Publication date:
November 2022
Authors:
Pablo Tomasi
James Crawshaw

Service Assurance in Private Mobile Networks

Closing the loop

Commissioned by:

Brought to you by Informa Tech

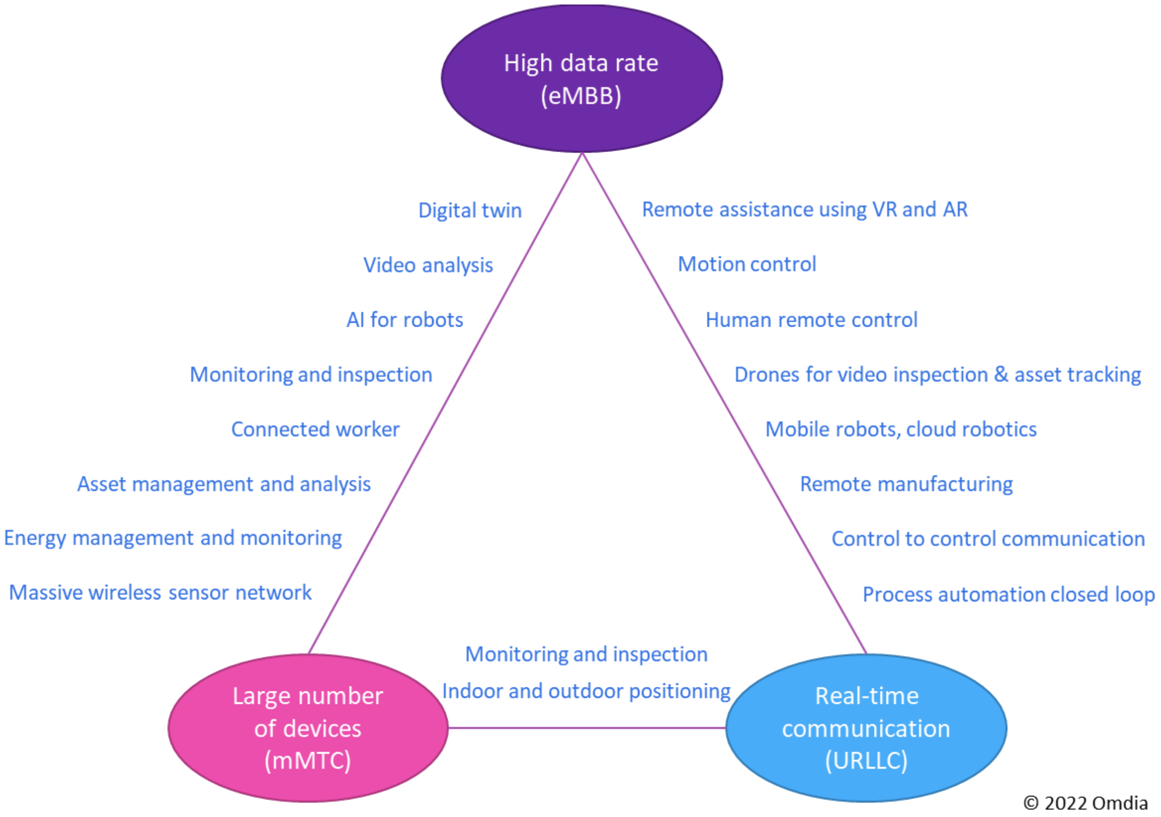
Contents

Executive summary

The private networks market is a rapidly growing opportunity across many verticals on the back of multiple convergent trends including spectrum liberalization, the need for better security and control, and the increasing need for data-heavy applications. Private cellular is driving the transformation of asset-heavy industries such as manufacturing (see **Figure 1**), transport and logistics, energy, and mining.

Since these industries require stringent connectivity performance and have strict KPIs that must be met by the network, as the market grows so does the need for network monitoring and service assurance. This is key to meeting the service level agreements (SLAs) struck between the enterprise and the private mobile service provider. Full visibility across network, service, and application assurance will grow in relevance because cellular is entering new verticals where it must demonstrate its ability to meet the specific needs of the enterprise.

