analysys mason

PERSPECTIVE

BUILDING COST-EFFICIENT CLOUD-NATIVE 5G SA NETWORKS: A TCO COMPARISON

Gorkem Yigit, Caroline Chappell and Luwen Meng

FEBRUARY 2023

analysysmason.com

Contents

1 Executive summary

The 5G network has been conceived as a cloud-based network in which all functions are expected to run on a horizontal network cloud rather than on siloed virtualized platforms. Leading telecoms operators are beginning to deploy the 5G standalone (SA) core; this is a set of cloud-native network functions (CNFs) that will require operators to accelerate their adoption of cloud-native infrastructure. The cloud-native 5G SA core also requires operators to commit to a cloud-first, horizontal approach to running the network with very high levels of automation.

Cloud-native clouds enable operators to adopt open and disaggregated architecture; cloud-native infrastructure is sourced independently from vendors' CNFs. However, operators must choose between two main approaches to disaggregated cloud deployment. The first option is to build a private network cloud by integrating multiple technology components including compute and storage hardware, cloud technology platforms, software-defined networking (SDN) and, in advanced cases, orchestration capabilities. We call this the do-it-yourself (DIY) private cloud deployment model. The alternative is to use the hyperscale-based infrastructure and advanced automation frameworks offered by public cloud providers (PCPs). Operators that are planning their 5G SA core deployments and are looking to deploy virtualized/Open RANs in the future must decide on their approach to cloud-native infrastructure; a holistic total cost of ownership (TCO) analysis is critical.

Analysys Mason, in collaboration with Microsoft, has analyzed the TCO of deploying a cloud-native 5G SA network using a PCP cloud solution based on Azure Operator Nexus compared with that using the DIY private cloud model. The TCO model considers three greenfield deployment scenarios for the cloud-native 5G SA core in consumer macro networks, modeled for two hypothetical Tier-1 operator profiles (in Western Europe and in Latin America). In this report, we discuss the key findings of this analysis (Figure 1.1).

1.1 The TCO of on-premises Azure Operator Nexus deployments is 38% lower than that for DIY deployments

Our 5-year TCO model shows that the Azure Operator Nexus on-premises scenario has a TCO for cloud-native 5G SA deployments that is up to 25% lower than that for the DIY private cloud model. The Azure Operator Nexus on-premises scenario can also offer a TCO reduction of up to 38% for cloud infrastructure (CaaS, PaaS, OS, SDN and cloud hardware) and operations, when

FIGURE 1.1: OVERVIEW OF THE TCO ANALYSIS RESULTS [SOURCE: ANALYSYS MASON, 2023]

	Azure Operator Nexus on-premises (5-year)	Azure Operator Nexus hybrid cloud (5-year)
Overall TCO savings compared to the DIY model	25%	28%
Cloud infrastructure and operations TCO savings compared to the DIY model	38%	43%
Opex savings compared to the DIY model	44%	

excluding CNF-related capex and opex components, which are assumed to be equal for all scenarios.

The main driver of the TCO savings in the Azure Operator Nexus scenarios is the reduction in opex that is enabled by the more automated and efficient cloud infrastructure and CNF operations that are supported by Azure Operator Nexus's comprehensive cloud platform and as-a-service operations model. Indeed, our TCO study revealed that the opex associated with building, deploying and maintaining a DIY-based cloud-native network can be substantial, and operators often do not have a complete understanding of these costs. Our research and interviews with large Tier-1 operators indicate that operators face major challenges with managing their private clouds and on-premises data centers, which leads to high operating expenses in terms of staffing and tools. Our model shows that Azure Operator Nexus's comprehensive and consistent cloud environment, automation framework and managed service capabilities can reduce the number of repetitive, time- and resource-consuming and error-prone tasks for the main cloud-native network operations by 58%, resulting in opex savings of up to 36% compared to DIY private cloud model. The details of these operational efficiencies are discussed in section 4.2.

The use of the Azure Operator Nexus cloud platform can also lead to a reduction in capex when compared to a DIY private cloud model. Using Azure Operator Nexus's predesigned and validated infrastructure greatly reduces the costs associated with implementing and integrating cloud hardware as well as testing. This results in a capex saving of 11–17%.

1.2 Operators can further optimize cloud-native network TCO by using Azure Operator Nexus hybrid cloud architecture

Our TCO analysis shows that deploying a cloud-native 5G SA network using Azure Operator Nexus hybrid cloud architecture can result in even greater cost savings over a DIY private cloud model. Indeed, the overall TCO can be reduced by an additional 2% and 3% for a Western European operator and a Latin American operator, respectively, by deploying a set of control plane functions and management applications on Azure public cloud, while the remaining network functions are on-premises in operator data centers. These results are discussed in section 4.3.

These further TCO savings are primarily attributed to a reduction in on-premises hardware costs, a shift from high up-front capex to a more optimized consumption-based opex and the ability to avoid overprovisioning hardware for peak usage. These savings can potentially be further optimized by better workload allocation in the public cloud environment.

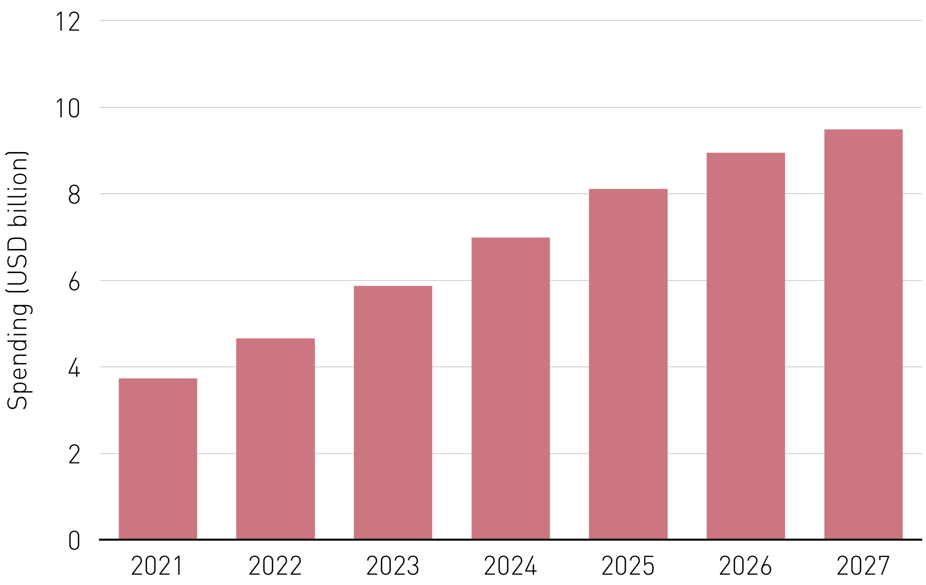
2 5G networks are driving operator investment in cloud-native infrastructure

2.1 The mobile core is responsible for the majority of operators' spending on network clouds

The 5G network has been conceived as a cloud-based network in which all functions are expected to run on a horizontal network cloud rather than on siloed virtualized platforms. It is therefore not surprising that mobile core deployments are the main driver of operators' network cloud investments (Figure 2.1). Many operators started their journey to the network cloud with the 4G evolved packet core (EPC), which is a key constituent of the 5G non-standalone (NSA) core. Leading operators are now beginning to deploy the 5G SA core; the pace of these deployments will increase from 2023 and will drive spending growth on network cloud infrastructure for the mobile core over the next few years.

