

**2024**

# Cloud-native network transformation and the 5G edge

**Kerem Arsal**  
Senior Principal Analyst,  
Networked Edge  
— Omdia

**Roberto Kompany**  
Principal Analyst,  
Mobile Infrastructure  
— Omdia

**Pablo Tomasi**  
Principal Analyst,  
Private Networks  
— Omdia

# Contents

<b>Executive summary</b> .....	<b>3</b>
<b>SECTION 01</b>	
<b>5G slow to reach full potential so far</b> .....	<b>5</b>
This is tied to slow and delayed deployments of 5G SA, which enables new services that can translate into new revenue streams.....	6
Without 'true' 5G networks, edge computing on telecom networks has also struggled to flourish.....	6
CSPs count many challenges in their edge deployments.....	7
CSPs acknowledge their lack of infrastructure readiness and technical challenges in IT and network domains as their biggest hurdles.....	8
...and view Opex and Capex as the two trailing obstacles.....	8
<b>SECTION 02</b>	
<b>5G edge computing now set for strong growth</b> .....	<b>10</b>
CSPs value the versatility of edge computing, which brings both internal and external benefits.....	11
Confidence in presence of demand breeds confidence in the future.....	11
...with applications and premium connectivity at the edge viewed as key revenue streams in the future.....	12
To capture demand, edge infrastructures are set to expand toward highly distributed computing.....	13
Omdia expects networked edge uptake to grow over the next several years, leading to an opportunity of more than \$26bn of IaaS and SaaS by 2032.....	13
<b>SECTION 03</b>	
<b>Essential role of network cloudification for CSPs</b> .....	<b>15</b>
Becoming cloud native is not only to pursue the edge computing opportunity; it ranks among the highest overall priorities for CSPs.....	16
... because it offers many benefits and suggests a paradigm shift for them.....	16
In the core, cloudification will bring benefits of agility, efficiency and scalability.....	17
RAN is the largest capex spend for mobile operators; its virtualization will enable both software and geolocation disaggregation.....	17
RAN disaggregation will then lead to centralized computing, facilitate CUPS and drive new edge services' business models.....	18
<b>SECTION 04</b>	
<b>Challenges in the journey to cloud native networking</b> .....	<b>20</b>
Managing complexity and interoperability are the main challenges to 5G cloud core deployments; business case clarity is not a concern.....	20
Integration challenges are the primary obstacles to the adoption of open vRAN.....	21
<b>SECTION 05</b>	
<b>Keys to success and the role of open source</b> .....	<b>23</b>
A common cloud layer can act as a platform of interoperability to reduce vendor fragmentation.....	23
Kubernetes is a powerful approach to container orchestration, especially when supported by services that offer visibility, control and management of clusters.....	24
Telco clouds may run in confined environments due to strict requirements, but CaaS platforms will be agnostic to network and third-party workloads.....	25
CSPs will receive very frequent updates to their applications through CI/CD principles.....	25
Platforms that can support the co-existence of virtualized and containerized network functions will be critical in managing the transition period.....	26
Analytics will create network awareness ensuring new differentiated and guaranteed service delivery and monetization.....	27
<b>SECTION 06</b>	
<b>Private 5G networks and edge computing</b> .....	<b>29</b>
Selected examples of spectrum liberalization initiatives.....	30
Different private 5G deployment options meet different enterprise needs.....	31
Private 5G and edge computing align well to serve the enterprise.....	32
Examples of enterprises leveraging private 5G and edge computing.....	32
<b>Conclusion</b> .....	<b>33</b>
<b>Appendix</b> .....	<b>34</b>
5G core network functions and definitions.....	35
Omdia.....	36
Canonical.....	36

# Executive summary

**Realizing the full potential of 5G networks, whether to enable new services and revenue streams or to achieve operational efficiencies and scalability of applications, remains one of the biggest challenges for communication service providers (CSPs) around the world.** According to a recent global analysis by Omdia, there has been no statistical relationship between mobile ARPU changes and 5G uptake between 2020 and 2023. Arguably, this is largely because most 5G deployments have been non-standalone (NSA), which means the networks continue to leverage the 4G core. Further they are not built using cloud native cores, limiting the network's agility, resiliency and scalability and therefore cannot natively support key capabilities, such as 5G edge computing, which can stimulate innovative use cases and drive revenue growth.

Despite a slow initial uptake, CSPs report great optimism about the potential of 5G edge computing and plan to expand their edge infrastructures toward highly distributed computing fabrics suitable for the era of artificial intelligence.

When computing comes closer to end users and devices, and it is integrated with network functions, workloads can be optimized for low latency and bandwidth savings (e.g., relative to public cloud) while applications can run near or within customer premises to satisfy privacy, control and performance requirements.

To truly flourish, edge computing on telecom networks ideally needs connectivity and computing domains to meet at and build upon a common denominator of containerization and cloud native principles.

CSPs recognize this, and view cloudification of both the core and RAN to be among the biggest technological drivers of edge computing.

- With 5G SA (standalone) core, CSPs can localize and scale user plane function (UPF) instances according to demand, and efficiently steer and break traffic out where needed and depending on applications.
- In the RAN, developments around network disaggregation, cloudification, and open RAN boost the possibility of using shared hardware and software for both network functions and IT workloads on the same infrastructure.
- Private 5G networks are also ranked highly by CSPs as a driver of edge computing; these networks also rely on cloud cores and local UPFs in enterprise environments.

Moving to cloud native networks is a top transformational priority for CSPs but there are challenges to resolve.

According to Omdia surveys, managing multiple clouds and hybrid environments, clashes between cloud and legacy systems, and interoperability across vendors are key concerns both in the core and RAN domains.

To tackle these challenges and help CSPs in their journeys toward cloud native networks and 5G edge, there are six key elements of success:

- 1 A common cloud layer to cut across vendor siloes and take advantage of a broad ecosystem
- 2 Automation and orchestration that leverages Kubernetes as the underlying force
- 3 Workload-agnostic cloud platforms / CaaS for network functions and IT
- 4 Carrier-grade support for continuous integration and deployment (CI/CD)
- 5 Transition management between virtualization and containerization
- 6 Network awareness and intelligence for better customer experience and new services

Open-source technologies can play a major role in achieving these elements.

By acting as vendor-neutral cloud layers, open source platforms can bridge different hardware environments and network applications. They can simplify automation and orchestration built on Kubernetes, which is inherently open source anyway. With support for both virtualized and containerized workloads, they can provide unified platforms to host and orchestrate legacy and cloud native applications. With a vast ecosystem of developers and already strong adoption, open source can become a true engine of innovation for CSPs in their journeys to cloud native networking.

96%

CSPs\* that will have launched fully commercial edge computing deployments within the next two years

x12

Projected growth of installed edge servers on public telecom networks between 2023 and 2032

99%

CSPs\* that expect some or substantial revenue growth from edge computing

#2

Priority ranking of 'becoming a cloud native organization' among CSPs (out of nine priorities asked)

\* In the US, the UK and Germany

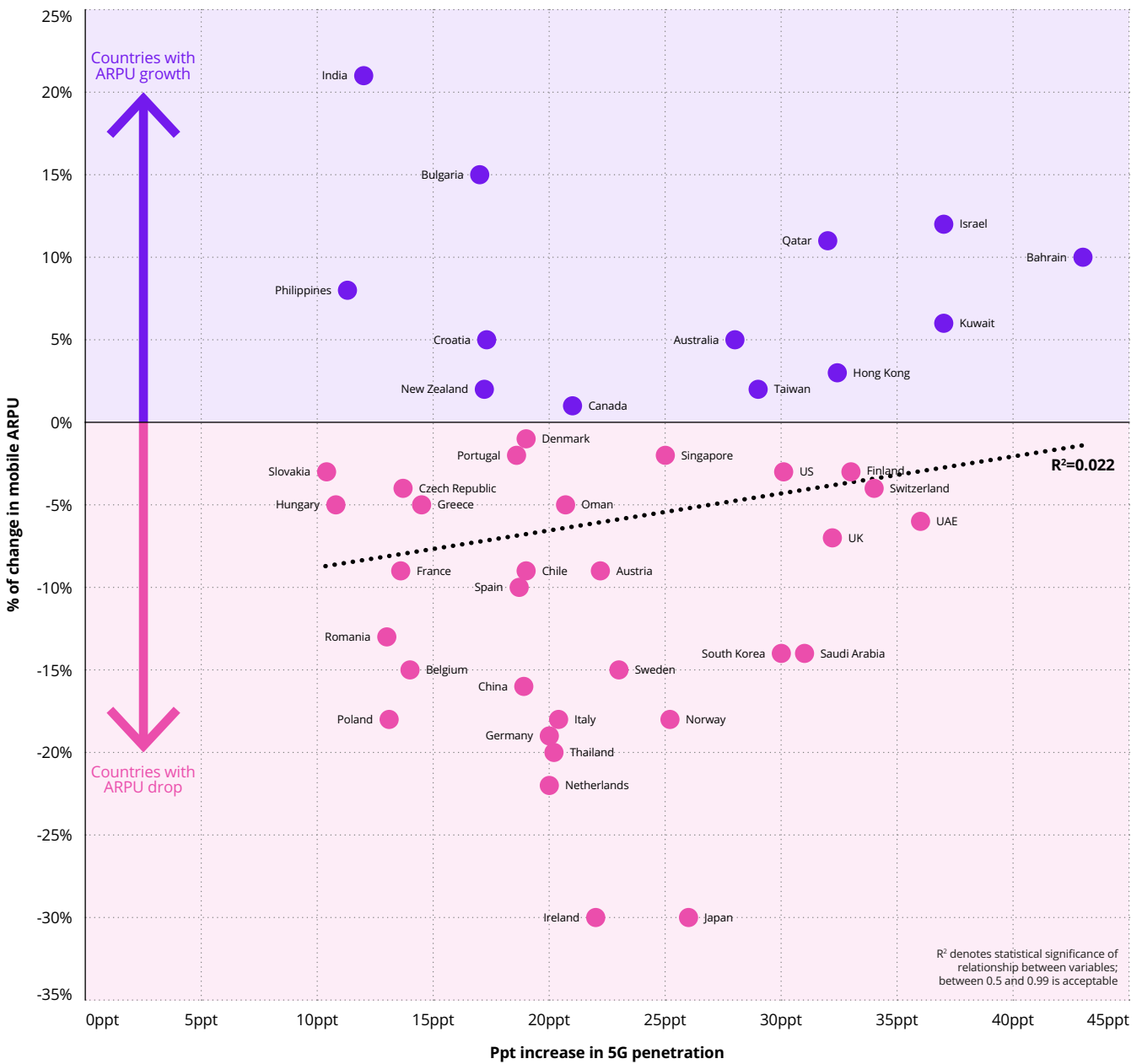
## SECTION 01

“5G monetization has been poor due to a lack of 5G SA deployments, which in turn limited the uptake of edge computing and the arrival of new revenue-generating use cases and services”

# 5G slow to reach full potential so far

There has been no clear relationship between growth in 5G uptake and changes in mobile ARPU.

**FIGURE 1**  
Relationship between % of change in 5G penetration and % of change in ARPU, 2020-23



SOURCE: OMDIA, WORLD CELLULAR INFORMATION SERIES DATABASE 2023

## This is tied to slow and delayed deployments of 5G SA, which enables new services that can translate into new revenue streams

Since 2019, the number of 5G deployments has grown around the world. Of the 700+ mobile operators covered in Omdia's database, those with commercial 5G offerings have increased from 75 to nearly 300 by the end of 2023. Most of these deployments have been non-standalone (NSA) versions of 5G, i.e., they continue to rely on 4G core (EPC) and are largely radio overlays on 4G infrastructures.

According to Omdia's Mobile Core Market Tracker, by the end of 2023, there were only 47 5G SA rollouts, comprising

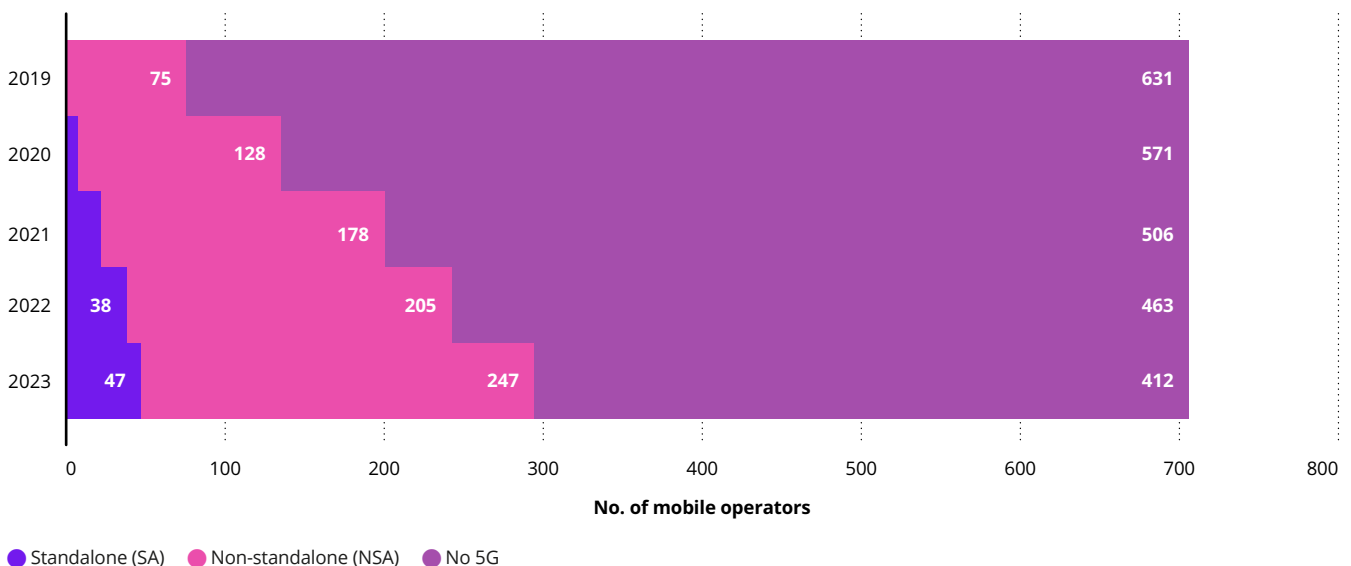
15% of all 5G deployments worldwide. Surprisingly, this ratio has remained unchanged between 2022 and 2023. In 2023, more than 40 5G NSA networks were launched vs. 12 5G SA additions.

While this approach has allowed CSPs to pace their investments and to introduce a new network generation into their markets (even if by name), 5G NSA brings only modest performance improvements over 4G, relative to what an end-to-end 5G network with a 5G core (SA) can achieve. Moreover, 5G NSA does not enable many

use cases that 5G SA can, such as those requiring ultrareliable low-latency or those powered by multi-access edge computing or network slicing.

In short, 5G NSA, while a differentiating label to market, only has limited actual end user appeal, and therefore limited potential for sustained ARPU uplift. In fact, according to Omdia's data, there has been no clear relationship between the rise of 5G penetration and changes in mobile ARPU around the world (see Figure 1).

**FIGURE 2**  
Mobile operators and 5G deployments worldwide, 2019-2023



SOURCE: OMDIA, MOBILE CORE MARKET TRACKER 2H 2023, GSA

## Without 'true' 5G networks, edge computing on telecom networks has also struggled to flourish

'True' 5G standalone (SA) networks should combine cloud native cores with virtualized / containerized RAN (NR), enabling a digital fabric of applications and services on highly distributed computing nodes at the network edge, supported by capabilities, such as slicing.

