Telcos, it's time to value SaaS

Demystifying SaaS and public cloud security

White paper

There is no issue of greater concern to telecommunications service providers (telcos) than data security. Relied on for critical services, telcos devote significant resources to protecting their customers and operations from unauthorized data access and disclosure. Up to now, that's made many reluctant to shift their network operations and management to software-as-a-service (SaaS) models that rely on the public cloud. But as cost savings, speed and business agility increasingly become competitive must-haves, telcos need to overcome this historical reluctance and seize the full benefits of SaaS. This white paper looks at how key questions around telecom SaaS security have been answered by leading public cloud providers including AWS, Google Cloud and Microsoft Azure, and SaaS providers such as Nokia.

Co-authored with:

Contents

Introduction

Trust is at the core of the relationships between telcos and their customers. It is earned by reliably handling and protecting massive volumes of data at rest, in transit and in use, and ensuring the uninterrupted availability of business-critical and societally essential services while meeting stringent security requirements.

What is telecom SaaS?

Telecom SaaS is subscription-based, cloud-native software service that delivers solutions to achieve specific business outcomes. It enables a fully digitalized business experience and fully automated services lifecycle for any carrier-grade network.

Given what's at stake, telcos have held back from adopting software-as-a-service (SaaS) for network operations and management. They're used to owning all aspects of the network and securing its perimeter how they see fit. Switching from on-premises infrastructure to the cloud might understandably seem risky.

Yet telcos are especially well positioned to gain by adopting SaaS because they can be both SaaS consumers and SaaS providers. By leveraging the services offered by SaaS and cloud providers, telcos can deliver subscription-based services to their own customers as interest grows in telco-specific SaaS offerings like network-as-a-service (NaaS) and network-slice-as-a-service (NSaaS).

This paper explores some of the key telco questions about SaaS data security and how they are addressed by leading cloud service providers. It is based on Nokia's extensive network security and operations experience as well as perspectives from experts at AWS, Google Cloud and Microsoft Azure.

> **"The stakes are incredibly high for telcos, so of course they're risk-averse. They need high availability, resiliency, assured performance — and data security."**
>
> Microsoft PRAMOD NAIR, LEAD SECURITY ARCHITECT, MICROSOFT

What influences telecom SaaS security?

As enterprises continue to adopt SaaS, they are proving the benefits of cloud-based software delivery: faster rollouts of new services and accelerated time to value, lower upfront capital expenses, automated software upgrades and generally greater agility to respond to market conditions as they evolve.