In particular, investing in the 5G SA core will require operators to accelerate their adoption of cloud-native infrastructure, which will need to be operated and managed using cloud-native automation. Network function virtualization (NFV) was conceived, as far as possible, as an extension of operators' existing operations, while the cloud-native 5G SA core requires operators to commit to a cloud-first approach to running the network. Experience with deploying and automating the cloud-native mobile core will serve operators well as they move to applying cloud-native technologies to the RAN in the future.

FIGURE 2.1: OPERATORS' SPENDING ON NETWORK CLOUD INFRASTRUCTURE FOR THE MOBILE CORE, WORLDWIDE, 2021–2027 [SOURCE: ANALYSYS MASON, 2023]

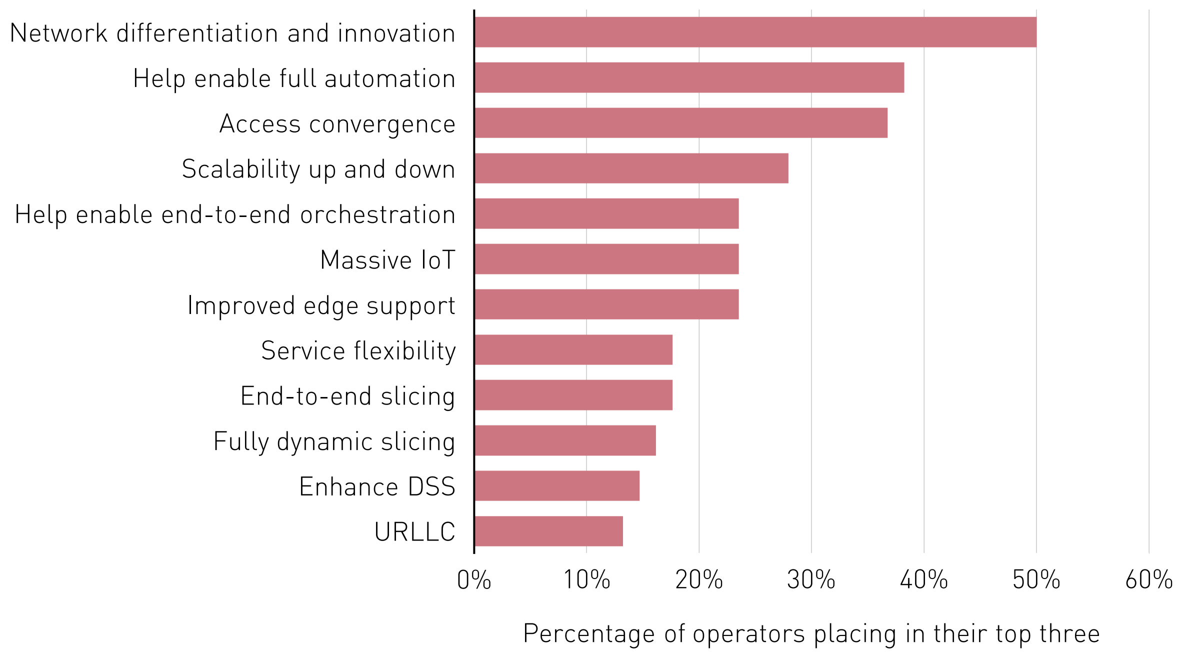


2.2 Cloud-native infrastructure and automation are key to unlocking the benefits of 5G

The 5G SA core is key to operators' ambitions to generate new enterprise revenue growth using advanced services such as network slicing. Operators need specific technical capabilities to achieve network slicing, including the ability to scale cloud-native mobile core functions up and down to meet the needs of individual customers and to orchestrate functions end-to-end to create customized private networks. A recent Analysys Mason survey confirms that such capabilities are some of the top benefits that operators expect from the 5G core, alongside the ability to both differentiate and innovate services in supporting roles and achieve full automation (Figure 2.2).

The benefits of scalability, flexibility and orchestration are intrinsically delivered by cloud-native clouds that have full cloud-native automation capabilities. Operators are finding that their choice of cloud-native network cloud can significantly influence the performance and cost of a mobile core based on the level of cloud-native automation that such an environment can provide.

FIGURE 2.2: DRIVERS OF IMPLEMENTING A 5G SA CORE, WORLDWIDE, OCTOBER 2022[1] [SOURCE: ANALYSYS MASON, 2023]



[1] What are the most important drivers for implementing a 5G SA core, in terms of your commercial model?; n = 68.

3 Cloud-native networks are driving a shift from vertically integrated stacks to disaggregated cloud platforms

3.1 Operators must decide how to source cloud-native infrastructure for 5G

Operators that are planning their 5G SA core deployments and are looking to implement virtualized/Open RANs in the future must decide on their strategies for cloud-native infrastructure. Cloud-native clouds are horizontal in nature. They enable operators to shift away from vertically integrated stacks in which network functions are tightly bound to a vendor's virtualized execution environment and towards open and disaggregated network cloud deployment models in which cloud-native infrastructure is sourced independently from vendors' CNFs. Operators are showing a growing interest in building horizontal cloud-native network clouds, and we anticipate that disaggregated models will account for the largest share of spending on mobile network cloud software infrastructure in 2024.[2]

Operators no longer face a straightforward choice between sourcing cloud-native infrastructure as part of a vendor-integrated stack (the strategy that most operators followed in the NFV era) and building private horizontal network clouds from multiple disaggregated technologies. PCPs are introducing a further option: the ability to use a version of their cloud-native platforms that is tailored for telecoms workloads, either on- or off-premises or via a hybrid private/public deployment model. Each deployment model (which we call 'single-vendor-integrated', 'DIY' and 'public cloud platform') has benefits and drawbacks, which we will briefly assess in the following sections.

3.2 Vendor-integrated stacks limit flexibility and choice, but retain appeal for certain operators

Single-vendor, vertically integrated stacks have remained the predominant model for deploying virtualized network functions (VNFs) over the past 10 years, but they have not delivered the promised benefits of NFV. Most operators have experienced minor capex savings from moving to COTS hardware and little, if anything, in the way of opex savings because they continue to operate VNFs as virtualized appliances. However, this model continues to appeal to operators because it does not disrupt their operational processes, deployment is quick due to minimal integration challenges and operators only need deal with a single vendor for maintenance and support.