With only 5G NSA, some performance improvements are achieved, but the paradigm does not shift to the "fusion of connectivity and computing" that true 5G networks can bring. Without this step change, third-party cloud infrastructures and innovative applications have no incentive to benefit from and flourish on

telecom networks. This, in turn, limits the new revenue opportunities for CSPs.

Not surprisingly, without sufficient cloudification of mobile networks, neither at the core nor the RAN, edge computing uptake on these networks has also been limited. Many CSPs have launched commercial edge products, but these are often served only on a few centralized nodes.

For the last few years, networked edge / MEC has been a highlight expectation of the type of infrastructure and computing architecture that 5G would enable. However:

- Omdia estimated only around 100K networked edge / MEC servers installed on public telecom networks by the end of 2023.
- Only a negligible number of vRAN units has been used for anything but RAN workloads in the same period. vRAN and Open RAN are both journeys to cloudification, but they are still too nascent to expand to edge computing for third parties.
- Demand from enterprises has stayed limited, with only 4% of large enterprises claiming some adoption for 5G edge computing / MEC.

FIGURE 3

Adoption of 5G networked edge / MEC has been very slow, still comprising only a miniscule portion of the global IT infrastructure

0.4%

% of networked edge / MEC servers in all servers shipped globally, 2023

c.50K networked edge / MEC servers shipped in 2023, as opposed to 11m total server shipments.

3.6%

% of networked edge / MEC in CU-DU server shipments for vRAN, 2023

Of the c.150K units of CU-DU servers shipped in 2023, only c.5K used for / linked to networked edge applications

4.0%

% of large enterprises reported using 5G MEC, incl. private and public networks, 2023

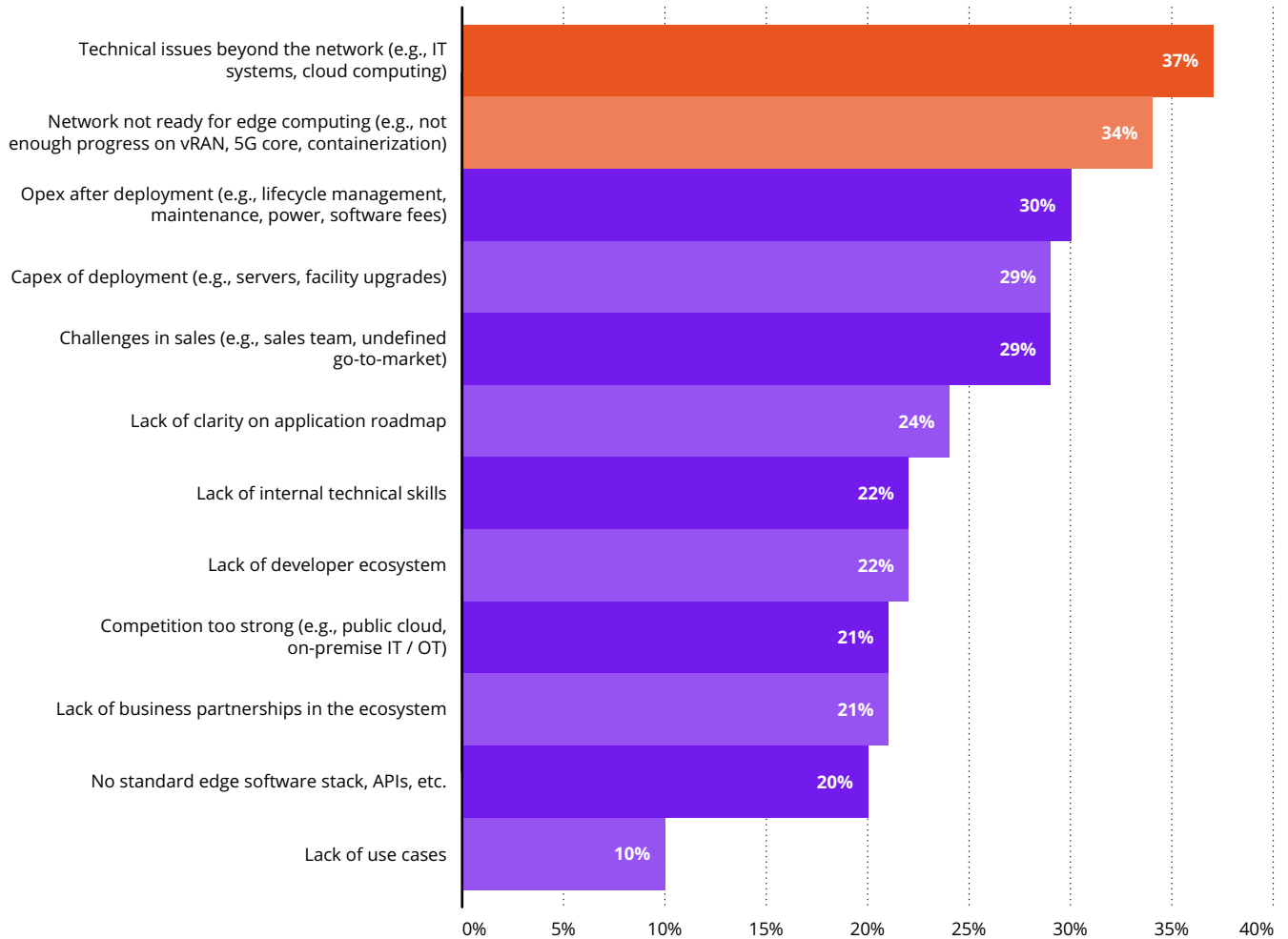
Only 4% of large enterprise (1000+ employees) respondents of Omdia's Enterprise 5G IT survey report having adopted MEC

SOURCE: OMDIA, WORLDWIDE CSP NETWORKED EDGE TAM AND FORECAST, 5G ENTERPRISE IT SURVEY (ALL 2023)

## CSPs count many challenges in their edge deployments

FIGURE 4

What are the top barriers to depolying edge applications?




SOURCE: OMDIA, CSP EDGE COMPUTING SURVEY, APRIL 2024 NOTE: N=135

CSPs acknowledge their lack of infrastructure readiness and technical challenges in IT and network domains as their biggest hurdles...


To truly flourish, edge computing on telecom networks require connectivity and computing domains to meet at and build upon a common denominator

of containerization and cloud native principles. Without these foundations in place, solutions are likely to remain clunky and limited in their ability to scale.



**CHALLENGE:**  
**Network not ready for edge computing**  
*(e.g., not enough progress in vRAN, 5G core, containerization)*

- Edge computing on telecom networks ideally requires cloud native architectures with containerized core and RAN functions.
- While core cloudification and 5G SA enable the effective and scalable distribution of User Plane Functions (UPFs) for local breakouts, traffic steering, and application proximity to end users, virtualized RAN can contribute to the dissemination of cloud computing at far edge nodes.
- For both domains, network disaggregation and purpose-agnostic usage of hardware and software across telco- and non-telco workloads are strong enablers of a highly-distributed computing topology.




**CHALLENGE:**  
**Technical issues beyond the network**  
*(e.g., IT systems, cloud computing)*

- Edge computing requires internal IT systems and end user applications to work in tandem with network functions and resources.
- On one hand, the OSS and BSS functionalities should be able to support intelligent automation and orchestration of a highly distributed computing topology, while also enabling service provisioning, assurance and charging for edge computing capabilities specifically.
- On the other hand, applications for external customers should seamlessly work with and adapt to changes in network conditions by working with CNFs, such as network exposure, slicing, and edge node selection.

...and view Opex and Capex as the two trailing obstacles


It is not cheap to create the “data center” or the “server room” infrastructures of varying sizes needed for highly distributed computing on telecom networks and the ongoing management of many edge nodes can amount to considerable

spend. Running edge computing cost-effectively across many nodes ideally requires centralized remote management capabilities with cloud automation and orchestration tools.



**CHALLENGE:**  
**Capex of deployment**  
*(e.g., servers, facility upgrades)*

- Upgrading edge nodes for computing can involve costly site upgrades for capabilities, such as power, space, servers and networking equipment, including switches and cabling.
- Most far edge nodes would not host more than a few server units and require no more than tens of kW of power, but at more centralized nodes like exchange offices, upgrades can lead to significant costs.
- Hardware spend depends greatly on the desired number and configuration of servers; these could range from a few units of general-purpose servers at far edge nodes to full racks of application servers, equipped with GPUs, at more central locations. These servers also need replenishing once in every few years.



**CHALLENGE:**  
**Opex after deployment**  
*(e.g., lifecycle management, maintenance, power, software fees)*

- Edge nodes require care after deployment. They come with energy consumption due to the usage of computing resources, as well as ongoing spend related to maintenance and security – like the opex items of data centers.
- Virtualization / containerization software used for edge computing also creates recurring costs (e.g., license fees – often priced at a ‘per socket’ basis).
- The goal of cloud native edge computing on telco networks is to reduce truck rolls, not increase them. However, deploying, scaling, and orchestrating applications and network functions, in accordance to demand and the underlying hardware at many edge nodes can be overwhelming, if not supported by cloud native tools and methods for automation and workload orchestration.



## SECTION 02

“Despite early challenges, there is a lot of optimism around networked edge and expectations of growth; CSPs are planning to expand their infrastructures toward highly-distributed computing”

# 5G edge computing now set for strong growth

Despite all the challenges, many CSPs have deployed commercial offers that leverage edge computing on their networks, and more are planning to do so.

## The challenges that CSPs face do not put them off from commercial deployments and bringing edge products to market.

Since 2020, there have been 140 edge announcements on 5G networks by CSPs around the world (more when CSPs' edge data center initiatives are added into the mix without necessarily relating it to 5G).

More than half of CSP survey respondents in the US, the UK and

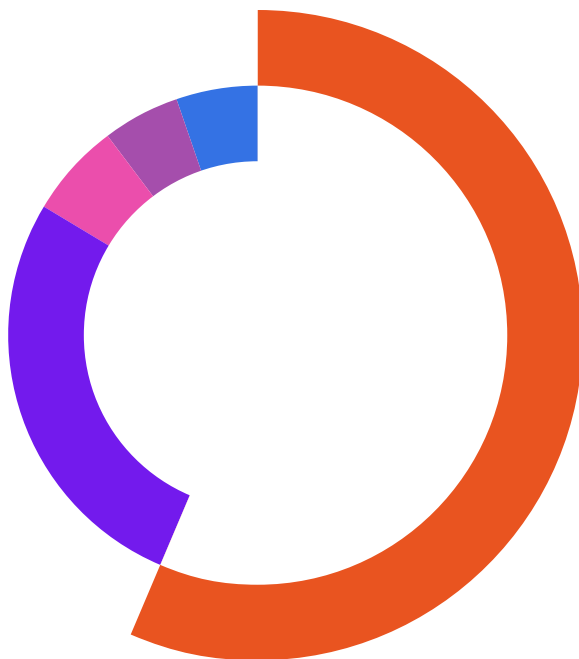
Germany reported having full commercial rollouts, across private and / or public network environments. The remaining respondents are also keen to add networked edge into their portfolio within the next two years at most – 90% of this group will have completed their commercial launches within the next two years.

In short, edge computing plays an essential role in CSPs' activities. As the

initial hype around the topic has been replaced by realism, edge computing stopped being a “thing” to sell but became a valid position in the cloud continuum that is activated as part of a larger solution for customer requirements, such as low latency, reliability, or security and privacy.

FIGURE 5

What is the current state of your organization's edge computing deployment?

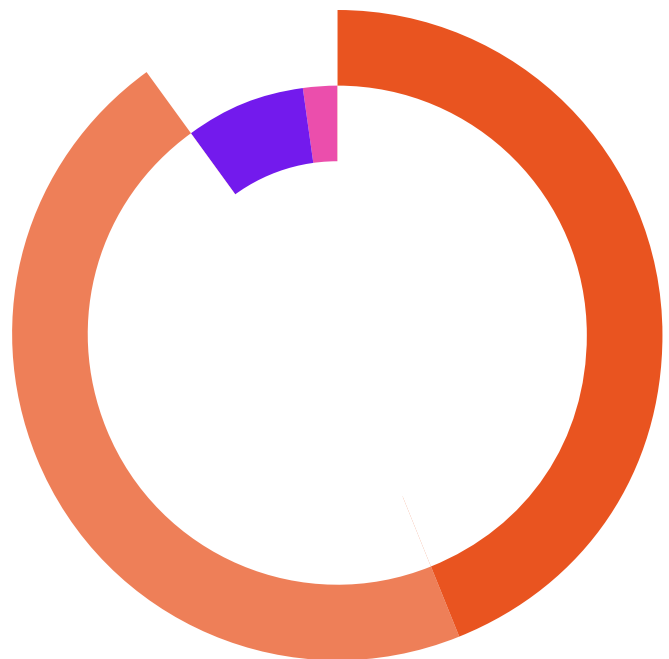


- Full commercial deployment (56%)
- Early-stage commercial deployment (27%)
- Pilot deployments and testing (6%)
- Planning deployment and trials (5%)
- Exploring use cases, technical requirements, and / or vendors (5%)

SOURCE: OMDIA, CSP EDGE COMPUTING SURVEY, APRIL 2024 NOTE: N=135

FIGURE 6

When will your organization complete its commercial deployment of edge computing?



- Within 12 months (44%)
- Within 24 months (46%)
- Beyond 24 months (8%)
- Don't know (2%)

SOURCE: OMDIA, CSP EDGE COMPUTING SURVEY, APRIL 2024 NOTE: N=59

## CSPs value the versatility of edge computing, which brings both internal and external benefits

The appeal of edge computing comes primarily from its versatility. As a topology driven by cloud native principles for both network functions (NF) and IT workloads, it offers both significant internal and external benefits to CSPs. According to Omdia's 2024 survey, the internal and external motivations to deploy edge are almost evenly split.

While network cost savings, operational efficiencies and scalability are more internal-focused, better customer experience, new use cases and revenue

streams stand out as more external-oriented incentives.

A key aspect of edge computing is to manage traffic with local breakouts and effective routing with distributed UPFs. This can create significant cost savings by relieving unnecessary data traffic journeys on transport networks. This is a motivation enterprises would also share as they also want to control their data transfer costs.

