



# Telecom SaaS for Dynamic, Scalable Networks

Understanding the benefits, overcoming the  
barriers and seizing the potential

NOKIA



Mobile connections will grow 3.5 times from 2023 to 2030<sup>1</sup>

3.5X

Half of all data will be processed at the network edge<sup>2</sup>

+50%

The network API market is forecast to reach 35B USD by 2023<sup>3</sup>

Source: STL partners "Network API forecast" report, May 2024

35B USD

47% of the global population is unserved or underserved by modern communications technology<sup>4</sup>

47%

# To thrive in the 5G era and beyond, CSPs must evolve their networks

The low-latency, high-capacity connectivity made possible by 5G is enabling new kinds of services, applications and business models. Eager to reap the benefits, enterprises are increasingly looking to deploy artificial intelligence and machine learning (AI/ML), virtual and augmented reality applications, Internet of Things (IoT) an increasingly growing number of devices, and other 5G-enabled innovations.

But even as 5G rollouts become more widespread, its full potential remains largely untapped because it has been challenging for communications service providers (CSPs) to generate a return on their 5G investments.

## 5G is transforming the communications industry

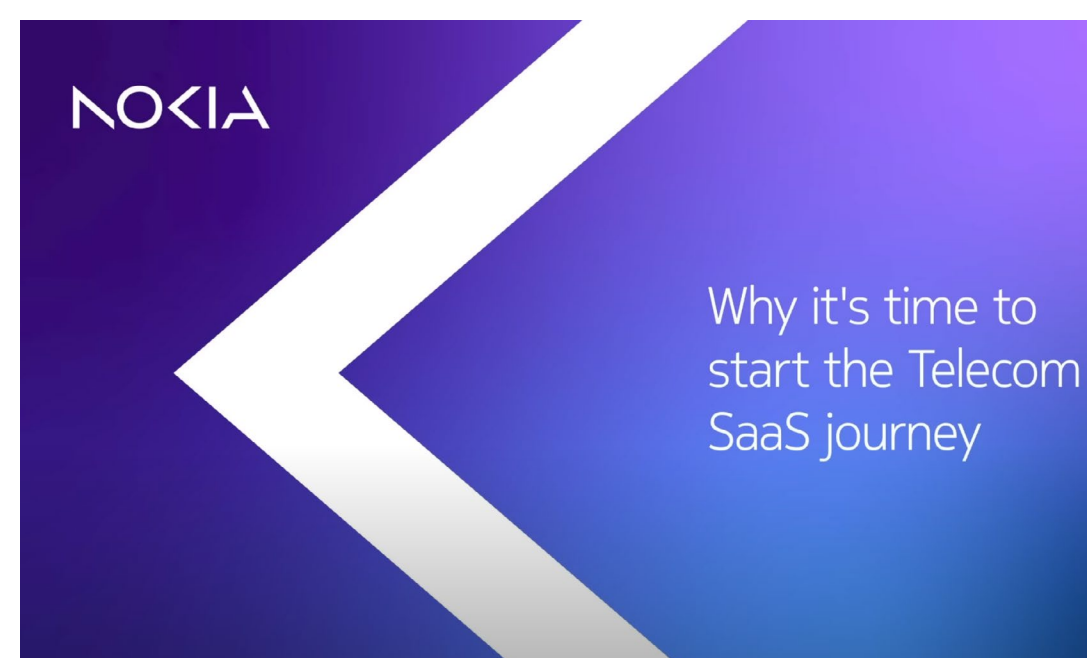
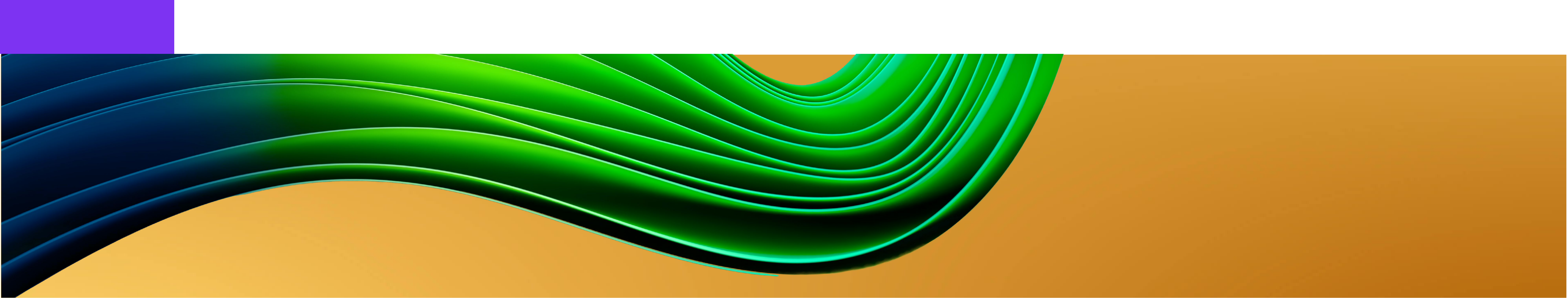
The complexity of 5G has revealed the limitations of traditional network management models, making it difficult and time-consuming for CSPs to develop new features and services for the enterprise market. Adding pressure is a massive boom in mobile connections.

[The number of connections is projected to grow 3.5 times from 2023 to 2030<sup>1</sup>](#), with two-fold growth in IoT and machine-to-machine connections expected over the same period. CSPs need to scale and adapt their networks to support growing numbers of devices, especially as enterprises embrace IoT and Industry 4.0 technologies.