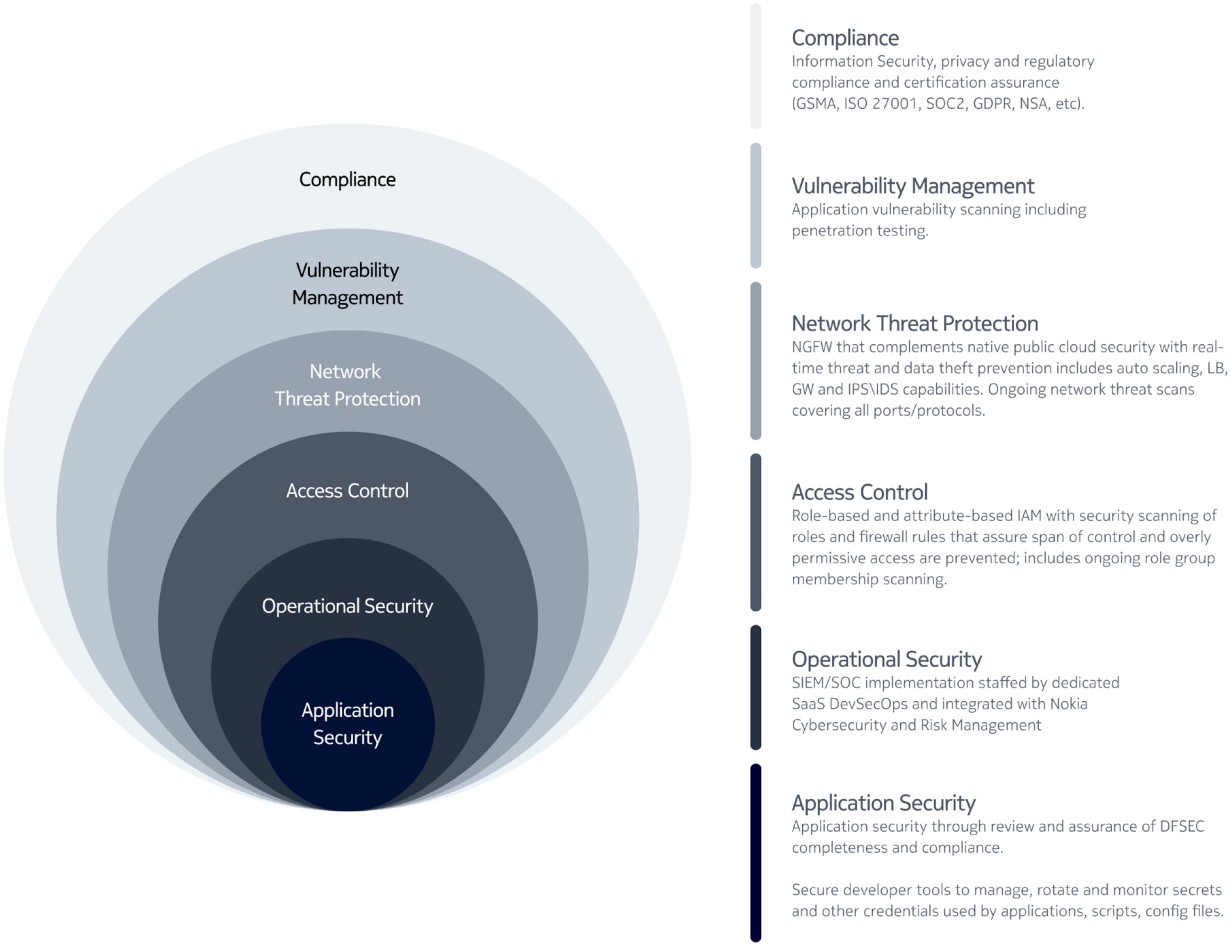
Telcos have been reaping similar benefits by adopting SaaS for business support system (BSS) functions such as order-to-cash processing, but have so far been reluctant to go all-in on SaaS for analytics, security assurance or network management due to concerns about data security, privacy, residency and sovereignty.

Security is key to getting full value from their investments in 5G, which requires evolving from closed pipe networks to open ecosystems. That demands zero-trust architectures, extended threat detection and response (XDR) capabilities, digital certificates and other strategies to mitigate risk.

The public cloud raises questions of how to ensure end-to-end security of SaaS data and workloads when the infrastructure is shared and provided by an external party. The answers involve three interdependent layers in telecom SaaS and the public cloud, each one the domain of a different party:

1. The infrastructure layer — offered by public cloud providers
2. The SaaS user's network layer — the traditional telco arena
3. The application layer — where SaaS providers deliver their services

Figure 1. Defence-in-Depth - Nokia CNS SaaS six security layers



One of the first and most important steps in any public cloud SaaS deployment is clarifying the relationships, responsibilities and boundaries among the parties responsible for these layers. This is commonly referred to as the Shared Responsibility Model, defined by the UK National Cyber Security Centre as:

> ...the fundamentals of who looks after the security of your data and services. As with any outsourcing agreement, there is a joint responsibility for the security and availability of data and workloads in a cloud service that is shared between the cloud provider and the customer of that service. The amount of responsibility that each party must own will depend on the type of service and how the service provider has chosen to implement it.[1]

Under the Shared Responsibility Model, cloud service providers are responsible for securing the infrastructure (hardware, software, networking and facilities) that their cloud services run on. Public cloud providers must adhere to international standards when designing and operating their security program and controls (i.e., protections and countermeasures put in place to minimize and facilitate response to security risks). Independent third-party auditors constantly verify this, issuing certifications and audit assessments that cloud service providers make available to their customers as proof they are fulfilling their portion of the Shared Responsibility Model.

SaaS providers (such as Nokia) are responsible for security within the cloud. That includes correctly configuring and managing any infrastructure services they use, and designing and operating their applications securely.

SaaS consumers (in this case, telcos) remain responsible for securing network content and complying with regulations. Their responsibilities include implementing proper identity and access management (e.g., strong passwords, multi-factor authentication, access and policy controls) and securely connecting to and using the SaaS (e.g., use of Transport Layer Security endpoints and properly configured encryption).

With this three-party model, telcos benefit from the cloud and SaaS providers' best practices and investments in security, resulting in a highly secure SaaS environment.

