Capgemini engineering

THE TELECOMMUNICATIONS INDUSTRY EMBRACES CLOUD-NATIVE ENGINEERING

To maximize the benefits of cloud-native solutions requires a shift from a hardware-centric to a software-centric model

Table of contents

Executive Summary

Cloud-based or cloud-native applications have long been the standard for most enterprises. However, 5G networks have become the focus for communications service providers (CSPs) over cloud-native applications in vertical applications, as they leverage technology and modeling approaches such as network function containerization, service-oriented architecture, software-defined networking, network-as-a-service, cloudification, etc.

Network function virtualization (NFV) was introduced in 2012, and most CSPs adopted emerging network virtualization methodologies by replacing physical network functions (PNFs) with virtual network functions (VNFs) and replacing legacy appliances with virtual machines (VMs) running on cloud or standard IT hardware.

Nonetheless, CSPs realize that traditional virtualization is not enough. Instead, they must focus on cloud-native practices, which can help to reduce cost, boost productivity, improve operational efficiency, and deliver engaging end-user services.

5G service relies on the functionality of edge computing, edge resource processing, and distributed intelligence to provide the best services to customers, which require greater operational flexibility and can be achieved by cloud-native services.

Recent examples of hybrid cloud

Today, many organizations are considering hosting their 5G network functions using a hybrid cloud model. Recently, among the 30-plus internet service providers (ISVs) partnering with Google Anthos on 5G technology are seven manufacturing companies, including IoT companies, building technology for such things as cloud-based controls for warehouse robotics and providing augmented reality (AR) and virtual reality (VR) headsets to factory technicians.[1] Here are four examples:

- **Ericsson put its 5G on Google Cloud's Anthos**: Google Cloud is working with Ericsson to develop 5G and edge cloud solutions to aid CSPs with their digital transformation. As a result, organizations have the opportunity to digitally transform their businesses with 5G and cloud capabilities such as artificial intelligence and machine learning[2]
- **AT&T partners with Google on 5G enablement**: Google and AT&T are testing AT&T's 5G network with advanced Google Cloud technologies such as artificial intelligence, machine learning, the Kubernetes container orchestration platform, and edge computing tools aimed at benefiting specific industries, including retail, construction, and transportation[3]
- **Nokia teams up with Google Cloud on 5G core NS edge**: Nokia and Google Cloud will work to validate, optimize, and develop cloud-native network functions and co-innovate new solutions that will help CSPs deliver 5G connectivity and services at scale[4]
- **Casa Systems extends 5G standalone core availability to Google Cloud's Anthos**: Google Cloud's Anthos will support additional deployment opportunities for Casa Systems' 5G SA Core, enabling service providers and enterprises to provision agile services that are deployable anywhere, from the edge of the network to public clouds, private clouds, and carrier networks[5]

1. Joseph Kovar, "Google Expands Anthos 5G Ecosystem With Over 30 New Tech Partners," Dec 8, 2020, CRN https://www.crn.com/news/cloud/google-expands-anthos-5g-ecosystem-with-over-30-new-tech-partners
2. "Ericsson puts its 5G on Google's Anthos," Jun 29, 2021, Light Reading https://www.lightreading.com/service-provider-cloud/ericsson-puts-its-5g-on-googles-anthos-/d/d-id/770552
3. Joseph Tsidulko, "Google, AT&T Partner On 5G Enablement," Mar 5, 2020, CRN https://www.crn.com/news/cloud/google-at-t-partner-on-5g-enablement
4. Dianna Goovaerts, "Nokia teams with Google Cloud on 5G core, edge," Jan 14, 2021, Mobile World Live https://www.mobileworldlive.com/featured-content/top-three/nokia-teams-with-google-cloud-on-5g-core-edge
5. Casa Systems, Inc. "Casa Systems Extends 5G Standalone Core Availability to Google Cloud's Anthos," Jun 9, 2021, Globe Newswire https://www.globenewswire.com/news-release/2021/06/09/2244410/0/en/Casa-Systems-Extends-5G-Standalone-Core-Availability-to-Google-Cloud-s-Anthos.html

Overview

Today's CSPs need to accelerate the pace of innovation by delivering services and capabilities to customers faster, which may not be possible with the existing legacy systems. To be agile, flexible, efficient, and provide total cost of ownership (TCO), organizations must leverage cloud infrastructure and technologies and break down services into smaller components. (See Figure 1.)

CSPs can deploy services, software, and capabilities in a much more dynamic way and utilize their infrastructure much more efficiently with cloud-native services. For the current environment, cloud-native means desegregating the sets of applications into smaller sets of microservices, containerization, serverless architecture, and CI/CD pipeline that can be instantiated and brought up and torn down in a much more dynamic fashion.