On the other hand, the vertically integrated model has disadvantages for operators that want to control their own destinies. It results in vendor lock-in,

[2] For more information, see Analysys Mason's Network cloud infrastructure: worldwide forecast 2022–2027.

which can limit operators' access to the innovations and best-in-class functions that are being developed by a broader ecosystem. Operators therefore have fewer opportunities to differentiate their network capabilities and services. Operators also fail to benefit from cloud economics because every function runs in its own siloed environment, hence the lack of opex savings.

3.3 DIY private clouds require deep pockets to build and maintain

Operators that want the benefits of an open, horizontal cloud that can support network functions from multiple vendors have traditionally built such clouds themselves from disaggregated components, including compute and storage hardware, cloud technology platforms, SDN and, in advanced cases, orchestration capabilities. Operators have built DIY private clouds to support their mobile packet cores and IMS, though few have demonstrated that they are disciplined enough to run these and other functions on the same network cloud. More commonly, operators have accrued multiple DIY private clouds, each dedicated to a single network function.

Even when operators have managed to create a multi-vendor DIY private cloud, they have dispersed its operations among multiple network function owners, thereby perpetuating functional silos and reducing the opportunities for opex savings. At the same time, operators have had to contend with the complexities of a disaggregated cloud environment in which different cloud technologies evolve at different rates and provide different approaches to automation. Building and maintaining integration and automation across all network cloud components (including network functions) imposes a continual overhead on the operators that take this route. However, operators that master DIY private clouds believe that they have a strong opportunity to differentiate their networks and avoid relying on any single component supplier.

3.4 PCPs offer a new approach to network clouds based on their hyperscale cloud technologies and high levels of automation

PCPs are now entering the network cloud market and are bringing their massive investments in cloud technologies, automation frameworks and skills with them. They and their operator customers argue that cloud infrastructure is a commodity that does not provide competitive differentiation to a network owner, but that can be used to gain large economies of scale. PCPs offer managed services and very high levels of automation that minimize the challenges of building and operating disaggregated clouds. They also offer flexible deployment options: their cloud stacks can run on-premises or via a hybrid private/public cloud model.

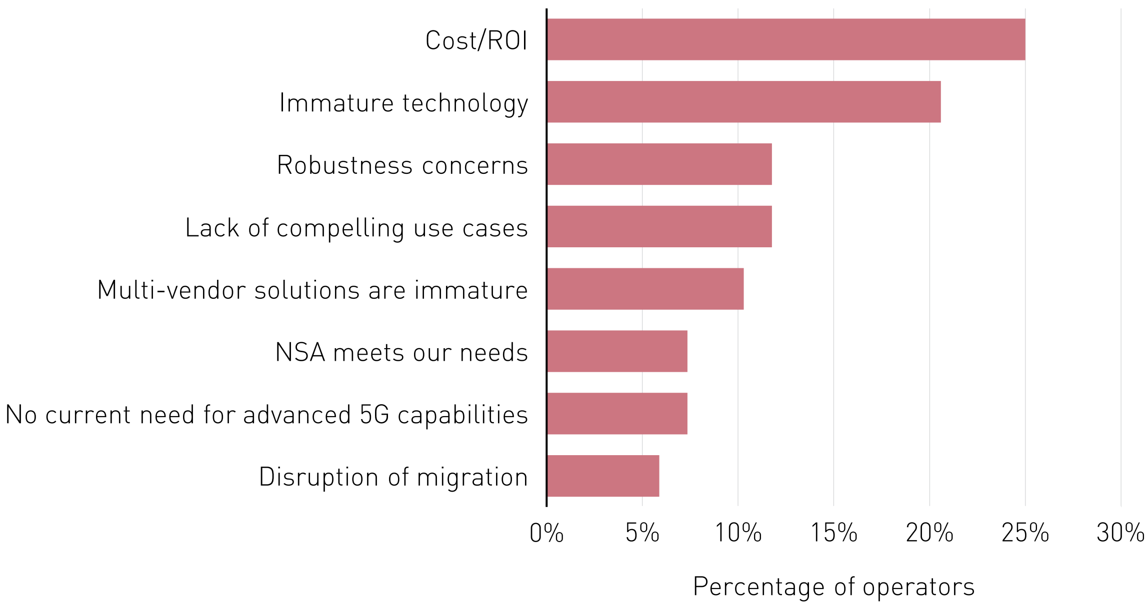
However, PCP cloud deployments are still nascent. Operators also face potential data sovereignty and regulatory issues if PCPs do not operate their public clouds from multiple in-country locations, and operators need a strategy to overcome the gap between the 'three nines' of availability that PCPs typically provide and the carrier-grade 'five nines' of availability expected by operators.

3.5 Operators must understand the full cost implications of disaggregated deployment models to guide their cloud platform choices

Cost/ROI is the top barrier to the adoption of 5G SA according to our 2022 operator survey (Figure 3.1). Operators regard cloud deployments as expensive given the uncertain ROI, especially those operators that have built disaggregated private clouds themselves to support previous generations of VNFs. Such operators report little, if any, reduction in opex from these DIY cloud platforms because building and operating a private network cloud on-premises is highly complex and therefore consumes significant time and resources. Operators must maintain large operational headcounts to carry out slow, manual processes or build new automation solutions for their private clouds. Typically, operators do not understand the true extent of these costs.

Analysys Mason has developed a robust TCO model to analyze the capex and opex of the various disaggregated network cloud models and to reveal the complete set of costs associated with them in order to advise operators that are making disaggregated cloud platform decisions.

FIGURE 3.1: BARRIERS TO 5G SA NETWORK ADOPTION, WORLDWIDE, 2022[3] [SOURCE: ANALYSYS MASON, 2023]



[3] What are the main barriers for implementing a 5G SA core?; n = 68.

4 Azure Operator Nexus can reduce the TCO of 5G SA network cloud infrastructure by up to 43% compared to a DIY private cloud

Analysys Mason, in collaboration with Microsoft, has analyzed the TCO of deploying a cloud-native 5G SA network using a PCP cloud solution based on Azure Operator Nexus compared with that using the DIY private cloud model. We created a set of models to assess the capex and opex associated with cloud-native mobile core networks and their operations. We then used these models and alongside inputs from Tier-1 operators that adopted the DIY private cloud model for their 5G SA networks to analyze the benefits of implementing a common, managed cloud platform and automation framework, such as Azure Operator Nexus, instead of using the DIY private cloud model.