Figure 1: Potential 5G use cases in manufacturing


High data rate (eMBB)
Digital twin
Video analysis
AI for robots
Monitoring and inspection
Connected worker
Asset management and analysis
Energy management and monitoring
Massive wireless sensor network
Remote assistance using VR and AR
Motion control
Human remote control
Drones for video inspection & asset tracking
Mobile robots, cloud robotics
Remote manufacturing
Control to control communication
Process automation closed loop
Monitoring and inspection
Indoor and outdoor positioning
Large number of devices (mMTC)
Real-time communication (URLLC)
© 2022 Omdia

Source: Omdia, *Demystifying Private 5G in Manufacturing: How to Seize a New Opportunity*

The private mobile opportunity

The private networks market is a nascent opportunity for a wide set of companies. The adoption of private networks across industries is being driven by spectrum, enterprises' need for security and control, and their evolving need for data-demanding and highly reliable applications, which cannot be adequately served by existing technologies such as Wi-Fi.

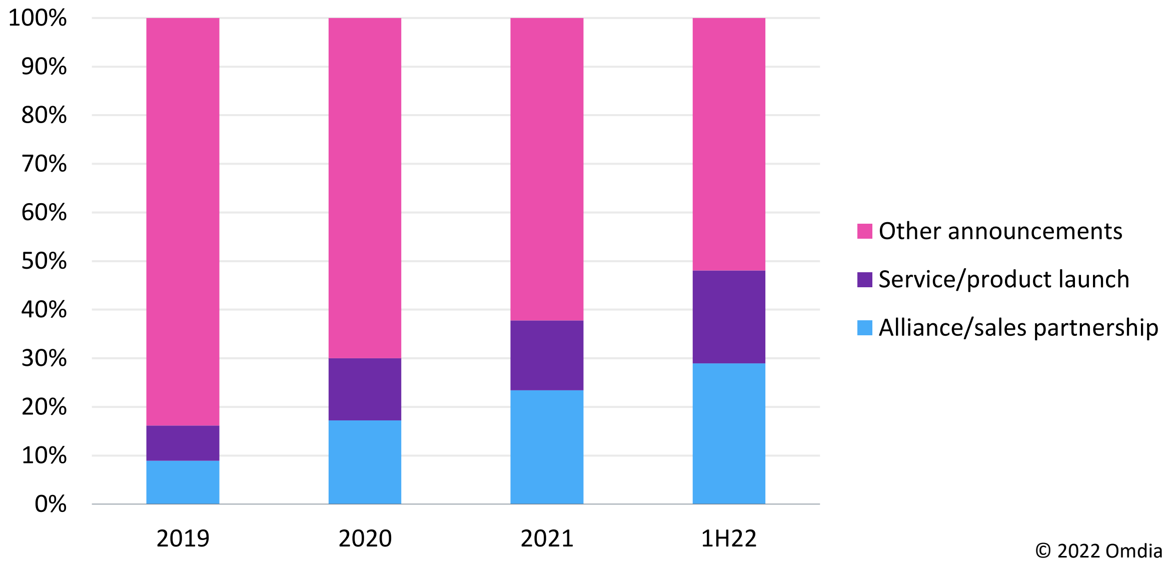
Spectrum liberalization has been the main trend jump-starting the private networks market. Alongside early movers such as Germany (3.7GHz band), the US (3.5GHz band Citizen Broadband Radio Services, CBRS), and Japan (2.5GHz, 28GHz, 4.6–4.9GHz), the trend of spectrum liberalization has seen multiple regulators unlocking spectrum for use by enterprises: recent examples include Finland, South Korea, India, and Brazil.

The need for a technology that addresses the security worries of the enterprise has also pushed the adoption of private networks. In fact, according to Omdia's *Private LTE and 5G Network Enterprise Survey Insight – 2021*, almost two out of three surveyed enterprises (59%) see security, data management, and privacy as a key driver of private networks adoption.

Additionally, applications such as automated guided vehicles (AGVs), remote-controlled cranes, and augmented reality / virtual reality (AR/VR) require low latency, high availability (five nines), and predictability. Given the stringent requirements of the industrial environment, even a relatively small improvement in performance can bring a significant ROI to the enterprise. Though existing technologies can, to a certain degree, serve these applications, scaling the applications while not compromising performance is a challenge. This is why cellular is gaining a foothold in this market.

