GSMA Intelligence

TREND MICRO

Securing private networks in the 5G era

June 2021

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with nearly 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at www.gsma.com

Follow the GSMA on Twitter: @GSMA

Author:

Sylwia Kechiche, Principal Analyst, IoT & Enterprise

This report was authored by GSMA Intelligence with support from Trend Micro

GSMA Intelligence is the definitive source of global mobile operator data, analysis and forecasts, and publisher of authoritative industry reports and research. Our data covers every operator group, network and MVNO in every country worldwide – from Afghanistan to Zimbabwe. It is the most accurate and complete set of industry metrics available, comprising tens of millions of individual data points, updated daily.

GSMA Intelligence is relied on by leading operators, vendors, regulators, financial institutions and third-party industry players, to support strategic decision-making and long-term investment planning. The data is used as an industry reference point and is frequently cited by the media and by the industry itself.

Our team of analysts and experts produce regular thought-leading research reports across a range of industry topics.

www.gsmaintelligence.com

info@gsmaintelligence.com

Securing private networks in the 5G era: the operator perspective

45%	of surveyed operators consider it extremely important to invest in security to help them achieve a long-term enterprise revenue goal.
41%	of surveyed operators reported vulnerabilities related to network virtualisation as a challenge they face when offering 5G-based services.
48%	of surveyed operators see not having enough knowledge or tools to discover and solve security vulnerabilities as a top challenge, which is further exacerbated by a limited pool of security experts for 39% of surveyed operators. Operators want to focus on security, but to do so they will need to partner to build up their offering.
51%	of surveyed operators are prioritising IT/cloud vendor partnerships to improve private network security, while only 22% are looking to security vendors to meet this need. If operators are looking to differentiate their offerings, using security vendors can offer greater flexibility.
51%	of surveyed operators reported that multi-access edge computing (MEC) is a key part of their strategy for addressing enterprises' private network needs within the next two years, highlighting the need to focus on security at the edge.
18%	of surveyed operators secure either their edge or endpoints. Security at the edge and for endpoints is a critical part of a complete solution portfolio for private networks.

Security from an enterprise perspective

25%

of surveyed enterprises that haven't amended their cybersecurity practices regard addressing security concerns as not being their responsibility. However, security is everyone's responsibility. Enterprises have to ensure their data is protected, while customers are responsible for the security of their own devices and the data they generate, regardless of where it is stored. For enterprises, protecting customer data requires security operations and security zoning concepts to effectively identify network anomalies and minimise the negative impact of a security event.

55%

of surveyed enterprises see private wireless networks as very important to successful IoT deployment. Network security is a key consideration, as anything that is connected – even in a private network scenario – can be attacked by a cybercriminal. Digitising processes and operations by implementing IoT, AI/ML and 5G together with increased IT/OT convergence means there are multiple new threat vectors. An end-to-end view of security is required.

37%

of surveyed enterprises that haven't amended their cybersecurity practices expect IoT solutions to already be secure by default. Many enterprises, especially smaller ones, fall victim to basic attacks because they lack the baseline protection and a minimum level of digital hygiene. Risk assessments are a must to understand an organisation's security risk tolerance; operators can help determine this