The real-time data demands of 5G applications are also pushing data processing closer to the point of consumption: the network edge. This trend will continue as the network becomes more distributed, [with more than half of enterprise-managed data being created and processed at the network edge by 2025<sup>2</sup>](#). CSPs will need to strengthen their edge computing capabilities to adapt.

The challenges facing CSPs are deepened by the fact that nearly half the world's population is still unserved or underserved by modern communications technology. According to the United Nations, almost [3.6 billion people globally have no Internet connectivity at all.](#)





### VIDEO: Why it's time to start the telecom SaaS journey

CSPs are grappling with the challenges brought by rising network complexity, explosive mobile traffic growth and the increasing need for edge computing capabilities. [Watch this 90-second video for an overview of why telecom SaaS is the solution.](#)

In the past, CSPs overbuilt their networks to address demand and reach underserved geographies. Instead, CSPs can act on the opportunities that lie within these challenges by applying the software-as-a-service (SaaS) model to their network management functions.

### SaaS is the key to unlocking 5G's potential

Many CSPs already use SaaS on the IT side, subscribing to everything from productivity suites like Microsoft 365 to customer relationship management platforms like Salesforce.

That's because SaaS offers greater flexibility, scalability, cost-effectiveness and other advantages over traditional ownership models. With telecom SaaS, that same

approach is applied to telecommunications network management and operations functions. It empowers CSPs with new levels of operational efficiency and agility so they can accelerate service rollouts and reduce capital costs.

Together with technologies like automation and AI, telecom SaaS is part of a broader transformation CSPs must undertake to drive greater business agility while managing higher traffic volumes and evolving enterprise market demands — and find greater success in the 5G era.

### Starting the telecom SaaS journey

It's understandable for CSPs to have reservations about telecom SaaS. It marks a significantly different way of doing things,

using a proven IT service delivery model that has nevertheless only recently been applied to the telecommunications context. But CSPs' reservations are largely due to how new it is, driven by misconceptions about what telecom SaaS is and how it works.

This e-book will provide the understanding CSPs need to embrace telecom SaaS with confidence. It starts with a clear explanation of telecom SaaS. It covers the many benefits of this new approach and demonstrates its advantages over non-SaaS deployments for key applications. And it addresses the three most common hurdles to telecom SaaS, helping CSPs overcome concerns about total cost of ownership (TCO), loss of control and security in the public cloud.





### **VIDEO: Turbocharging 5G innovation with telecom SaaS**

For a deeper dive on how telecom SaaS can accelerate time to value and lower TCO in the 5G era, [watch the panel discussion with Nokia's President of Cloud and Network Services, Raghav Sahgal, and Forrester Research Principal Analyst Dan Bieler.](#)

# What is telecom SaaS?

Traditionally, CSPs have accessed the software they need to run their operations through custom, on-premises infrastructure. But this approach is holding them back. To manage the complexity of 5G and meet the fast-evolving expectations of their customers, they need a new way of doing things.

They need telecom SaaS.

### **A new model for a new era of telecommunications**

With telecom SaaS, CSPs access their business and operations software through the public cloud, paying usage-based subscription fees on periodic basis. The applications themselves and the underlying cloud infrastructure are managed by the SaaS provider. This approach removes the responsibility from CSPs of having to purchase and manage on-premises servers

and other hardware to support the applications they use.

Server capacity planning and maintenance also fall under the SaaS provider's responsibility. When a new SaaS offering is enabled, the service will scale up to provide all the capacity that application requires.

Similarly, as business needs change, the service can scale down to ensure the CSP isn't paying for more cloud resources than they need. The CSP also doesn't have to spend any time downloading updates or installing new versions of the software because the SaaS provider handles any patches or upgrades that are required.

### **How telecom SaaS differs from IT SaaS**

The concept behind telecom SaaS is the same as any IT SaaS offering. Both types of SaaS services are bought as a subscription,

with fees typically tied to usage and paid on periodic schedule, and both are based on cloud-native software. Where they differ substantially is in the level of availability, resilience, performance and security.

No business wants to be left without access to a key application, but the reality is that SaaS workloads in the cloud do sometimes go offline. When it's an IT SaaS application that's unavailable, the disruption to day-to-day activities may be inconvenient but something many businesses can endure. The situation is different for CSPs, who must meet strict service-level agreements (SLAs) with their customers. Because of this, any amount of downtime can come with significant financial or reputational consequences.

That's why telecom SaaS offerings are engineered for extreme reliability. As cloud-native software, telecom SaaS applications are containerized, meaning they're packaged with everything they need to operate. Those containerized applications are hosted on secondary servers and can be spun up in moments should the primary host fail. Applications are also hosted at the edge cloud, where they're much closer to the end user and their devices. This helps ensure the ultra-reliable low-latency communications and rapid round-trip times that enterprise customers require for their industrial robots, augmented reality, autonomous vehicles and other Industry 4.0 applications.

Specialized capabilities like these extend to other areas critical to CSP services and operations. In short, the main difference between telecom SaaS and IT SaaS is that telecom SaaS is engineered to provide carrier-grade availability, scalability, resiliency, performance and security through the cloud, with all the advantages that entails.