> **"It really is a shared responsibility, with the cloud provider securing the infrastructure and cloud services, the network vendors making sure their apps or network functions are secure, and the network operator handling security at that network and operational layer."**
>
> ISHWAR PARULKAR,
> CHIEF TECHNOLOGIST FOR TELECOM, AWS

1 National Cyber Security Centre, 2022. Cloud Security Guidance.

Telcos can trust SaaS security

Many industry experts believe that SaaS is as secure as on-premises software, if not more so. Just as telcos recognize the importance of the critical services they support, cloud service providers are relied on by customers in virtually every industry imaginable, including the highest levels of government, the financial sector and the military. At any point in time, at least one-quarter of the world's Internet traffic runs through the public cloud.

Because cloud service providers operate at scale, their security practices need to be uniform and designed for the highest levels of protection. This enables telcos to benefit from the same high standards used by organizations with the most stringent security requirements, such as banks. At the same time, serving many customers across all sectors around the world has given cloud providers unparalleled exposure and insight into security incidents and vulnerabilities, enhancing and accelerating their ability to identify, mitigate and prevent a broad range of cyber threats.

> "Cloud providers are under intense and constant scrutiny. Not a day goes by without them being audited or assessed. There's no hiding and no wiggle room for non-compliance. Their brands are at stake and they protect them mightily."
>
> PHILIP BLANCHAR, HEAD OF SAAS DELIVERY AND SRE OPERATIONS, NOKIA CLOUD & NETWORK SERVICES

As public cloud providers' brand reputations depend on maintaining security and privacy, they have made massive investments in technologies, people and resources to build top-tier capabilities in security at scale. Plus, the scale and economics of the cloud make it possible for cloud providers to invest more in security than any single enterprise alone. That includes spending on systems, technologies and techniques to address the four primary areas of SaaS concern, which apply to enterprises across all sectors (and not just telcos):

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 to benefit the individuals or organizations the data relates to.

Data sovereignty
Transparency and control over access to and transfer of data.

SaaS and data security

THE ISSUE: Protecting data from unauthorized access and rapidly identifying and containing security incidents when they occur.

Public cloud providers understand their businesses hinge on meeting customer expectations of data security. They provide extensive frameworks and systems, and work with customers and partners to ensure clear, mutual understanding of the responsibilities at each layer. Security is a core pillar of AWS' Well-Architected Framework, built into Google Cloud's trusted infrastructure approach and acknowledged by Microsoft Azure as "job one in the cloud". Nokia, as a SaaS provider, has its own array of security capabilities and commitments. While each entity may use different language, techniques and services related to security, their approaches are complementary, focusing on prevention and supported by a zero trust "detect and contain" stance.

Some specific elements used across leading public cloud and SaaS providers include:

- **Defense in depth:** Protecting data and other assets with multiple layers of security, network segmentation and boundary protection, traffic logging and monitoring, host-based intrusion detection and prevention, vulnerability assessments and remediation.
- **Isolation:** Ensuring system reliability engineers (SREs) and all other personnel can't access customer data, or the hardware that data runs on, without authorization. This would mean, for example, that an infrastructure SRE is restricted from accessing application workloads permitted for application SREs.
- **Encryption:** Encrypting hardware as well as data in transit and at rest.
- **Durability and availability:** Ensuring the integrity of customer data and its availability using technical measures such as backups and replication that ensure data is durable.

To build trusted relationships, cloud providers are transparent with customers about the controls they have in place to secure the cloud. "Transparency reporting has emerged as a valuable practice to demonstrate transparency and accountability," according to IDC[2]. This includes transparency with respect to the cloud provider's technical, contractual and institutional obligations, as well as providing timely and proper notification and reporting of any security incidents and the related regulatory mandates involved, such as the EU's General Data Protection Regulation (GDPR).

All major cloud and SaaS providers will provide audit reports when requested by customers, highlighting in detail which certifications they have received from organizations such as the International Organization for Standardization (ISO 27001), the Cloud Security Alliance (CSA), the GSM Association (GSMA), or System and Organization Controls 2 (SOC2) auditors and others. (By earning these certifications, cloud and SaaS providers relieve telcos from the burden of having to do the same, which can be a costly and time-consuming process.) The cloud and Saas providers will also provide detail on how they work to maintain compliance with security requirements.

To ensure data availability in the event a node dies or a data center goes offline due to a cyberattack or natural disaster, the cloud provider will replicate and sync the affected data to another data center in the same city or region. This provides the highest levels of resilience and availability while adhering to relevant data residency laws.