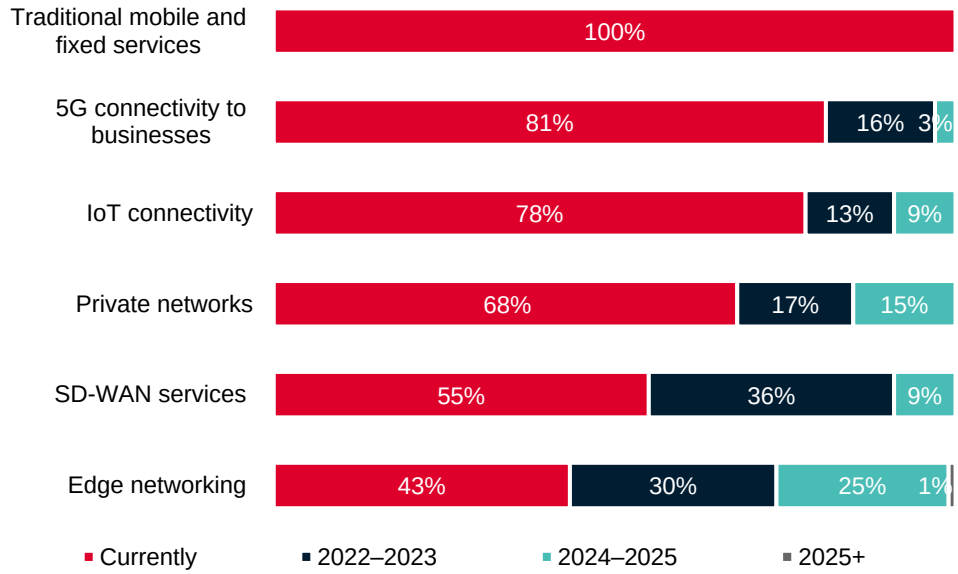
Defining private networks

Private networks	• A private (mobile) network is where network infrastructure is used exclusively by devices authorised by the end-user organisation. The infrastructure is typically deployed in one or more specific locations owned or occupied by the organisation. Devices that are registered on public mobile networks will not work on the private network unless specifically authorised. • These are more formally known as 'non-public networks', but the term 'private network' is more commonly used across vertical industries.
Network slicing	• Network slicing is a logical separation of the network that allows bandwidth to be allocated to specific services. The slices can be tailored to the needs of an organisation in terms of required quality of service, speed, security and latency. Network slicing will also be available on the public 5G network to provide seamless service operation for hybrid private/public network use cases.
Edge computing	• Edge computing brings compute capabilities closer to consumers and enterprise end users, enabling very low latency and customised local services. This is of particular interest to industrial customers, as it enables them to take more control over localisation of data, authorisation and security.

On the road to pervasive 5G connectivity

- **5G connectivity offered by most.** 81% of operators claim to sell 5G to SMEs and corporates. While 5G network rollouts are on the rise, it is unlikely that all of these operators are able to offer “pure” 5G (Release 15 and above). It likely reflects the industry buzz around 5G, with 4G often leveraged to offer services marketed as 5G. In limited cases, operators offer FWA, using established B2B distribution channels.
- **Private networks on the horizon.** 68% of operators currently offer private wireless networks (4G/5G), specifically deployed for enterprise customers. The remaining operators plan to have them in place by 2025.
- **Room for growth beyond core connectivity.** A smaller proportion of operators are currently selling SD-WAN and edge services, but the majority expect to offer these by 2025. The past year has seen a lot of cloud and telco partnership deals related to MEC, with IT/cloud vendors the preferred partners for around a quarter (26%) of operators.

Which of the following communications services do you currently sell to your enterprise customers and, if you don’t, when do you expect to do so?
Percentage of respondents. N=100.