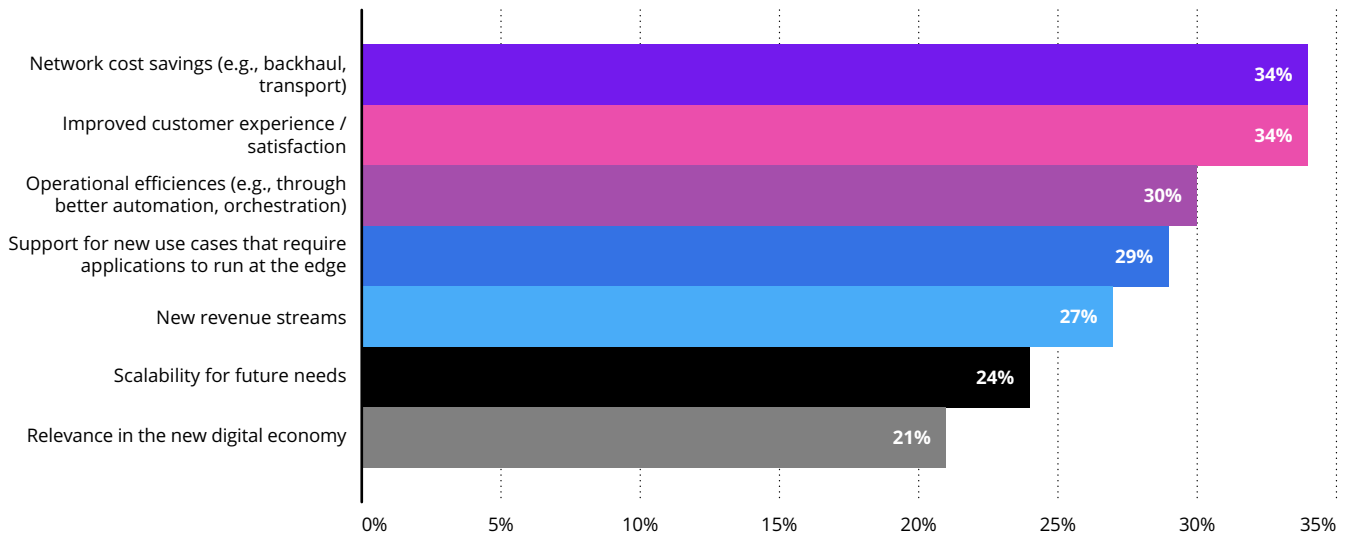
Local UPF instances enabled by 5G cloud core are also key to enabling and supporting new use cases and improving

customer experience by linking networks to applications where they are closest to end users. Whether for ultralow latency or for data privacy, sovereignty or control, this opens door to new revenue streams.

Cloud-native and Kubernetes-supported edge computing also allows for enhanced automation, orchestration, and self-healing capabilities, as well as the ability to scale resources up and down at nodes when they are (not) needed.

FIGURE 7

What are the biggest incentives for your organization to deploy edge computing?



SOURCE: OMDIA, CSP EDGE COMPUTING SURVEY, APRIL 2024 NOTE: N=135

## Confidence in presence of demand breeds confidence in the future...

Unlike a few years ago, when there were serious concerns about the absence of a 'killer app' to drive the growth of edge computing, CSPs no longer see "lack of use cases", and therefore demand, as a big barrier to their edge deployments. In Omdia's survey, it was the bottom-ranked challenge by a long distance.

Confidence in the presence of demand breeds confidence in future success.

86% of respondents in Omdia's CSP Edge Computing survey reported being "optimistic" or "very optimistic" about the future of edge computing\*.

This optimism comes both from expectations of internal efficiencies and those of new revenue streams. Almost all respondents reported expecting some (60%) or substantial (39%) new revenue to come from edge computing in the future.

CSPs see revenue to be generated most both by end user applications (57%) and premium connectivity features (53%).

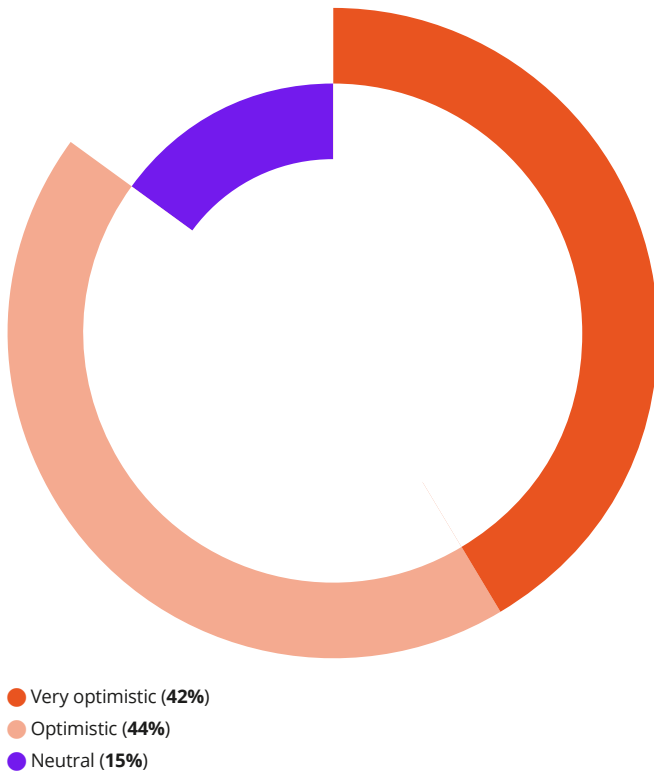
End user applications include both vertical-specific solutions and horizontal technologies that enable edge use cases, such as AI/ML processing, computer vision, new media and XR, drones, etc.

Premium connectivity relates to edge-enabled quality of experience, such as latency, jitter, or reliability, with application-specific policies and network slicing.

CSPs also anticipate the modernization of their edge infrastructures to create revenue opportunities for hosting and selling their own and third-parties' computing resources and platforms.

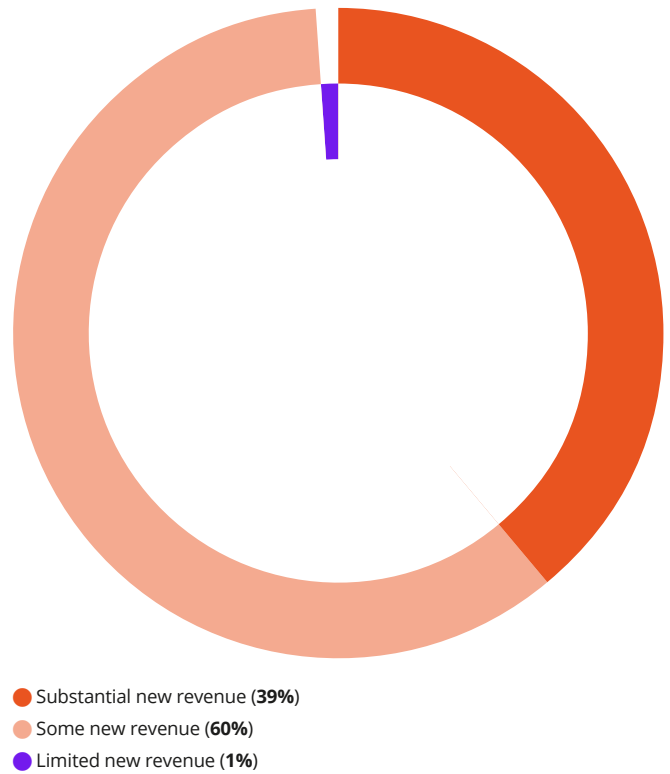
\* The question included options for 'pessimistic' and 'very pessimistic'

**FIGURE 8**  
How optimistic are you regarding the future of edge computing on telco networks?



SOURCE: OMDIA, CSP EDGE COMPUTING SURVEY, APRIL 2024 NOTE: N=135

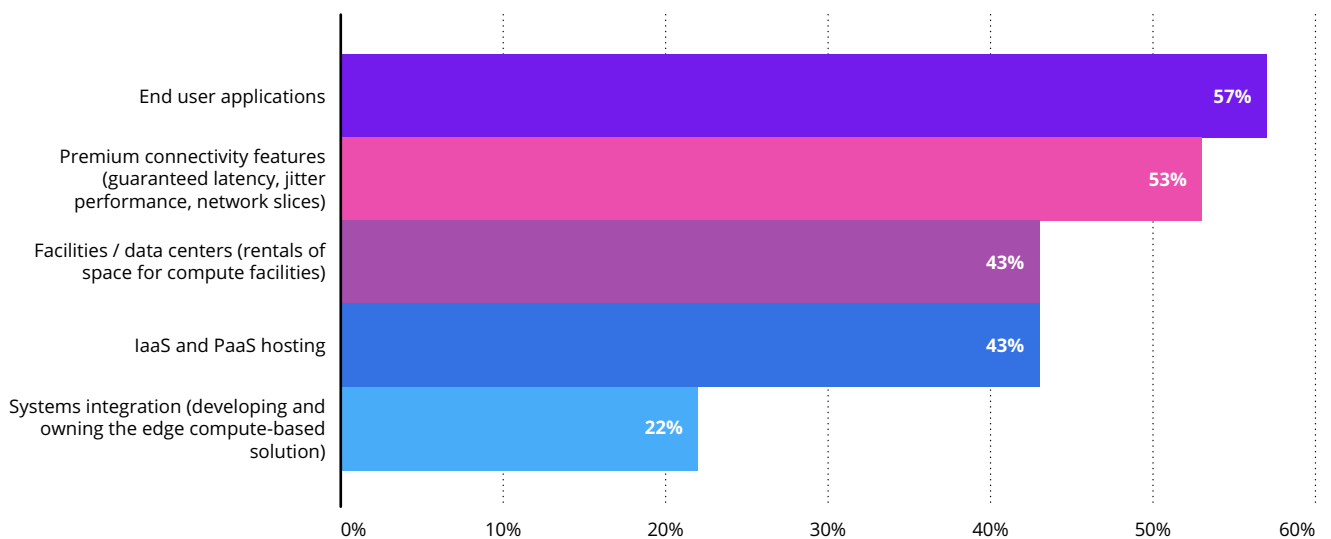
**FIGURE 9**  
Which best characterizes the size of the new revenue opportunity that edge computing can create in your organization?



SOURCE: OMDIA, CSP EDGE COMPUTING SURVEY, APRIL 2024 NOTE: N=135

...with applications and premium connectivity at the edge viewed as key revenue streams in the future

**FIGURE 10**  
Which areas of edge computing have the greatest likelihood of driving revenue growth for your organization?



SOURCE: OMDIA, CSP EDGE COMPUTING SURVEY, APRIL 2024 NOTE: N=135

## To capture demand, edge infrastructures are set to expand toward highly distributed computing

Currently, most CSPs have preferred to launch edge computing at the near edge of their networks (often with partnerships with public cloud providers), such as metro data centers and transport aggregation nodes. Due to this initial focus, more than 60%

of the respondents in the US, the UK and Germany have reported having less than 30 nodes made available for edge applications, excluding private networks.

This, however, is set to change toward a much more distributed computing

environment. More than a quarter of CSP survey respondents believe that in five years, they will have more than a hundred edge nodes – half of which expect more than five hundred.

FIGURE 11

How many locations is your organization's edge deployment currently in, and how many do you expect within five years (excluding private networks)?

### CURRENTLY



### WITHIN 5 YEARS

● Less than 10 ● 10-29 ● 30-99 ● 100-500 ● More than 500

SOURCE: OMDIA, CSP EDGE COMPUTING SURVEY, APRIL 2024 NOTE: N=135

## Omdia expects networked edge uptake to grow over the next several years, leading to an opportunity of more than \$26bn for IaaS and SaaS by 2032

All the optimism, confidence in demand, and growth expectations, along with expansion plans of edge infrastructures will translate to an overall market growth.

Despite a slow initial start, Omdia projects the installed base of edge servers on public networks worldwide to grow from around 100K in 2023 to around 1.2m units in 2032, with the expectation that, by this time, 5G core and vRAN will have truly scaled as key enablers of uptake of new edge services and applications.

The computing resources and the applications that run on them will grow to an annualized revenue potential of more than \$26bn (IaaS and SaaS) within the same period. While this corresponds to a relatively small portion of the larger public cloud market as it is today, it is still a sizable opportunity that all players in the digital value chain will want to capture.

These projections are informed by, and already provide hints at, the direction of travel. Currently, the strongest region in terms of adoption is China and the advanced markets of Asia-Pacific, where 5G core has been deployed extensively and applications run on thousands of UPF nodes.

This fundamental driver of edge computing will gradually expand to other

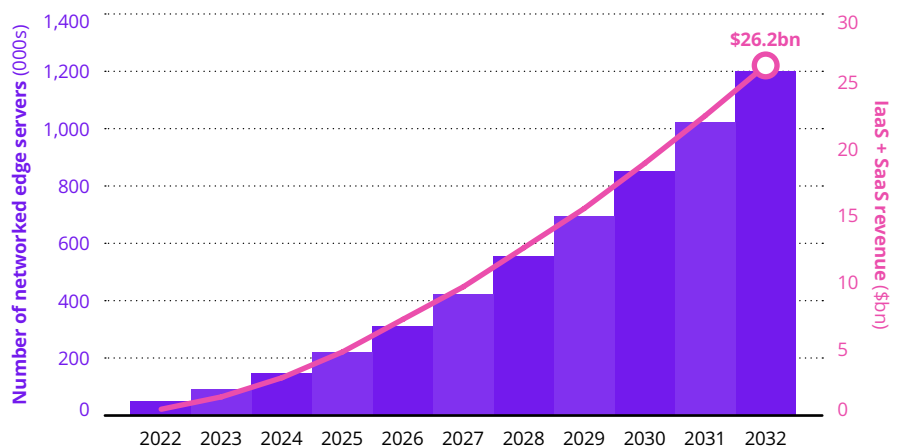
markets, where 5G SA is being rolled out at scale and cloud native architectures are starting to be adopted.

These forecasts would be even higher when edge computing on private mobile networks are also included. Omdia expects the market for private mobile networks to

grow by around 270% between 2023 and 2028, from \$3.4bn to \$9.3bn. According to Omdia's enterprise survey, one in three enterprises that buy private mobile networks also purchase edge computing alongside it as part of a larger solution.

FIGURE 12

Networked edge servers (installed base) and related IaaS + SaaS revenue, 2022-2032



SOURCE: OMDIA, WORLDWIDE NETWORKED EDGE FORECAST, 2023



## SECTION 03

“CSPs recognize network cloudification as key to capturing edge computing opportunities and see becoming cloud native as a big priority due to its many benefits – both from technical and operational perspectives”

# Essential role of network cloudification for CSPs

Network cloudification across all domains, and disaggregation, is the biggest expected driver of edge computing for telcos.

**The expected growth in networked edge and the highly distributed computing that it will create will be driven first and foremost by cloudification of telecom networks.** According to Omdia's survey, CSPs expect cloudification across all network domains, core, RAN, and transport, to be the biggest enablers of edge.

Network cloudification also precedes other technological developments as an underlying enabler for other capabilities. For instance, network APIs and exposure, slicing and computing for AI/ML all work best with cloud native principles.

CSPs rightly rank mobile cloud core clearly at the top (51% of responses). With

5G standalone, CSPs gain the ability to localize and scale UPF instances according to demand, and to efficiently steer and break traffic out where needed. These capabilities play the biggest role in bringing applications closer to end users, and CSPs recognize this.