Our TCO model analyzes three greenfield deployment scenarios for the cloud-native 5G SA core in consumer macro networks, as detailed in Figure 4.1. These scenarios are modeled for two

FIGURE 4.1: TCO MODEL DEPLOYMENT SCENARIOS [SOURCE: ANALYSYS MASON, 2023]

Scenario	Deployment model	Cloud software infrastructure (CaaS, PaaS, OS and SDN control)	Cloud hardware infrastructure (compute, storage and network)	Cloud infrastructure operations (Day 0, 1 and 2)
DIY private cloud	All functions are deployed on-premises	Operators build their own by procuring and integrating components from multiple vendors	Operators build their own by procuring and integrating components from multiple sources	Operators are fully responsible for the management of the entire lifecycle
Azure Operator Nexus on-premises	All functions are deployed on-premises	Operators implement Azure Operator Nexus (an integrated suite of cloud software infrastructure elements that is delivered as-a-service via a subscription model)	Operator procures the hardware infrastructure directly from OEMs based on prescriptive BoM provided by Azure	Azure provides managed services for the on-premises cloud infrastructure operations
Azure Operator Nexis hybrid	User plane functions are deployed on-premises and some control plane and management functions are deployed on the public cloud	The same Azure Operator Nexus platform is deployed both on-premises and in the Azure cloud	On-premises: same as above Public cloud: Azure cloud	Azure provides managed services for hybrid cloud infrastructure operations

hypothetical Tier-1 operator profiles: one from Western Europe and the other from Latin America. Each profile reflects the real-life subscriber numbers, network traffic and design and cost parameters for operators in these geographies.

Key modeling assumptions

The key modeling assumptions for the two operator profiles are provided in Figure 4.2. 5G SA core architecture and components (Figure 4.3) are modeled in

FIGURE 4.2: KEY MODELING ASSUMPTIONS FOR THE OPERATOR PROFILES [SOURCE: ANALYSYS MASON, 2023]

Attribute	Tier-1 operator in Western Europe	Tier-1 operator in Latin America
Country mix	Germany, Spain and the UK	Brazil and Mexico
Total number of 5G connections	14 million in year 1 and 50 million in year 5	0.5 million in year 1 and 40.6 million in year 5
Total 5G traffic	4800PB in year 1 and 29 000PB in year 5	375PB in year 1 and 6750PB in year 5
Total number of server nodes	300 (year 5)	220 (year 5)

FIGURE 4.3: KMODELING ASSUMPTIONS RELATED TO TECHNOLOGY AND ARCHITECTURE [SOURCE: ANALYSYS MASON, 2023]

Attribute	Assumption
Modeled network components	Cloud-native 5G SA functions including AMF, SMF, UPF, NRF, NSSF, SDM and policy management
Capex parameters	Hardware, software and professional services for CNFs, network orchestration and element management systems
Opex parameters	• Cloud software infrastructure (CaaS and OS) are assumed to be subscription-based for both the DIY private cloud and Azure Operator Nexus-based models • Costs of public cloud infrastructure usage in the hybrid Azure Operator Nexus scenario • Support and maintenance for software and hardware components • Headcount (FTE) hours for Day 0,1 and 2+ operations • Power and space
Length of analysis	5 years

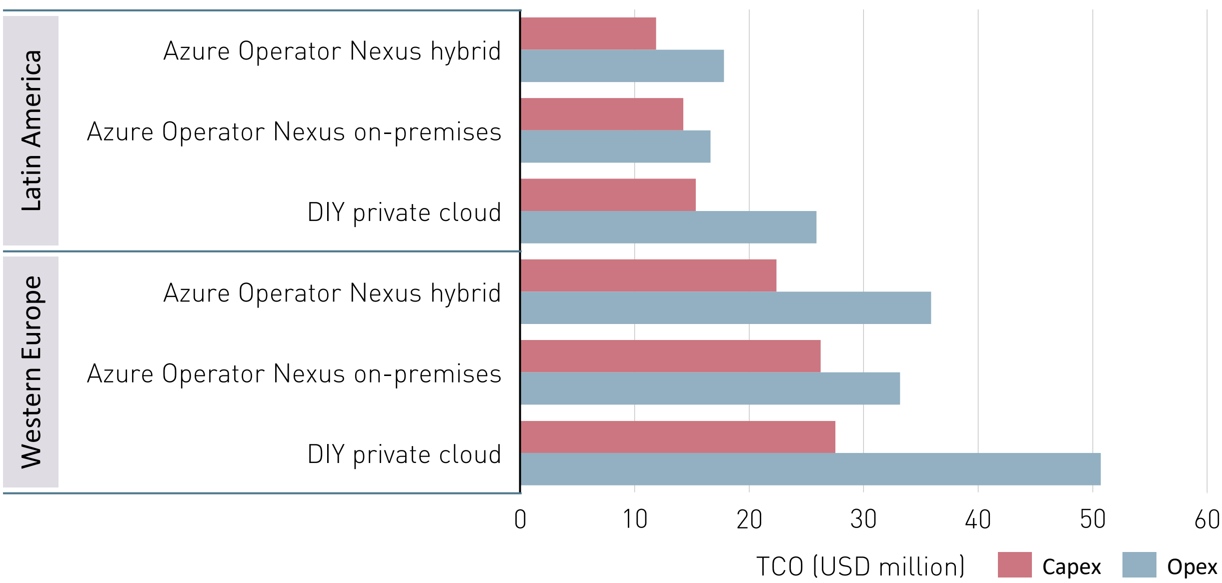
the same way for both profiles, and labor costs reflect the regional variances for both the DIY private cloud and Azure Operator Nexus-based deployment scenarios.

4.1 The hybrid Azure Operator Nexus model offers the lowest overall TCO of all scenarios

Figure 4.4The cloud infrastructure and operations TCO of the shows the cumulative, 5-year TCO of a cloud-native 5G SA network deployment for each of the three scenarios. The overall TCO of the Azure Operator Nexus on-premises scenario is 24% lower than that of the DIY private cloud deployment for the Western European operator and 25% lower for the Latin American operator. Opex reduction enabled by the increased automation and efficiency of the cloud infrastructure and CNF operations is the main driver of the TCO savings in the Azure Operator Nexus scenario. Azure Operator Nexus's comprehensive and consistent cloud environment, automation framework and managed service capabilities can reduce the FTE working hour requirements for the main cloud-native network operations by 59% compared to the DIY private cloud model and can reduce opex by up to 36%. The operational efficiencies that can be achieved with Azure Operator Nexus are discussed in section 4.2.

The hybrid cloud implementation of Azure Operator Nexus provides the optimal TCO of all scenarios because it enables further capex and opex savings compared to the Azure Operator Nexus on-premises scenario by allocating suitable workloads to the Azure public cloud. This helps operators to achieve higher scalability and utilization levels and reduce on-premises hardware costs, as discussed in section 4.3.

