Delivering premium services on private networks with automated assurance and closed-loop automation

Contents

Publication Date: June 24

www.radcom.com

Introduction

With the power of 5G, operators can provide enterprise customers with private wireless networks (PWN), also known as private mobile networks (PMN), that deliver advantages such as security, privacy, ultra-low latency, enhanced mobile broadband, and massive device density. These private networks will be used by many different organizations, such as public safety organizations (police, ambulance, fire brigade) and other different verticals, such as smart factories, airports, hospitals, transport services, logistics, etc. These private networks will also provide the infrastructure for more automation, security, and productivity in these innovative industry use cases.

A PWN is designed to serve the specific needs of a private company or organization. This can include enterprise customers as well as local municipalities or government organizations. For enterprise customers, the PMN provides a guaranteed level of service that is harder to provide with a public mobile network.

For telecom operators, PWNs serve as an opportunity for additional revenue through which they can deliver a wide range of use cases across these diverse industry segments. Such networks function like a scaled-down version of a public mobile network and run on licensed, unlicensed, or shared spectrum.

When deploying a private network, each enterprise will obtain pre-defined, customized capabilities that will enable the development of its mission-critical apps and services. So that different customers can have a private network that meets their needs. For example, a private network that uses drones to inspect assets will require high bandwidth to transmit HD video. A smart factory that wants to use predictive maintenance to collect data from many sensors requires extremely low latency. Each private 5G network will serve the needs and requirements of each specific use case.

The demand for private networks based on 5G technologies is expanding, with hundreds of enterprises that have been or are currently investing in private networks. The private 5G network market is predicted to reach $47 billion by 2036 , growing at a CAGR of 40% between 2024-2036[1].

[1] https://www.researchnester.com/reports/private-5g-network-market/5654#:~:text=Global%20Market%20Size%2C%20Forecast%2C%20and,network%20was%20USD%202%20Billion.

Private Network Overview

Private networks are built for the exclusive use of a particular enterprise. All the devices operating on the network are part of a closed network community. Such networks are deployed in a specific location to deliver customized functionality in terms of connectivity, coverage, capacity, tailored security, and high quality of service.

Devices registered on public mobile networks won't work on the private network except when given specific authorization. A private network is essentially a trusted network in which enterprises pay to receive SLA-guaranteed performance beyond that of a public network concerning quality of service (QoS), quality of experience (QoE), connectivity, and security.

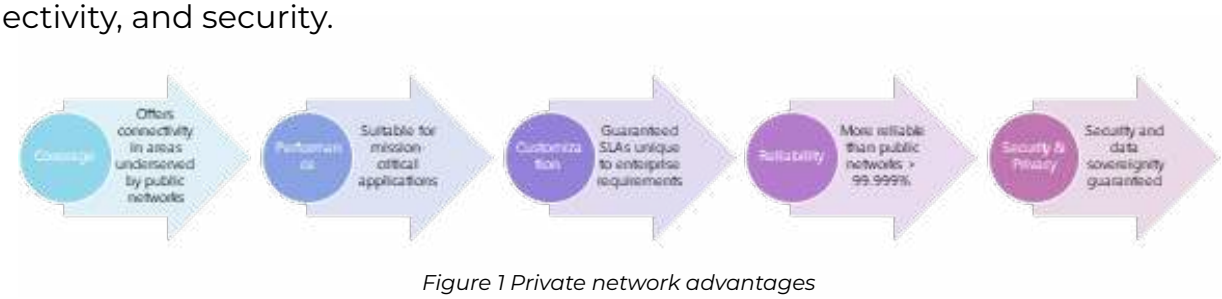

Figure 1 Private network advantages

These fit-for-purpose, high-performing private mobile networks are widely deployed through many vertical industry sectors. For example, Mercedes-Benz "Factory 56" in the automotive sector in Germany claimed to be the world's first private network designed to aid automotive manufacturing[2]. The rollout of private networks in Thailand by Nokia and NTT also spread across multiple business parks, providing enterprises and others access to efficient industrial IoT, machine learning, and AI. Each of these networks is using private networks to drive digitalization and lead the implementation of innovative solutions.