### SaaS is the way forward for CSPs

Accessing operations functions including network management, provisioning, security, analytics, billing and more through SaaS represents a major shift in how CSPs do business. But given the widespread adoption of SaaS platforms by businesses around the world, most CSPs likely already have a significant SaaS presence on the IT side. As the SaaS market continues to grow, more cloud-native telecommunications functions will appear — and it will be in CSPs' best interests to take advantage.

Many of the same benefits IT SaaS applications offer can be gained through telecom SaaS, and these will be critical to success in the 5G era and beyond. Advantages of telecom SaaS deployments like enhanced business agility, lower-cost scaling and accelerated innovation are what will allow CSPs to meet the needs of customers and markets that are moving faster than ever before.

More than 90% of enterprises worldwide use SaaS in some form<sup>1</sup>

>90%

SaaS will account for 23% of CSPs' total spend on OSS/BSS by 2027<sup>2</sup>

23%

SaaS can reduce time to market for new services by 69% to 77%<sup>3</sup>

77%

CSPs can reduce IT costs by 25% over five years by moving to telecom SaaS<sup>4</sup>

25%



Figure 1: Telecom SaaS benefits at a glance



# Telecom SaaS empowers CSPs to unlock the full potential of 5G

CSPs can benefit in significant ways by adopting telecom SaaS solutions for analytics, security, network management and other operational functions. With on-demand access to the applications they need to run their businesses and networks, and free from the restrictions and resource requirements of on-premises infrastructure, CSPs can realize:

- Faster time to value
- Reduced barriers to innovation
- Increase business agility
- Improved reliability
- Reduced costs and energy consumption
- More robust security

## Faster time to value

CSPs are under constant pressure to innovate and launch new services to stay competitive and meet customer demands, but that can be challenging in conventional telecom environments. Complex on-premises infrastructure and highly customized software stacks mean any new product or service

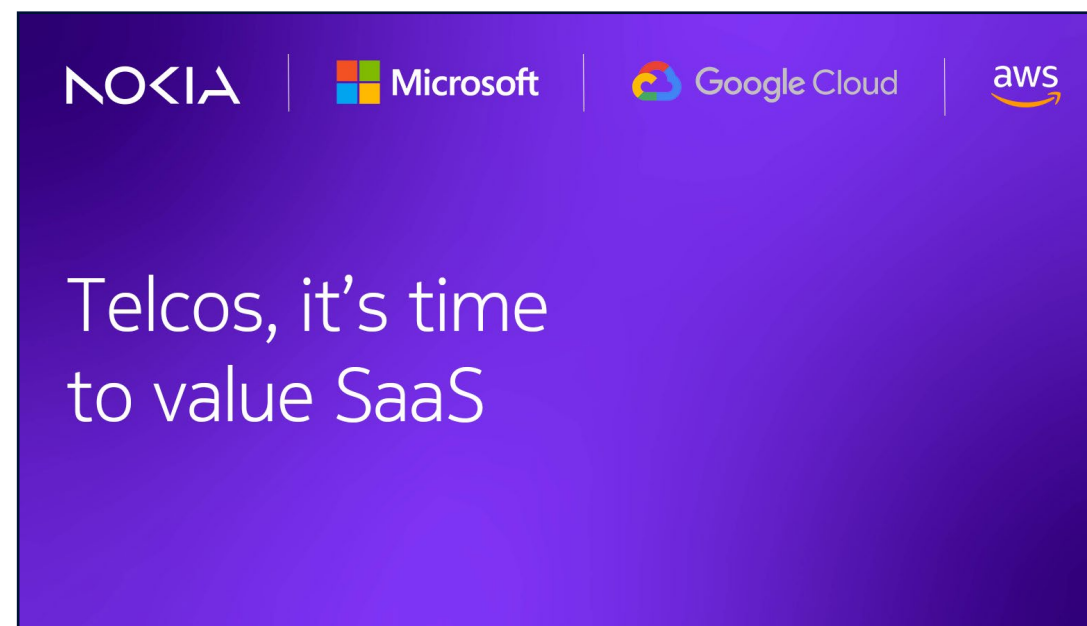
roll-out can require time-consuming and expensive changes to core systems.

With telecom SaaS, a CSP can easily and cost-effectively innovate, iterate and update with low upfront investment. This approach can reduce development time from months to days. It also lowers the cost of failure enough that CSPs can feel comfortable and encouraged to experiment with new products and services, moving on quickly from those that don't yield the desired return on investment.

## Reduced barriers to innovation

Traditional, on-premises telecommunications solutions tend to be expensive to buy and maintain. Telecom SaaS solutions are typically offered on-demand, with CSPs charged based on a more reasonable and affordable subscription- and usage-based model.

Transitioning to a SaaS model also accelerates procurement and deployment. This allows CSPs to experiment with many different services to understand the value they offer before committing long term.



### WHITE PAPER: Demystifying SaaS and public cloud security

Given what's at stake, CSPs understandably have many questions about SaaS data security when it comes to telecom SaaS. [Read the white paper for perspectives from security experts at Google Cloud, Amazon Web Services, Microsoft Azure and Nokia.](#)

### Increase business agility

Scaling up existing business and operations functions or introducing new ones is difficult under conventional telecom models. It often involves purchasing and installing new hardware that the CSP then must maintain along with the rest of their on-premises infrastructure. Telecom SaaS solutions are designed to be scalable, increasing or reducing capacity and adding or removing features as business needs evolve —without requiring expensive upgrades.