FIGURE 4.4: CUMULATIVE, 5-YEAR TCO FOR THE THREE CLOUD-NATIVE 5G SA NETWORK DEPLOYMENT SCENARIOS [SOURCE: ANALYSYS MASON, 2023]



4.2 The cloud infrastructure and operations TCO of the Azure Operator Nexus on-premises scenario is up to 38% lower than that for the DIY model due to a reduction in opex

Figure 4.5 and Figure 4.6 show the cloud infrastructure and operations TCO (which excludes CNF-related costs) for the two on-premises deployment scenarios for a Tier-1 operator in Western Europe and in

FIGURE 4.5: CLOUD INFRASTRUCTURE AND OPERATIONS TCO FOR THE ON-PREMISES MODELS, WESTERN EUROPE [SOURCE: ANALYSYS MASON, 2023]

TCO component		DIY private cloud	Azure Operator Nexus on-premises	Comparison of Azure with DIY
Capex	Hardware (compute, storage and network) including implementation and integration services	USD11 650 000	USD10 380 000	–11%
	Total capex	USD11 650 000	USD10 380 000	–11%
Opex	Cloud platform	USD3 536 842	USD4 502 920	+27%
	Hardware support and maintenance	USD5 384 784	USD4 779 668	–11%
	Labor (FTE hours)	USD30 850 000	USD12 820 000	–58%
	Power and space	USD1 680 000	USD1 680 000	0%
	Total opex	USD41 451 627	USD23 782 588	–43%
Total TCO (5-year)		USD53 101 627	USD34 162 588	–36%

FIGURE 4.6: CLOUD INFRASTRUCTURE AND OPERATIONS TCO FOR THE ON-PREMISES MODELS, LATIN AMERICA [SOURCE: ANALYSYS MASON, 2023]

TCO component		DIY private cloud	Azure Operator Nexus on-premises	Comparison of Azure with DIY
Capex	Hardware (compute, storage and network) including implementation and integration services	USD6 530 000	USD5 440 000	–17%
	Total capex	USD6 530 000	USD5 440 000	–17%
Opex	Cloud platform	USD1 656 782	USD2 094 582	+26%
	Hardware support and maintenance	USD3 003 615	USD2 479 239	–17%
	Labor (FTE hours)	USD15 430 000	USD6 400 000	–59%
	Power and space	USD420 000	USD420 000	0%
	Total opex	USD20 510 397	USD11 393 821	–44%
Total TCO (5-year)		USD27 040 397	USD16 833 821	–38%

Latin America, respectively. The cloud infrastructure and operations TCO for the Azure Operator Nexus scenario is 36% and 38% lower than that for the DIY private cloud in Western Europe and Latin America, respectively. The slight difference in TCO savings between the operator profiles is mainly caused by the greater scalability and cost advantages of the Azure Operator Nexus architecture and subscription-based model in Latin America because this deployment starts from a very small base and scales up quickly over 5 years.

Our TCO model shows that the capex of the on-premises Azure Operator Nexus scenario is11–17% lower than that of the DIY private cloud model. Both scenarios are based on industry-standard COTS hardware components with similar specifications and costs, but Azure Operator Nexus enables indirect capex savings thanks to its predesigned and validated infrastructure. This leads to a major reduction in the cost of cloud hardware implementation, integration and testing.

One of the key findings from our TCO analysis is that there is significant amount of opex attached to the lifecycle operations of cloud infrastructure and CNFs, and operators are not usually fully aware of the size of these costs. Our research and interviews show that operators are struggling with the private cloud and on-premises data center management and automation, and are burdened by the cost of large operational headcounts. This is due to:

- unfamiliarity with cloud-native technologies and a lack of in-house expertise to operate and automate cloud-native networks
- highly fragmented and not-fit-for purpose management and automation tools and slow, manual data center processes
- different automations for different network functions and for between infrastructure and network functions, which results in limited economies of scale, integration issues and the need for complex network orchestration mechanisms.

We collected granular, real-life data for headcounts and FTE hours for each of the major cloud-native network operational processes from several large Tier-1 operators to examine the true costs of operating DIY private clouds and to enable a complete TCO assessment. Our data and analysis show that FTE hours are the biggest contributor to the total cost of a 5G SA network deployed using a DIY private cloud and can account for up to 40% of the overall TCO.

One of the main benefits of the Azure Operator Nexus cloud platform is that it provides operators with a comprehensive set of integrated cloud automation tools, PaaS and managed services expertise in order to enable users to achieve highly automated cloud-native network operations with significantly fewer FTE hours. Conversely, operators that take the DIY approach need to stitch together all of these components by themselves, which is highly complex and involves significant risks. They must also perform their own lifecycle management, which is opex-heavy. For example, AT&T built its Airship cloud using the DIY model, but was unable to get it to function like a public cloud. Other CSPs have employed multiple vendors/systems integrators to build their cloud platforms and automations, but each time they have ended up reinventing the wheel for themselves and have built unique cloud automations that cannot be reused for other functions.

Our model shows that Azure Operator Nexus scenario can reduce the opex associated with FTE hours by up to 59%. It can also reduce the opex associated with cloud infrastructure and CNF operations by 43% in Western Europe and 44% in Latin America. Most of the opex savings enabled by the Azure Operator Nexus model come from the ability to automate and remotely manage cloud infrastructure operations, as shown in Figure 4.7. Figure 4.8 illustrates the cumulative breakdown of the FTE hour cost reductions.

In addition to cloud infrastructure, Azure Operator Nexus can also help operators with the automated management of several key CNF operational processes, especially when the operator streamlines and simplifies its CNF platform services environment using Azure-managed PaaS solutions (such as logging, monitoring, AI/ML, CI/CD and DevOps tools). Operators can achieve the FTE hour reductions in CNF operations that are shown in Figure 4.9 by following this approach. Conversely, operators that use the DIY model implement fragmented, vendor-specific platform services and tools and manage their lifecycle by themselves. Figure 4.10 provides a cumulative breakdown of Azure Operator Nexus FTE hour cost reductions by each CNF process.

4.3 Adopting a hybrid cloud architecture based on Azure Operator Nexus could result in a cloud infrastructure and operations TCO reduction of 43%

We assessed the capex and opex implications of using hybrid cloud architecture for a cloud-native 5G SA network (Azure Operator Nexus hybrid), where some of the control plane functions (AMF and policy management) and management applications (network orchestration and element managers) are deployed in the Azure public cloud and the rest of the network functions are deployed on-premises in operators' data centers. Our model shows that this scenario can reduce the TCO compared to DIY model as follows.

- The overall TCO for a Western European operator is 26% lower (compared to 24% for the on-premises model) and the cloud infrastructure and operations TCO is 38% lower (compared to 36% for the on-premises model).
- The overall TCO for a Latin American operator is 28% lower (compared to 25% for the on-premises model) and the cloud infrastructure and operations TCO is 43% lower (compared to 38% for the on-premises model).