Operators offering private networks need to see the enterprise-wide data on a private network and understand the root cause of any issue when it arises, whether a problem is based on geographical location, different services like video, VoLTE, or specific network failures. Operators need real-time insights into the private network and know what is happening "right now." They need access to all the data from the RAN, edge to core, and manage their business with multiple enterprise customers from one unified pane of glass, and even forecast potential issues based on trends so they can troubleshoot before a problem escalates into a crisis.

Network Slicing and SLAs

Private networks and network slicing open a new market for operators. The customer is an enterprise with mission-focused apps and services that need to guarantee a certain performance level. As a result, operators will sign a stringent SLA (Service Level Agreement) contract with each enterprise or SME to ensure a certain quality of experience.

This shift requires real-time detection and even prediction of service degradations, requiring the solving of detected issues extremely fast. To be profitable, operators are expected to provide high levels of automation in their network provisioning and operations.

[2] https://www.telecoms.com/oss-bss-cx/nokia-and-ntt-team-up-for-5g-private-network-push-in-thailand

Private Networks Deployment Options

A 100% private, enterprise network

An enterprise deploys a RAN and core dedicated network in a set location, built to deliver a pre-defined purpose for its sole use. In this model the network is totally private and completely detached from any public mobile network.

A physically isolated private network can be deployed in different ways; on-premises, or in the cloud and can be split so that all network functions are built on premise. Alternatively, the user plane for the data traffic can be separated from the operator's data center and placed within each company's data center to improve the security level and reduce latency. This would allow the operator to manage the signaling traffic and provide monitoring capabilities to the customer.

Hybrid network

The network deployed is a blend of public and private infrastructure. For example, a slice of the public RAN may be combined with a dedicated on-premises core network.

Network slicing

Operators can deploy a virtualized private network using 5G network slicing over a public network. An enterprise may obtain most of the advantages of a private network without the costs or complexities of deploying and operating an on-premises network. Each network slice is an isolated end-to-end network tailored to fulfil diverse requirements requested by a particular application or service on the same physical network infrastructure.