### Improved reliability

CSPs have long favored on-premises solutions because, if well maintained, they can offer carrier-grade reliability, achieved by offering five-nines availability (i.e., 99.999% service uptime). As the cloud has evolved, that same level of reliability is now possible with telecom SaaS. CSPs also benefit from offloading responsibility for the overall performance of underlying infrastructure to the SaaS provider, which includes updates and maintenance.

### Reduced costs and energy consumption

On-premises telecommunications infrastructure often comes with significant power and cooling needs, which is why [energy can account for 15% to 40% of a CSP's operating expenses. Each new deployment only adds to the energy costs CSPs must cover.](#)

Telecom SaaS reduces costs for CSPs by moving the infrastructure required for network operations and management into the cloud, where it becomes the responsibility of the SaaS provider. This not only helps CSPs lower their operating expenses, but also makes it easier to meet their commitments to corporate social responsibility including ESG objectives, comply with environmental regulations and strengthen their brand in an increasingly eco-conscious world.

### More robust security

SaaS and public cloud security is more comprehensive and rigorous than ever before. Cloud providers invest a great deal

of resources into security technologies

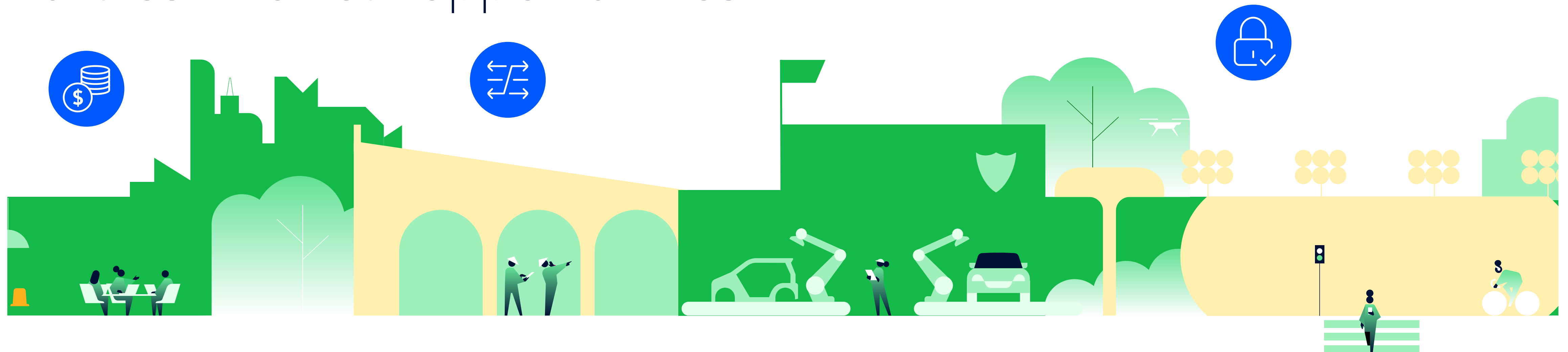
and procedures to prevent data breaches and maintain their customers' trust. Overall, the level of security CSPs can expect from telecom SaaS deployments is on par with — if not superior to — traditional on-premises software deployments.

Telecom SaaS security isn't just about preventing data breaches - It also ensures complete confidentiality and 100% data integrity at the appropriate level of availability based on robust, role-based access controls.

By deploying a SaaS-based solution, CSPs can effectively transfer some of the risks of security management to the SaaS vendor.



# With the right understanding, CSPs can turn telecom SaaS hurdles into real opportunities



Despite the many benefits of telecom SaaS, some CSPs are reluctant to access their network management and operations functions through the cloud. Three hurdles in particular make it challenging for them to embrace telecom SaaS. But with a clear understanding of the realities of telecom SaaS, which the next few pages will provide, CSPs can overcome these hurdles and seize the advantages that will underpin their 5G success.

## Hurdle 1: Total cost of ownership

Many CSPs perceive the total cost of ownership (TCO) of telecom SaaS to be higher compared to the conventional perpetual licensing model, which involves an upfront cost to buy a software license and indefinite usage rights.

## Hurdle 2: Control

Technology leaders often prefer to maintain direct control over their hardware and software. This preference allows them to customize and configure each element to their exact specifications and choose when and how network software is upgraded. Consequently, some may be cautious about shifting to SaaS services, as they believe it might reduce this level of control.

## Hurdle 3: Security

Compliance and security officers might have reservations about sending workloads and data outside their controlled environments.

When this outside environment is the public cloud, it can raise concerns about the security, privacy, residency and sovereignty of data both at rest and in transit to and from the cloud.