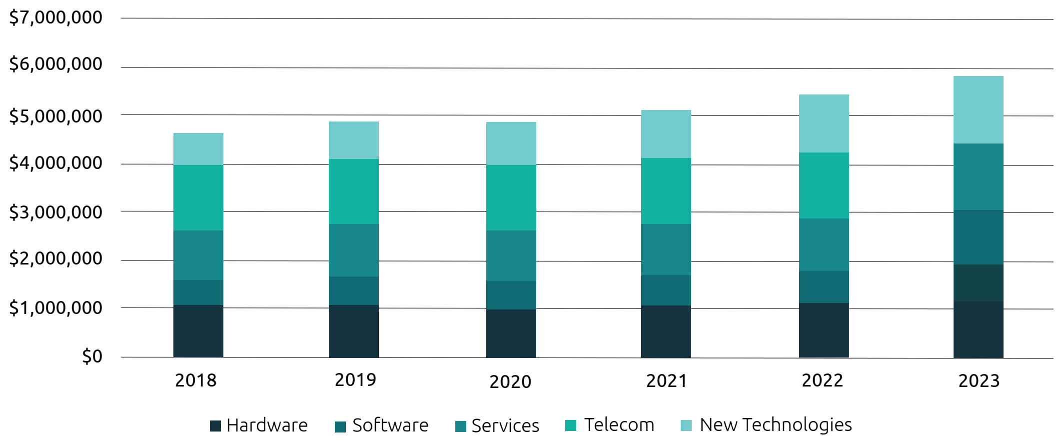


Figure 1: Global information communication technology spending 2018-2023
$ in millions, constant currency
Source: IDC[6]

Cloud-native refers to the practices that empower an organization to build and manage large-scale applications. They can achieve this goal by using private, hybrid, and public cloud providers.[7] In addition to scale, organizations need to be agile when integrating customer feedback and adapting to the surrounding technology ecosystem.

However, it could take longer than expected for CSPs to initialize and deploy a service and make it available to customers. Cloud-native engineering shortens the cycle in terms of how applications are rapidly deployed and brought into services, monetized, and then torn down and replaced when demand wanes. To benefit from cloud-native services, organizations will need to retool their processes, become more software-driven and change their culture from a hardware-centric model to a software-centric model.

6. J"IDC – Global ICT Spending, Forecast 2020-2023," IDC https://www.idc.com/promo/global-ict-spending/forecast
7. "Introduction to Cloud Native," Jul 22, 2021, Truong https://www.truongbui.com/posts/introduction-cloud-native

What is cloud-native engineering?

Cloud-native engineering empowers organizations to design and develop scalable, agile, cost-effective applications and run them in dynamic environments such as on-premises or in public, private, or hybrid clouds. A cloud-native application consists of microservices working together in an application that can be scaled easily. These microservices are often packaged in code along with libraries and dependencies to run anywhere. In a cloud-native app, the application code is designed, built, and delivered very differently than it would be for conventional, monolithic apps. Cloud-native engineering enables loosely coupled systems that are resilient, manageable, and observable to be combined with robust automation, allowing engineers to make changes frequently.

An engineering team can use cloud-native tooling to deliver value to customers quickly and easily extend to new features and technologies. These are the main reasons why an organization needs to adopt cloud-native technologies. However, when training cloud-native tooling, there are two communities to address: business and technical stakeholders.

There are many business benefits from the adoption of cloud-native solutions, including:

- **Total cost of ownership (TCO)**: Understanding TCO helps businesses determine the difference between short-term and long-term costs of a product or system. It enables them to make informed purchasing decisions by considering the various options when selecting the right vendor.[8] For example, public clouds, such as AWS, have many purchasing options such as one-year or three-year subscriptions, on-demand resources, etc., and many payment options such as all upfront, partial upfront, and no upfront payments

- **Global trade management (GTM)**: The cloud provides continuous integration and deployment capabilities that enable businesses to take new products and services to market faster. Also, shorter release cycles allow them to experiment with new ideas and strategies based on customer feedback

- **Agility**: Cloud-native solutions give businesses greater agility and speed in a highly competitive marketplace so they can make strategic adjustments to meet rapidly changing customer demand

- **Flexibility**: Cloud-native solutions support auto-provisioning, such as self-service, without any manual intervention

- **Scalability**: Cloud-native solutions can be automatically upscaled and downscaled as the business requires, which helps manage and reduce the overall cost

- **Service availability**: Cloud-native solutions reduce downtime and ensure the product is available to customers based on service level agreements (SLAs)

The adoption of cloud-native solutions provides many technical advantages:

- **Continuous automation**: Continuous integration and continuous delivery (CI/CD) release services with no human intervention

- **Microservices architecture**: Isolated services help apps minimize downtime and increase flexibility by using different technologies and scalability

- **Containerized serverless architecture**: Application deployment in a containerized environment (e.g., on servers or in a serverless architecture) makes use of an orchestrator to manage thousands of services hosted within the container environment with self-healing and minimal effort

- **Observability**: Provides the ability to troubleshoot and debug each component independently

- **Security**: Organizations can choose secure platforms based on their requirements, and automation provides the capability to recover faster from an attack

- **Disaster recovery and high availability**: Advantages include maximizing uptime, fault tolerance, rapid recovery of resources, and faster workload mobility

8. David Wallen, "Total Cost of Ownership: Why It's Important for Businesses," Nov 11, 2020, Spanning https://spanning.com/blog/total-cost-of-ownership-why-its-important-for-businesses/

The cloud-native landscape

The cloud-native landscape has a large number of services to leverage cloud-native technologies. These services are required to execute a variety of cloud-native applications. In addition, other services can be used to improve application quality, such as service proxy, discovery, mesh, networking and policy, distributed database and storage, streaming and messaging, container registry, runtime, and software distribution. (See Figure 2.)