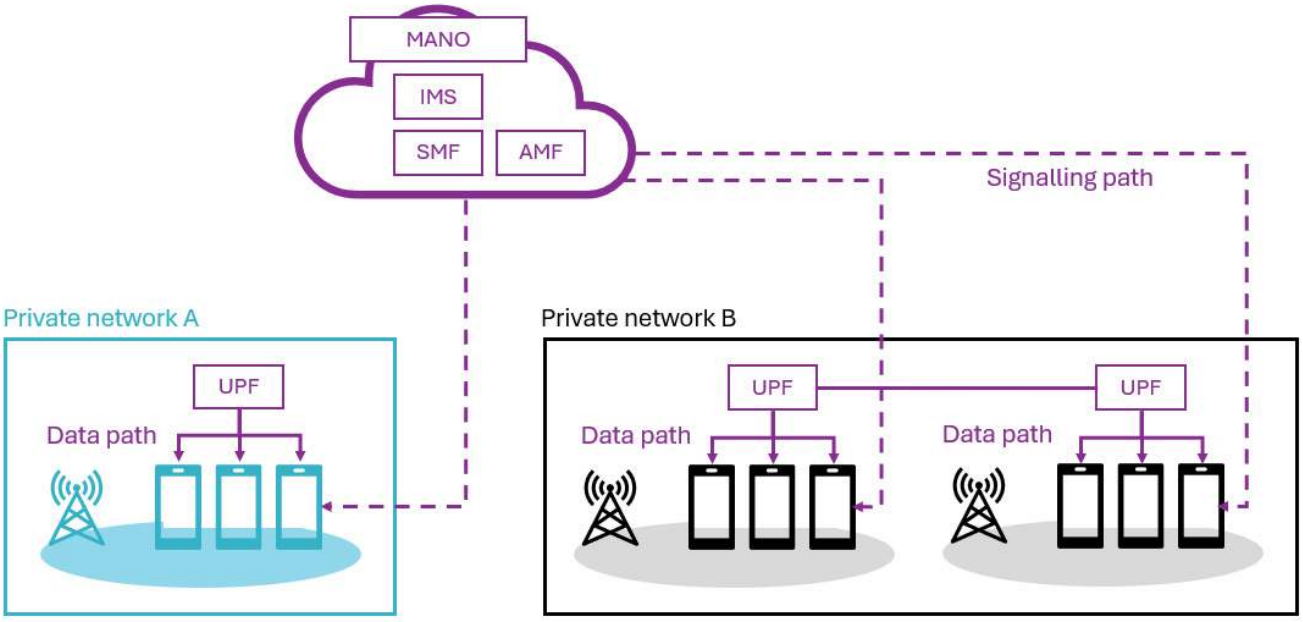

Figure 2 Private networks with user-plane on-premise

RADCOM Private Wireless Networks (PWN) Assurance Solution

SLA Monitoring

Operators need to constantly monitor stringent service level agreements (SLAs) that define key performance indicators (KPIs) and key quality indicators (KQIs) to ensure the demands of enterprise customers are met. Operators must continuously ensure SLAs are being met and quickly isolate and remediate issues when they do occur.

RADCOM PWN Assurance Solution offers a comprehensive SLA monitoring and assurance solution across 3G, 4G, and 5G voice and data services, providing end-to-end visibility from the RAN to the core across different locations, architectures and vendors. The information is collected and captured at a central site for KPIs, advanced analytics, session tracing, and troubleshooting. It is a powerful tool that enables the network to be monitored by operators, system integrators, and even enterprise users. In a scenario where an operator or integrator is responsible for thousands of private networks, one platform in the cloud can manage all these networks securely and ensure privacy through multi-tenancy.

RADCOM PWN Assurance Solution ensures SLAs:

- Quality of service (QoS): ensuring key KPIs such as throughput, latency, radio coverage, packet loss, and others are fully met
- Quality of experience (QoE): assuring key KQIs regarding reliability, availability, security, etc.
- Operation level agreements: certifying mean time to repair (MTTR), reporting, alerting, etc.

It is critical that operators comply and, therefore, monitor SLAs at both an enterprise and individual user level. With RADCOM PWN Assurance Solution, operators can quickly and effectively validate SLAs, ensure network and service performance, isolate network degradations, and proactively resolve issues. Capabilities include:

- Complete visibility into your private networks QoS and QoE.
- Proactive and continuous monitoring of QoE and QoS to confirm SLAs.
- Advanced troubleshooting and root cause analysis to find and resolve issues quickly.
- Anticipating service degradations in real-time and set up alarms to notify if any SLAs are breached.