All these trends are creating a new market that will reach $6.5bn by 2026, up from $1.7bn in 2021, according to Omdia estimates. This is also an opportunity that will open new revenue streams across all verticals but particularly industrial verticals (manufacturing, transport and logistics, and energy and utilities), which will contribute more than 60% of the market revenue by 2026. Since cellular is not currently a leading technology in these verticals, private networks are creating new revenue streams. There is also an opportunity to sell additional services and technologies alongside the private network. According to Omdia research, 97% of surveyed enterprises would buy additional services, while 96% would buy additional technologies. The market is preparing to seize this growth: new service/product launches represented 19% of all market announcements in the first half of 2022 alone, up from 14% of announcements for full-year 2021.

Figure 2: A market preparing for growth: Alliances and new products, relevance over all private networks announcements



Source: Omdia

The private mobile ecosystem

The nature of the private networks opportunity, which cuts across the telecoms, IT, and operational technology (OT) space, means that multiple players from diverse backgrounds can leverage existing assets and become leading competitors in the private networks market.

The fragmented and complex nature of this market means that there are significant opportunities for partnerships to target specific market segments. For instance, a company such as Kajeet, with a strong history in the education sector, will be a relevant player in that vertical, while a company such as siticom will be a strong player in manufacturing.

Virtually every technology player has an interest in private networks, but the following are the key categories that are actively competing to bring private networks to the enterprise:

- Network vendors
- System integrators (SIs)
- Industrial vendors
- Private networks specialists
- Mobile network operators (MNOs)
- Hyperscalers

Table 1 expands on each of these categories.

Table 1: The private networks ecosystem

Company category	Right to play and strength	Category challenges
Network vendors	This was the first category of players that started looking at private networks as an emerging opportunity. This category includes both specialists such as Athonet or Druid and global vendors such as Nokia and Huawei.	Network infrastructure vendors need to maintain a large ecosystem of go-to-market partners, and because the first-mover advantage of some players is finishing, the challenge for each vendor is to become the preferred partner for the service provider or for the enterprise.
System integrators	Since private networks are a brownfield market there is a big opportunity for system integrators. Omdia data shows 37% of enterprises selected integration as a key challenge to private networks implementation. NTT and Capgemini are two examples of the category.	Spectrum liberalization is underway, but there are still many countries where spectrum is exclusively held by telecom operators. So for multi-country projects any SI will likely need to strike partnerships with telcos. Furthermore, as enterprises seek simplicity there is a risk that SIs will foster complexity instead.

Industrial vendors	Industrial vendors have the in-depth knowledge of the vertical and of the solutions needed by the enterprise. They have existing products, solutions, and enterprise trust. Siemens and Bosch are examples.	They are not experts in 5G, and it is possible that they will underestimate how complex the technology really is. Having in-depth understanding of an industrial vertical does not make them the most suited 5G providers by default.
Private networks specialists	These companies have developed their solutions in markets where spectrum has been liberalized to target this specific segment. They often had a first-mover advantage, and in contrast to larger players they are laser focused (and dependent) on the success of this market. Examples include Edzcom and Federated Wireless.	Scaling in a sustainable way may be a challenge for new and smaller companies. Their dependency on a new market also means they will be exposed to any possible slowdown or unexpected market challenge. They will also face increasing competition from larger players with deep pockets.
Mobile network operators	MNOs are expert in 5G technology and sometimes they also have expertise in managing critical networks, for instance, for safety and security. They can serve the enterprise with multiple services and technologies including cybersecurity and SD-WAN. Examples include AT&T and Vodafone.	Though they serve many enterprises, they may not be serving critical needs of the enterprise, such as connectivity on the factory floor. Therefore, in many verticals they are de facto outsiders. They also need to learn how to sell solutions rather than just selling 5G as a silver-bullet technology.
Hyperscalers	They have expertise in enterprise digitization and in the role of cloud and edge within these projects. They are the ecosystem players by definition, and they have the skill set, workforce, and capability to bring innovation into the private networks market. Examples include Amazon Web Services (AWS) and Microsoft.	They are platform players that seek to bring a cloud-like approach to the private networks market to deliver ease of consumption, scalability, and replicability. This is a long-term opportunity, and the current reality of the market is one of hands-on projects and tailoring of a network of solutions. As a result, their approach may not work for many enterprises' needs.