FIGURE 4.7: OPEX BENEFITS RELATED TO CLOUD INFRASTRUCTURE OPERATIONAL PROCESSES OF THE AZURE OPERATOR NEXUS MODEL COMPARED TO THE DIY MODEL [SOURCE: ANALYSYS MASON, 2023]

Operational process	Benefits of the Azure Operator Nexus model over the DIY model	Potential reduction in FTE hours
Mean time to repair (MTTR)	Azure Operator Nexus provides closed-loop automation with real-time analytics/AI for the monitoring, root-cause identification and remediation of the entire cloud infrastructure. This is fully managed by operators in the DIY private cloud model and requires the equivalent of 7 FTEs' annual working hours per year. Fewer than 1.5 FTEs' annual working hours are required per year for the Azure Operator Nexus model.	80%
SecOps	Azure Operator Nexus provides full security lifecycle management and expertise including security monitoring, incident response, proactive identification and fixing of vulnerabilities, roll-outs of security updates/patches and tests. This requires only around 1.6 FTEs' annual working hours per year.	70%
Network deployment and provisioning	• Azure Operator Nexus provides a Day 0 and 1 zero-touch automated deployment model for cloud infrastructure resources and ensures that the correct OS features and firmware are installed and provisioned. In a DIY private cloud environment, there are usually many moving parts that come from multiple vendors and a significant amount of engineering work is required to deploy and validate the infrastructure. • Azure Operator Nexus provides simplified and consistent hardware infrastructure BoM based on a pre-certified design of compute, storage and networking resources, which reduces the design costs and risks of inconsistent DIY environments. It also accelerates hardware procurement. • Logistics and systems integrator partners of Azure Operator Nexus put everything together and deliver it to the operator, thereby reducing rack/stack/cabling efforts.	75%
SysAdmin	On-going lifecycle management processes such as server management, OS/firmware upgrades and patching are delivered remotely by Microsoft, thereby reducing the need for dedicated SysAdmin FTEs.	80%
Cloud configuration	• Azure Operator Nexus provides automated configuration and validation of cloud software (Kubernetes/CaaS, OS) and hardware resources. • Azure Operator Nexus includes advanced fabric automation with fully integrated SDN capabilities to connect physical and logical networks to the cloud. This is a highly complex process and DIY operators usually do this in a manual way using spreadsheets and scripts.	70%
CI/CD pipeline	The coherent cloud infrastructure components of the Azure Operator Nexus platform enables streamlined and efficient CI/CD processes that are supported by Azure Operator Nexus PaaS and CI/CD tools compared to siloed DIY cloud infrastructure environments.	80%
Monitoring and observability set-up	Cloud hardware, software and applications are all in the same Azure Operator Nexus environment and come with curated, out-of-the box monitoring and observability capabilities. DIY clouds usually consist of different set-ups that require manual stitching. This can be error-prone, slow and costly to carry out.	80%

FIGURE 4.8: BREAKDOWN OF AZURE OPERATOR NEXUS FTE HOUR COST SAVINGS BY CLOUD INFRASTRUCTURE OPERATIONAL PROCESSES [SOURCE: ANALYSYS MASON, 2023]

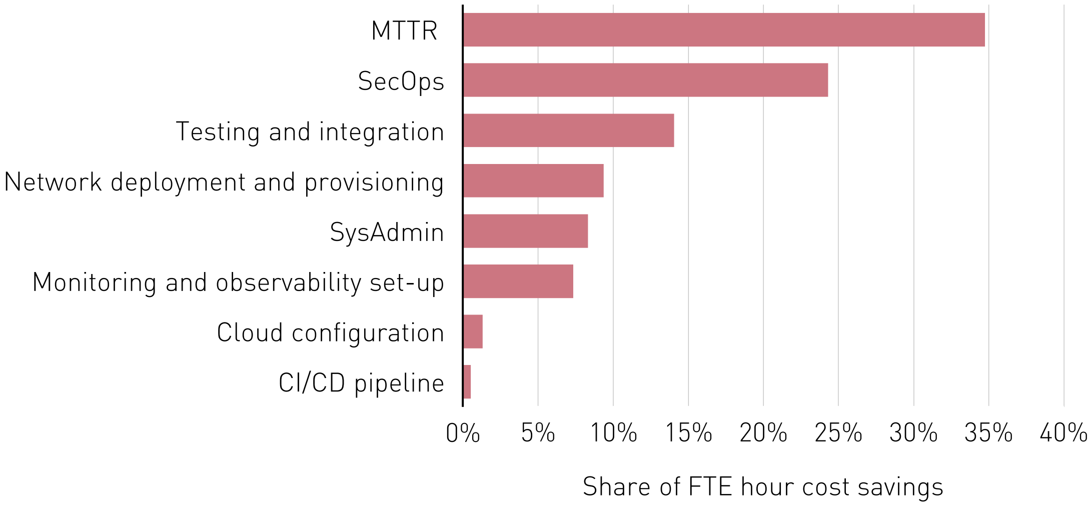


FIGURE 4.9: OPEX BENEFITS RELATED TO CNF OPERATIONAL PROCESSES OF THE AZURE OPERATOR NEXUS MODEL COMPARED TO THE DIY MODEL [SOURCE: ANALYSYS MASON, 2023]

Operational process	Benefits of the Azure Operator Nexus model over the DIY model	Potential reduction in FTE hours
xNF onboarding and deployment	• Azure Operator Nexus hardware and software pretesting and certification can reduce the effort and costs of CNF onboarding processes. • Azure Operator Nexus also works with a large ecosystem of CNF vendor partners whose CNF images and Helm charts are onboarded to a standard marketplace catalog and plugged into Azure PaaS.	40%
SecOps	The Microsoft security team performs the full security lifecycle of CNFs on behalf of the operator and the operator therefore only needs to allocate limited working hours to oversee the processes.	70%
CI/CD pipeline	Azure Operator Nexus technology (PaaS and GitHub) and expertise is delivered in an integrated and efficient manner, whereas DIY environments are usually a patchwork of multiple pipelines and technology islands, which increases the cost and complexity of CI/CD pipeline set-ups.	50%
Monitoring and observability set-up	Azure Operator Nexus provides a unified observability platform that includes a coherent set of out-of-the-box components and a single pane of glass for CNFs and cloud infrastructure. DIY approaches usually lead to fragmented and complex monitoring and observability environments that are more expensive to build and manage. The savings here are lower than those related to cloud infrastructure because many CNFs still depend on their proprietary, closed element management systems (EMS), which restricts the automation capabilities.	50%

FIGURE 4.10: BREAKDOWN OF AZURE OPERATOR NEXUS FTE HOUR COST SAVINGS BY CNF OPERATIONAL PROCESSES [SOURCE: ANALYSYS MASON, 2023]