- Containerization allows lightweight, portable applications that run uniformly and consistently anywhere. Its benefits include higher scalability, lower infrastructure operating cost, portability, faster deployment, lightweight applications, and better security

- Orchestration tools help manage containers by putting tasks together to process workflow and provide multiple features such as auto-scaling, auto-healing, provisioning, decommissioning of pods, upgrades, etc.

- Microservice architecture and application definition consists of many loosely coupled, autonomous, and self-contained services. These services communicate through a well-defined application programming interface (API), with the internal implementation of each service hidden from other services. As a result, it provides faster deployment, guaranteed up-time, resiliency, robustness, improved fault isolation, and maintainability

- Serverless architecture is a cloud-native execution model that provides on-demand computing resources and removes the overhead of managing and operating the infrastructure. Serverless typically falls into two categories: Backend-as-a-Service (BaaS) and Function-as-a-Service (FaaS)

- DevOps CI/CD delivery provides automatic updates, rollouts, rollbacks, and testing when the source code of the application changes, which helps the organization gain agility and with GTM to take new products and services to market faster

- Observability and analysis are cloud-native tools for aggregating, correlating, and analyzing the performance data of distributed applications and infrastructure for monitoring, troubleshooting, and debugging the application to meet SLAs and business requirements. There are several tools that can provide a complete system overview based on logs, metrics, and traces

- Service proxy, discovery, mesh, networking, and policy are features of service discovery, health checking, routing, load balancing, authorization, admission control, data filtering, etc.

- Distributed database and storage, streaming, and messaging are cloud-native tools that provide a reliable way to store data across a cluster of machines in single or distributed databases

- Container registry stores, signs, and scans content and can use container runtime instead of container registry. There are many tools available for secure software distribution

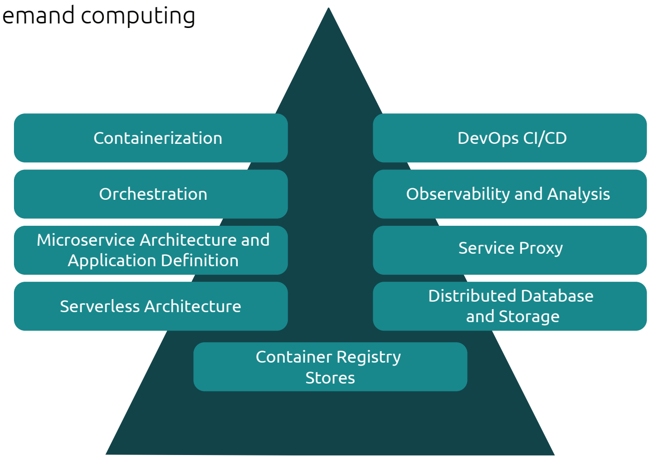


Figure 2: The cloud-native landscape
Source: Capgemini Engineering

Challenges for CSPs

Most CSPs use centrally located private clouds. The key benefits include scalability, elasticity, agility, lower cost, and better governance.

The typical CSP cloud is automated and orchestrated to provide network functions and capability on demand; scalable to support scale-up (horizontal scaling - adding more computing power) and scale-out (vertical scaling - adding more machines) with some switching and routing platforms and adaptively provide on-demand capabilities; and flexible. In addition, a CSP cloud must be secure, policy-driven and physically and virtually reliable to quickly identify, isolate, and repair unhealthy nodes on the network. Because of these features, the demand for cloud-native services is expected to post strong growth over the next few years. (See Figure 3.)

Early CSP clouds replaced network elements in large VNFs, which are much harder to maintain, require a lot of cloud resources, and use legacy operations. Many legacy operations are manual, which reduces speed and cannot provide rapid deployment of services.

In addition, there were no standard processes for developing and benchmarking VNFs in traditional VNF-based cloud architectures, which led to a lack of VNF architectural guidelines and vendors with no standard protocols or configuration policies for VNFs. As a result, manual efforts were required to configure, update, and test VNFs, making it difficult for CSPs to implement NFV successfully.

There are additional constraints related to the functioning of CSP clouds:

- **Migration**: Cloud computing profoundly impacts the software development life cycle (SDLC). Manual upgrades or even cloud deployments are prone to errors, so there is a dire need to clearly define the servicing of the application and automate the process. In many scenarios, the reference deployment architecture used by the enterprise on-premises is different than the one in the cloud. There are many scenarios, both technical and non-technical, in which on-premises applications cannot be moved directly to the cloud. The options are to create a new application that will use the cloud or port the application to the cloud. The main issues in