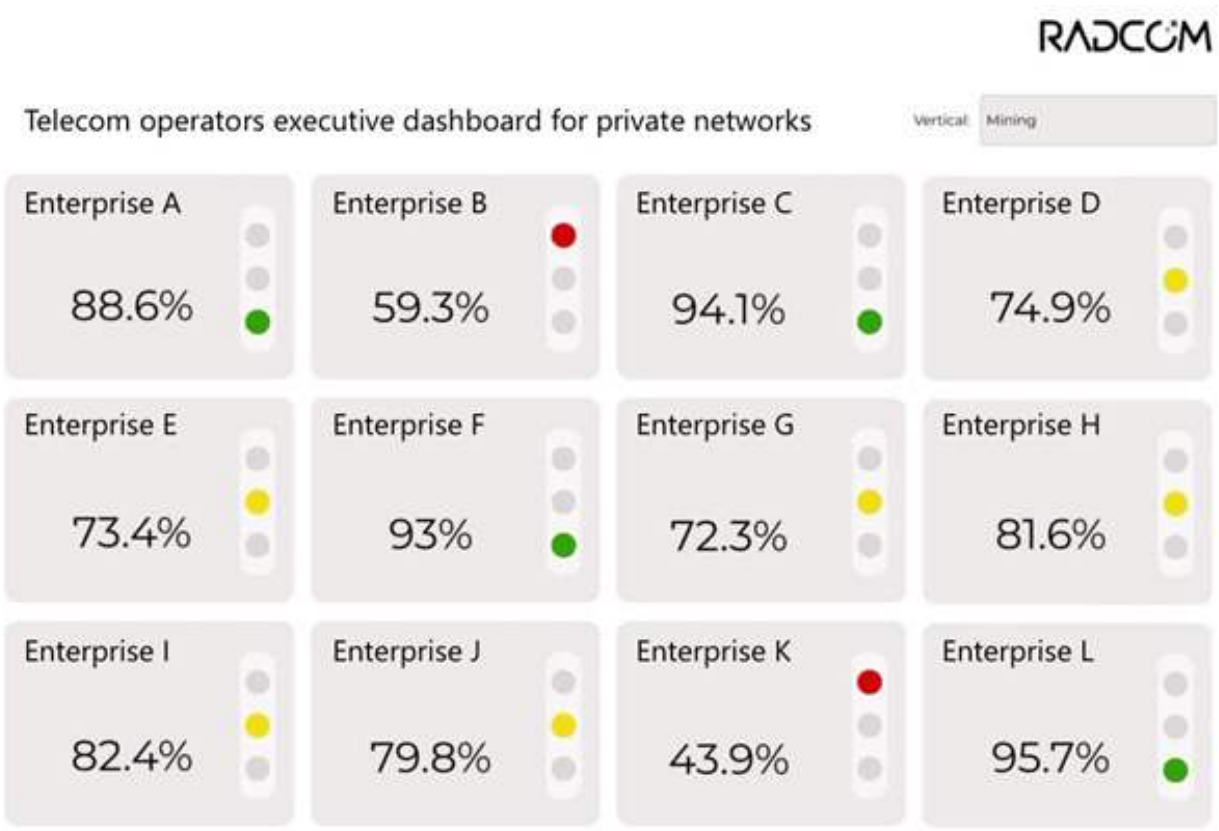

Figure 3 - Monitoring multiple enterprise networks and SLAs with multi-tenancy assurance

The solution gives operators a bird's-eye view of the network. It allows operators to set KPI thresholds according to the SLAs. It provides a quick solution to access all the data through dashboards with real-time alerts for network issues and drill down to troubleshooting views that help reduce the mean time to repair (MTTR). This is crucial as failing to deliver on SLAs invokes high penalties, with some agreements stipulating penalties of as much as 5% of the quarterly payment per single incident when breaching the SLA.

Operators serving multiple enterprises must access enterprise-wide data and ensure that individual enterprise users receive the expected performance. SLAs are often likely to be met on a per-user, per-device basis. All this must occur while monitoring hundreds of private networks with different SLAs for each enterprise.

By looking at the actual performance of the network and notifying users about any breach of the SLA in real time, RADCOM PWN Assurance Solution offers predictive network and service analytics, looking a few hours or days ahead using AI and machine learning to help predict a breach of the SLA, giving operators enough time to prevent or mitigate the issue before it affects users. When a closed-loop solution such as a network data analytics function (NWDAF) is deployed, the process can be fully automated, with issues being predicted and resolved without manual intervention before users are affected.

Multi-Tenancy

RADCOM PWN Assurance Solution offers a multi-tenancy software architecture in which multiple tenants (a telecom operator and multiple enterprise customers) can use the same platform and underlying assurance backend. The tenants are prohibited from accessing, sharing, or using other tenants' data, ensuring the solution's security and privacy.

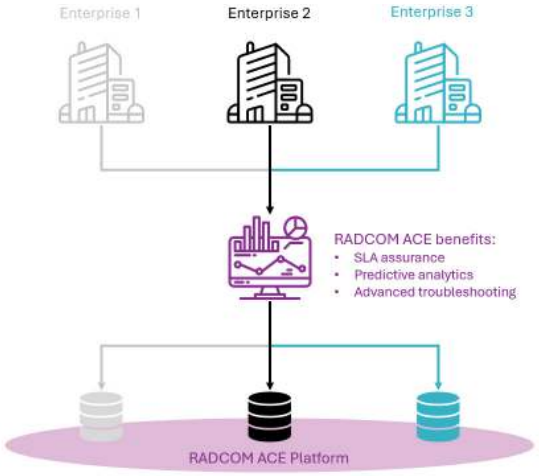

Figure 4 - RADCOM ACE offers multi-tenancy for privacy and security

In addition, through multi-tenancy, a customized user ecosystem is possible, and operators can analyze and summarize several enterprise customers' data with one database server.

AI/ML-Driven Capabilities

Additionally, built-in AI/ML capabilities can monitor each KPI and KQI to detect and predict anomalies and deviations from SLA and trigger automated closed-loop corrective actions. This will provide automatic, data-driven adjustments and insights that are not possible to attain through manual network monitoring.

Powered by these advanced capabilities, RADCOM PWN Assurance Solution generates centralized analytics, delivers cross-domain private network troubleshooting, and complete service and customer experience visibility. It provides a comprehensive network assurance approach, monitoring and troubleshooting each private network deployment at the service level and improving customer experience end-to-end.