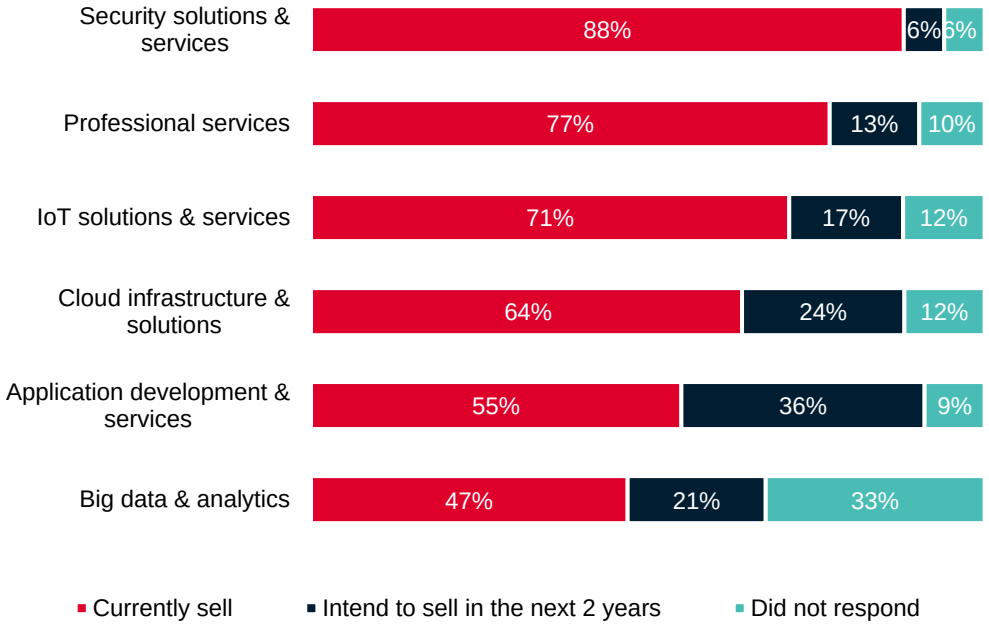


Source: GSMA Intelligence Operators in Focus Survey 2021

Operators are committed to security

- **Nearly all operators offer security.** The proportion of surveyed operators offering security services and solutions increased slightly to 88% in 2021, from 85% in 2020. The importance attached to investing in security grew significantly too.
- **Security is paramount.** According to our research, 85% of enterprises have amended their security practices as a result of IoT deployments, primarily to establish a "security-first" strategy as a USP (61%) and to protect business reputation (52%). When choosing an IoT solution, security is a key factor for 57% of enterprises.
- **More eyes on security**. In a recent report, we highlighted how the ecosystem has to come together to secure IoT and ensure end-to-end security across the entire value stack. Furthermore, recent attacks highlight software supply-chain sensitivity, ecosystem interdependency and the need for teams within enterprises to collaborate on security to ensure visibility across different departments.

Which of the following non-communications services do you currently or plan to sell to your enterprise customers within the next two years?
Percentage of respondents. N=100.

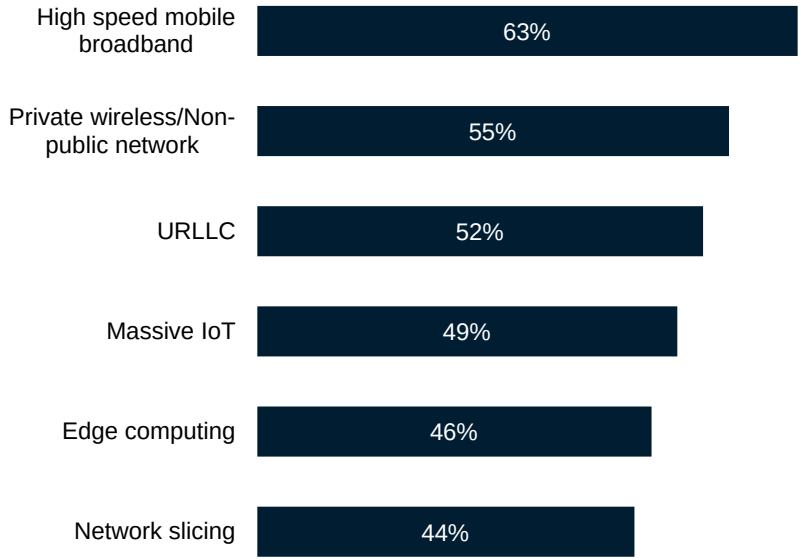


Source: GSMA Intelligence Operators in Focus Survey 2021

5G features are important to the successful implementation of IoT

- **The digital transformation imperative.** 5G's benefits in terms of lower latency, faster transmission speeds and increased network capacity (massive IoT) open the door to the digital transformation of enterprises and enable new use cases. Ultra-reliable, low-latency communication (URLLC) is one of several new features supported by the 5G new radio (NR) standard, with 52% of enterprises viewing it as very important to the success of IoT.
- **High-speed broadband on top.** In 2020, 30% of operators stated their 5G marketing to enterprises focused on faster speeds as 5G's main feature. It follows that enterprises identified high speeds as the most important capability (63% of those surveyed).
- **The allure of private networks.** When asked about the importance of private networks to successful IoT deployments, 55% of enterprises said they were very important, ahead of edge computing and network slicing.

Very important features to achieving success in IoT deployments
Percentage of respondents. N=2,873.