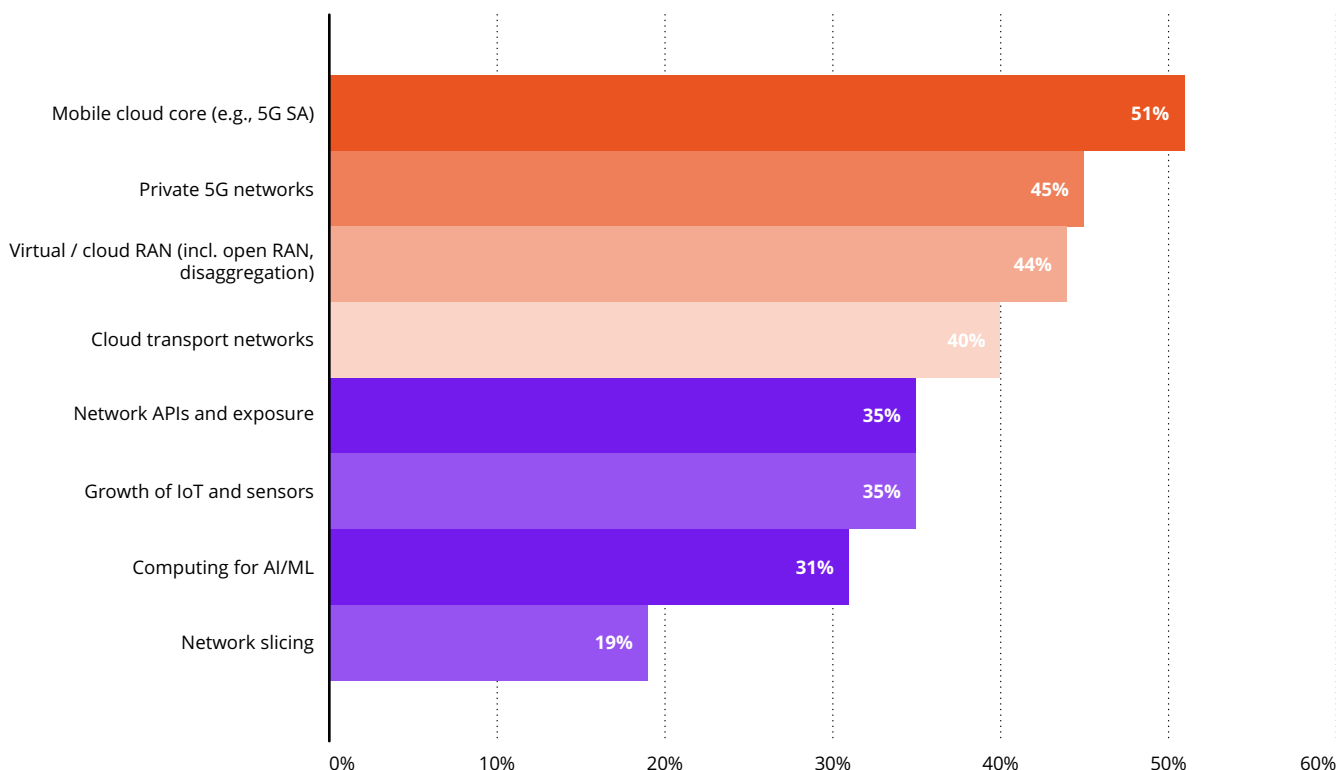
The separation of control and user plane functions (CUPS) is the underlying principle that allows the management of control planes in centralized cloud environments and the distribution and scaling of UPFs as and when needed.

In the RAN domain, virtualization and containerization has been slower to progress (vs. the core), but developments

around network disaggregation and Open RAN boost the possibility of using shared hardware and software for both network functions and IT workloads on the same infrastructure – a major enabler of distributed computing, especially at the far edge of networks.

Private 5G networks, ranked #2 with 45% of responses, are also related to the journey of cloudification. They rely heavily on the availability of cloud core and the consequent UPF placement for success of edge computing with enterprise environments.

**FIGURE 13**  
Which of the following will be the strongest drivers of growth in edge computing on telecom networks?



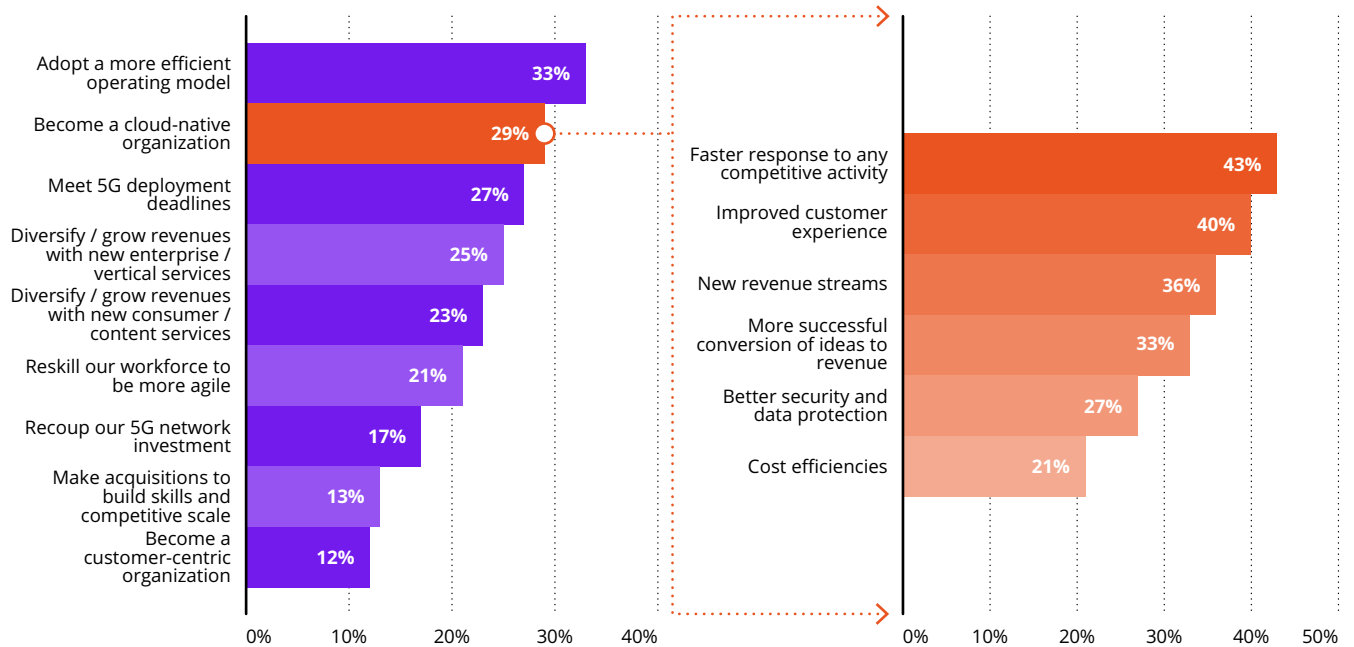
SOURCE: OMDIA, CSP EDGE COMPUTING SURVEY, APRIL 2024 NOTE: N=135

Becoming cloud native is not only to pursue the edge computing opportunity; it ranks among the highest overall priorities for CSPs...

FIGURE 14

CSP organizational priorities over the next 24 months

CSPs' expected benefits from migrating to cloud native technologies



SOURCE: OMDIA NOTE: N=135

... because it offers many benefits and suggests a paradigm shift for the CSPs

CSPs see becoming a cloud native organization as a top priority in the next two years (29% of responses), above and beyond the context of edge computing– with positive externalities on almost all other objectives.

Becoming cloud native does not only apply to networks and IT systems, but also to ways of working. For networks and IT, cloud nativeness brings a technical common denominator of working with containers and microservice architectures, both on bare metal and agnostic to operating systems, and on virtual machines.

As such a lightweight and modular approach to application deployment comes with speed and flexibility, it also creates a need to manage the complexity of many moving pieces and lifecycles. Thus, to obtain the full benefits of their 5G investments, CSPs must embrace new and more efficient ways of working, such as adopting automation tools and relying more on software skills to manage their cloud infrastructures.

Another key feature of being cloud native is continuous integration, continuous testing, and continuous

deployments (CI/CT/CD). CSPs will use these tools to increase the rate of new software rollouts and necessary upgrades.

These upgrades include timely security fixes and patches, critical to telecom networks, and upgrades to introduce new revenue generating services to the market quickly and meet deployment timelines.

Omdia believes that the objective of becoming cloud native aligns well with the other top priorities of CSPs: Cloud nativeness paves the way toward a more efficient operating model (33% of respondents), it enables efficient 5G rollouts, and helps the launch of new services quickly.

CSPs expect many customer-facing benefits from being cloud native. While agility in relation to competitive dynamics ranks at the top (43% of responses), better customer experience and new revenue streams are also mentioned by many respondents. For CSPs to be able to compete in the marketplace and get return on their huge 5G infrastructure investments, they must be able to respond quickly to changing customer needs and requirements.

Further, CSPs have told Omdia that the 5G networks are becoming more and more complex so they must leverage new tools, such as automation, to not only reduce their costs (21% of responses), but also orchestrate new network slices and deliver the right key performance indicators (KPIs) to address new revenue streams.

Ideally, cloud nativeness should also bring some cost efficiencies. In the long run, a modular, scalable and flexible architecture built on containers and microservices can take advantage of commercial off the shelf (COTS) servers to reduce hardware expenditure and decrease software license fees, especially when open source technologies are adopted.

To facilitate a new era of opportunities, 5G networks (and beyond) will be built using cloud native technologies, which for the first time will equip CSPs with the ability to behave more like the hyperscalers. This is a paradigm shift for CSPs and a step change from operating physical infrastructure or even the virtualized deployments used for 4G networks.



## In the core, cloudification will bring benefits of agility, efficiency and scalability

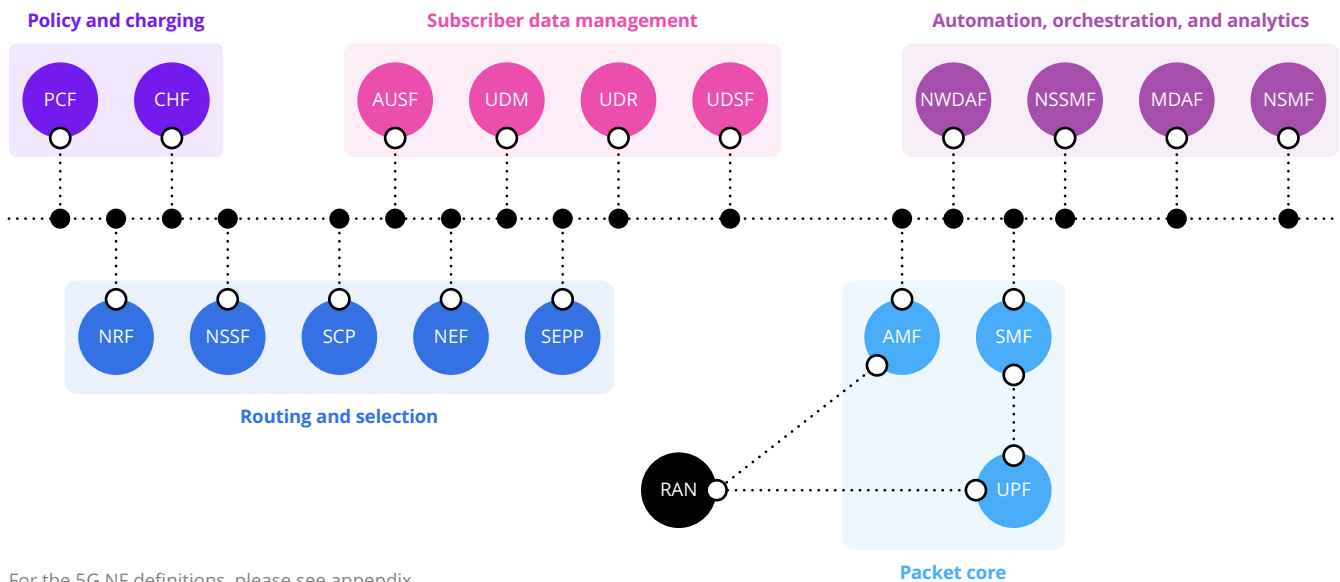
Many CSPs started their 5G upgrade journeys in the last four to five years, but most of these have only upgraded to deliver 5G in the NSA mode. CSPs that want to successfully deliver new revenue generating use cases, such as AR/VR, low altitude economy for example drone services, must embark on deploying the 5G SA core using cloud native technologies. This will ensure they can utilize new toolsets, such as automation to operate the core with simplicity, openness, and confidence.

Unlike the 4G evolved packet core (EPC), where the NFs were implemented in a peer-to-peer (P2P) architecture, the 5G core utilizes service-based architecture (SBA), which adopts service-oriented software design principles. The NFs are linked together on the service-based interface (SBI), a common bus, creating a service mesh as shown below. This approach aligns well with cloud native principles.

A 5G core built using cloud native principles will facilitate the use of microservices that run-in containers

enabling modular function designs, which in turn are more efficient than virtual machines (VMs) used in the EPC. In addition, cloud native enables agility, efficiency and scalability, which means that when a new services is instantiated, for example using network slicing capabilities, the relevant resources can be spun up and scaled up for the required time and torn down, releasing the resources, when no longer needed.

**FIGURE 15**  
The 5G core service-based architecture



For the 5G NF definitions, please see appendix

SOURCE: OMDIA, ADAPTED FROM 3GPP R17 TS23.501

## RAN is the largest capex spend for mobile operators; its virtualization will enable both software and geolocation disaggregation

The telecom industry has been on the virtualization journey for over a decade, yet achieving full RAN virtualization has proven more challenging than that with other network domain components, such as the core.

Open vRAN combines the principles of open RAN and vRAN, i.e., the disaggregation of the RAN into subsystems that interoperate via open interfaces and the virtualization of the baseband software functions: central unit (CU) and distributed unit (DU), or CU only.

It is this disaggregation of subsystems together with the open fronthaul

interface that facilitates multivendor integration, one of the principal drivers for open vRAN as sought by many CSPs, that want to get out of vendor lock-ins by the incumbent players.

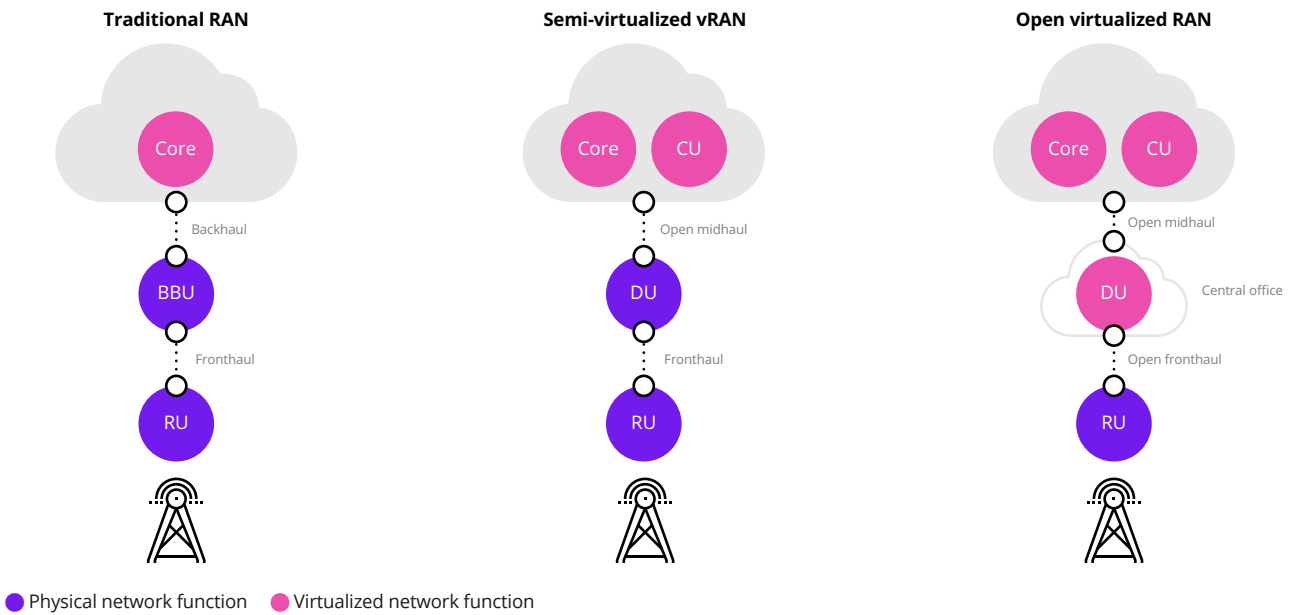
The performance of the vDU in open vRAN has struggled to match that of traditional purpose-built equipment. vDU is the most compute-intensive component of the RAN and the solutions, including chipsets necessary have so far been less efficient, however, this is beginning to change.

