# Private Connectivity Over Cellular for Business Services

## Deliver a superior 5G/4G cellular network optimal for digitization and services in industry verticals

AT A GLANCE:

- **Reliable enterprise networking solution** for digitization, communications, and collaboration with virtually zero downtime
- **Guaranteed coverage** for areas Wi-Fi does not adequately address with virtually zero downtime
- **Reduced latency** for latency-sensitive applications
- **Superior quality of service** (QoS) with guaranteed connectivity for high-throughput, mission-critical applications
- **Predictable service level agreements** (SLAs) to meet the demands of various applications, location, and timing
- **Higher degree of security** with a ring-fenced network managed and operated by the enterprise
- **Cost-effective solution** comparable to, if not better than, Wi-Fi alternatives
- **Centralized management** offering granular control of how resources are used and traffic is prioritized
- **Operator-backed**, supporting both data and voice continuity from public to private domains
- **Multi-vendor** ecosystem of certified network function providers

The proliferation of connected devices in consumer and enterprise markets is driving requirements that traditional Wi-Fi networks cannot address. As enterprises move on their digital transformation journey, the transformation and automation of their operations and processes require high-performance and secure communications while accommodating the continuous expansion of applications, devices and users.

Private LTE and 5G connectivity is becoming the leading consideration for coverage, capacity, security, reliability and guaranteed quality. Private LTE and 5G cellular services offer a scalable solution suitable for enterprise, mining, auto manufacturing, and hospitals. Private LTE solutions are also suitable for telco edge cloud micro data centers, which can provide sliced connectivity to a smart city or a stadium hosting tens of thousands of concurrent connections.

### An opportunity for the service provider

Communications service providers (CSPs) are in a race to roll out 5G networks for increased capacity and low-latency networks. At the same time, enterprises and other business services are looking for highly reliable and secure cellular connectivity. Private cellular is an opportunity for the CSPs. Extending their core networks to the telco edges and enabling on-premises private use cases could be a new revenue opportunity.

The digital transformation journey has created a high demand for private networks. While enterprises can certainly deploy a Private LTE network, they face several implementation challenges: mobile network expertise, spectrum acquisition, and the cost of building and operating a private network.

CSPs are primed to maximize their revenue growth, leveraging their existing network and spectrum assets. Opportunities include:

- Growth in mobile and IoT devices and a continuous appetite for increased and reliable connectivity leads many enterprises to rethink how they need to connect.
- Requirement for improved security with granular levels of access control.
- A new wave of data-intensive devices being used for monitoring, surveillance, and video processing requires dedicated bandwidth.
- The digital transformation of many industry verticals require real-time data to optimize processes and increase revenue streams.

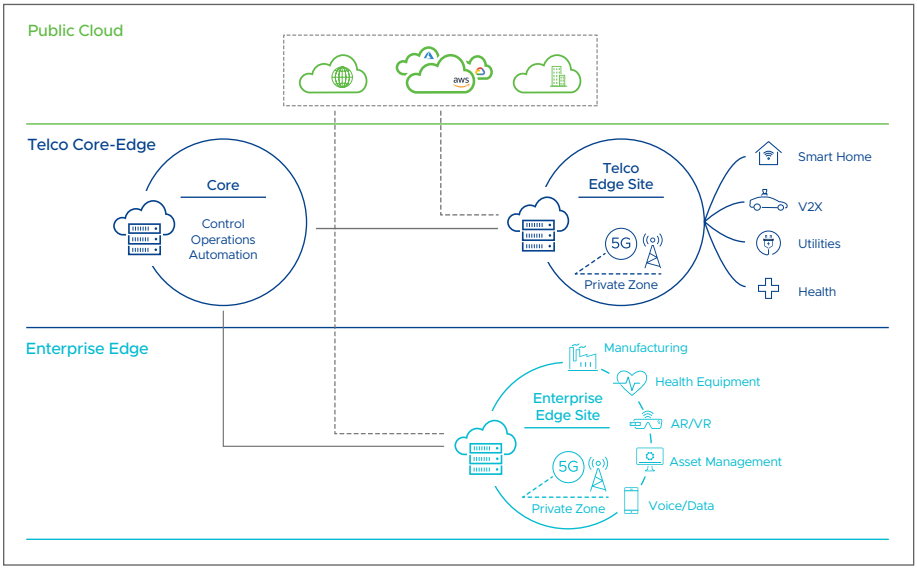


FIGURE 1: CSPs delivering Private Cellular Connectivity from the Telco Edge or On-Premises

## VMware Private Connectivity solution

VMware's Private Connectivity solution delivers a set of core infrastructure components with an ecosystem of partners to realize a solution to meet different scale, capacity and service-class requirements. The solution can be deployed on-premises with a fully packaged radio and mobile packet core providing reliable cellular connectivity as a single tenant solution. Local breakout is possible at the on-premises edge, with management and operations centralized into the service providers regional or central data center.