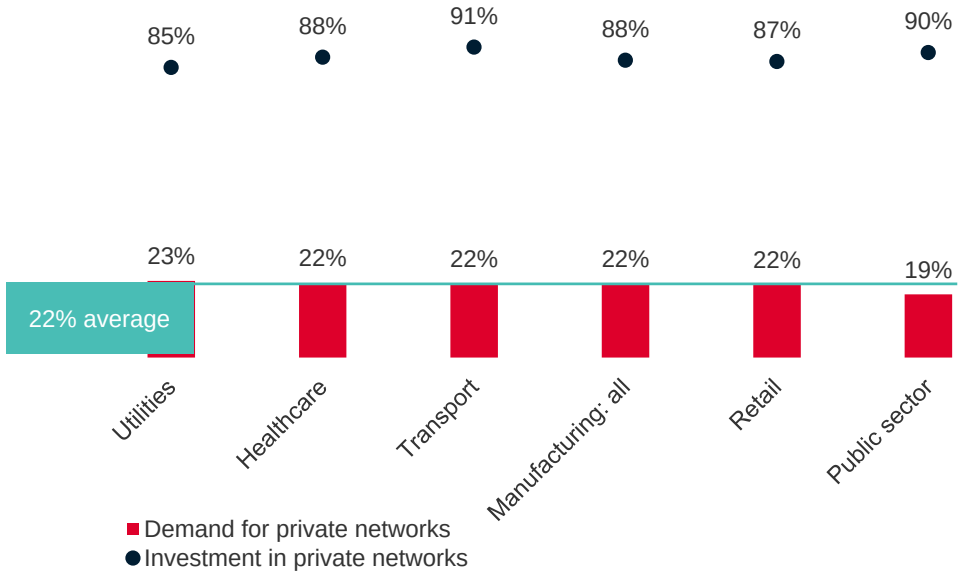


Source: GSMA Intelligence Enterprise in Focus Survey 2020

Enterprises require location-specific coverage

- **The raison d'être of private networks.** Enterprises principally choose to deploy a private network to gain more control over their network – often to isolate it from the public network but also to address requirements for higher availability, lower latency and enhanced privacy (keeping the data on premises and compliant with data regulations).
- **Demand for private networks is consistent.** Almost a quarter of surveyed enterprises said they require location-specific coverage in 2020. Of those that require a private network, 88% on average have either already invested in or would be likely to invest in their own private network.

Private network needs and investment plans among verticals
Percentage of respondents with localised network coverage requirement for IoT deployment. Of those, percentage that have invested or are likely to invest in a private network. N= 2,772.

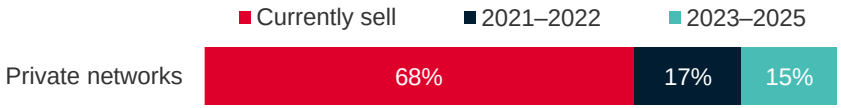


Source: GSMA Intelligence Enterprise in Focus Survey 2020

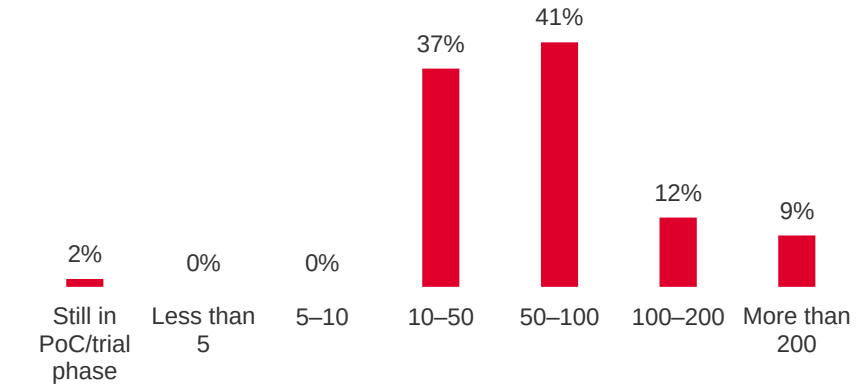
Operators are already offering private networks to enterprise clients

- **Private networks are here to stay.** 68% of operators claim to currently sell private wireless networks specifically deployed for enterprise customers. The rest are planning to do so by 2025. These could utilise various deployment models, from public dedicated networks through hybrid networks (network slicing, public/private campus, private RAN with public core) to private networks. Within these various models, network slicing and edge computing add the benefits of QoS, privacy, security and specific SLAs.
- **Upwards of 10 customers.** The vast majority of surveyed operators stated they have between 10 and 100 private network enterprise customers. These numbers include use of multiple access technologies. Some are likely virtual networks, due to the large volumes indicated by operators.

Operators and private network status



How many private network customers do you have?
Proportion of those that currently offer. N=68.