Open vRAN continues to mature, which is one of the reasons, why beyond the greenfield CSPs, such as Rakuten

Mobile and Dish, there have been very few brownfield deployments. Verizon and Vodafone are two examples of CSPs that are deploying open vRAN at a large scale.

Single-vendor open RAN has now been presented as a new industry trend, with several cases where the same vendor provides the RU and the DU/CU. However, if a deployment is open vRAN (and not just open RAN), even if the same vendor provides both the RU and the baseband software, the system is still considered multi-vendor as it introduces new servers and cloud infrastructure vendors in the RAN domain.

**FIGURE 16**  
RAN evolution to open vRAN



SOURCE: OMDIA

## RAN disaggregation will lead to centralized computing, facilitate CUPS and drive new edge services' business models

The disaggregation of RAN into its components enables centralization of these functions, for example by placing the CU at the near edge location. In the near-term (see Figure 17), when sufficient fibre network is available in the fronthaul (such as the case in Japan and S. Korea), mobile operators will also be able to move the DU to a near edge location, creating not just cost efficiencies at the RAN sites, but also a centralized compute platform, an enabler to run use cases, beyond just RAN functions.

To do this, however, will require the near edge servers to be adequately equipped, for example with the necessary

hardware accelerators for the DU function. The near edge location is also ideal (in terms of distance to end user and hence latency delivered) for edge applications. Examples of these are image processing for AR/VR or cloud gaming use cases.

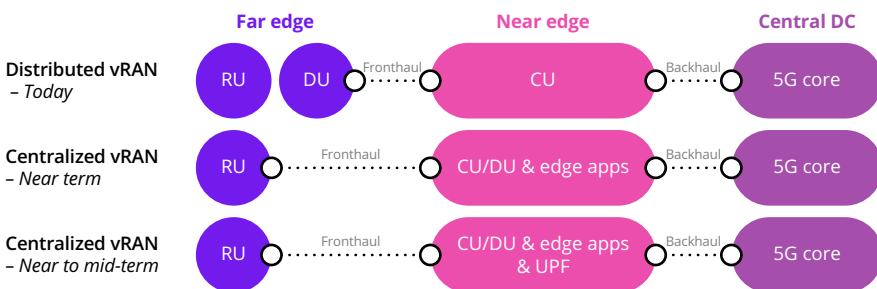
Instantiating the UPF function, a 5G core network function, at the near edge, will further facilitate CUPS and enable local breakout of data traffic, reducing transport costs.

The dawn of network slicing will also drive new business models to be created by delivering specific network key performance indicators (KPIs) as

the combination of hardware, edge applications and cloud native technologies will turn near edge locations into powerful revenue generating assets for CSPs.

For this architecture to be performant and secure in the near to mid-term, CSPs' vRAN software and third-party hardware must be fully tested together. CSPs will also benefit from a horizontal cloud platform across the three domains, core, edge and RAN, utilizing the power of a single automation and orchestration toolset to run use cases.

**FIGURE 17**  
Network architecture will evolve to support new use cases



Centralized vRAN refers to the pooling of baseband processing resources at hub points on the nearer edges of mobile networks versus having the RAN compute resources at individual mobile sites. Connected with fronthaul links, these hub points can be located as far as 20km away from the antennas and act as access aggregation points for mobile networks. Therefore, centralization of RAN is only relative to the distributed mobile architectures of today; it does not suggest that all baseband processing will concentrate in a few core network locations.

SOURCE: OMDIA

## SECTION 04

“However, network cloudification has not been without its challenges neither in the core nor in the RAN; multi-vendor interoperability, complexities of multiple cloud environments, and management of co-existing legacy and cloud native applications and systems stand out as problems that need tackling”

# Challenges in the journey to cloud native networking

Despite nuances, cloudification challenges are highly similar across core and RAN domains.

Managing complexity and interoperability are the main challenges to 5G cloud core deployments; business case clarity is not a concern

**The delay in 5G cloud native core investments is partly related to the persistently adverse global economic conditions and higher-than-usual interest rates, which make large scale investments challenging.** With high cost of debt, in many markets, integrated operators had to juggle resources across their 5G and fiber investments.

In 2023, Omdia surveyed 109 CSPs in North America, Europe, and Asia & Oceania on core networks (respondents from both advanced and emerging markets). This survey revealed some specific challenges that CSPs faced in their

5G core deployments, beyond the macro conditions.

CSPs largely agreed that 5G core deployments were complex due to the need to manage and interoperate multiple environments, whether they are multi-cloud, multi-vendor, or a combination of cloud and legacy components.

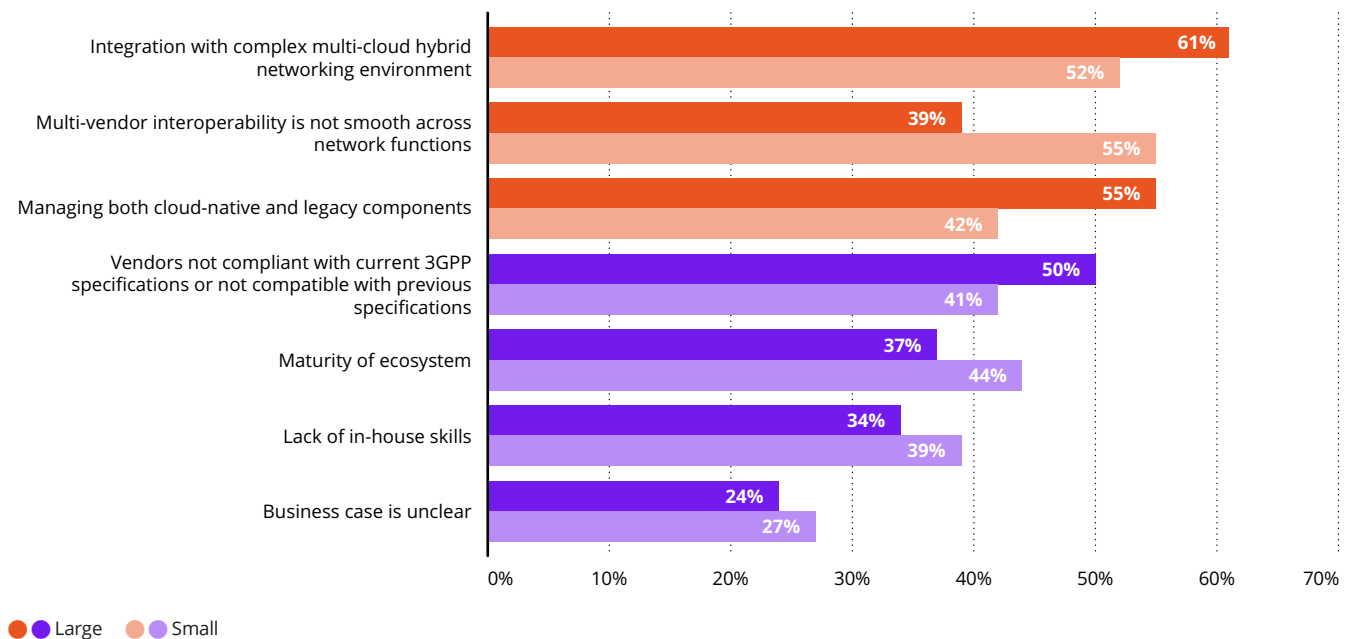
Main challenges noted by the CSPs were complexity of integrating multi-cloud hybrid networking environments and multi-vendor interoperability challenges across NFs. The latter is a bigger headache for smaller CSPs, who lack more the in-house skills and

resources to deploy and manage complex platforms.

The co-existence of 5G cloud native core functions with legacy networks has been mentioned as another top challenge.

Strikingly, 'business case clarity' was the least of their concerns. This implies a belief that (a) 5G cloud native core is necessary, and that (b) the demand for the use cases that 5G core enables is largely there. In other words, had strategic and technical hurdles not been there, investments in 5G cloud native core would pay off with benefits surpassing the costs.

**FIGURE 18**  
CSPs' main challenges in deploying 5G cloud native core network



SOURCE: OMDIA, SERVICE PROVIDERS CORE NETWORKS SURVEY - 2023 EXTENDED VERSION (SEPTEMBER 2023)

## Integration challenges are the primary obstacles to the adoption of open vRAN

In 2023, Omdia also conducted a separate survey of 106 CSP respondents about open vRAN and RAN, covering deployment motivations and challenges.

It is no surprise that the top challenges mentioned by the respondents are the complexity and costs associated with integration of multi-vendor solutions and integration with legacy networks. These two concerns were also at the top in the 2022 survey, representing persistent obstacles to adoption.

Due to the potentially high diversity of vendors in open vRAN scenarios, in 2023, most Omdia conversations with vendors and CSPs circled around who should lead and champion implementations.

'Limited vendor choice' and 'vendors' unproven track record' are other important challenges (35% and 34% of respondents, respectively). CSPs should, however, understand that open vRAN ecosystem is still emerging.

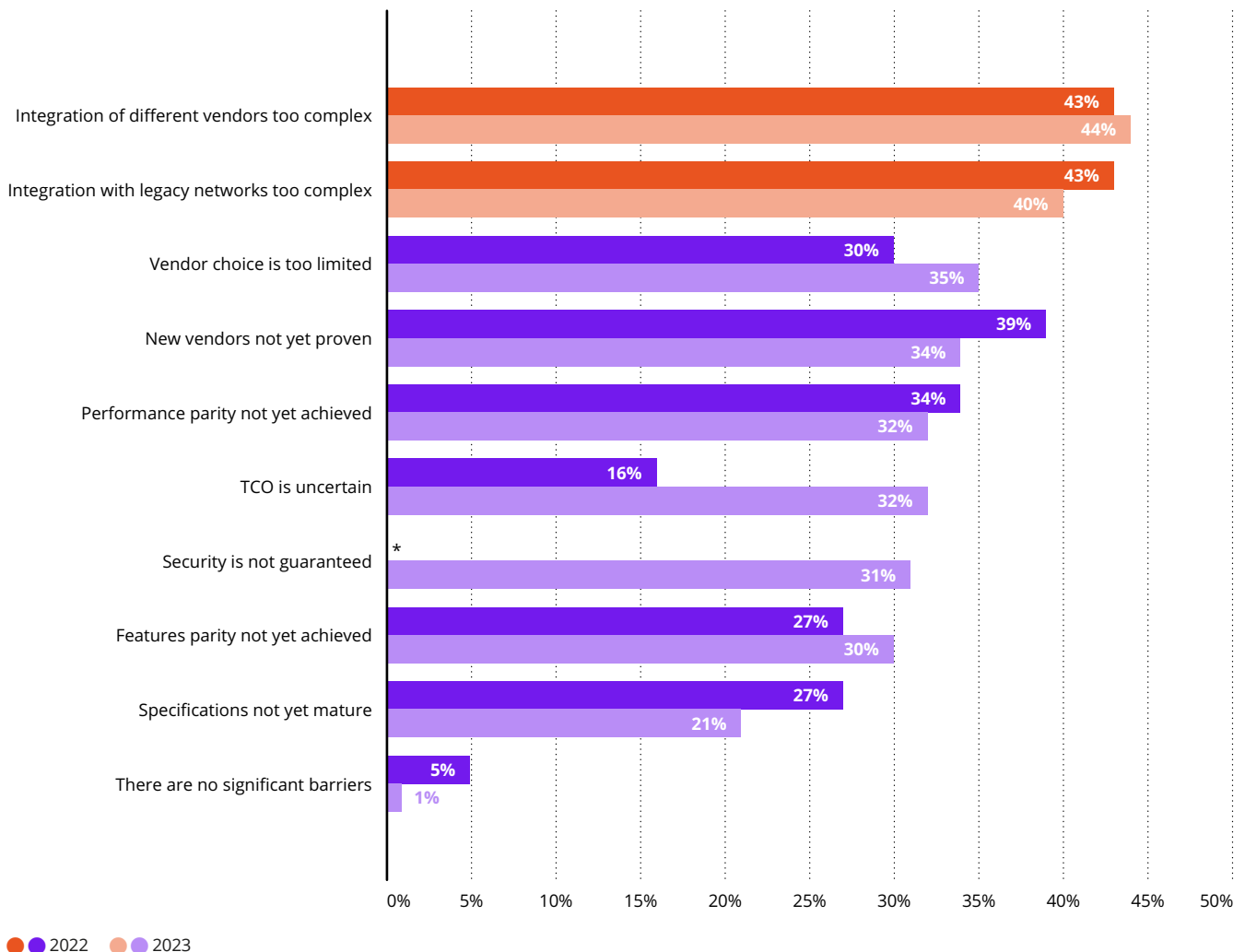
In the case of proprietary vRAN products from the large incumbent

vendors, uptake will depend mostly on when legacy contracts expire. The recent Ericsson and AT&T deal shows intent by a large incumbent vendor, and this will likely incentivize the open vRAN ecosystem to push forward and compete.

In 2023, respondents that selected 'TCO uncertainty' as a main barrier doubled (32%). In stubbornly tough industry and macroeconomic contexts, CSPs prioritize cost control and appear hesitant toward large scale investments unless they really must.

FIGURE 19

What are the main barriers to multi-vendor open vRAN adoption? (Select up to three)




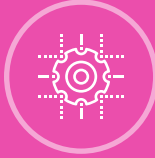




SOURCE: OMDIA SERVICE PROVIDERS RAN SURVEY 2023 NOTE: 2022 N=103 | 2023 N=106 | \* "SECURITY IS NOT GUARANTEED" WAS NOT INCLUDED IN THE 2022 SURVEY.

## SECTION 05


“What can CSPs do to tackle challenges of cloudification and what are the elements of success in their journeys to cloud native networks and edge computing?”

# Keys to success and the role of open source

So, what can CSPs do to tackle these challenges effectively and prepare better for their journey toward cloud native networks and edge computing?

 <p>A <b>common cloud</b> that can cut across telecom vendor siloes and take advantage of a broad ecosystem</p>	 <p><b>Automation and orchestration</b>, leveraging Kubernetes as the underlying force</p>
 <p><b>Workload-agnostic cloud platforms / CaaS</b> for NFs and IT workloads</p>	 <p><b>Carrier-grade support</b> for continuous integration and deployment</p>
 <p><b>Transition management:</b> from virtualization to containerization</p>	 <p><b>Network awareness and intelligence</b> for better customer experience and new services</p>

## A common cloud layer can act as a platform of interoperability to reduce vendor fragmentation



A **common cloud** that can cut across telecom vendor siloes and take advantage of a broad ecosystem

CSPs that pursue a multi-vendor architecture for their core, edge, and RAN deployments face integration and management challenges, thus higher costs. This issue is exacerbated when each vendor delivers its network functions together with its own cloud and infrastructure layer, adding to the operational complexity.

