity hardware to lower the costs of web server provisioning with public cloud hosts and to optimize software development processes.

**LTE**
Long Term Evolution.

**MME**
The Mobility Management Entity deals with the control plane. It handles the signaling related to mobility and security for E-UTRAN access.

**NEF**
Network Exposure Function exposes capability information and services of the 5G CN Network Functions to external entities.

**Network Function (NF)**
The NF is a functional block within a network infrastructure that has well-defined external interfaces and functional behavior.

**Network Functions Virtualization (NFV)**
NFV is the principle of separating network functions from the hardware they run on by using virtual hardware abstraction.

**NRF**
Network Repository Function maintains the NF profile of available NF instances and their supported service.

**NSSF**
Network slice selection function is a cloud-native network function that supports network slice selection capabilities in the 5G system.

**N3IWF**
Non-3GPP InterWorking Function.

**OSS**
Operations Support System.

**PCF**
Policy Control Function supports a unified policy framework to govern network behavior and provides policy rules to Control Plane function(s) to enforce them.

**PGW**
The Packet Data Network Gateway is the point of interconnect between the Evolved Packet Core (EPC) and the external IP networks. The PGW provides connectivity from the UE to the external Packet Data Network (PDN) by acting as the point of exit and entry of traffic for the UE.

**SCP**
Service Communication Proxy.

**SEPP**
Security Edge Protection Proxy protects the connection between service consumers and service producers from a security perspective.

**SGW**
The Serving Gateway is the point of interconnect between the radio-side and the EPC. This gateway serves the UE by routing incoming and outgoing IP packets.

**SMF**
The Session Management Function (SMF) provides session management within a Fifth Generation Standalone Architecture (5G SA) core network at the highest level.

**UDM**
Unified Data Management supports user identification handling and access authorization based on subscription data along with subscriber management.

**UDR**
Unified Data Repository supports the storage and retrieval of subscription data, policy data, structured data, and application data.

**UDSF**
Unstructured Data Storage Function supports storage and retrieval of information as unstructured data by any NF.

**UPF**
The User Plane Function is a fundamental component of the 5G core infrastructure system architecture that allows for the packet processing, traffic aggregation, and management functions to be moved to the edge of the network.

**Virtual Evolved Packet Core (vEPC)**
Virtual Evolved Packet Core is a framework for mobile networks' voice and data processing and switching. It is implemented by Network Functions Virtualization (NFV), which virtualizes the functions of an Evolved Packet Core (EPC).

**Virtualized Network Function (VNF)**
A VNF is an implementation of an NF that can be deployed on a Network Function Virtualization Infrastructure (NFVI).

This document is provided “as-is.” Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Some examples are for illustration only and are fictitious. No real association is intended or inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Microsoft Azure