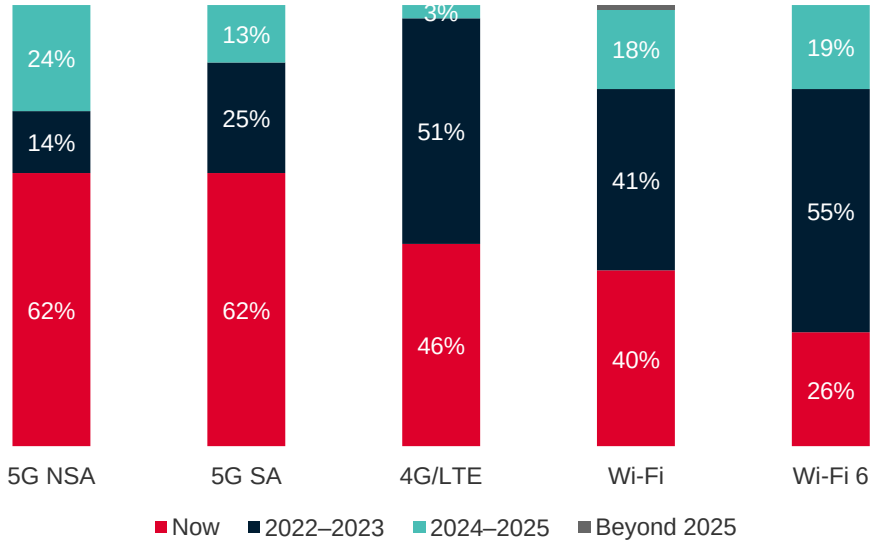


Source: GSMA Intelligence Operators in Focus Survey 2021

Operators are addressing the opportunity via a mix of tech

- **A mix of technologies, with mobile leading.** Historically, Wi-Fi has been the connectivity choice for private networks. However, mobile technologies (4G/LTE and 5G) are better suited to OT network requirements of high volume, high reliability, mobility and always-on operations.
- **4G/LTE shouldn't be ignored.** Testing the viability of network slicing by rolling out private LTE networks ahead of 5G makes sense. Private 5G networks can build on existing LTE ones, which often use 5G-ready equipment.
- **On the road to 5G SA.** 5G SA offers the most benefits related to eMBB, massive IoT and critical IoT, allowing support for a range of devices and applications with more demanding bandwidth requirements than Wi-Fi and 4G (including wireless robots and real-time video surveillance). In the future, 5G SA will also deliver time-sensitive networking for high-precision devices. However, 5G SA has so far only been deployed in a handful of countries, suggesting a disconnect between marketing and commercial realities.
- **Wi-Fi is familiar to enterprise IT.** Wi-Fi is already well established within the enterprise IT network environment. Wi-Fi 6 promises to deliver significant bandwidth gains over earlier generations of Wi-Fi networks. Looking ahead, 5G and Wi-Fi, including Wi-Fi 6, will co-exist and complement each other in private network deployments.

Which technologies are you using for private wireless network deployments?
N=100



Source: GSMA Intelligence Operators in Focus Survey 2021

5G meets location-specific coverage requirements through a variety of deployment scenarios

Main characteristics of deployment scenarios

Public network	Public network with SLAs	Public network with network slicing	Public network with local infrastructure	Standalone private network (operator spectrum)	Standalone private network (non-operator spectrum)
• Wide area mobility • Efficient use of infrastructure, operations and spectrum • Standard service-level agreements • Mobile edge computing within public network	• Leverages operator expertise, solutions and spectrum portfolio • Superior customer support and SLAs • QoS for prioritising critical devices and applications • Mobile edge computing within public network	• Network resources are dedicated and customised • Greater data isolation, security and privacy, and further SLA customisation (availability and reliability) • Edge computing on the operator edge	• Managed service with dedicated RAN under SLAs • Choices regarding localisation of data/control • On-site edge computing gateways • Interoperability with public network	• Dedicated network • Managed service or leasing of spectrum • Full control over design, deployment, operations and SLAs • Edge computing on the operator or customer edge	• Isolated network with no interoperability with public network • Direct responsibility for spectrum access and usage • Independent design, procurement, operation and radio plan