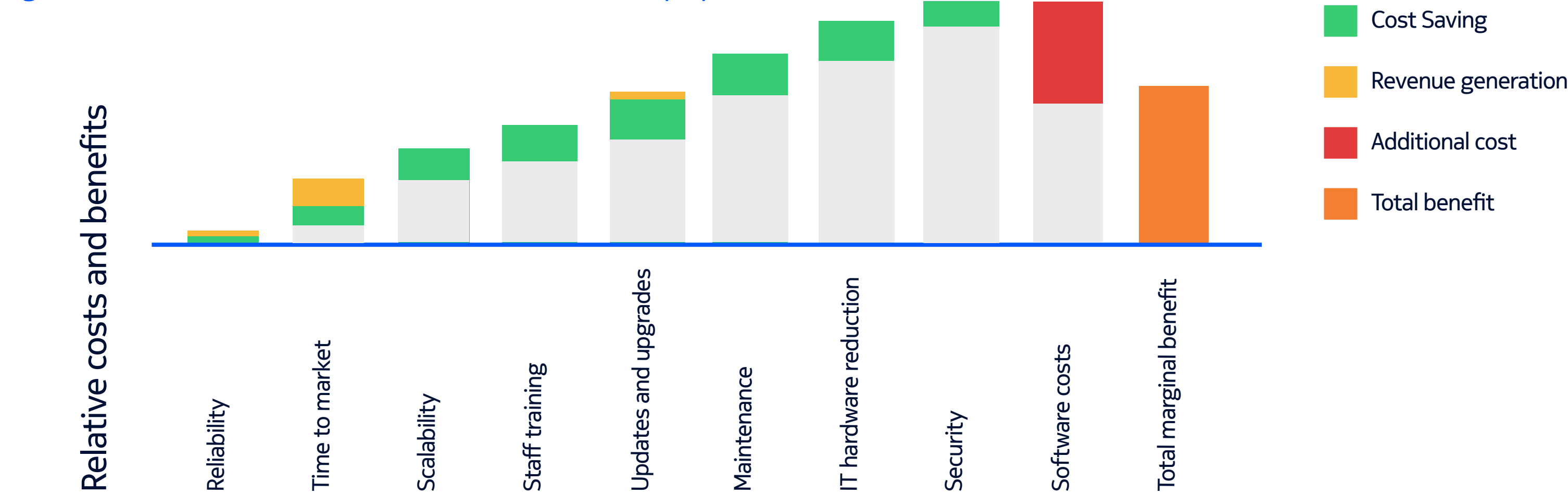


# Reality 1: The ROI of a telecom SaaS deployment exceeds long-term software costs

Most CSPs recognize that SaaS is a multi-period expense, with software costs distributed over time rather than upfront. Even still, the idea of perpetual licensing may seem better because it means a one-time cost rather than ongoing, recurring expenses. What this view misses are the many hidden operational costs of non-SaaS deployments.

For non-SaaS deployments, CSPs have to buy and use their own physical or cloud infrastructure. With this comes a wide range of additional costs related to logistics, power, cooling, storage, backup and disaster recovery, compliance with regulatory requirements, and more. The CSP is also responsible for managing and operating that infrastructure over time, and the software itself needs to be manually patched and updated to stay current. This requires in-house staff with the expertise to carry out these responsibilities, which adds on hiring and training costs.

Figure 2: Estimated relative costs and benefits of SaaS deployments



None of these responsibilities or their costs apply to the CSP using telecom SaaS. Instead, the SaaS vendor takes on those tasks in exchange for an all-inclusive subscription fee, predictable periodic fee. This makes it easier to forecast financial spending and also spreads out investment risk over time, with some of that risk shared with the SaaS vendor.

everything accounted for, [moving to a telecom SaaS deployment can reduce CSPs' IT costs by 25% over five years.](#)

### Beyond cost savings

SaaS deployments can also help generate revenue to offset the recurring expenses. CSPs can easily scale up capacity to test new products and services. If a pilot project

succeeds, the CSP can bring it to market much faster — and start monetizing it sooner — compared to a non-SaaS deployment. Otherwise, the CSP can simply scale the service back down, incurring a lower cost of experimentation than with an upfront, on-premises investment.



# Reality 2: Telecom SaaS empowers innovation and strengthens competitiveness

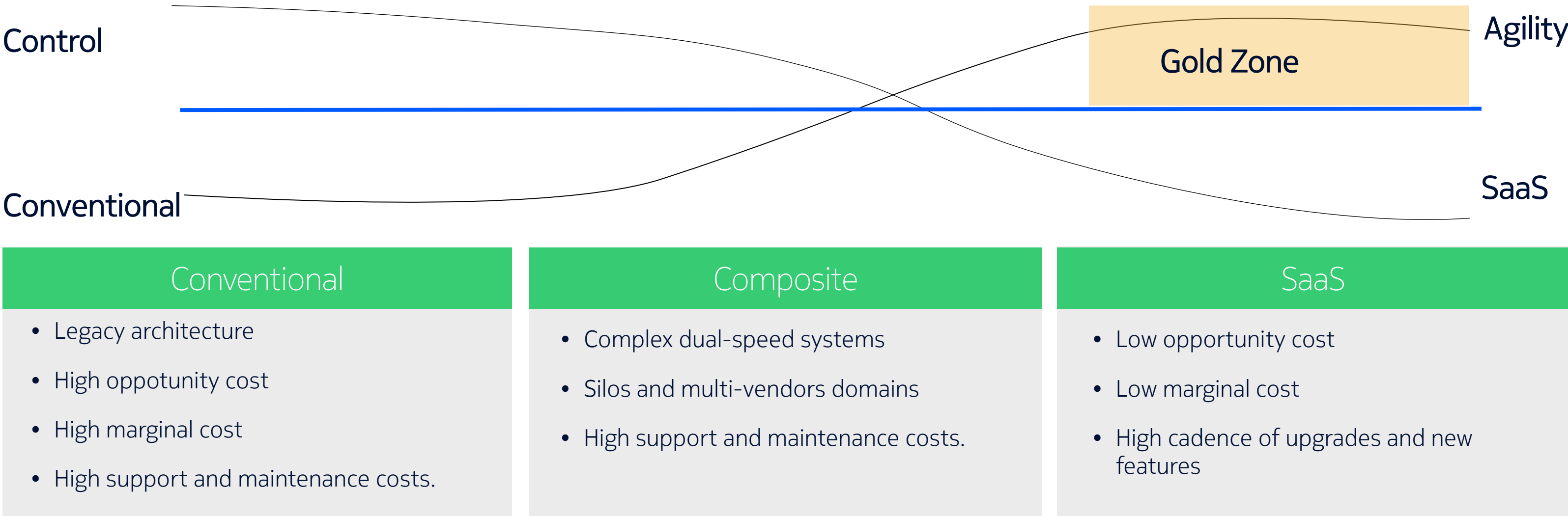
Telecom SaaS solutions offer very granular management of operations and accounting. CSPs can see their exact SaaS usage and spending, review incidents, and more — providing a level of visibility that’s not always present in self-managed, non-SaaS software.