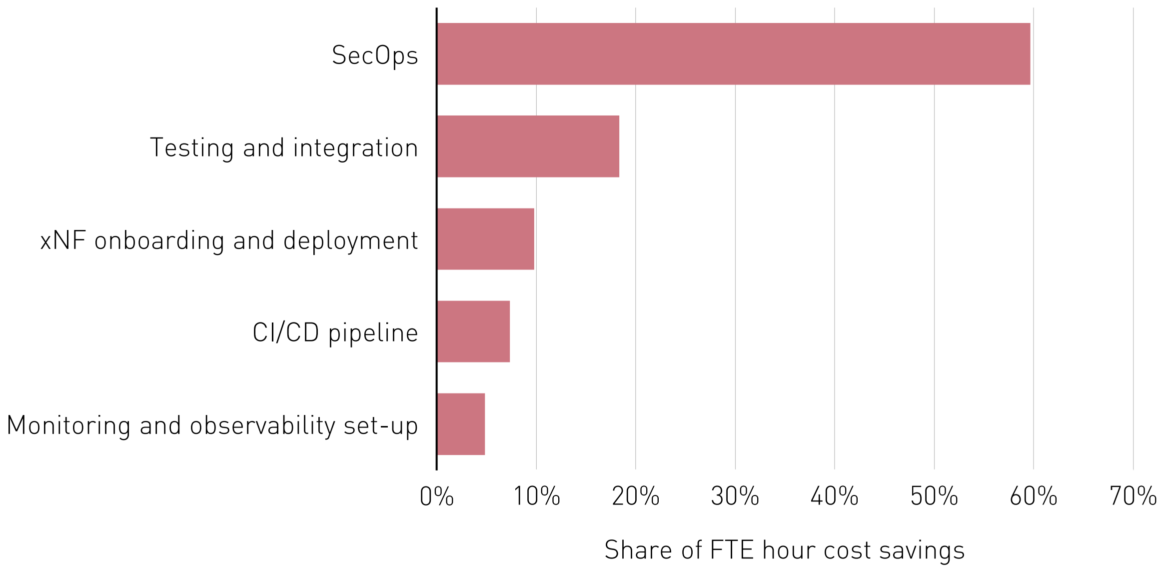


Figure 4.11 shows the capex and opex savings of this hybrid architecture for a Western European operator (see Figure 6.6 in the annex for the data for a Latin American operator). These savings mainly come from the following factors and can potentially be enhanced by further optimizing the workload allocation by using the public cloud environment more.

- The reduced on-premises hardware footprint and associated costs lead to lower hardware capex and related opex (such as energy and support and maintenance costs).
- A portion of the hardware infrastructure investment shifts from high up-front capex to consumption-based opex, which delivers an optimized cost model.
- The use of public cloud infrastructure eliminates the need for overprovisioning hardware for peak times, which leads to higher utilization and scalability

FIGURE 4.11: CLOUD INFRASTRUCTURE AND OPERATIONS TCO FOR ALL THREE DEPLOYMENT SCENARIOS, WESTERN EUROPE [SOURCE: ANALYSYS MASON, 2023]

TCO component		DIY private cloud	Azure Operator Nexus on-premises	Azure Operator Nexus hybrid	Comparison of Azure hybrid with DIY
Capex	Hardware (compute, storage and network), including implementation and integration services	USD11 650 000	USD10 380 000	USD6 520 000	–44%
	Total capex	USD11 650 000	USD10 380 000	USD6 520 000	–44%
Opex	Cloud platform	USD3 536 842	USD4 502 920	USD3 039 045	–14%
	Hardware support and maintenance	USD5 384 784	USD4 779 668	USD2 835 531	–47%
	Labor (FTE hours)	USD30 850 000	USD12 820 000	USD12 820 000	–58%
	Public cloud usage	0	0	USD6 608 393	N/A
	Power and space	USD1 680 000	USD1 680 000	USD1 170 000	–30%
	Total opex	USD41 451 627	USD23 782 588	USD26 472 969	–36%
Total TCO (5-year)		USD53 101 627	USD34 162 588	USD32 992 969	–38%

5 Conclusions and recommendations

Cloud-native infrastructure is critical to enable operators to achieve the benefits that they expect to derive from deploying a 5G SA core, including the ability to support advanced network services. Cloud-native infrastructure enables operators to shift away from vertically integrated network function stacks to more open and disaggregated network cloud deployment models that support access to innovation within a larger network function vendor ecosystem. Operators need to understand the complete set of costs associated with the various approaches to sourcing a disaggregated cloud platform. This will allow them to make an informed decision about which cloud deployment model they should use to futureproof their 5G infrastructure (both core and RAN).

Our TCO study shows that there is substantial amount of opex attached to DIY private clouds due to the cloud-native automation challenges outlined in this paper. This can be detrimental to operators' ability to deliver automated and competitive 5G and edge services. A comprehensive and coherent cloud-native platform and automation framework delivered via an as-a-service model (such as Azure Operator Nexus) can help operators to significantly reduce their private cloud opex and optimize the TCO of a cloud-native 5G SA network implementation. In addition, hybrid cloud architecture can potentially offer a more flexible and scalable network environment, which can improve the TCO/business case for cloud-native networks.

We provide the following recommendations for operators that are evaluating cloud-native 5G SA network deployment models and architecture to identify the optimal implementation approaches.

- **Operators should choose the right cloud platform and operational model for their 5G SA networks in order to achieve their service and automation ambitions.** Cloud infrastructure is increasingly critical for the network and for 5G monetization opportunities, so it needs to be state-of-the-art, operationally efficient and delivered and managed using industry best practices. Operators that want to build true cloud environments for their 5G networks should embrace open, disaggregated network cloud models. These networks should be based on proven cloud-native platforms and automation frameworks that minimize the costs and challenges of building and operating disaggregated clouds and deliver programmable infrastructure to maximize service agility and innovation within a strong, open ecosystem.
- **Operators should assess their operational readiness and in-house capabilities in order to conduct a complete TCO analysis.** It is difficult and

time- and resource-consuming for many operators to build and operate cloud-native networks on private clouds. Operators need to undertake a detailed examination of their cloud and data center processes and in-house operational capabilities to reveal their hidden costs and operational challenges. This will enable operators to build a more-holistic TCO/business case based on automation that will guide their technology vendor and cloud delivery model investment decisions.

- **Operators should devise a long-term plan to streamline and converge their existing and new clouds onto common cloud platforms and automation frameworks.** Several advanced operators have taken the DIY path to build their disaggregated network clouds, but their progress has been stalled due to technical and operational challenges (such as integration and automation/orchestration complexity and a lack of in-house skills and expertise). They have accumulated multiple network cloud silos using various tightly integrated xNFs and clouds, and have built specific automations that are not transferrable to other clouds. Operators that are starting to implement 5G SA and vRAN/Open RAN need to have a long-term plan to streamline and converge these clouds using common cloud platforms and industry-standard PaaS and cloud-native automation frameworks. Our TCO analysis shows that using the Azure Operator Nexus platform and its as-a-service model is a highly cost-efficient way of building new cloud-native networks, and operators could consider extending it to other cloud domains, including their existing network cloud silos.
- **Operators should consider adopting hybrid cloud architecture for their cloud-native networks.** Our TCO analysis demonstrates that hybrid cloud architecture could deliver additional cost savings with commercial and deployment flexibility benefits. However, this option is still relatively new to network clouds, and operators should first follow a step-wise approach starting from low-hanging fruit functions and use cases (such as those related to the control plane and policies). Operators that take this path must carefully evaluate their vendor and cloud platform choices to ensure that they meet their performance/QoS, data sovereignty/privacy, security and support/SLA requirements.