Source: Omdia

The need for service assurance

According to trade association techUK,[1] “a key driver for the increased adoption of private networks today is the ability to support demanding applications and quality of service guarantees.” The techUK report goes on to recommend that companies deploying private mobile networks should “Ensure you consider system and process integration with other OT/IT/cloud infrastructure, as well as identity management, security and compliance, service assurance and access control.” In this section, we explore the topic of service assurance in more detail.

As enterprises deploy private mobile networks, they will set service level objectives (SLOs) that reflect the importance of the wireless connectivity to their business. If the network is simply for connecting sensors that report back small measurements from time to time, and missing a measurement is no big deal, then a service assurance system is probably overkill. But if the application is more critical to the successful operation of the business, or to safety, a service assurance system can become a critical component.

Availability: How many nines?

Consider one criterion that might be part of the SLO: availability. As **Table 2** shows, the typical availability of a public mobile network service is 99.9%. That translates into downtime of around nine hours per year. For factory automation, however, we might want to reduce that downtime by an order of magnitude. For drone control an acceptable downtime might be another order of magnitude lower, and for remote robot control a further order lower still.

Given that mobile operators already have extensive service assurance systems for their public mobile services, it is likely that these more demanding applications shown in **Table 2** will do so too. Serving sensitive and mission-critical applications will require real-time detection and even prediction of service degradations. The root cause of the issues that are detected or predicted must be determined quickly and a solution reached.

[1] techUK, “Private networks: A user guide,” May 2022, www.techuk.org/asset/BC976B78-5F42-4837-9DBFAF802876625A/

Table 2: Availability requirements of different mobile services

Availability	Downtime per year	Example services
99.9%	8.8 hours	Public mobile network
99.99%	53 minutes	Factory automation
99.999%	5.3 minutes	Drone control
99.9999%	32 seconds	Remote robot control

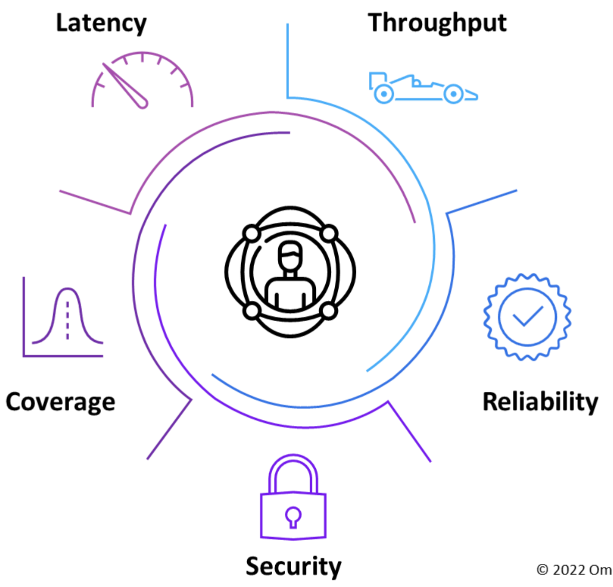
Source: Omdia

Other service level objectives

The SLO for a private mobile network does not just relate to availability. Other factors, such as throughput and latency, might affect the overall quality of service or experience as indicated in **Figure 2**. These requirements might also exceed what is typically provided by a public mobile network, which is after all a best-efforts service.

If the management and operation of the network is outsourced to a third party (e.g., a managed service provider), the SLOs of the enterprise will be turned into an SLA. Breaching the terms of this agreement usually leads to penalties for the managed service provider (MSP). Even if the network is managed in-house, the team responsible will be held accountable if the performance has a negative impact on the operations of the business. Therefore, service assurance is a key part of the network solution and should not be an afterthought.