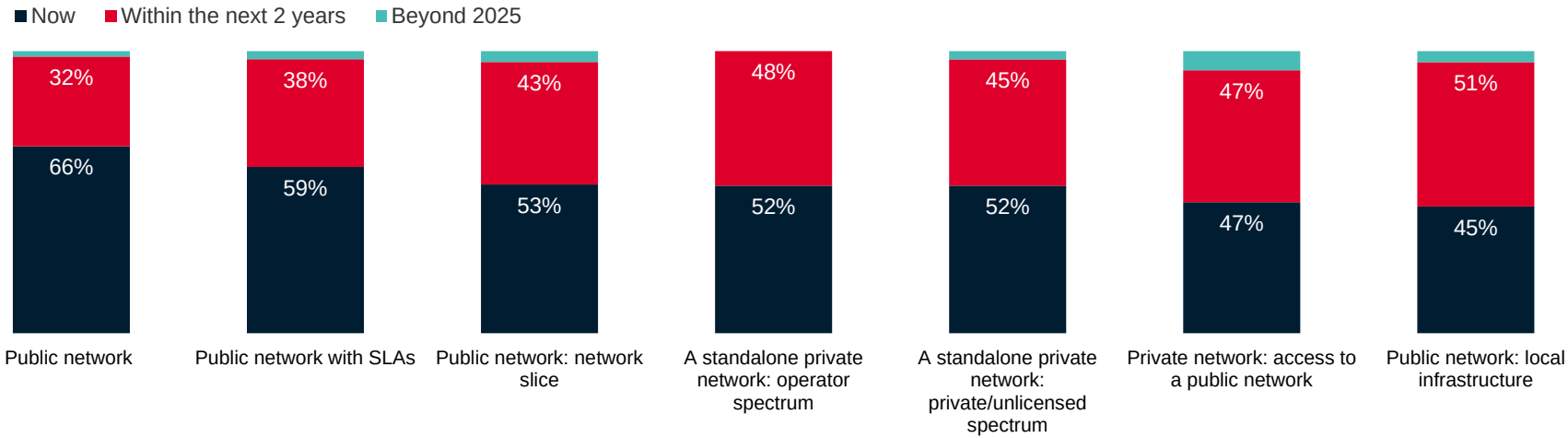
Source: GSMA Intelligence analysis

Operators will use a range of deployments models in the short term

- **Leaning towards public network for now.** The majority of operators (66%) are looking to public networks to address enterprise requirements related to private networks, followed by public networks with SLAs (59%). However, a variety of options will be supported over the next few years, with operators experimenting with different deployment modes to cater to customer needs. The longer term view remains uncertain, and different factors are at play at the regional level.

- **In MEC we trust.** Computing will move closer to the edge, as edge computing is key to 5G's success. Operators are already putting their MEC strategies in place, hoping to reap the benefits; over the next two years, 51% see local infrastructure (e.g. on-site edge computing gateway) with access to the public network as the leading approach.

Thinking about deployment models for private networks to serve your enterprise clients' requirements, which of the following approaches will you use? Those that offer/plan to offer private networks and/or 5G. N=100.