Multi-vendor architecture also creates challenges for the vendors, as they must certify their network functions on multiple cloud platforms, including those of CSPs, other vendors', and public cloud providers (PCPs).

As edge computing on telecom networks becomes more widespread, NF deployments and orchestration across many different telco clouds on many nodes will also become extremely challenging.

To tackle this fragmentation and operational complexity, CSPs can deploy a single 'common' cloud platform between diverse compute and NF environments, eliminating the need to manage multiple vertical stacks and offering a vendor-agnostic layer of modularity and interoperability layer in the middle.

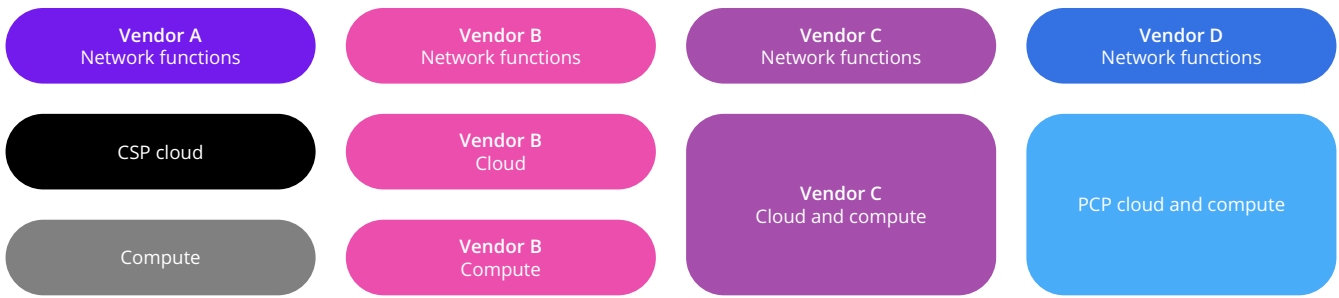
The concept of the 'common' cloud should serve to highlight the value that

CSPs place on operational simplicity and the need for NF providers to operate outside walled gardens to be truly helpful to network operators.

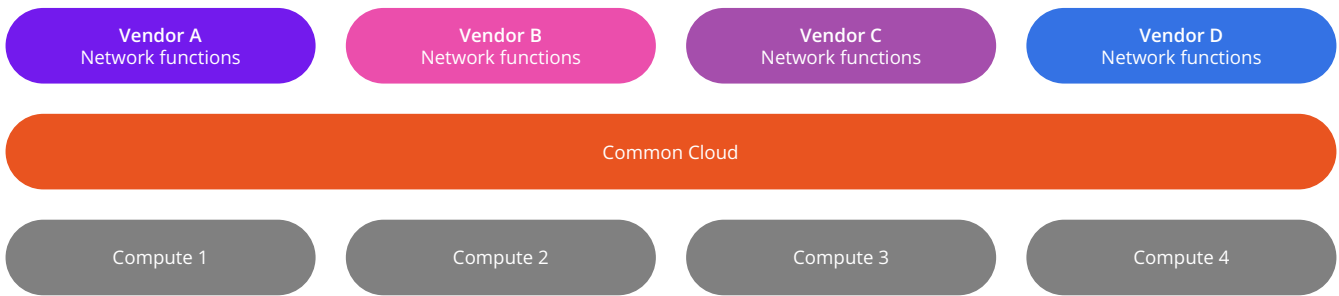
While some vendors can highlight the benefits of vertically-integrated cloud layers and NFs, such benefits should erode with the growing adoption of cloud native networking, where containerization and microservices are the common denominators for all NFs.

Open-source cloud platforms can be an important enabler here. By acting as neutral middle layers, they can help CSPs take advantage of a vibrant ecosystem that is fed with the certification of NFs by many vendors and best-of-breed applications, while also reducing the sense of vendor lock-in at the cloud layer.

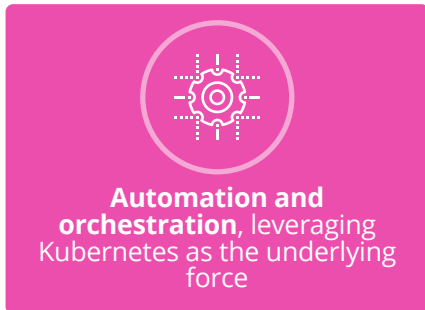
**Cloud and network function multi-vendor fragmentation**



**Common cloud layer**



Kubernetes is a powerful approach to container orchestration, especially when supported by services that offer visibility, control and management of clusters



As an open source system with inherent capabilities of automated rollouts, load balancing, self-healing and scalability,

Kubernetes is the leading approach to container orchestration and management. As network functions are being containerized, CSPs are also seeing and appreciating the raw power of Kubernetes despite its relatively late entry into telecoms.

The fundamental logic of Kubernetes to coordinate application delivery and resources between master and many worker nodes is also highly suitable for edge computing. Again, ideal for edge devices, there are lightweight, single-node versions of Kubernetes.

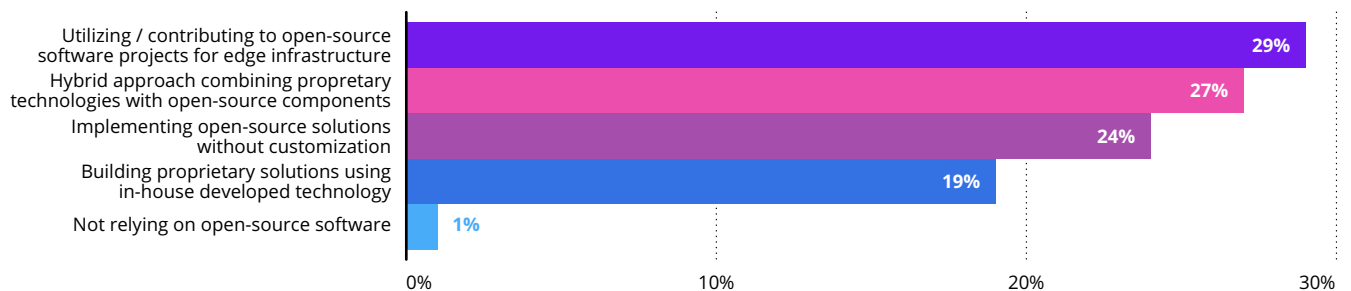
While extremely powerful, managing Kubernetes clusters can become difficult

in large and highly distributed topologies with many nodes, different service requirements, and heterogeneous hardware environments.

Therefore, to gain better visibility, control, and customization over performance, resource utilization, and applications, operators should consider the use of commercial distributions or managed Kubernetes services.

In fact, CSPs already have a wide spectrum of usage of open source for edge computing, often with some customization or combination with proprietary technologies.

**FIGURE 20**  
Which best describes your approach to using open source technologies in edge computing?



SOURCE: OMDIA, CSP EDGE COMPUTING SURVEY, APRIL 2024 NOTE: N=135



## Telco clouds may run in confined environments due to strict requirements, but CaaS platforms will be agnostic to network and third-party workloads



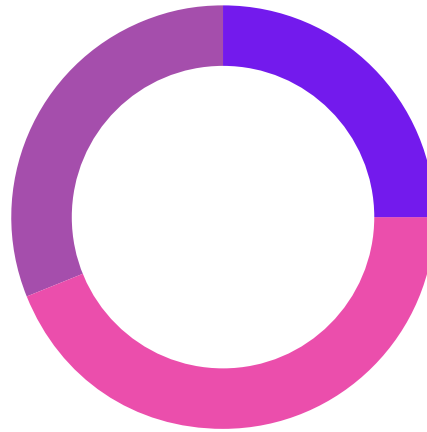
While the separation of the telco and IT clouds is currently needed due to specific requirements of telecom networks, a shared cloud platform / CaaS adept at both workloads is a valid long-term vision for operators.

Dependencies between network and IT workloads (key for edge computing) can be created and managed much simpler in such a shared infrastructure. According to a recent Omdia survey, nearly one in three respondents believe that the convergence of hardware and software infrastructures for network functions and IT workloads is more than a remote possibility.

Also, almost all CaaS platforms offered by network vendors are capable of hosting and running third party

**FIGURE 21**

**What is your long-term view on using 'shared hardware and software infrastructures' to run both telco workloads (e.g., network functions) and IT workloads (e.g., enterprise workloads) on telco cloud?**



- Telco cloud software and hardware will probably remain isolated from other IT clouds and hardware (25%)
- Servers may be used as shared hardware for both telco- and non-telco workloads, but telco clouds will probably remain isolated (44%)
- Both servers and cloud platforms will probably be increasingly shared across telco and IT workloads (31%)

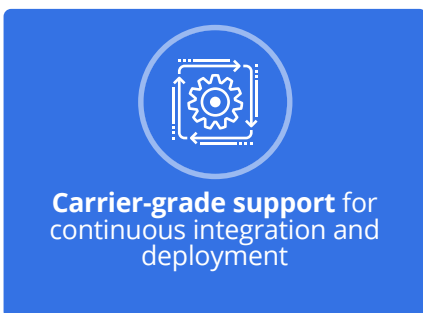
SOURCE: OMDIA, CSP EDGE COMPUTING SURVEY, APRIL 2024 NOTE: N=135

applications, in addition to their core duty of orchestrating virtualized and containerized network functions.

Cloud platforms that are already equally credible in and familiar with both telco and enterprise domains carry a particularly strong potential to realize this vision.

Given the need for control over performance, compliance and security, it is possible, and probably preferable, to run the telco workloads in confined environments, but containerization is certainly leading to convergence.

## CSPs will receive very frequent updates to their applications through CI/CD principles



Cloud-native ways of working involve continuous integration and development (CI/CD) methodologies for applications development and upgrades. Also, the underlying tools, such as Git repositories, provide a single source of truth for the code and configuration infrastructures of operators.

Having access to a strong carrier-grade support mechanisms can help operators automate the pipeline of integration, testing, and deployment of applications. In telecoms, this will be especially important given the need for security fixes, regulatory

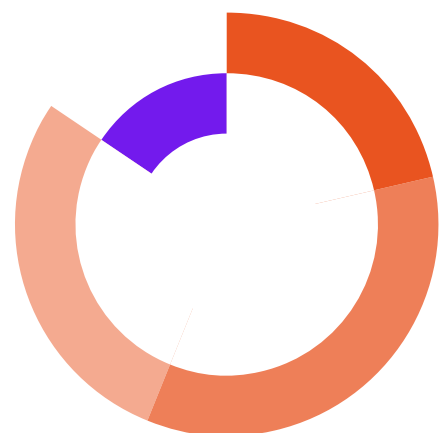
compliance, and many mission-critical NF updates by multiple vendors.

The move to containerized network functions opens up the possibility for much more frequent software updates because each microservice can be patched separately rather than the entire application at once.

By adopting CI/CD and DevOps principles, CSPs expect a much more frequent flow of updates than before. While in today's 'outdated' world, it can take many months to upgrade a network function, by adopting cloud native operating principles, 93% of CSP respondents anticipate updates within a month, at the latest. In fact, more than half expect weekly updates.

**FIGURE 22**

**How frequently do you expect upgrades to network functions?**



- Daily (21%)
- Weekly (34%)
- Monthly (28%)
- Quarterly (15%)

SOURCE: OMDIA, SERVICE PROVIDERS CORE NETWORKS SURVEY - 2023 EXTENDED VERSION (SEPTEMBER 2023) NOTE: N=109

Platforms that can support the co-existence of virtualized and containerized network functions will be critical in managing the transition period



**Transition management:**  
from virtualization to containerization

Except for rare cases of greenfield deployments, most CSPs do not start their journey to cloud nativeness from scratch.

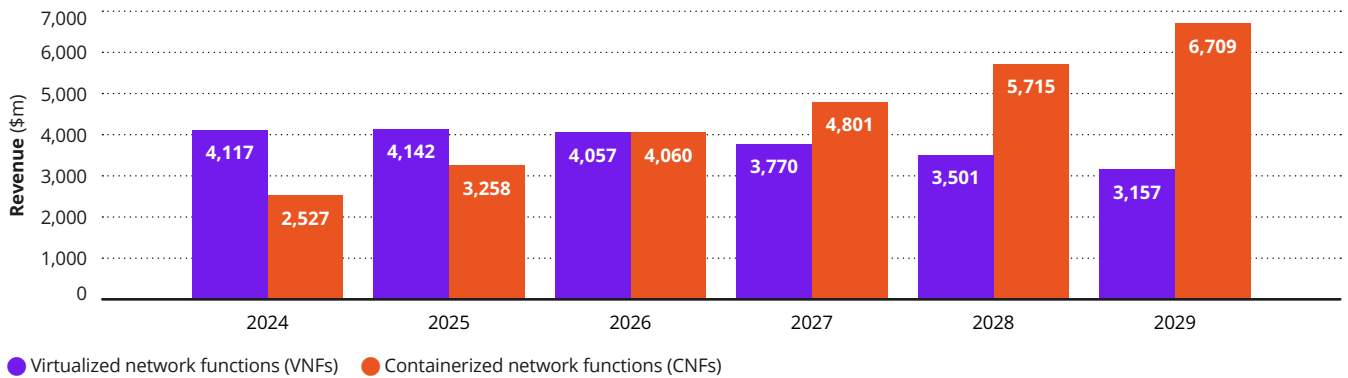
While running 4G core functions in virtual machines is relatively mature, CSPs are now coming to grips with running 5G core functions as containerized workloads.

This period of co-existence is captured in Omdia's telco cloud revenue forecasts. According to the projections, there is already a significant movement to CNFs,

but by 2029, containerization will truly take over.

As this transition happens, CaaS platforms that support both VNFs and CNFs through a common framework and tooling can ease the transition from existing VM environments to containers. Unified automation for the provisioning and management of both VNFs and CNFs can hold the key to a realistic and successful migration.