2 IDC, 2022. Trusted Cloud: Overcoming the Tension Between Data Sovereignty and Accelerated Digital Transformation

> “System security is critical for telecommunication companies. Cloud and SaaS providers must have verifiable controls and clear technical solutions both to ensure and demonstrate that their systems are secure.”
>
> Google Cloud NELLY PORTER, HEAD OF PRODUCT, CONFIDENTIAL COMPUTING AND ENCRYPTION, GOOGLE CLOUD

SaaS and data privacy

THE ISSUE: Ensuring compliance with privacy laws and regulations across multiple jurisdictions and regimes.

Data privacy is a complex and high-stakes issue for telcos and cloud providers alike. When customer privacy is impacted through unauthorized access to data, individuals may suffer, company reputations can be tarnished and stiff financial penalties may be triggered.

Europe has overarching privacy regulations and frameworks such as the GDPR and the Cloud Infrastructure Service Providers Europe (CISPE) Code of Conduct. Other jurisdictions, such as the United States, have multiple regulations and requirements that must be navigated carefully, such as the industry-specific Health Insurance Portability and Accountability Act (HIPAA) for health data and the Payment Card Industry (PCI) standard for payment card transactions. Public cloud providers have invested in conforming their privacy practices toward meeting these standards as applicable for their own and customers’ purposes, outside of consideration of telco workloads.

> “Our public cloud is tailored for local data privacy regulatory requirements and we offer customers the same secure-by-design infrastructure, built-in protection and global network that we use in our own daily business.”
>
> Google Cloud JAMBI GANBAR, PRODUCT MANAGER, TELCO, GOOGLE CLOUD

One of the most crucial types of data to protect is personally identifiable information (PII). Masking, tokenizing and/or removing PII data is not simple, and what’s classified as PII varies by organization and sector according to the determinations of regulators and corporate privacy and legal teams.

Cloud providers and SaaS providers dedicate significant time and resources to comply with data privacy laws and regulations in the jurisdictions and sectors where they operate. They are committed to a range of

tactics and techniques to safeguard data privacy, including:

- Maintaining **end-to-end controls** and clarifying responsibilities across the layers of the public cloud environment.
- **Restricting access, use or sharing of customer data** without permission except in very strictly defined situations. Even then, cloud providers have pushed back on law enforcement requests that seem too broad.
- Following disciplined processes for keeping **accreditations, certifications and regulatory knowledge** up to date.
- Using **confidential computing and externally managed keys** to encrypt data in use, at rest and in transit.

Privacy comes first, even when working with law enforcement

While cloud service providers and SaaS providers are committed to cooperating with law enforcement agencies to protect against cybercrime, fraud, terrorism and other unlawful activities, all requests to access data are scrutinized thoroughly. Any request considered to be excessive, inappropriate or in violation of privacy laws and regulations will be challenged. In the case of Nokia as a SaaS provider, if asked by a national government to provide data on a specific telco's users, Nokia refers the request to the affected telco customer and does not hand over the information directly. As part of transparency reporting, cloud service providers may also report on such requests from law enforcement and the actions taken in each case.

Cloud providers deploy policies and controls to protect data on their infrastructure. If a SaaS provider such as Nokia has access to a public cloud, only Nokia and its customers can access the related data: the cloud provider has no login permissions or privileges, and their systems and policies prohibit their own personnel from interacting with it except in strictly defined circumstances, such as by customer request or if access is essential to prevent fraud or comply with the law.

SaaS providers are subject to the same audit and assessment processes as major cloud providers. They must demonstrate network segregation to regulatory and certification bodies and show that no customer's data (including device identities, subscriber identities, SIM details and more) is inadvertently accessible to another customer or their own employees.

Nokia contains SaaS customer data within the secure and protected cloud instances that run the customer's SaaS solution. The data is not moved or allowed to leave that protected space without customer security and privacy review and approval — for example, if needed for some purpose outside the SaaS application.

Collaborative industry efforts such as GAIA-X are defining common approaches to data privacy within cloud infrastructure while enabling new technologies, applications and opportunities. Cloud providers are part of these initiatives, and many work directly with regulators to help them understand the cloud and align regulations with the cloud's capabilities.

SaaS and data residency

THE ISSUE: Ensuring control over the physical location of data.

Data residency laws mandate that data must stay within a country's national borders. That's why many cloud providers allow customers to choose where they want their services hosted. This is one of the principles of Cloud Infrastructure Service Providers Europe (CISPE) Code of Conduct: that customers can choose to store their data exclusively in the European Economic Area (EEA).