A SaaS deployment also changes what CSPs have control over compared to traditional models. In doing so, SaaS can unlock new opportunities that weren’t possible before. That’s because the in-house resources can focus on more strategic business priorities, instead integration and operation functions that now fall under the SaaS vendor’s responsibility can instead focus on more strategic business priorities. That might include launching new value-added services or building application development ecosystems.

### SaaS as an innovation engine

SaaS environments are particularly well suited to the kind of innovation a CSP’s employees might engage in without the time-consuming responsibility

Figure 3: Comparing control and agility for conventional vs. SaaS models



Source: Appledore Research. Agility with Control

of creating and managing their own technology components. Application developers can use software development kits and APIs to embed network capabilities and SaaS components into their offerings to create new kinds of apps and experiences. To trial these, CSPs can scale their service up or down as resource requirements demand — and more rapidly bring to market

the experiments that prove a success. Under this model, CSPs are liberated from the limitations of underlying systems. With that comes greater business agility, empowering CSPs to reach the “gold zone” — the optimal space for seizing new opportunities with minimal cost investment.

Ultimately, CSPs need to compare the benefits of retaining direct control over hardware platform sizing, purchasing and lifecycle cost management and other conventional areas, with those they stand to gain in agility and innovation by embracing SaaS. They might find that those traditional functions are best left to an expert partner.



# Reality 3: Telecom SaaS is as secure as on-premises software, if not more so



Data security and privacy are critically important to CSPs, so it's understandable why they may be hesitant to embrace a new model where they no longer own all aspects of the network. When it comes to telecom SaaS, four common areas of concern for CSPs are:

- Data security: Ensuring the confidentiality, integrity and availability of all data, including personal data.

- Data residency: Maintaining knowledge of and control over the location of data.
- Data privacy: Controlling access to and providing protections for the collection, use, storage and deletion of personal data.
- Data sovereignty: Keeping data under the control and laws of a specific jurisdiction.

SaaS environments are as secure as traditional on-premises software deployments, if not more so. Cloud providers and SaaS vendors invest substantially

more in security systems, technologies and capabilities than many CSPs can match. That includes spending specifically to address the areas of data security, residency, privacy and sovereignty. This heavy investment in security is vital to their business: just one data leak or breach could ruin their reputation.

## Ensuring data security in the cloud

SaaS vendors employ robust security frameworks to meet their customers' expectations of data

security. That includes working with customers and partners to clarify each party's responsibilities for securing data and services in the cloud. Under the Shared Responsibility Model, cloud providers are responsible for securing the infrastructure on which their cloud services operate, SaaS vendors for security within the cloud, and CSPs for protecting the data stored in the cloud (i.e., by implementing strong identity and access management controls on their endpoints).





To meet their responsibilities, SaaS vendors use a multi-layered, defense-in-depth approach. This includes application security, operational security managed by a dedicated team, role-based access control, real-time threat and data theft protection, vulnerability management (e.g., penetration testing), and regulatory compliance and certification assurance. Cloud providers and SaaS vendors also bring extensive knowledge in areas like regulatory compliance and data encryption, based on their experience in delivering cloud services to enterprises worldwide.

#### **Protecting the privacy of data**

The fact that telecom SaaS uses the public cloud is of particular concern to CSPs, as they may believe this gives the cloud provider and SaaS vendor unrestricted access to any data stored there. In fact, cloud providers enforce strict data isolation policies that prevent access without a customer's authorization. Cloud providers and SaaS vendors also employ end-to-end security controls across all layers of the public cloud, advanced encryption to protect data at every stage, and zero-trust security principles for effective identity management.

On the compliance side, cloud providers and SaaS vendors maintain fully certified teams — both to serve their customers' compliance needs and to ensure their own compliance with the data privacy laws and regulations in the jurisdictions in which they operate. Independent audits verify their ability to comply with those regulations and standards.

#### **Dictating where data is processed and stored**

CSPs and other enterprises may be subject to data residency laws, which require that data stay within their country's national borders rather than being processed and stored in an outside jurisdiction. Recognizing this, many cloud providers give customers the option of where their services are physically hosted. Customers retain this control over where their data is processed and stored at all times, backed by contractual assurances.