Figure 3: Service level objectives for private mobile networks



© 2022 Omdia

Source: Omdia

Bear in mind that the service assurance function in private mobile is not just there to monitor the wireless radios. Instead, it must cover multiple domains, including

- Radio access network
- Transport/backhaul links between radio nodes
- Packet core responsible for signaling
- Systems such as IP multimedia subsystem or voice and video services
- Telco cloud infrastructure used to host virtualized network functions (VNFs)

The need for service assurance is even greater when the network comprises multiple vendors (antennae, base-station, etc.) and possibly multiple technologies (Wi-Fi, 4G, 5G).

Measuring quality of experience and automating root cause analysis

Part of the value-add of a service assurance solution, beyond basic network monitoring, is to measure the quality of experience that the users (humans or machines) perceive. To do this requires an understanding of the impact of different KPIs on the service experience. A key quality indicator (KQI) is created that applies different thresholds to different KPIs and aggregates them using a weighting factor that best reflects their relative importance.

This KQI should be continuously monitored to prove (or disprove) that the agreed SLOs are being met. When KPI thresholds are breached or anomalies are detected, these should be flagged to the network manager so that further investigation can be undertaken. Furthermore, if a pattern of anomalies is detected, the service assurance system should be able to predict, with an estimated confidence, the likelihood of a service degradation taking place (and quantify its impact). The system should rank detected issues based on their likely service impact, enabling network engineers to prioritize their work.

Service assurance should provide some automated root cause analysis (RCA) to help network engineers narrow down the list of potential causes of a problem. It should include troubleshooting tools so they can easily investigate logs and run tests with synthetic traffic to identify the source of the degradation.

Assessing network, service, and application performance

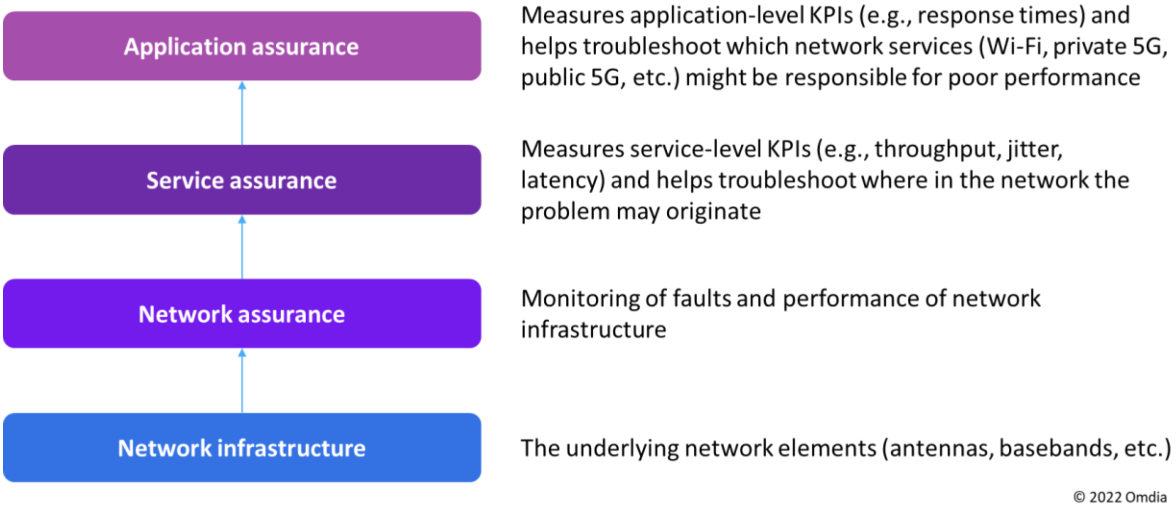
As **Figure 3** indicates, assurance is not just about ensuring network performance metrics are all “green.” The service level objectives for a private mobile network should cover

- **Network performance:** for example, latency, throughput, packet loss

- **Service performance:** for example, availability (in time), coverage (in space), mean time to repair, security
- **Application performance:** for example, response time of applications and other user experience indicators

The key is to identify and rectify problems before the users are affected. This requires analysis of application and service level KPIs as well as the underlying network performance metrics. With service assurance, enterprises can get the visibility and scale to deliver, assure, troubleshoot, and optimize complex distributed services for robotic and industrial automation applications. An end-to-end view of service quality covers multiple underlying technologies and multiple vendors, both on campus and over wide areas (e.g., the public mobile network), providing a single pane of glass into network visibility.