When customers store data in the cloud, they maintain control over where that data is stored and who has access to it. Cloud providers uphold those parameters with contractual assurances, helping customers with their technical and organizational compliance with data residency requirements.

Also available are hybrid options, where a portion of a service is always localized on-premises. In hybrid situations, the decision about what gets deployed to the cloud and what stays local depends on data privacy requirements as well as technical factors such as latency. New ultra-fast edge applications like those emerging with the rise of multi-access edge computing (MEC) and NSaaS offerings require a lot of local processing and make data residency decisions functionally significant. Enterprises that understand the risks associated with application failures and long-term disruptions will pay close attention to such considerations.

Customers can verify their SaaS and cloud service providers have the necessary controls in place by carefully reviewing their compliance programs and ensuring that contracts provide adequate protections.

> "Giving customers the choice of which region and 'availability zone' they want their data stored in — physically separate data center locations within the region — helps achieve enhanced resiliency and reliability for telco workloads deployed in the public cloud."
>
> Microsoft PRAMOD NAIR, MICROSOFT

SaaS and data sovereignty

THE ISSUE: Meeting the data sovereignty requirements of a specific jurisdiction.

Data residency addresses **where** data is stored. Data sovereignty provides for transparency and control over data. Sovereignty requirements are often imposed by national governments to protect critical industries or infrastructure, such as communications networks, defense installations and government systems.

The cloud value proposition is based on centralizing workloads across customers to realize benefits of cost, elasticity and economies of scale. However, data sovereignty requires more control over that process. Information and workloads must be specific to a region or community, bringing the cloud within

specified boundaries.

- Establishing operations in customer countries and **running data locally** in each country
- Enabling customers to choose the region in which their data is processed
- **Adjusting security postures** such as encrypting key generation so keys stay in the control of the right entities within the right borders

> "We are committed to offering customers the most advanced set of sovereignty controls and features available in the cloud to meet their digital sovereignty requirements without compromising on the capabilities, performance, innovation, and scale of the AWS Cloud."
>
> ISHWAR PARULKAR,
> CHIEF TECHNOLOGIST FOR TELECOM, AWS

Telcos can rest assured their security teams have full oversight and authority over their SaaS data. They will have final say concerning activity involving their data, including whether it needs to leave a specific environment or authorized location.

The telco's role in SaaS security

Under the Shared Responsibility Model, telcos that use SaaS applications have a direct part to play in security assurance. Adopting a zero-trust stance that assumes security incidents are inevitable is recommended for today's threat environment, with a focus on detecting and containing threats that enter the network.

Other aspects of zero-trust frameworks include defining data-recovery procedures; building on lessons learned from past incidents; implementing authentication, authorization and accounting (AAA) best practices; separation of duties; diligent logging, auditing and transparency; and end-to-end data protection. Automating manual processes and minimizing the need for direct access to data can also add to the protections.

While a lot of emphasis is placed on the technologies behind zero-trust and XDR security, ensuring the right steps are followed at the right times, every time is equally important.

Overall, there are six distinct SaaS security areas telcos can contribute to:

- **Application security:** Cloud providers maintain extremely secure infrastructure with strong data encryption, but security also depends on the strength and safeguarding of user passwords. SaaS providers will typically provide usernames and passwords for their offerings, but telcos are responsible for protecting endpoints against phishing, social media exploitation and compromised access. That involves implementing and enforcing stringent policies and processes around password management. Securing communication among applications and between applications and users requires controls

such as web application firewalls (WAF) to enforce stricter authentication and inspection of API queries. Telcos should implement foundational security controls based on secure development lifecycle (SDL) and continuous integration and development to strengthen their security posture, while software bill of materials (SBOM) mechanisms help identify vulnerabilities in open-source software components of cloud-native workloads.

- **Operational security:** The principle of least privilege — with a "default deny", need-to-know posture — should be applied to ensure users only get access to accounts and processes they need to perform their job duties. As with application security, telco operations staff must adhere to best practices and procedures for password and data sharing. To detect anomalies in all the different layers and domains of the network — from users and infrastructure to applications, automation and orchestration — telcos should also seek to establish end-to-end visibility.
- **Access control:** Two levels of access are typically granted for any application: one for regular users and one for administrators. Telcos should regularly review access controls for SaaS users, ensuring all accounts are valid by assessing if each user is still in a role that warrants their assigned level of access and capabilities. Structured approval processes are needed when granting new users access to SaaS applications. This ensures that, in the case of an audit, a telco can demonstrate why certain people were approved for higher levels of access, when the access was requested, when it was approved and by whom. It is also important to have clearly defined access-removal processes for auditing and compliance verification. These are often overlooked by many organizations.