#### **Maintaining data sovereignty in the cloud**

While data residency specifies the jurisdictional boundaries in which data must be processed and stored, data sovereignty concerns who has the rights and control over that data based on where the processing and storage is happening. Set by national governments, data sovereignty requirements typically demand greater levels of transparency and control over data than would normally be the case in the cloud. This might include enabling customers to choose the exact jurisdiction their data is processed in, establishing operations to run data locally, and adjusting security processes to ensure control of certain entities remains within specified borders.

Some cloud providers can offer such features and controls as required. This ensures in-house CSP security teams retain full oversight and authority over data flowing through a telecom SaaS service, supporting compliance with data sovereignty requirements.



**WHITE PAPER: The role of AI-based solutions in controlling energy use**

High energy prices and regulatory demands are pressuring CSPs to make their networks more energy efficient — without affecting the customer experience. AI-based software delivered as a service can dynamically adjust energy consumption with network performance to meet CSPs' sustainability goals while maintaining quality of service.

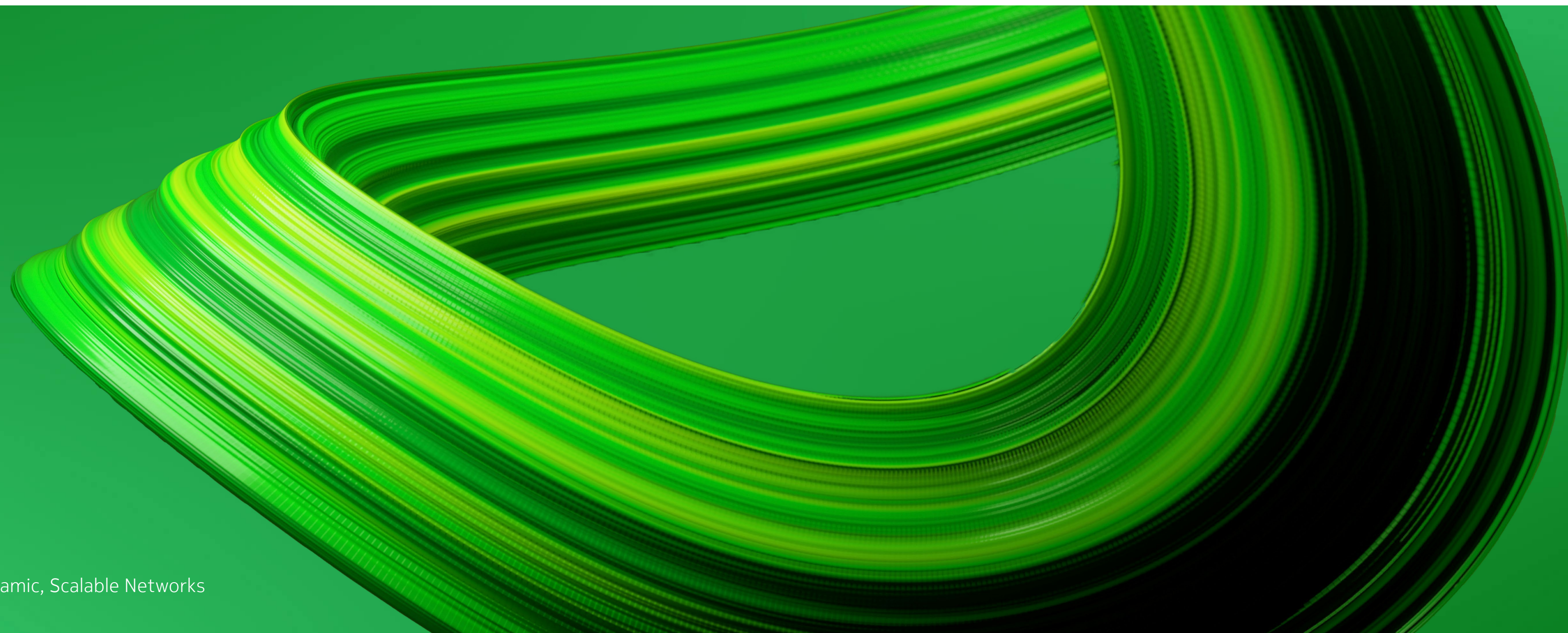
[Read the full white paper.](#)

# How Nokia helps secure and deliver SaaS at scale

Nokia SaaS is designed for the telecom industry, based on our deep telecom domain knowledge — so you can trust that our SaaS environment is reliable, secure and tailored to your specific challenges and opportunities.

Our mission is to create technology that helps the world act together by delivering innovative, contemporary SaaS networks and services, and by enabling our customers to rapidly deliver new, profitable communications services to their respective markets. With a breadth and depth

of portfolio unmatched in the industry, Nokia can help you meet your business goals and stay ahead of the competition







### How Nokia helped NTT and NTT DOCOMO enable in-network computing

The popular belief is that advanced applications like extended reality (XR), AI-powered video analysis and the metaverse require devices with high processing power. NTT and NTT DOCOMO want to change that so customers can access demanding applications like these on any device. To achieve this, the company developed an in-network service acceleration platform (ISAP) that offloads data processing from devices and leverages the cloud to deliver services that require high processing power, like 3D rendering, with low latency regardless of a device's specifications.

Nokia's 5G core SaaS offering, which enables the ISAP to dynamically allocate network resources to support near-edge computing based on the performance of mobile devices and the processing demands of services. Together, ISAP and 5G core SaaS have demonstrated the potential for in-network computing to bring high-performance 5G use cases to any device — and to serve as the foundation for future, 6G-era applications.