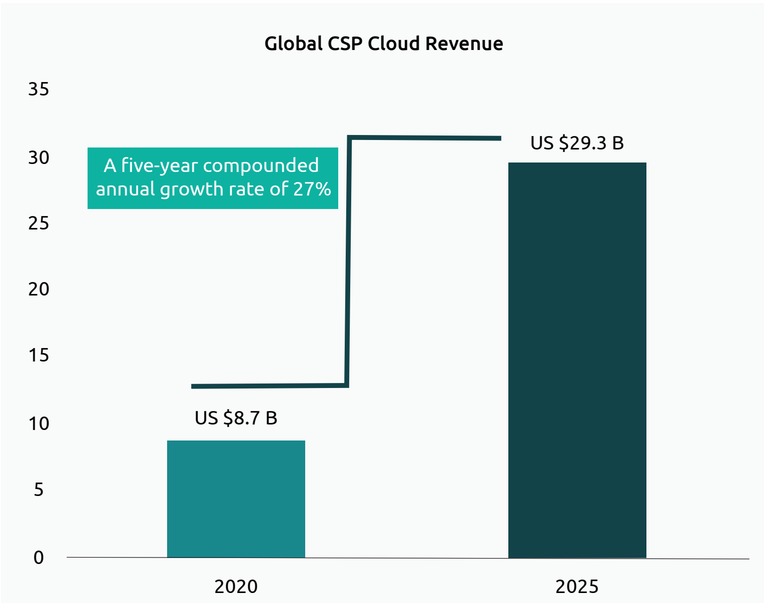


Figure 3: Strong growth ahead for CSP cloud revenue

Source: ABI Research[9]

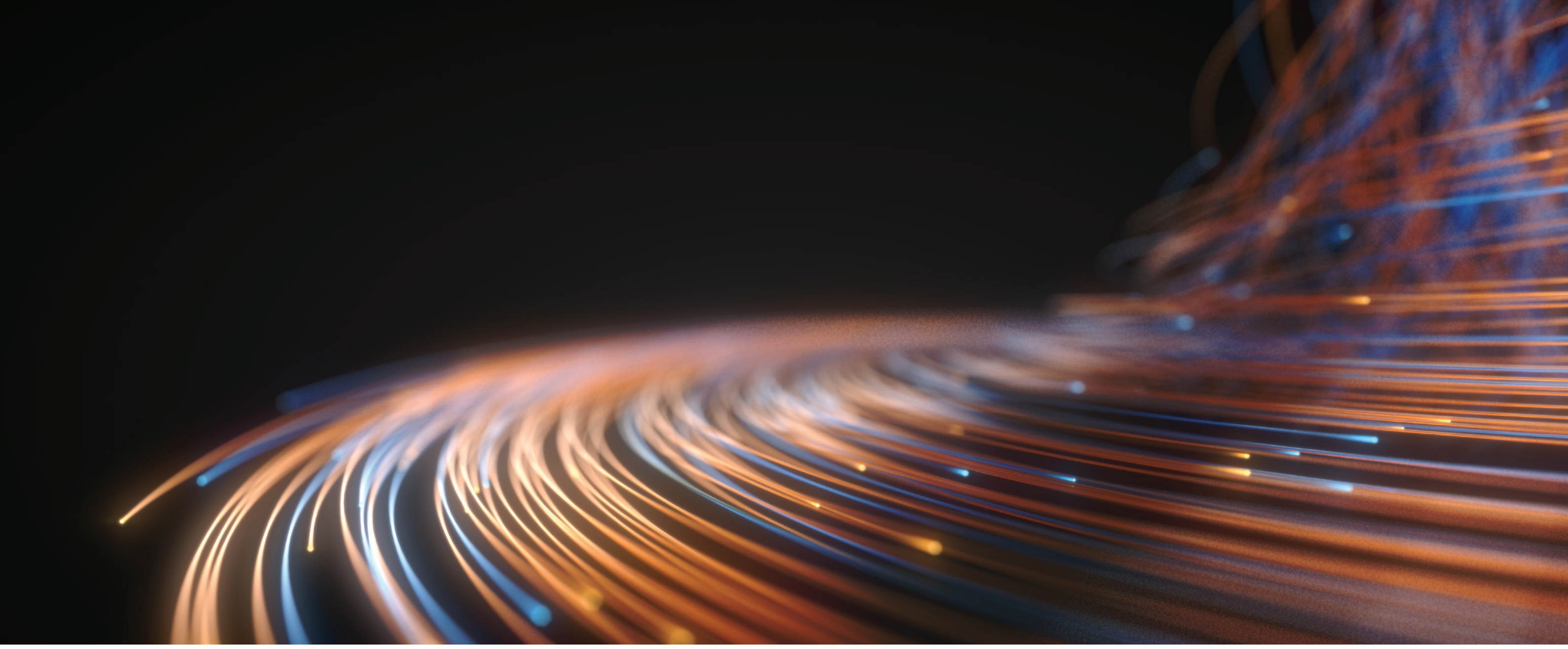
9. "Global Telco Cloud Revenue Will Grow to US$29.3 Billion by 2025," Nov 24, 2020, ABI Research https://www.abiresearch.com/press/global-telco-cloud-revenue-will-grow-us293-billion-2025/#:~:text=market%20advisory%20firm%2C-,ABI%20Research,-in%20its%20new

application design are cloud storage and encryption of ephemeral data, integration with cloud backup services, load balancing across geographies, integration of cloud security mechanisms across applications, patches for network boundaries, and identity management across clouds

- **Privacy and security**: Security solutions in telecommunications address data integrity, service availability, accountability of offerings, the confidentiality of data, and authenticity of user-access issues. The CSP's cloud provider must address all of them. Security concerns include, but are not limited to, the accidental release of protected data, user authentication, and access controls. Virtualized systems come with security issues primarily arising from misconfiguration. There are three primary security goals for virtualized systems: operational correctness, failure resilience, and virtual machine isolation. The abuse of cloud computing technologies by professionals working in the public cloud is not under any customer's control, so there should be a standard for limiting malicious insiders. Common threats include API insecurities, shared technology and cloud software vulnerabilities, data leakage, and account and traffic hijacking