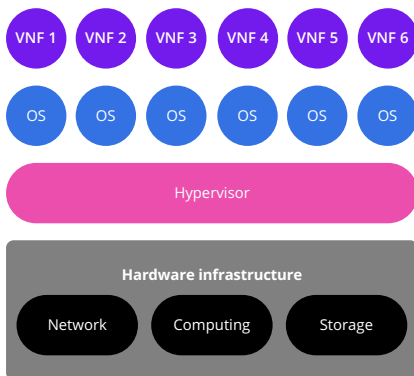
**FIGURE 23**  
Global telco network cloud infrastructure management – Virtual machines and containers, 2023–29



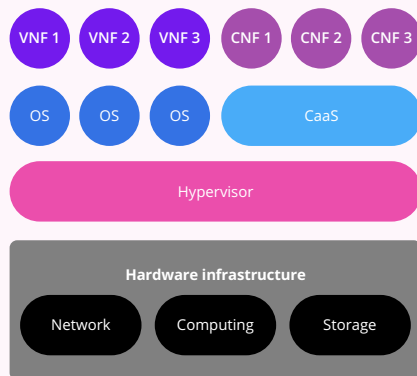
SOURCE: OMDIA TELCO NETWORK CLOUD TRACKER – 2024 ANNUAL FORECAST REPORT NOTE: N=135

**FIGURE 24**  
The ability to run containerized network functions both on hypervisors and on bare metal will also help CSPs in their journey to cloud nativeness

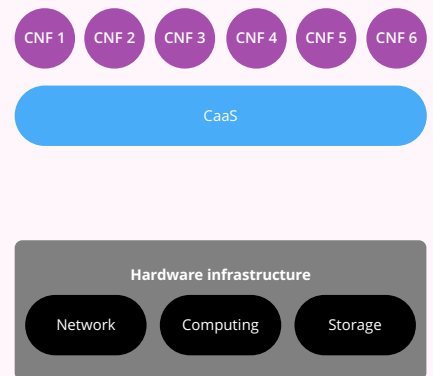
**Scenario 1:**  
Only virtualized deployment



**Scenario 2:**  
Cloud-native NFs on virtualized platform



**Scenario 3:**  
Upgrade to bare-metal deployment



SOURCE: OMDIA

Analytics will create network awareness ensuring new differentiated and guaranteed service delivery and monetization



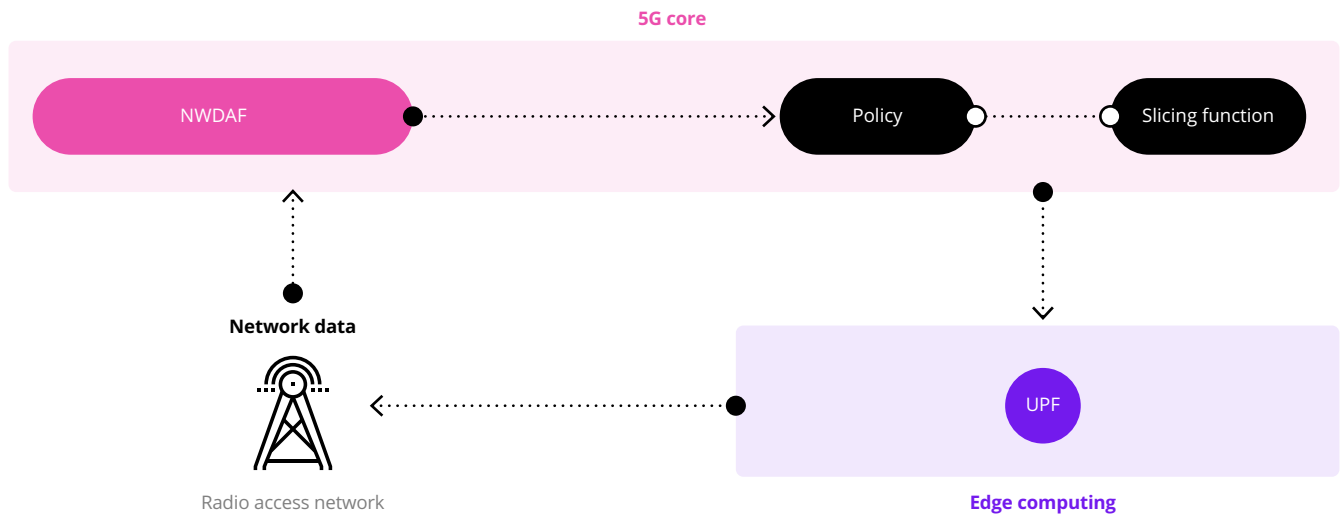
As CSPs migrate their networks to 5G SA and beyond, they will have the opportunity to provide not just higher QoS, but also differentiated and guaranteed capabilities based on awareness and intelligence, especially to the higher premium customers.

The 5G cloud native core will introduce new network functions, such as network slicing function and the network data analytics function (NWDAF). The latter will benefit from network wide data sources available and utilize analytics to deliver

suggestions to other networks functions, such as the policy function and the edge computing nodes that house NFs, such as the UPF.

Closed-loop management between the core network functions and other network domains will ensure specific customers get the relevant KPIs, for example an improved uplink resource, delivered for the duration required through allocating a network slice and release of those resources, when it is detected that the capability is no longer required.

**FIGURE 25**  
NWDAF uses of live network data to allocate new resources to end users



SOURCE: OMDIA

## SECTION 06

“Network cloudification does not only benefit operational efficiencies and enable new services on public networks; it is also a critical element of the growing market for private mobile networks and edge computing”

# Private 5G networks and edge computing

Private 5G networks, enabled by cloudified core functions, emerge as new opportunities driven by multiple trends.

**The development of the private 5G market is underpinned by multiple trends from both the demand and supply sides.** While 5G has started as a new technology in many vertical markets including factories, ports, and hospitals, enterprises are showing increased commitment to it, as evident in the clear shift from trials and tests to actual network rollouts in the last few years.

Overall, the private networks' market will grow from \$3.4 billion in 2023 to \$9.3 billion in 2028, representing a key opportunity for the cellular and IoT ecosystem to gain new customers' logos in previously untapped markets.

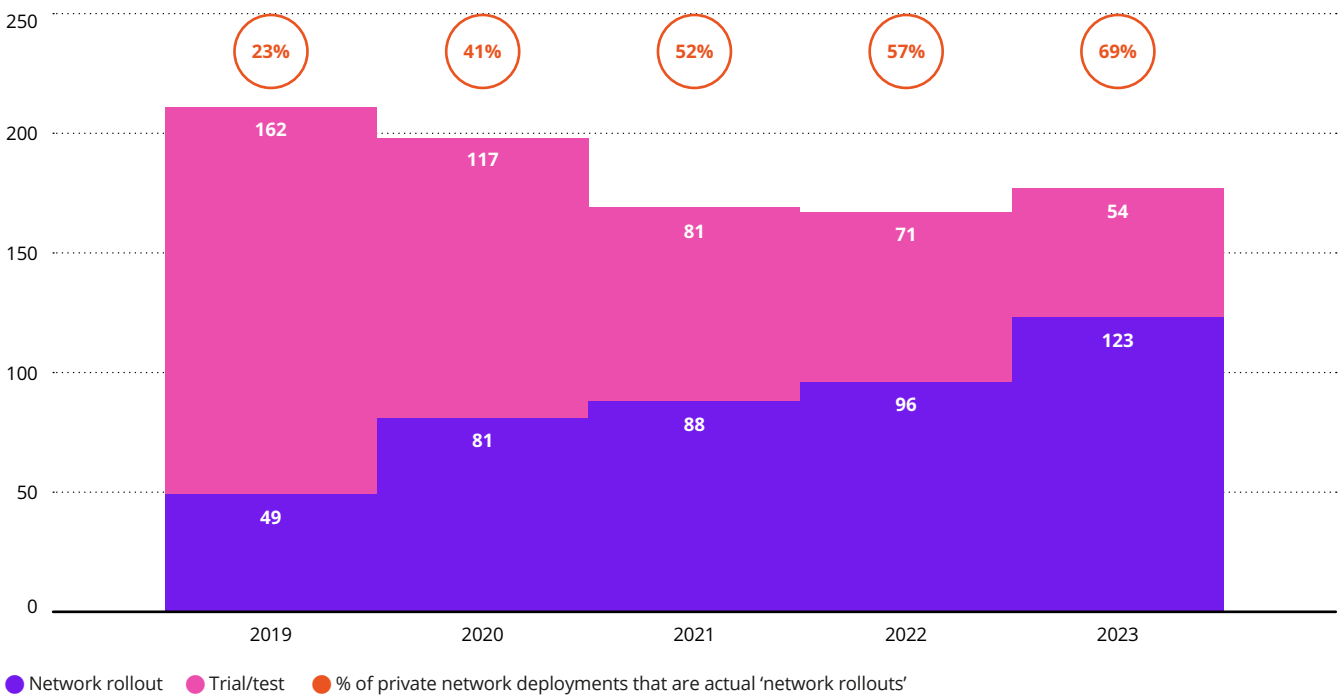
**Demand side drivers:**

- Security and control are essential for an enterprise digital transformation.
- New use cases such as machine vision or drones require higher network performance alongside a more efficient computing environment.
- Existing technologies are not evolving on par with the new use cases.
- Flexibility is becoming central to enterprises to adapt to fast-paced international changes in demand, production, and regulations.

**Supply side drivers:**

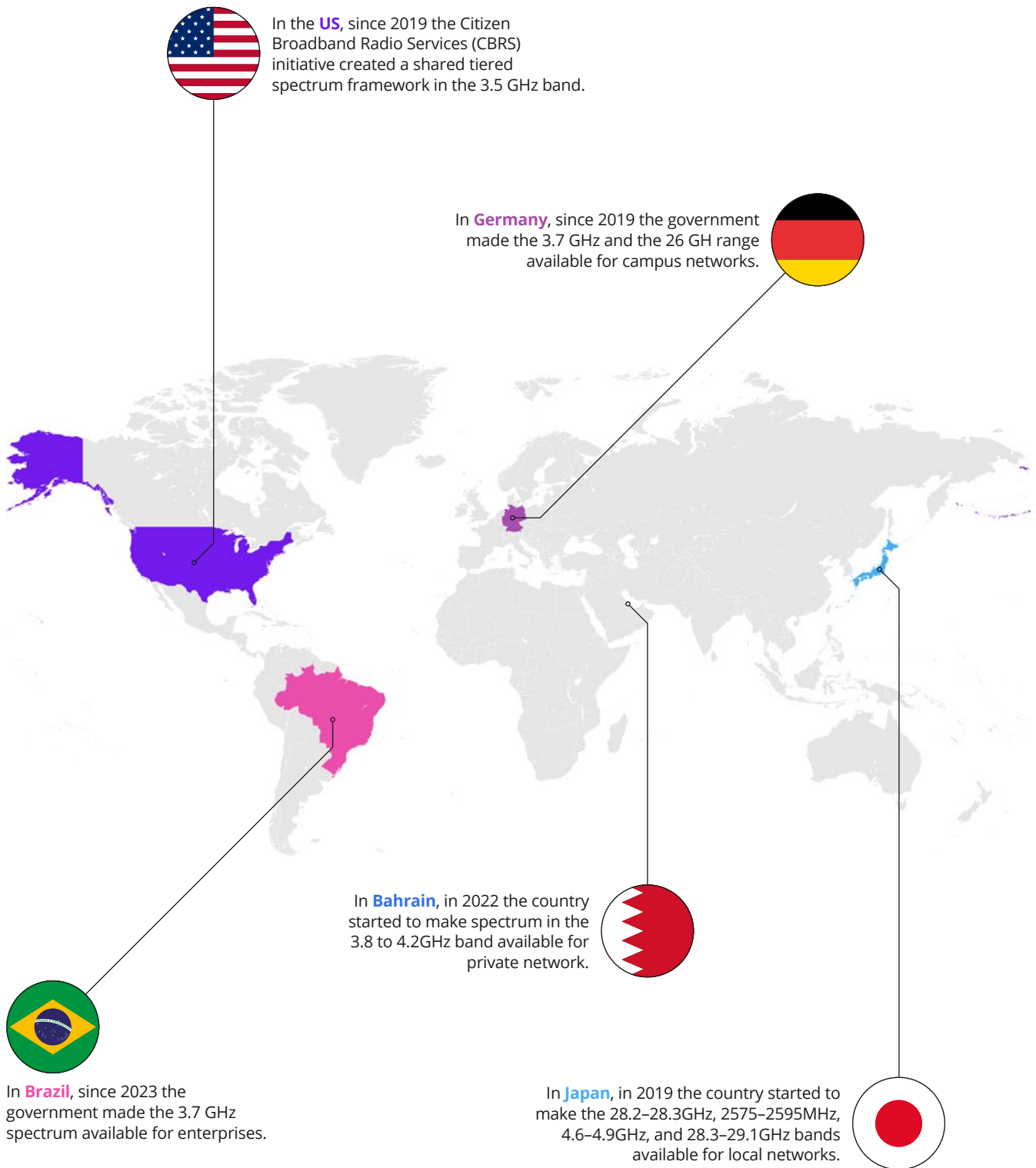
- 5G networks' expansion to deliver new revenues and RoI is a key driver. Particularly, cloud native 5G-SA can enable more flexibility in the network to serve the enterprise by deploying UPFs locally and near the customer premises to cater for their specific connectivity and computing needs.
- Spectrum liberalization is underpinning the market with most major economies providing a spectrum regulatory framework allowing enterprises to access spectrum.
- Multiple providers and vendors from both the ICT and OT ecosystems have launched private 5G products serving different verticals.

**FIGURE 26**  
Publicly announced trials and network rollouts show a market moving from test to real deployments



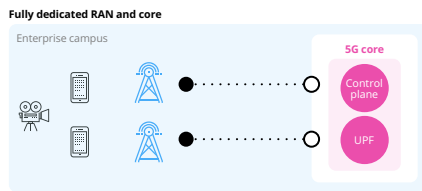
SOURCE: OMDIA, LTE AND 5G PRIVATE NETWORKS TRACKER - 1Q24 DATABASE

## Selected examples of spectrum liberalization initiatives

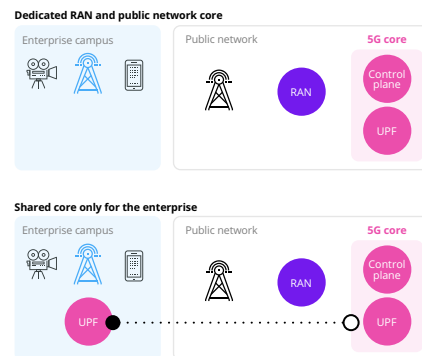


## Different private 5G deployment options meet different enterprise needs

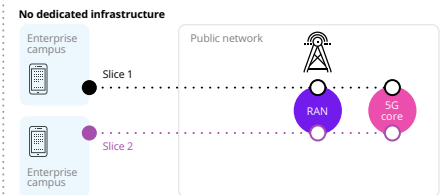
### Fully dedicated private network



### Hybrid private network



### Public network-based network slicing



Cloud native 5G SA core is critical for the automation and networking capabilities needed to deliver these options at scale

- In this scenario, all the infrastructure (RAN and core) is deployed for the sole use of the enterprise. This is currently the most common type of private 5G.
- The main benefit from this architecture is in the fact that the enterprise is in full control of the network. They can oversee the network's operation and maintenance, or they may choose to have a partner doing that.
- All data generated by the network remain within the enterprise control as none of it touches the public network, which also helps with data regulations and compliance.
- The network can be tailored to all the specific needs of the enterprise from coverage and radio design to throughput, latency, and uplink requirements.
- This solution is ideal for enterprises with critical needs such as mines and factories.

- In this scenario part of the infrastructure is shared between the private and the public network.
- This architecture provides the greatest flexibility for the provider and for the enterprise. This is because the enterprise can choose to leverage and share the RAN or part of the core from the public network.
- Having dedicated RAN but with the core from the public network helps with reducing overall costs while ensuring good coverage of the facility.
- With part of the core network potentially being deployed on site for the enterprise, hybrid networks can still provide strong performances.
- This solution is ideal for enterprises that may have workers or assets moving in and out of the private network such as in transport and logistics.

- All the infrastructure used to deliver the private network belongs to the public network.
- Assuming the enterprise is in a country with advanced public 5G network coverage (including 5G-SA), this will be the fastest option as no additional infrastructure needs to be deployed by the enterprise.
- The main benefit of network slicing will be about cost, as the infrastructure capex is already borne by the telecom operator rather than the enterprise.
- More than any other option, network slicing could be used to support temporary networks which may require to be active only for a limited amount of time as one-offs or for a limited time during the year.
- This solution is ideal for enterprises with very large coverage needs or with limited budgets.