### How Nokia helped Elisa accelerate time to value

Automation has been a focus for Elisa for more than a decade as it looks to achieve greater business agility and operational efficiency. To advance its efforts in a world of increased operational complexity, Elisa was in search of automated solutions built specifically for the 5G era. The company was already familiar with the SaaS model, having adopted IT SaaS many years ago for Salesforce, Workday and other applications.

Nokia and Elisa partnered to experiment with new kinds of 5G-enabled services and experiences in the Nokia Arena in Tampere, Finland. This included use cases based on virtual and augmented reality experiences for hockey games, concerts and more. The partnership, supported by an ecosystem of app developers, is a strong example of the innovation potential of telecom SaaS, which made it faster and more cost-effective for Elisa to test out pilot projects like those staged at the Nokia Arena.





# Nokia can enhance key network management and operations functions with telecom SaaS — today

## 5G core

To manage growing traffic volumes and create new sources of revenue, CSPs must move away from the static, monolithic core network functions of previous generations. A scalable core allows CSPs to quickly meet enterprise demands for Industrial 4.0 applications, the metaverse and other network-intensive innovations. Through APIs, they can expose core network capabilities to facilitate collaboration with partners in the B2B2X value chain.

With Nokia [5G core SaaS](#), CSPs have more time and resources to dedicate to other business priorities — like creating new services to generate ROI from their 5G assets.

## Cybersecurity

The longer a security breach takes to detect, the higher the damages and costs a CSP will incur. The trouble is that with the high volume of network activity,

it's more challenging than ever for them to quickly detect breaches so mitigation can start as soon as possible.

[Nokia NetGuard Cybersecurity Dome](#) gives CSPs automated, SaaS-based security that shortens response times and greatly reduces how long it takes to remove an attacker once detected.

## Smart analytics

Software analytics help CSPs draw insights from the data that passes through their network, which they can use for a range of strategic purposes: from optimizing energy consumption to enhancing the customer experience.

With the Nokia AVA suite of analytics solutions, CSPs can drive improvements across their operations with insights and recommendations powered by AI/ML. It includes functions for [customer and mobile network insights](#), [Network Data Analytics function](#), [fixed network insights](#), and [energy efficiency](#).

Nokia's telecom SaaS framework allows CSPs to deploy these solutions over their preferred public cloud for a lower TCO than traditional models.

## Charging

To support the monetization of 5G, [many CSPs are looking to migrate their business support systems to the cloud, with real-time charging the top priority](#).

[Nokia convergent charging solutions](#) provide real-time rating and charging capabilities that empower CSPs to support and monetize new 5G use cases while providing an optimal experience for consumers and enterprises. The telecom SaaS version (Nokia AVA Charging as a Service) accelerates 5G business support system transformation, offering CSPs the fastest track to a charging system that's suited to the dynamic needs of the 5G era.

[Experience telecom SaaS in action with an interactive demo](#)



# Voices of the customers

**NOKIA** | **O2 Telefónica**

“SaaS is not new for us in general. We want to change the entry barrier in Telecoms and therefore, we want to drive the SaaS revolution in the network.”

Mallik Rao  
CTIO, Telefónica Deutschland



**NOKIA** | **elisa**

“Telecom SaaS is not just about operational efficiency, but also the faster time to market.”

Markus Kinnunen  
Vice President Cloud Services, Elisa



**NOKIA** | **CITYMESH**

“We believe Nokia's Core SaaS will play an important role in strengthening Citymesh's position as a national B2B operator as we transition from MVNO to MNO and enhance our network operations.”

Robin Leblon  
Chief Technology Officer, Citymesh



**NOKIA** | **Globe**

“We're very pleased to expand our partnership with Nokia through its AVA for Energy SaaS solution. Efficient energy consumption is a strategic imperative for our network decarbonization initiatives and net zero targets.”


Yoly Crisanto  
Chief Sustainability and Corporate Communications Officer  
Globe Group



**NOKIA** | **Telia**

“Telco SaaS and telco APIs are important catalysts for creating new services and experiences for our customers.”

Jari Collin  
CTO, Telia Finland



**NOKIA** | **docomo** | **NTT**

“We're thrilled to showcase in-network computing for the future network in collaboration with NTT DOCOMO, NTT, and Nokia's 5G Core SaaS. Our partnership aims to explore use cases, architectures, and promote future network global standardization.”

Hiroyuki Oto  
Senior VP, GM of 6G Network Innovation Dept.  
NTT DOCOMO





# References

[GSMA report – The Mobile Economy 2023](#)

[United Nations Broadband Commission for Sustainable Development report – The State of Broadband](#)

[TBR Insight Center white paper – The Clear Business Case for Telecom SaaS](#)

[Valuates Reports market report – Global Software as a Service \(SaaS\) Market Report, History and Forecast 2016-2027](#)

[Analysys Mason research report – The A-to-Z of SaaS Purchasing](#)

[Analysys Mason white paper – Controlling energy use: the role of AI-based solutions](#)

[Appledore Research white paper – Agility with Control: How SaaS models will deliver a new era of competitiveness for telcos](#)

[Nokia white paper – Telcos, it's time to value SaaS: Demystifying SaaS and public cloud security](#)



Nokia OYJ  
Karakaari 7  
02610 Espoo  
Finland

Tel. +358 (0) 10 44 88 000

CID:214051

[nokia.com](https://nokia.com)



**About Nokia**

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2024 Nokia