For enterprises with a distributed topology, the radio functions can be placed on-premises with low-latency connections to a telco edge micro data center hosting the mobile packet core functions, local breakout and, optionally, an edge computing infrastructure for applications and content. As a hierarchical topology, control plane function and management and operations functions can be housed in a regional data center within its own administrative ownership.

Managing the onboarding and lifecycle management of network functions and services deployed at various edge locations is a key component to ensuring a successful Private LTE rollout. VMware's Telco Cloud Automation orchestrates and automates network functions and services from core data center to edge with a centralized catalog giving access to all onboarded network functions.

A centralized SIM management system manages the various end-point identities across the business tenancy. Furthermore, an eSIM design further facilitates the move from a public macro network to a private network seamlessly. The distributed nature of the topology not only provides secure private enterprise network with local breakout to the internet and other services, but also enables interoperability and scalability with the broader multi-cloud ecosystem of hyperscalers and other software as a service (SaaS).

**End-to-end security** ensuring data information and devices are protected from malicious attacks

**Highest levels of QoS** with guaranteed performance, ultra-low latency and more control

**Reliable infrastructure** with high availability of bandwidth even at peak times with zero downtime

## Superior connectivity: predictable SLAs

Placing a dedicated spectrum, radio, and packet core at an enterprise does not imply reliable connectivity and SLAs. Different service classes from high throughput to ultra-low latency require a curated design and optimized configuration. While dedicated APNs and QCI configuration at the packet core and radio layers can be implemented, the VMware solution also optimizes the partner network functions with the needed virtual and physical infrastructure.

Proper resource isolation, overlay and underlay network configurations, compute alignment, and workload placement are required to prioritize traffic for mission-critical functions. In addition, appropriate security policies and safeguards are required to ensure unwarranted attacks and vulnerabilities. Real-time monitoring and dynamic optimization of workloads is further integrated.

## Edge cloud transformation: telco and enterprise edges

There are multiple placement options to build out an LTE/5G network—on-premises or on an edge cloud that meets application requirements for latency and throughput. For an on-premises solution—say for a factory floor, mine, or building—the footprint of the solution needs to scale to meet the physical constraints.

In a telco edge (multi-tenant) deployment scenario, the footprint may be less constrained. However, the design, networking, and security policies need to be factored in carefully. The interoperability of the multi-vendor solution is also a key consideration. Various vendors are at play for the virtual central unit (vCU), the user plane functions, the control plane functions, and value-added services.

This solution also requires modular interconnect with a multi-access edge computing (MEC) solution or a virtual content delivery network (vCDN). VMware certifies and validates the partner ecosystem, composability, and interoperability across its solutions.

## Seamless voice, messaging and data continuity

Two key advantages to providing private connectivity is delivering a private cellular network for data and also seamless continuity for voice. The user can receive and make calls as they travel between private and public networks. Connecting the core and private networks, in addition to centralized eSIM management, gives the operator a unique advantage for voice and messaging service continuity.

## Highly secure networking

A private connectivity network by default provides an isolated network in terms of restricting user access. It creates a ring-fenced network with access to local service and content, and which is excluded to those attached to the network.

VMware virtual infrastructure and overlay networking also provides security for networks traveling both north–south and east–west between virtual machines and containers. It restricts access to networks and virtual machines. There might be local files hosted on the private network, multimedia for operations and procedures, content and services in the public cloud provider networks, or even the open internet. Traffic management toward local content, telco MEC services, public cloud SaaS services, and local breakout to the internet from the private cellular networks can be controlled and audited.

LEARN MORE

For more information about VMware's Private Connectivity solution, please visit *telco.vmware.com* or contact your VMware representative.

## Integrate operations management and automation

With a highly distributed topology, operations and management are critical components of the solution. The telco orchestrator provides onboarding and management agility by managing distributed workloads and their lifecycle.

Having an integrated solution that dynamically discovers, monitors and isolates issues in a timely manner is key, and VMware Smart Assurance does exactly that. It presents a single pane for temporal performance metrics across a correlated spatial context of RAN, mobile packet core, and transport domains. It understands SLA measurements across the service delivery domains, and prioritizes impacts and spending intelligently. Real-time intelligence tied into the telco orchestration and SDN control fabric drives automated remediation.

**VMware, Inc.** 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com 