- **Latency**: Today, the cloud is unable to provide telecommunications-grade latency solutions. Intra-cloud latency combines network or internet latency to deliver total systemic latency. The latency guarantee must be end-to-end for complete quality-of-service provisioning, and edge devices must be reconfigured for cloud computing

- **Vendor lock-in and standardization**: Since the cloud vendor owns the infrastructure hardware, there are scenarios where it is difficult for the enterprise to trust the vendor. One such scenario is downtime or interruption in service due to a hardware fault. In this case, the enterprise must rely on the cloud vendor to recover from the disaster without the enterprise intervening. Therefore, open standards are needed to reduce vendor lock-in. Enterprises have come up with a solution to this type of problem by backing up their application data to another cloud. This inter-cloud concept is gaining popularity among CSPs that see it as a necessity rather than an option



Recommended approaches to mitigate challenges

NFV and software-defined networking (SDN) are by far the most disruptive technologies for CSPs. SDN provides network virtualization and automatically establishes connectivity between virtualized compute resources, whether they are virtual machines or legacy bare metal servers. Similarly, cloud computing and fully automated technologies are needed to deliver agile, flexible, and seamless service experiences across target architectures and transform networks.

Here, we discuss approaches to address and mitigate the challenges in the CSP cloud environment:

- **Foster collaboration and integration**: For a multi-vendor, multi-component CSP cloud platform to work, it is essential to ensure that all the elements can co-exist.[10] We must ensure that partners, vendors, solutions, network functions, and frameworks can:

  - Co-exist without conflicting with each other
  - Co-exist without depending on each other
  - Co-exist with legacy networking infrastructure
  - Co-exist with legacy IT infrastructure and operations and business support systems (OSS/BSS)

  None of these goals are achievable without significant cross-industry collaboration.

- **Multi-vendor CSP cloud is preferred**: In the multi-vendor CSP cloud, an iterative integration process built on agile and DevOps methodologies requires participatory collaboration so that course improvement is dynamic and timely while keeping the strategy in place. Furthermore, when deployed correctly, multi-vendor solutions promote better operator-to-partner collaboration and success while giving operators the flexibility and freedom to customize the CSP cloud platform under their control

- **Insufficient management and orchestration solutions**: Management and orchestration (MANO) includes sub-components to manage infrastructure and network functions. It brings them together for the provision of network services and to ensure integration with the operator's back-end systems. The key is that operators want to manage and organize the infrastructure and network functions, regardless of the vendor. This means that when parts of the chain fall off, they will be able to identify where and how and consider the parties concerned

- **Container-as-a-Service (CaaS)**: CSPs need to implement cloud-native solutions such as containers, microservices, and serverless architectures to provide scalability and automation. CaaS is the automated hosting and deployment of a containerized software package. CSPs can

10. "Telco Cloud: Why it hasn't delivered, and what must change for 5G," Feb 2020, Juniper Networks and STL Partners
https://stage.juniper.net/content/dam/www/assets/white-papers/us/en/stl-white-paper-telco-cloud-why-it-hasnt-delivered-and-what-must-change-for-5g.pdf

adopt container-based flexible NFV platforms with acceleration technologies for high availability of auto-scaling and containerized network functions (CNFs), co-related KPIs and policies, and dynamic lifecycle management

- **Cloud-native service providers**: Service providers are well-positioned to play a leading role in the rapidly evolving edge computing space. They have always been adept at providing services nationally and internationally and expanding network capacity to meet demand. Using the same mindset, they have built new virtual and hybrid cloud infrastructures, which have enabled them to move to the edge. They can run and deploy applications anywhere in their hybrid cloud and edge infrastructure.[11]

11. Susan James, Red Hat, "Service providers embrace multi-vendor model to deliver edge computing," Oct 21, 2020, Telecoms.com https://telecoms.com/opinion/service-providers-embrace-multi-vendor-model-to-deliver-edge-computing/

Cloud-native engineering trends

The way software is developed has changed since containers, microservices architectures, and cloud-native technology have gained popularity. Moving to cloud-native not only means migrating existing applications to a private or public cloud infrastructure but building applications in new ways to take advantage of new technologies.

The concept of cloud-native is disruptive to the traditional IT infrastructure and application platform markets, creating new players, technologies, and a new cloud-native technology ecosystem. (See Figure 4.)

The ecosystem is a collection of vendors, open-source projects, and communities that jockey to deliver value to customers in a cloud-native way.

A 2020 survey report from the Cloud Native Computing Foundation (CNCF) found that 95% of respondents use containers in the proof-of-concept (PoC), test, and development environments, and 92% use containers in production. (See Figure 5.) Kubernetes dominated the container market in 2020, with 91% of respondents reporting they use Kubernetes, and 83% of them using it in production.