Figure 4: Assurance of networks, services, and applications



Application assurance — Measures application-level KPIs (e.g., response times) and helps troubleshoot which network services (Wi-Fi, private 5G, public 5G, etc.) might be responsible for poor performance

Service assurance — Measures service-level KPIs (e.g., throughput, jitter, latency) and helps troubleshoot where in the network the problem may originate

Network assurance — Monitoring of faults and performance of network infrastructure

Network infrastructure — The underlying network elements (antennas, basebands, etc.)

© 2022 Omdia

Source: Omdia

Service assurance capabilities

A service assurance system is not a generic, monolithic application. Rather it is a suite of solutions that can be assembled to suit the specific needs of the team responsible for a private mobile network and the quality of experience it offers its users.

Components of this suite might include the following:

- **Throughput analysis:** measuring the throughput of the network, or a slice, for upstream and downstream sessions. The analysis could cover throughput from the perspective of the radio access network (RAN) and the user or user equipment. It might include the responsible cells or slice instances, gNodeB capacity, or issues with massive MIMO, hardware, coverage, and quality.
- **Traffic and capacity analysis:** several KPIs might be calculated and measured to indicate the status of capacity utilization and better understand the traffic situation in a network. These could include analysis by network node, slice, and most-affected cells. This would enable the most appropriate action, such as offloading traffic to small cells, to be identified.
- **Worst cell / cluster analysis:** providing a detailed analysis of worst-performing cells or cluster of cells. Collating metrics on performance, faults, and massive MIMO performance could enable cells and sites that do not meet specified criteria to be identified and remediated.
- **Alert surveillance:** providing a summary of near-real-time alarms across the network (from gNodeBs, etc.), with the ability to drill down and identify responsible network components (gNodeB, transport router, etc.).
- **Service quality and impact analysis:** monitoring of service quality KQIs such as service accessibility, integrity, mobility, retainability, and availability. Service impact would be calculated with the ability to drill down to the network level (RAN, core, and transport).
- **Site validation:** detection and reporting of deviations in configurations of 5G cells and sites that might lead to performance issues.
- **Site acceptance analysis:** identification of new sites based on launch dates or when flagged by inventory systems across RAN, core, and transport. Site acceptance readiness could be detected through monitored KPIs.
- **Registration analysis:** RCA and impact analysis to address Access and Mobility Function (AMF) registration issues or degradations.

- **Workflow automation:** automated workflows for network/service operations centers offer solutions for automating resolution of dropped calls, inter/intrafrequency mobility robustness optimization, carrier aggregation, and load balancing.

- **Small cell monitoring:** KPIs covering the collective performance of small cells (pico, femto, micro) deployed across different node types (Radio Dots, mRRU, aDAS, etc.). Private networks could be heavily composed of small cell networks with virtualized packet cores.

- **5G network slice assurance:** for static and dynamic mobile network slices an advanced RCA could make recommendations and trigger work orders that would lead to the redesign of services (e.g., updates 5G slice QoS/5QI based on business policy). It could also identify resource issues so that slice allocations can be orchestrated to maintain QoS and SLA guarantees.