> "Many telcos will give their own internally developed applications high levels of scrutiny but fail to review who has access to their external SaaS applications."
>
> NOKIA PHILIP BLANCHAR, NOKIA

- **Network threat protection:** If cloud connectivity is not secure, malicious traffic can cross over into the SaaS application. SaaS will be as vulnerable to cyber threats as the network it connects over. It's important for telcos to implement site-to-site VPNs, transport layer security (for API communication) and other secure methods of integrating with SaaS networks.
- **Vulnerability management:** Computers, mobile phones and remote access terminals also need to be secure in a SaaS scenario. Installing and maintaining anti-virus, anti-malware and anti-ransomware protection on devices, and implementing and enforcing policies such as prohibiting the use of removable media are essential.
- **Compliance:** If a SaaS provider is audited, customers can share evidence on its compliance with data security and privacy requirements. Telcos should be able to provide information like access logs or reports showing they are reviewing access levels on a quarterly basis.

Conclusion

Data security, privacy, residency and sovereignty are topics that telcos and other SaaS users cannot afford to dismiss. Given their responsibilities, it is absolutely right for them to interrogate the security claims of their SaaS providers and the cloud companies who host the services.

It is equally important for telcos to appreciate how comprehensive, rigorous and highly evolved SaaS and public cloud security are today. As this paper details, the technologies and procedures that are in place, and the resources that are dedicated to security, make SaaS and the public cloud highly secure, similar to traditional on-premises software deployments.

Telcos need the business agility, accelerated time to value and cost savings that SaaS delivers. They are already reaping similar benefits on the IT front with applications such as Microsoft 365 and Salesforce. With service-based architectures now available for 5G, telcos are better able to embrace the operational paradigms of the public cloud and SaaS than they were previously, when services were based on non-cloud-native architectures and telco-specific protocols. Moving network operations and management into the public cloud with SaaS is a natural evolutionary step rather than a big leap — and the key to unlocking a whole new era of benefits and capabilities.

About the authors

As a trusted partner for critical networks, Nokia is committed to innovation and technology leadership across mobile, fixed and cloud networks. Adhering to the highest standards of integrity and security, Nokia helps build the capabilities needed for a more productive, sustainable and inclusive world.

Philip Blanchar is Head of SaaS Delivery and SRE Operations for Nokia Cloud & Network Services.

Amazon Web Services (AWS) is one of the world's most comprehensive and broadly adopted cloud infrastructures, offering over 200 fully featured services from data centers globally. Millions of customers — including the fastest-growing start-ups, largest enterprises and leading government agencies — are using AWS to lower costs, become more agile and innovate faster.

Ishwar Parulkar is Chief Technologist for Telecom at AWS.

Google Cloud accelerates every organization's ability to digitally transform its business. It delivers enterprise-grade solutions that leverage Google's cutting-edge technology, all on the cleanest cloud in the industry. Customers in more than 200 countries and territories turn to Google Cloud as their trusted partner to enable growth and solve their most critical business problems.

Nelly Porter is Head of Product of Confidential Computing and Encryption at Google Cloud. Jambi Ganbar is Product Manager of Telco, Edge and 5G at Google Cloud.

Microsoft Azure is a highly secure cloud foundation that enables customers to reduce costs and complexity. Multi-layered, built-in security controls and unique threat intelligence help identify and protect telco and IT architectures, cloud-native workloads and SaaS deployments. With billions in investments in R&D and cybersecurity over the next five years, and with 3,500 security experts that monitor and safeguard data, Microsoft Azure is trusted by enterprises, service providers, governments and start-ups.

Pramod Nair is the Lead Security Architect at Microsoft focusing on telco security.

Further reading

1. AWS. AWS cloud services adhere to CISPE Data Protection Code of Conduct for added GDPR assurance. Blog post. February 2022.
2. Google Cloud. Google Infrastructure Security Design Overview. White paper. March 2022.
3. IDC. Trusted Cloud: Overcoming the Tension Between Data Sovereignty and Accelerated Digital Transformation. White paper. March 2022.
4. Microsoft. Microsoft Trust Center. Web page.

About Nokia

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

As a B2B technology innovation leader, we are pioneering the future where networks meet cloud to realize the full potential of digital in every industry.

Through networks that sense, think and act, we work with our customers and partners to create the digital services and applications of the future.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: CID213045 (January)