Edge and CUPS support

RADCOM PWN Assurance Solution fully supports control and user plane separation (CUPS), a critical feature for private networks. This flexibility ensures that the deployment location of the control and user plane components—whether in the same place or across three separate locations—does not affect its performance. RADCOM PWN Assurance Solution seamlessly correlates data across various private network deployment types and configurations, offering comprehensive support regardless of the network architecture.

Additionally, the solution supports edge assurance with a low-footprint front end that captures data using minimal resources at the edge, whether on-premises or in the cloud. This enables operators and their enterprise customers to efficiently monitor service-level agreements (SLAs).

Network Slice Assurance

RADCOM PWN Assurance Solution, built on the RADCOM ACE platform, enables operators to monitor each virtual slice end-to-end, mapping every XDR/KPI/KQI to the relevant service slice to understand the overall QoE and QoS and confirm compliance with SLAs. Its multi-tenancy capabilities enable operators to provide their enterprise customers with self-monitoring capabilities for each virtual slice so that hundreds or even thousands of enterprises can self-manage their slices while ensuring their isolation and complete data privacy. The solution provides operators with the following capabilities:

- Gain network performance insights per slice: Correlation algorithms map KPIs/KQIs to each network slice
- Understand subscribers' perception of QoE: Provides an overall CEI and CEI for each service per slice
- Know the severity of different KPI and service degradations: Grades the severity so you know what issues to prioritize
- Define KPI weights and service thresholds: Operators can set thresholds to match their business goals and strategies

Drill Down to Packet and Session Level

While most issues can be automatically resolved using a closed-loop approach, some of the most complex problems will require more traditional tools, such as KPI/KQI dashboards with the ability to drill down to session and packet views for manual deep-dive troubleshooting. A comprehensive assurance solution must, therefore, have both automated and manual options.

Closed-Loop Automation for Private Networks and Slicing

Delivering on the promise of private 5G networks and network slicing also means operators adopting automation to manage their network through the RADCOM PWN Assurance Solution with NWDAF - defined by 3GPP, to enable network data analysis for mobile core networks. Due to its complexity and the resources required for artificial intelligence and machine learning (AI/ML) to perform tasks such as predictive analytics, NWDAF is only sometimes considered an option for private network automation. RADCOM's NWDAF solution, however, offers a centralized NWDAF in the cloud with multi-tenancy capabilities and low-footprint "NWDAF proxies." These are deployed at the private network sites, allowing operators to extend the power of NWDAF to private networks cost-effectively.

RADCOM NWDAF supports dozens of analytics and closed-looped use cases for private networks and network slicing, such as IoT anomaly detection. It uses AI and ML to monitor the communications patterns of IoT devices and identify anomalies that would indicate a security or network issue. Automatic real-time detection triggers corrective action through a closed-loop interface to resolve the issue, for instance, by barring the offending or suspicious IoT device from the network.

For slicing, RADCOM NWDAF utilizes each KPI and KQI to detect and predict anomalies and deviations from SLA and trigger automated closed-loop corrective action. Built-in AI/ML capabilities can predict the future behavior of each network slice, therefore initiating a closed-loop action that can resolve the issue before it affects subscribers. This provides operators with automatic, data-driven adjustments and insights which are impossible to reach through manual network monitoring.

The benefits of RADCOM NWDAF include ensuring network slicing quality.

- Visibility into your network slices and their QoS/QoE
- Advanced troubleshooting and root cause analysis to find and resolve issues quickly
- Rapid self-healing and adjustments to a network's optimal configuration
- Proactive and continuous monitoring of QoE and QoS to confirm SLAs
- Automated anomaly detection
- Predictive analytics that can forecast issues before they occur

Use cases

Private networks can benefit many use cases across multiple verticals. Here are a few of the top use cases for private networks:

Use case	Description
Manufacturing	Ubiquitous, low-latency coverage for facility operations maximizes uptime and helps save costs. Enterprise customers can use the network for quality-of-service (QoS) traffic prioritization, high-definition video for quality control and inspection, remote industrial robotics, digital twins for simulation models, and remote maintenance and technical support through augmented reality (AR) or virtual reality (VR) applications.
Utilities	Dedicated bandwidth and low latency can give companies smarter ways to control energy flow and support utility distribution applications. Examples include drone surveillance, worker safety applications, remote equipment diagnostics, smart grids, automated power distribution, and machine learning for better data analytics.
Oil, gas and mining	Maintain a secure and robust network connection even in remote locations and harsh conditions. Application examples include autonomous and remote-operated drilling, surveillance videos and drone monitoring, high-precision positioning, seaport and terminal operations, AR/VR staff training, and preventive safety alerts.
Healthcare	The high reliability and lower latency can help support critical wireless device connections. Examples include supporting connected medical devices, inventory control, data security, video analytics and safety, and staff connectivity.
Retail	Help retail stores avoid congestion issues, improve coverage, performance, and security, and allow for the adoption of new digital initiatives. Application examples include proactive shelf restocking due to better inventory intelligence, responsive and relevant customer signage and visuals, automatic checkouts, and faster operational data insights.

Conclusion

In conclusion, private networks and network slicing are new and promising revenue streams for operators. They offer enterprise customers guaranteed service quality for mission-critical applications and services.

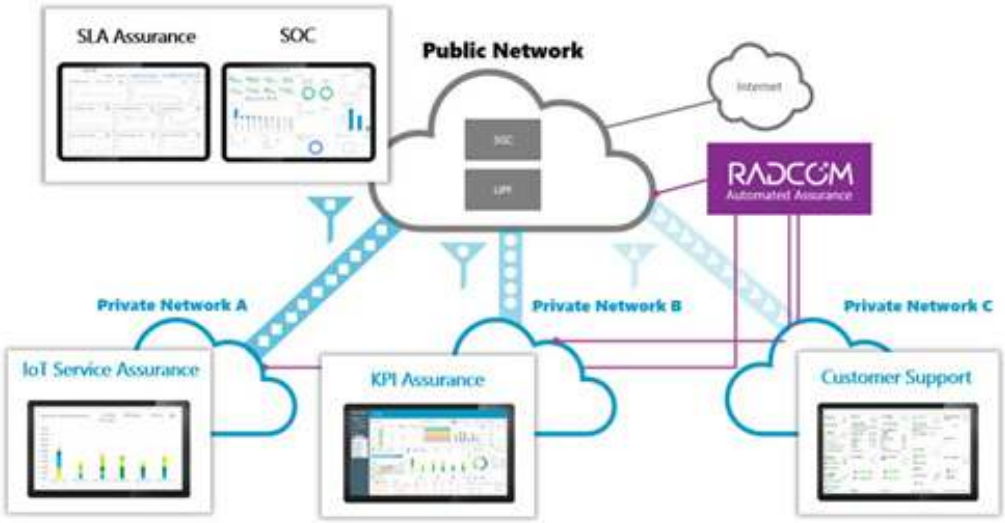

Figure 5 Offering SLA assurance for telecom operators and multiple enterprise customers

The RADCOM PWN Assurance Solution assures private mobile networks and network slicing and enables closed-loop automation. It allows operators to monitor, analyze, and detect degradations in real-time across all domains. This ensures that SLAs are met, and enterprise customers can seamlessly run newly digitized apps and services.

By leveraging RADCOM PWN Assurance Solution, the operator's enterprise customers can access a cloud-based self-service portal that provides self-monitoring capabilities to manage their private network and slices while ensuring their isolation and complete data privacy. This allows network managers on the enterprise side to see what's always happening and view statistics.

The portal shows the network status (active/inactive), the number of nodes in the network, and overall usage. Enterprises can view performance KPIs such as radio nodes, SIMs, data usage, network bandwidth, latency, and throughput. Each KPI can be viewed at different time intervals (daily, weekly, monthly), and enterprise customers can easily report issues.

Operators deploying the RADCOM PWN Assurance Solution can sell the self-portal capabilities to their enterprise customers as a value-added service. RADCOM PWN Assurance Solution is vendor-agnostic, supporting all types of private networks, network slicing , and hybrid configurations. It seamlessly integrates with different vendors, whether for the public or private segments of the network, all within a single platform. Moreover, the cloud-based deployment enables RADCOM to manage the backend in the cloud efficiently, ensuring scalability and flexibility.

With integrated AI/ML capabilities, RADCOM PWN Assurance Solution can automate this process and predict network issues while assuring a superior customer experience. Integrating into the network will enable operators to launch and wisely manage private LTE and 5G networks.