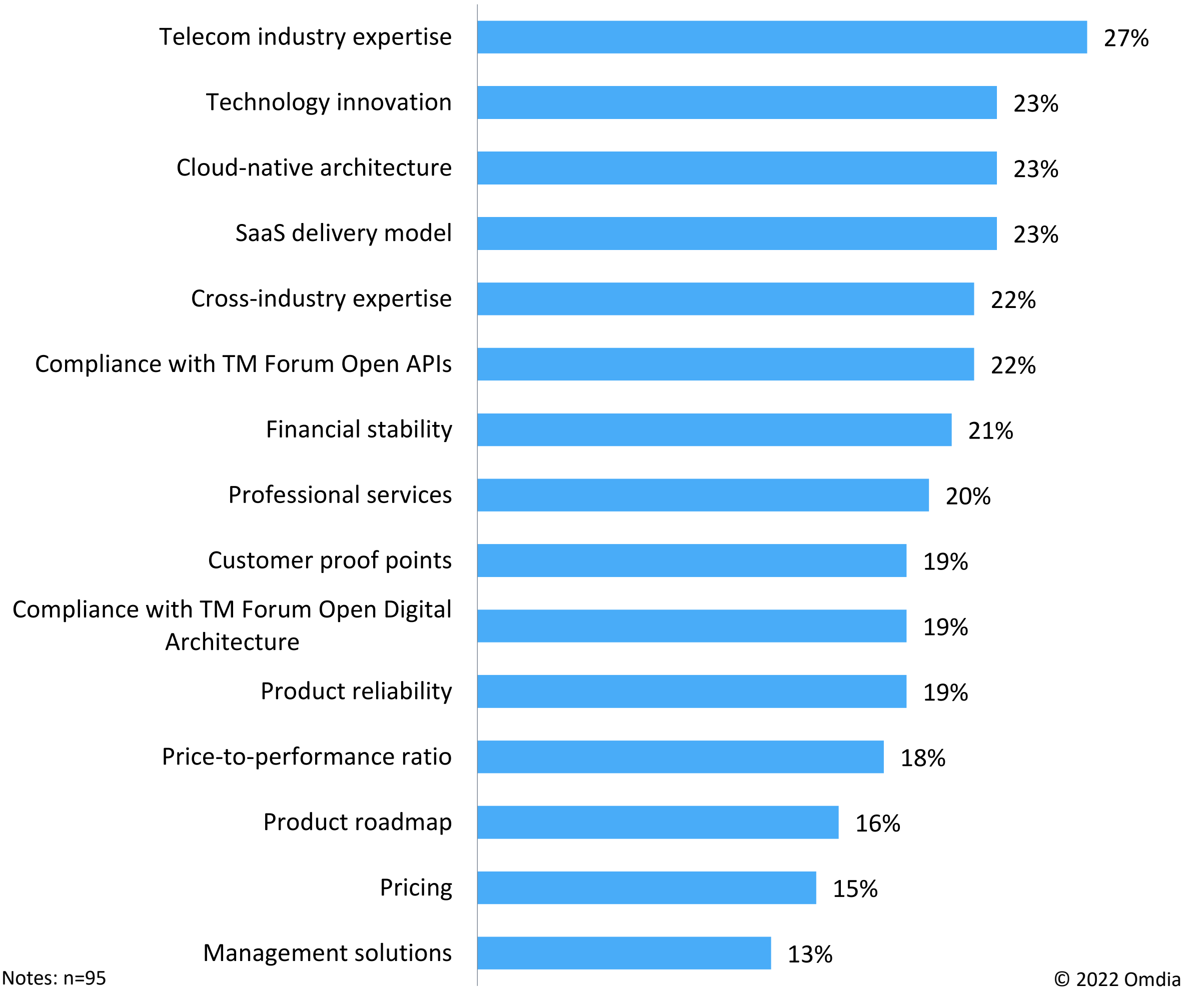
- **NFV performance management:** assuring the performance of VNFs, virtual infrastructure (NFVi), and physical infrastructure. It provides visualization of the compute hosts' performance across NFVi platforms and sites, identifying bottlenecks in storage, network, and compute.

The importance of domain expertise

Service assurance is a complex task that requires expertise in networks and data analytics, including artificial intelligence (AI). For private mobile, it is also paramount that the service assurance supplier should have a strong pedigree in the domain of mobile networks. As **Figure 4** shows, in the area of telco IT (operational and business support systems), telecom operators value industry expertise ahead of all other criteria when selecting vendors.

Private mobile is a relatively new domain. This being the case, enterprises should look for service assurance suppliers that have experience in the most directly comparable domain: public mobile networks. This is particularly relevant for use cases that roam between public and private mobile (e.g., for off and on campus).