New Use Cases	• Hybrid and multicloud • Edge computing
Technology Evolution	• Service mesh • Convergence of serverless iPass on Kubernetes • Bare-metal containers and microVMs
Ecosystem Maturity	• Third-party ISV support for containers • Support for stateful applications • Maturing projects beyond Kubernetes

Figure 4: Cloud-native emerging trends
Source: Gartner

12. "CNCF survey 2020: Use of containers in production has increased by 300% since 2016," Cloud Native Computing Foundation https://www.cncf.io/wp-content/uploads/2020/11/CNCF_Survey_Report_2020.pdf

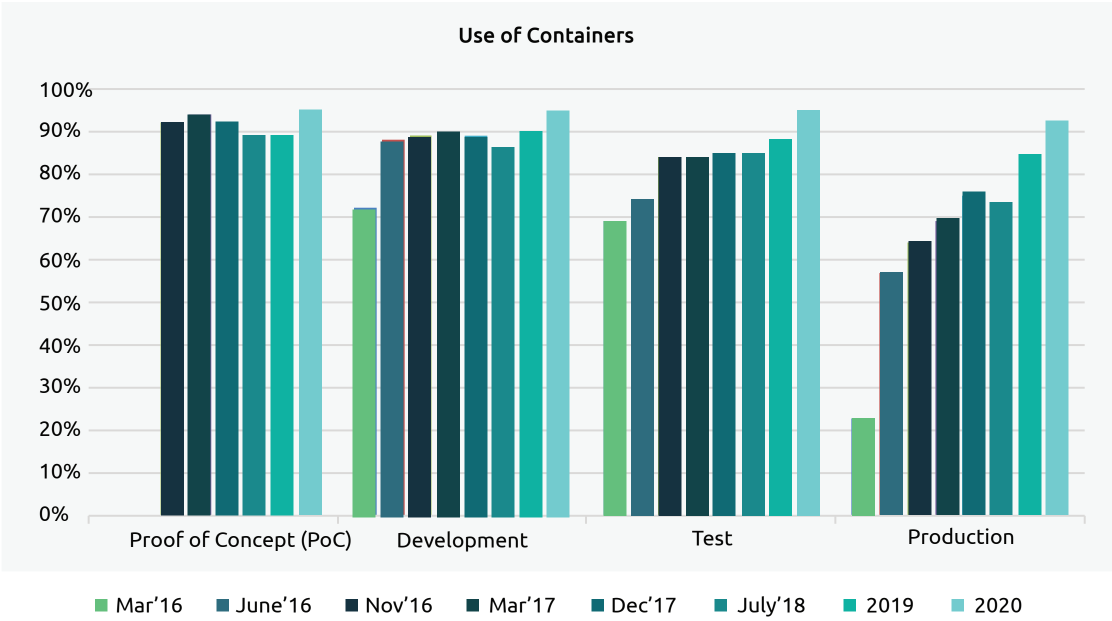


Figure 5: A steady rise in companies using containers – 2016-2020
Source: Gartner

According to a July 2021 Red Hat report, 88% of respondents said they use Kubernetes as their container orchestrator, with 74% using it in production. [13]

According to 51% of respondents, Amazon's EKS is the most widely used Kubernetes platform. (See Figure 6.)

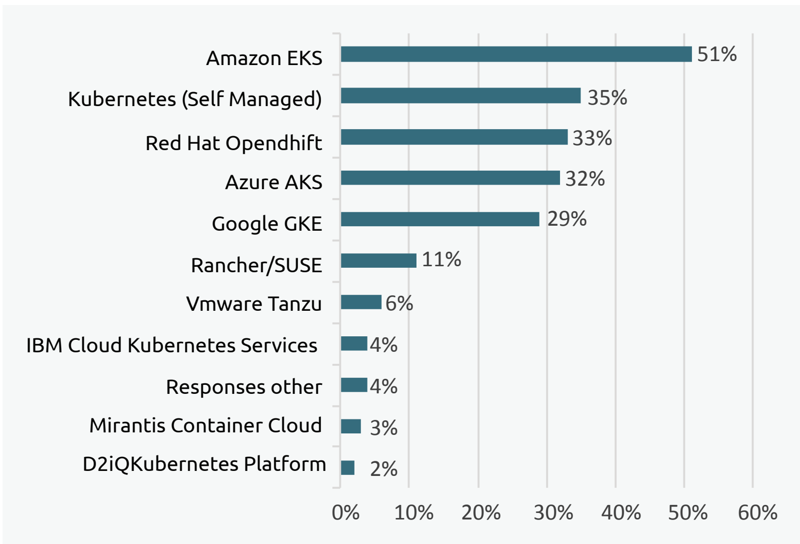


Figure 6: What Kubernetes platform do you use to orchestrate your containers?
Source: Red Hat

IDC reports that microservices have gained wide adoption and companies are now in the early phase of scaling out their architectures.[14] Microservices apps are already used in business-critical roles, with 24% of microservices apps identified as business-critical. According to IDC FutureScape, by 2022, 90% of all apps will feature microservices architectures that improve the ability to design, debug, update, and leverage third-party code; 35% of all production apps will be cloud-native.[15]

13. "Kubernetes adoption, security, and market trends report 2021," Jul 14, 2021, Red Hat State of Kubernetes Security Report https://www.redhat.com/en/resources/kubernetes-adoption-security-market-trends-2021-overview
14. "The Impact of Application Modernization on the Data Layer," IDC InfoBrief sponsored by Redis Labs https://redis.com/docs/application-modernizaton-impact-on-data-layer/
15. "IDC FutureScape: Multiplied Innovation Takes Off, Powered by AI, Distributed Public Cloud, Microservices, Developer Population Explosion, Greater Specialization and Verticalization, and Scaling Trust," Oct 30, 2018, IDC, Business Wire https://www.businesswire.com/news/home/20181030005105/en/IDC-FutureScape-Multiplied-Innova-tion-Takes-Off-Powered-by-AI-Distributed-Public-Cloud-Microservices-Developer-Population-Explosion-Greater-Specialization-and-Verticalization-and-Scaling-Trust

The CSP journey towards cloud-native solutions

In the last few years, CSP customers have been rapidly adopting cloud-native engineering solutions such as containers, microservices, and serverless architectures. These solutions deploy network functions and other applications and infrastructure as code (IaC) to avoid manual effort, focusing on a hybrid cloud approach instead of a private or public cloud solution.