6 Annex

This section provides details of the modeling assumptions and parameters of the TCO analysis.

6.1 Connections and traffic

FIGURE 6.1: TOTAL NUMBER OF 5G CONNECTIONS FOR EACH OPERATOR PROFILE [SOURCE: ANALYSYS MASON, 2023]

	Year 1	Year 2	Year 3	Year 4	Year 5
Tier-1 Western European operator	13 853 176	23 177 316	33 170 399	42 615 026	50 119 043
Tier-1 Latin American operator	466 243	2 657 645	10 954 262	24 541 296	40 633 546

FIGURE 6.2: ANNUAL 5G DATA TRAFFIC (PB) FOR EACH OPERATOR PROFILE [SOURCE: ANALYSYS MASON, 2023]

	Year 1	Year 2	Year 3	Year 4	Year 5
Tier-1 Western European operator	4765	9533	16 048	22 915	29 266
Tier-1 Latin American operator	375	889	2044	4141	6752

6.2 Cost parameters

- The costs for training and OSS/BSS integration for 5G SA core network components are excluded in all scenarios.
- CNF costs are normalized and averaged from various vendor price benchmarks used in Analysys Mason's consulting projects and regulatory models.
- Cloud infrastructure software (CaaS, SDN and OS) and COTS hardware costs are collected and normalized from various internal sources including Analysys Mason's consulting projects, regulatory models and operator surveys.
- Azure Operator Nexus and Azure public cloud usage costs are estimated based on Microsoft's guidance.
- FTE-related opex data was collected from Analysys Mason's survey of five Tier-1 operators that implemented a 5G SA core using the DIY model. The data includes the real-life frequency and duration of each operational activity and the number of FTEs involved. It has been normalized and averaged across these five operators.

- The lifetime of CNF licenses is assumed to be 5 years and COTS servers' lifetimes are assumed to be 3 years.
- Cloud hardware installation and provisioning costs are assumed to be 25% of the total hardware costs.
- Support and maintenance costs for all hardware elements are assumed to be 20% of the equipment costs.
- Support and maintenance costs for all software elements are assumed to be 14% of the software license costs.

FIGURE 6.3: SUMMARY OF LABOR COST PARAMETERS [SOURCE: ANALYSYS MASON, 2023]

Parameter	Value
Hourly cost of labor – Western Europe	USD100
Hourly cost of labor – Latin America	USD50
Cost trend of labor	2.0%
Number of working hours per year	1725

FIGURE 6.4: SUMMARY OF POWER COST PARAMETERS [SOURCE: ANALYSYS MASON, 2023]

Parameter	Value
Power (at a consumption of 48V per kWh) – Western Europe	USD0.10
Power (at a consumption of 48V per kWh) – Latin America	USD0.05

FIGURE 6.5: SUMMARY OF FLOORSPACE COST PARAMETERS [SOURCE: ANALYSYS MASON, 2023]

Parameter	Value
Rack units per standard rack	42
Rack floorspace (m2/rack)	4
Cost trend of floorspace	3%
Annual floorspace cost per square meter– Western Europe	USD3000
Annual floorspace cost per rackspace – Western Europe	USD12 000
Annual floorspace cost per square meter – Latin America	USD1500
Annual floorspace cost per rackspace – Latin America	USD6000

6.3 TCO breakdown for Tier-1 operator in Latin America for all three deployment scenarios

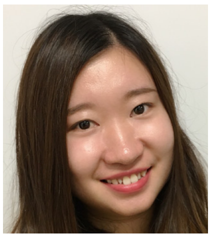
FIGURE 6.6: CLOUD INFRASTRUCTURE AND OPERATIONS TCO FOR ALL THREE DEPLOYMENT SCENARIOS, LATIN AMERICA [SOURCE: ANALYSYS MASON, 2023]

TCO component		DIY private cloud	Azure Operator Nexus on-premises	Azure Operator Nexus hybrid	Comparison of Azure hybrid with DIY
Capex	Hardware (compute, storage and network), including implementation and integration services	USD6 530 000	USD5 440 000	USD3 050 000	–53%
	Total capex	USD6 530 000	USD5 440 000	USD3 050 000	–53%
Opex	Cloud platform	USD1 656 782	USD2 094 582	USD1 371 717	–17%
	Hardware support and maintenance	USD3 003 615	USD2 479 239	USD1 118 739	–63%
	Labor (FTE hours)	USD15 430 000	USD6 400 000	USD6 400 000	–59%
	Public cloud usage	0	0	USD3 269 707	N/A
	Power and space	USD420 000	USD420 000	USD270 000	–36%
	Total opex	USD20 510 397	USD11 393 821	USD12 430 164	–39%
Total TCO (5-year)		USD27 040 397	USD16 833 821	USD15 480 164	–43%

7 About the author

Gorkem Yigit (Principal Analyst) is the lead analyst for the Cloud Infrastructure Strategies and Multi-Cloud Networking research programmes. His research focuses on the building blocks, architecture and adoption of the cloud-native, disaggregated and programmable digital infrastructure and networks that underpin the delivery of 5G, media and edge computing services. He also works with clients on a range of consulting projects such as market and competitive analysis, business case development and marketing support through thought leadership collateral. He holds a cum laude MSc degree in economics and management of innovation and technology from Bocconi University (Milan, Italy).

Caroline Chappell (Research Director) heads Analysys Mason's Cloud research practice. Her research focuses on service provider adoption of cloud to deliver business services, support digital transformation and re-architect fixed and mobile networks for the 5G era. She is a leading exponent of the edge computing market and its impact on service provider network deployments and new revenue opportunities. She monitors public cloud provider strategies for the telecoms industry and investigates how key cloud platform services can enhance service provider value. Caroline is a leading authority on the application of cloud-native technologies to the network and helps telecoms customers to devise strategies that exploit the powerful capabilities of cloud while mitigating its disruptive effects.



Luwen Meng (Consultant) is based in our Cambridge office. At Analysys Mason, she has worked on a variety of project types across a number of telecoms verticals, including supporting regulators, network operators, and vendors. Luwen has been active in modelling, report writing and desk research, supporting a range of clients based both in Europe and internationally. Luwen has a PhD in Chemical Engineering from the University of Cambridge.

Published by Analysys Mason Limited
North West Wing, Bush House
Aldwych
London WC2B 4PJ
UK
Tel: +44 (0)20 7395 9000
london@analysysmason.com
www.analysysmason.com
Registered in England and Wales
No. 5177472

Stay connected

You can stay connected by following Analysys Mason via Twitter, LinkedIn, YouTube or RSS feed.

- @AnalysysMason
- linkedin.com/company/analysys-mason
- youtube.com/AnalysysMason
- analysysmason.com/RSS/
- analysysmason.podbean.com