Figure 5: The most important criteria for choosing an OSS/BSS vendor



Notes: n=95

© 2022 Omdia

Source: Omdia

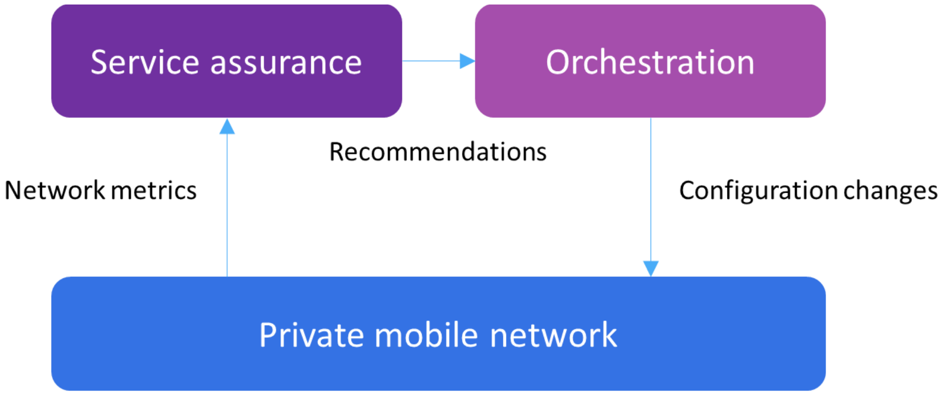
Enabling closed-loop automation

According to AWS,[2] automation and service assurance are important components of a mobile private network deployment. Network management system outputs are used as inputs to service assurance systems to trigger orchestration actions that help meet service level objectives. That, in essence, enables the automation of the network.

If machine learning is used to identify anomalies and conduct RCA, the automation can be taken to another level. The suggested root causes can be flagged to the service and domain orchestrators for them to carry out the appropriate corrective action before the user has even noticed the problem. This closed-loop corrective action can ensure SLOs are maintained in a way that would never be possible with manual network monitoring.

Of course, not all issues will be able to be resolved using this closed-loop approach, at least not the first time they occur. More complex problems will still require dashboards that allow engineers to drill down into session and packet data for troubleshooting. Closed-loop automation will not take away the need for dashboards overnight, but given time more and more issue resolutions should be capable of automation.

Figure 6: Closed-loop resolution of issues in private mobile networks



© 2022 Omdia

Source: Omdia

[2] Amazon Web Services, “Next-Generation Mobile Private Networks Powered by AWS,” 2022, https://docs.aws.amazon.com/whitepapers/latest/mobile-private-networks/mobile-private-networks.pdf

Conclusions and recommendations

Private networks are an emerging opportunity across many verticals where cellular has not been a dominant technology so far. Because of the complex nature of a private network and the stringent demands of the enterprise, service assurance is of paramount importance to guarantee that the private network performs as it should. In fact, any deployment will have an SLA based on the service level objectives of the enterprise. Breaching the terms of this agreement usually leads to penalties for the MSP; a loss of productivity, savings, or automation for the enterprise; and overall, a loss of credibility for cellular technology in these new markets. Assurance is therefore a critical component in any private network deployment. This goes well beyond the monitoring of the network but must include service and application assurance.

Any enterprise willing to deploy a private network to reach its specific goals (e.g., safety or productivity) should understand the importance of monitoring and assurance across all the domains of the private networks. It should work with partners that are experts in the field and that can help to guarantee that the SLAs that the enterprise has with its private network provider are respected.

For private network providers, it is essential to understand that visibility beyond the network performance into the application layer is critical to meet the needs of the enterprise. This is because any enterprise deployment is driven by needs beyond connectivity that will be served by applications. Ultimately, the enterprise will decide the success or failure of its deployment based on how the private network is able to deliver on specific application KPIs. This will open or close the door to future deployments for other sites and other enterprises.

Appendix

Methodology

This paper is based on Omdia’s ongoing research into private mobile networks and service assurance and the broader topic of service provider transformation leveraging new technologies such as AI.

Authors

James Crawshaw
Practice Leader, Service Provider Transformation
customersuccess@omdia.com

Pablo Tomasi
Principal Analyst, Private Networks and Enterprise 5G
customersuccess@omdia.com

Get in touch

www.omdia.com
customersuccess@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia’s consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the “Omdia Materials”) are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa Tech and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.