To steer traffic and terminate or break out locally, cloud-enabled UPF instantiations are key. This can deliver on the stringent requirements of fully dedicated deployments (performance and data) and leverage the scale of public networks when preferred.

**Processing data closer to the point of origin will remain critical across all architectural choices**

## Private 5G and edge computing align well to serve the enterprise

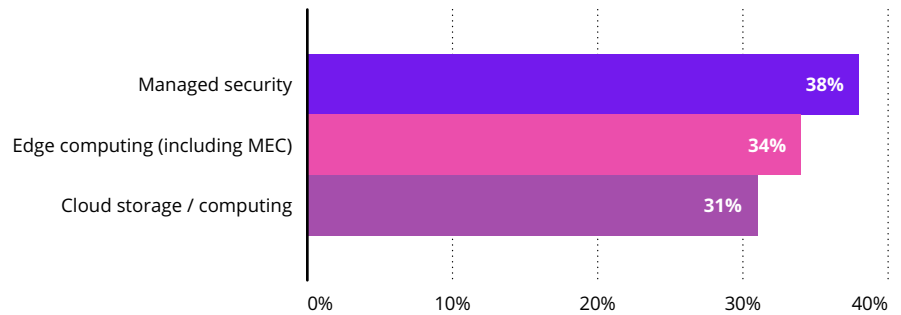
Private 5G networks are becoming a key enabler of an enterprises' broader digital transformation journeys. The technology is not purchased in a vacuum and in fact, enterprises are keen to combine it with security, edge computing, and cloud storage, often as part of the same deal. This underlines the need to provide a secure connectivity and computing solution to serve the enterprise.

Edge computing, including MEC, is becoming one of the most requested additions to private networks, based on Omdia's survey data of enterprises that currently have live private networks. This is due to several reasons:

- Having a single network/compute platform enables better performance compared to separate solutions.
- Combining the solutions offers better data security across connectivity and computing domains.
- There are cost savings by combining the solutions, compared to purchasing connectivity and computing separately.

**FIGURE 27**

### Top 3 technologies acquired by the enterprise with their private network



SOURCE: OMDIA, PRIVATE 4G LTE AND 5G NETWORK ENTERPRISE SURVEY INSIGHTS 2023 – PROVIDERS, SOLUTIONS, AND BUSINESS MODELS (ENTERPRISES WITH AN ACTIVE DEPLOYMENT) NOTE: N=271

- There are many applications that require stringent performance both in terms of connectivity, but also in terms of data processing and analysis. To serve these the private network must work

in tandem with an edge computing platform or solution. Examples of high requirement applications include machine vision and drones.

## Examples of enterprises leveraging private 5G and edge computing



**Vertical:** Healthcare **Geography:** Americas

A private 5G network and private 5G MEC were deployed at a hospital. The solution supports AR-assisted presurgical guidance with virtual 3D X-ray vision of CT and MRI scans as well as virtual supported-assisted medical learning.



**Vertical:** Manufacturing **Geography:** Americas

A private 5G network and 5G MEC were deployed for a large car OEM. The solution is used to enable digital workers (smartphone and tablets) but also for the automation of robotics and machinery and for wireless vehicle software updates.



**Vertical:** Transport **Geography:** EMEA

A private 5G network and MEC were deployed at a car testing facility. The solution supports real-time video and data transmission technology, C-V2X communication, and mobile/automotive of voice and data.



**Vertical:** Energy **Geography:** APAC

A private 5G and MEC were deployed at a mining site. The network supports audio and video communications as well as smart mining lamps, smartwatches, and other terminals.



# Conclusion

**While the early uptake of edge computing on telecom networks has been relatively slow due to a lack of 5G SA and cloudification across multiple network domains, this is set to change.**

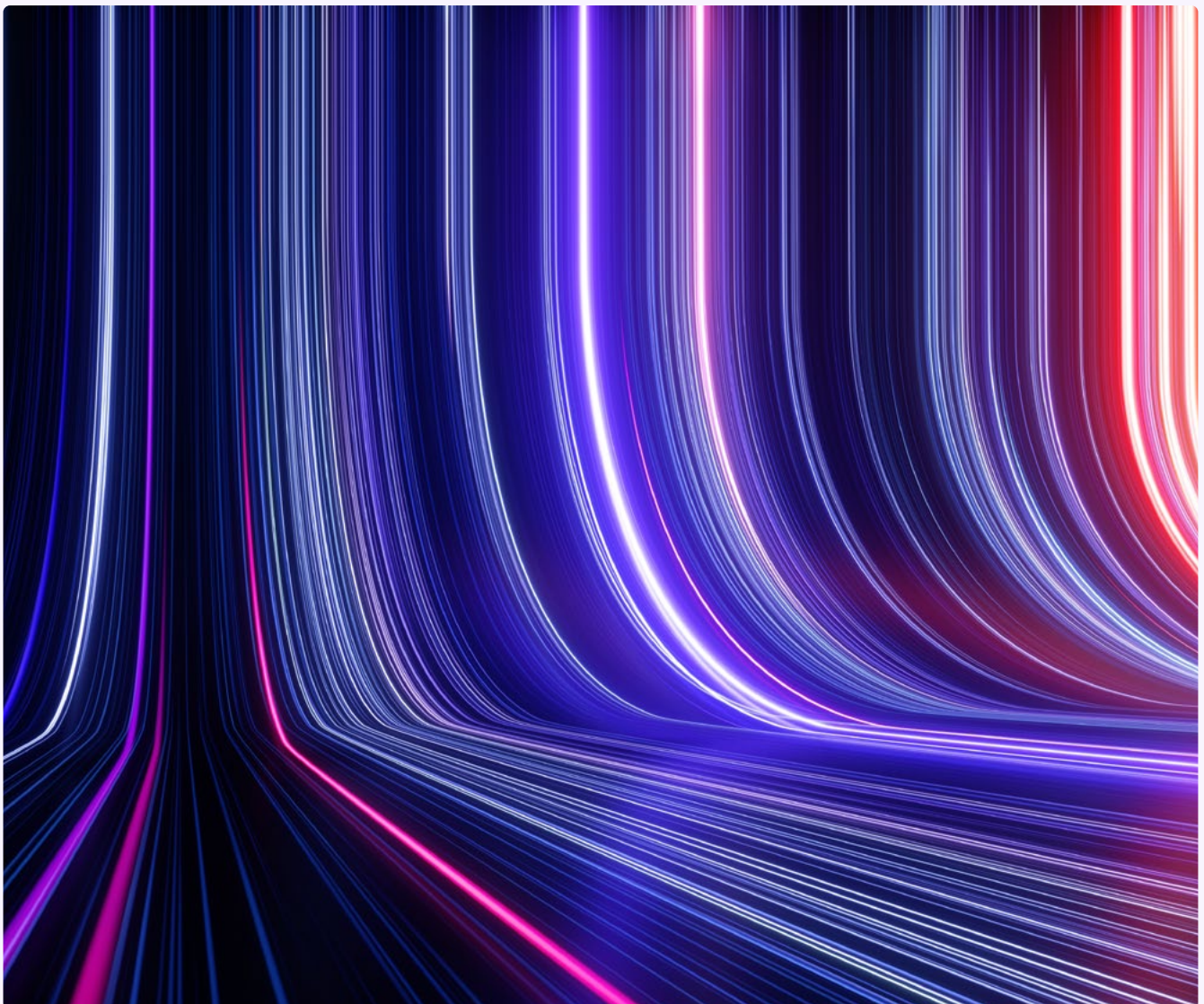
Driven partly by the recent boom of interest in artificial intelligence, CSPs have renewed optimism and strong revenue expectations from edge computing on public and private networks. They are planning to increase the number of their edge nodes significantly in the next few years to weave highly distributed computing fabrics on their networks.

Realizing the full potential of 5G and edge computing requires the fusion of

connectivity and computing based upon cloud native principles. Containerization and microservice architectures and Kubernetes-powered orchestration are not only critical for scalability, flexibility, and efficiency of application deployment, but also essential for rapid innovation and significantly reduced time-to-market for new services and revenue streams.

For CSPs, the journey to become a cloud native organization is a strategic priority but not trivial due to the complexity of their operations: managing multiple vendor interoperability, multiple cloud and virtualization environments, and the co-existence of legacy and cloud native

applications and systems are considerable challenges to address. Open-source technologies will have a key role to play in overcoming these obstacles, as they have the potential to (a) fuel the innovation engines of operators with constant input from a vast ecosystem, (b) act as neutral cloud layers between heterogeneous hardware environments and network functions from different providers and (c) natively run and orchestrate telecom and third-party workloads alike on shared software infrastructures.



# Appendix

The background features a series of glowing, concentric circles in shades of purple and blue, creating a tunnel-like effect. A bright, multi-colored spiral (purple, blue, and cyan) is centered in the lower half of the image, drawing the eye towards the center. The overall aesthetic is futuristic and digital.

# 5G core network functions and definitions

NETWORK FUNCTION	DEFINITION	DESCRIPTION
<b>AMF</b>	Access and mobility management function	Supports the termination of control plane signaling and carries out registration and authentication of devices based on predefined policies, preventing unauthorized access. It also carries out mobility management, facilitating handover procedures as the device moves between antenna masts, to ensure an uninterrupted service.
<b>SMF</b>	Session management function	Handles session management and interacts with the decoupled data plane by creating, updating, and removing protocol data unit (PDU) sessions and managing IP session context within the UPF. Policy and charging control rules from the PCF are also fed as templates into the UPF, for it to deliver quality of service (QoS).
<b>UPF</b>	User plane function	It processes user packet data, facilitating forwarding, routing and packet inspection as well as QoS handling. It interacts with the SMF and PCF and it is an evolution of the 4G control and user plane separation (CUPS).
<b>AUSF</b>	Authentication server function	The AUSF performs the authentication of user equipment (UE) as it connects, at switch-on, or during a handover procedure from a 4G network to a 5G network. It does so by ensuring the subscriber information is transmitted and stored securely. The AUSF stores authentication keys and provides the AMF with the necessary authentication services.
<b>UDM</b>	Unified data management	The UDM is a central repository of subscriber data including the subscriber profile, authentication data, and other service-related information. It ensures that user data sessions are set up and torn down correctly. A stateful UDM stores this data locally, while a stateless version stores it in the UDR. It interacts with other NFs, such as the AUSF and NRF.
<b>UDR</b>	Unified data repository	This is the database and repository of user-related data, including user profiles and application data. It stores the stateless information of the UE. It interacts with the policy control function (PCF) to ensure the correct subscriber quality of service (QoS) and charging policy information is obtained and enforced.
<b>UDSF</b>	Unstructured data storage function	The UDSF supports the storage and retrieval of unstructured data from other NFs.
<b>NEF</b>	Network exposure function	This NF exposes the 5G network's capabilities and services through established application programming interfaces (APIs), facilitating interaction with third parties, such as application developers.
<b>NRF</b>	Network repository function	The NRF provides a record of all NFs available on the platform, together with a profile of each and the services they support. When a new NF is brought up, it registers its IP address and capabilities with the NRF. A consumer NF will request the NRF to identify which NFs are registered with it and have the required capabilities and can act as a producer of services. It interacts with the SCP.
<b>NSSF</b>	Network slice selection function	The NSSF analyzes the requirements of a UE and matches those requirements with a network slice. In today's network slicing, the slices are predefined rather than autonomously orchestrated and for this, this NF must find the best match. The NSSF interacts with AMF, SMF, and PCF.
<b>SCP</b>	Service communications proxy	A critical function to create signaling efficiencies when a consumer NF requests a service from a producer NF. The SCP acts as intermediary between the two, shielding some of the complexities of the infrastructure. The SCP also communicates with the NRF.
<b>SEPP</b>	Security edge protection proxy	A security NF used for roaming and securing the network at the extremities ahead of interfacing with another network. Compared to previous generation networks, 5G networks use enhanced authentication procedures, such as mutual authentication to secure the communication between the device as it roams, and the SEPP plays a role in this with external networks.
<b>CHF</b>	Charging function	The CHF provides online and offline charging features for multiple services. Other measurable qualities beyond throughput will become key with 5G networks, such as latency, slice bandwidth, reliability, availability, security, and APIs, so the CSPs must be able to measure and charge for these.
<b>PCF</b>	Policy control function	The PCF considers device profile, subscription information, and real-time information to enforce rules for traffic steering, QoS, and charging. It also relies on information from other NFs, such as the network exposure function (NEF) and SMF.
<b>NWDAF</b>	Network data analytics function	This function provides data analytics of the operations and services of the network by processing and analyzing the network performance, user traffic patterns, and network load to deliver actionable intelligence to optimize QoS and overall user experience.
<b>NSSMF</b>	Network slice subnet management function	This function takes the slice requirements from the NSMF and ensures the necessary NF resources are made available and are instantiated.
<b>NSMF</b>	Network slice management function	This NF will keep the necessary information for several popular network slice templates for known use cases for fast provisioning.
<b>MDAF</b>	Management and data analytics function	The MDAF provides analytics information from network slices to ensure optimization of resources.

# Omdia

Omdia is a global technology research powerhouse, established following the merger of the research division of Informa Tech (Ovum, Heavy Reading, and Tractica) and the acquired IHS Markit technology research portfolio\*.

We combine the expertise of more than 400 analysts across the entire technology spectrum, covering 150 markets. We publish over 3,000 research reports annually, reaching more than 14,000 subscribers, and cover thousands of technology, media, and telecommunications companies.




Our exhaustive intelligence and deep technology expertise enable us to uncover actionable insights that help our customers connect the dots in today's constantly evolving technology environment and empower them to improve their businesses – today and tomorrow.

\*The majority of IHS Markit technology research products and solutions were acquired by Informa in August 2019 and are now part of Omdia.



Canonical, the publisher of Ubuntu, provides open source security, support and services. Our portfolio covers critical systems, from the smallest devices to the largest clouds, from the kernel to containers, from databases to AI. With customers that include top tech brands, emerging startups, governments and home users, Canonical delivers trusted open source for everyone.

Learn more at [canonical.com](https://canonical.com)

-  Canonical
-  Canonical
-  CelebrateUbuntu



The Omdia team of 400+ analysts and consultants are located across the globe

#### Americas

Argentina  
Brazil  
Canada  
United States

#### Asia-Pacific

Australia  
China  
India  
Japan  
Malaysia  
Singapore  
South Korea  
Taiwan

#### Europe, Middle East, Africa

Denmark  
France  
Germany  
Italy  
Kenya  
Netherlands  
South Africa  
Spain  
Sweden  
United Arab Emirates  
United Kingdom

#### Get in in touch

✉ [insights@omdia.com](mailto:insights@omdia.com)  
✉ [consulting@omdia.com](mailto:consulting@omdia.com)  
🌐 [omdia.com](http://omdia.com)  
✉ OmdiaHQ  
📺 Omdia

#### Citation Policy

Request external citation and usage of Omdia research and data via [citations@omdia.com](mailto:citations@omdia.com)

#### COPYRIGHT NOTICE AND DISCLAIMER

Omdia is a registered trademark of Informa PLC and/or its affiliates. All other company and product names may be trademarks of their respective owners. Informa PLC registered in England & Wales with number 8860726, registered office and head office 5 Howick Place, London, SW1P 1WG, UK. Copyright © 2024 Omdia. All rights reserved. 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") 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 and agents, 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.