- **From traditional to virtualization**: Virtualization creates an abstraction layer on physical hardware by using a hypervisor to enhance the system's operability and run multiple operating systems (OS) with the help of VM in a physical machine. Virtualization increases scalability, flexibility, agility, resource availability, performance, efficiency, and productivity and reduces downtime and cost. (See Figure 7.)

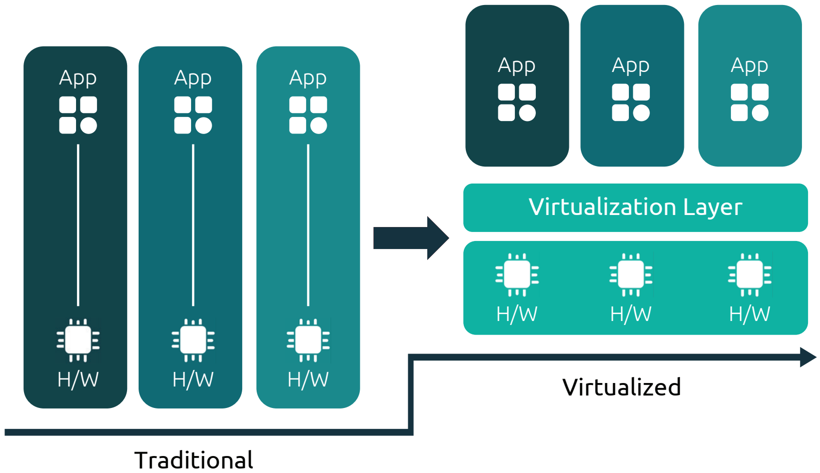


Figure 7: Traditional versus virtualization
Source: Capgemini Engineering

- **Virtualization to cloudification**: Clouds are IT environments with a set of principles and approaches that deliver on-demand computing resources such as servers, databases, storage, networking, and software over the internet. Clouds also use virtualization technology to increase productivity and performance and reduce operational costs. (See Figure 8.)

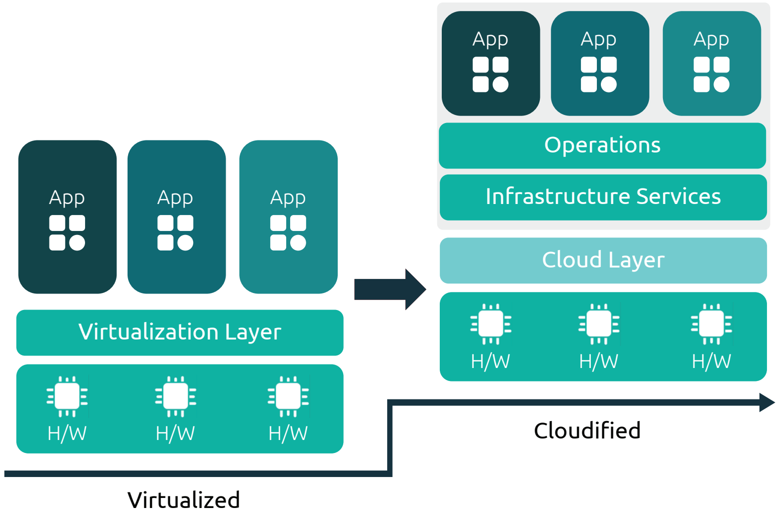


Figure 8: Virtualization versus cloudification
Source: Capgemini Engineering

- **From cloudification to cloud-native**: Cloud-native is an approach to building applications as a set of small, independent, and loosely coupled services and running them on containerized platforms that take advantage of the features of a cloud-computing environment. Cloud-native increases development speed and reusability and employs the CI/CD methodology and adopts the DevOps culture. (See Figure 9.)

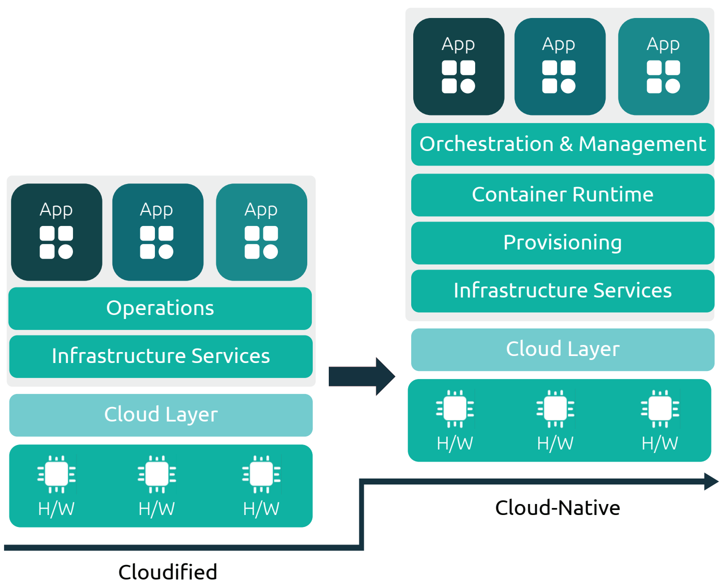


Figure 9: Cloudification versus cloud-native
Source: Capgemini Engineering

Benefits of cloud-native engineering for CSPs

Here are nine reasons to start the journey towards a cloud-native future:

- **Ensure a high degree of scalability**: CSPs migrating to the cloud can scale up or scale down their resources based on the requirement. By doing so, they can reduce costs as resource maintenance overhead is removed

- **Enable teams to focus on resilience**: Becoming cloud-native helps CSPs quickly recover from infrastructure issues, cyber-attacks, unpredictable network latency, transient faults, etc. In addition, the cloud-native landscape provides a well-architected approach that allows the system to self-heal

- **Faster release pace**: Telecommunications companies can innovate and deliver their products and services more quickly using cloud-native engineering. Now, applications use a microservices architecture that splits individual services into multiple independent microservices. In addition, they develop network software functions at the outset that take advantage of serverless computing functionality

- **Cost effective**: Cloud-native engineering leverages cloud resources and reduces an organization's operating and maintenance expenses. Serverless is a cost-effective method that lets CSPs run dynamic workloads in milliseconds using pay-per-use compute time. Being cloud-native allows staff time to focus on other revenue-generating functions

- **Superior customer experience**: Building a great customer experience, you need to ship new features fast and iterate constantly. Today, the focus is on liberating enterprise data by creating engaging customer and employee experiences. Cloud-native uses the DevOps methodology and helps CSPs reduce latency, strengthen security, provide automated customer support, predict customer preferences, and deliver new omnichannel digital experiences

- **Network automation**: Cloud computing helps automate manual processes such as designing, testing, deploying, orchestrating, and monitoring networks. Network automation can be achieved by continuous integration, continuous testing, and continuous deployment. As a result, modern networks can analyze their performance and respond to issues in real-time, which improves customer satisfaction

- **Avoid vendor lock-in**: Being cloud-native has many options to make infrastructure management more manageable. Today, with the proliferation of open-source and cloud technologies, hybrid and multi-cloud are becoming the norm. Enterprises typically use a combination of an on-premises datacenter and at least one public cloud platform. Even between cloud platforms, the conversation is graduated to enable portability in the cloud, so they never get locked into a single vendor

- **Generate new revenue streams**: CSPs can monetize their physical infrastructure by partnering with cloud service providers. Until recently, operators and hyperscalers were competitors. But partnerships between CSPs and cloud providers support further market growth. CSPs can offer their infrastructure to cloud providers to help bring customers to the edge by launching dedicated platform solutions for telecom infrastructure and integrating directly with 5G networks

Embrace the cloud-native discontinuity

Next-generation mobile networks will introduce many new network architectures and functionalities, which means network complexity will increase significantly. The cloud-native approach to network building is genuinely transformative. It fully automates the lifecycle management of network functions by providing rapid release, portability across private and public clouds, scalability, and continuous innovation with DevOps.

Unlike simple virtualization, cloud-native applications deliver efficiency, improve customer experience, and generate new revenue streams for CSPs. In addition, cloud-native engineering tools and strategies mitigate private cloud challenges and enhance network performance.

CSPs need to be aware of cloud-native behavior and the extent to which it represents discontinuity. Only companies ready to embrace the discontinuity inherent in a cloud-native approach will make it. Conversely, companies that stick with their current strategy and focus on vendor relationships are unlikely to survive.

Authors

Chhavi Chaturvedi
DevSecOps Engineer
Capgemini Engineering

Chhavi is part of the Product Services and Support team at Capgemini Engineering. She focuses on developing DevOps and AWS security solutions and delivering them to customers. Chhavi also has experience in public cloud security. She earned a master's degree in cybersecurity from the National Institute of Technology, Kurukshetra, India.

Sunny Kumar
Program Manager
Senior Cloud and DevOps Architect
Capgemini Engineering

Sunny is part of the Product Services and Support team at Capgemini Engineering. He is responsible for helping customers with their cloud and DevOps transformations.

Capgemini engineering

About Capgemini Engineering

Capgemini Engineering combines, under one brand, a unique set of strengths from across the Capgemini Group: the world leading engineering and R&D services of Altran – acquired by Capgemini in 2020 - and Capgemini's digital manufacturing expertize. With broad industry knowledge and cutting-edge technologies in digital and software, Capgemini Engineering supports the convergence of the physical and digital worlds. We help clients unleash the potential of R&D, a key component of accelerating their journey towards Intelligent Industry. Capgemini Engineering has more than 52,000 engineer and scientist team members in over 30 countries across sectors including aeronautics, space and defense, automotive, railway, communications, energy, life sciences, semiconductors, software, and internet and consumer products.

For more information please visit:

www.capgemini-engineering.com

Contact us at:

zerotrustblueprint@capgemini.com