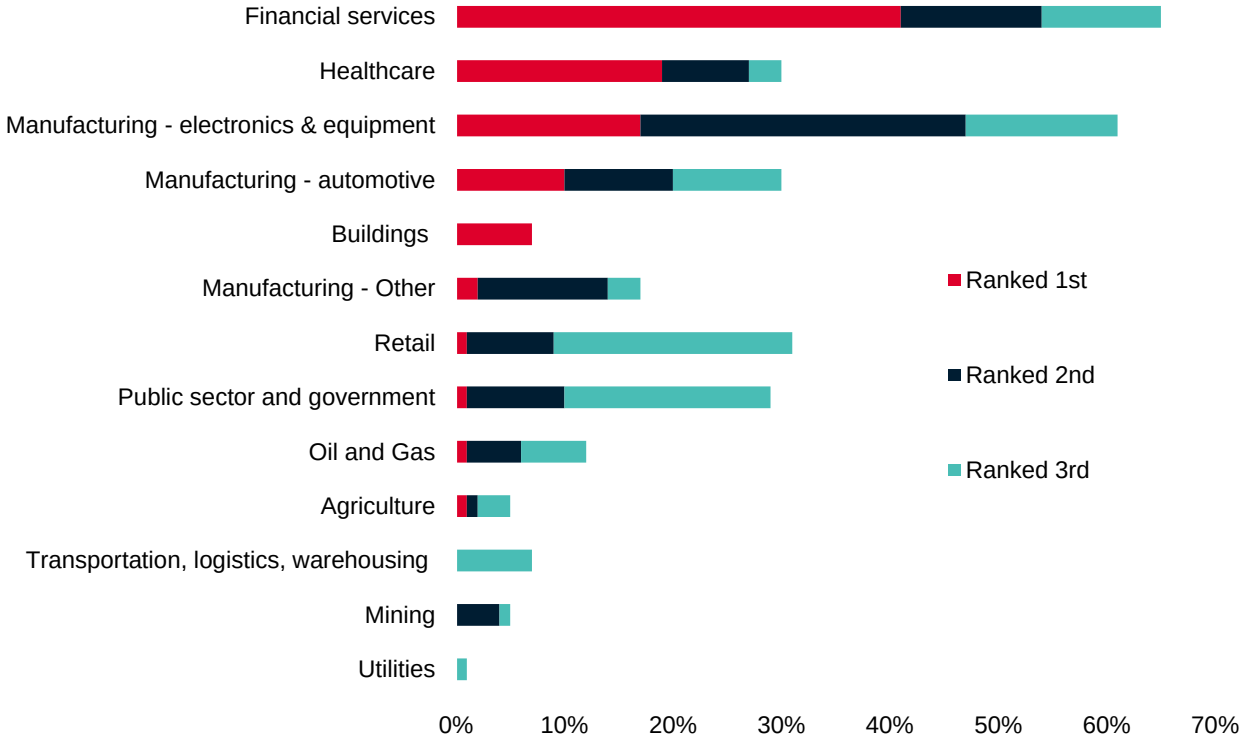


Source: GSMA Intelligence Operators in Focus Survey 2021

Operators see greatest demand for private networks in financial services, healthcare and manufacturing

- **Demand is real.** Financial services are far ahead of other verticals when it comes to dedicated coverage requirements – especially in Europe and Latin America. Healthcare, consumer electronics and automotive manufacturing also top operators' lists. Recent announcements on partnerships and tie-ups between operators and vertical players confirm these priorities.
- **Missed opportunities.** Operators seem to be less aware of opportunities in utilities, mining, and transportation, logistics and warehousing (including aviation and ports). These are verticals where equipment vendors such as Nokia are seeing requests for private networks. Buildings (public/enterprise venues) are an interesting case, ranked by 7% as the top opportunity (with demand mostly coming from Asia Pacific and North America) but not as a second or third option.

What are the top three industry verticals where you see demand for private networks (4G/5G)?
N=100.

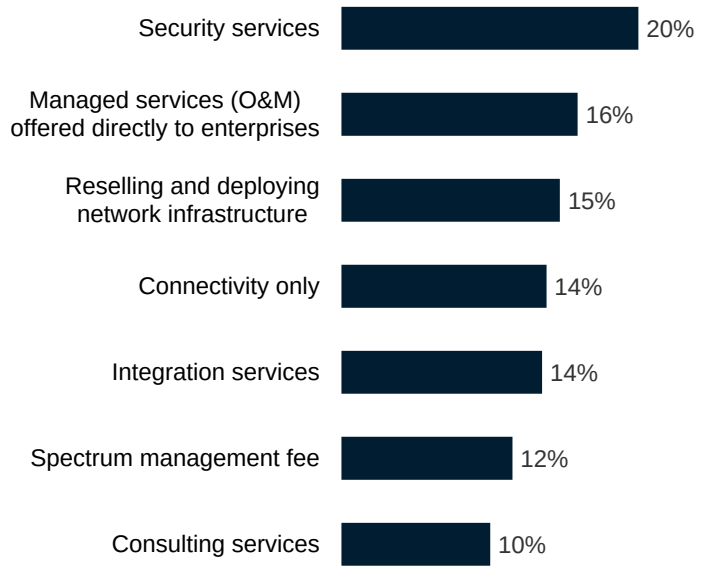


Source: GSMA Intelligence Operators in Focus Survey 2021

Operators need to define their roles in private networks

- **Betting on security.** 44% of operators have seen increased growth in demand for security services from their enterprise clients due to Covid-19. Furthermore, 45% of operators consider it extremely important to invest in security to help achieve a long-term enterprise revenue goal (compared to 22% in 2020).
- **Securing private networks.** 77% of operators are planning to offer security as part of their private network solution. They look to security as a top opportunity for revenue generation, forecasting 20% of 5G revenue to come from security.
- **Professional services offer returns**. Professional services include consulting (technical and business), systems integration and managed services, together accounting for 40% of operators' perceived revenue. This opportunity is skewed towards larger operators with IT capabilities or with a strong local channel to market via local systems integrators or IT value-added resellers.

Thinking of revenue opportunities coming from 5G private networks, what is the revenue distribution that you expect?
Percentage of total revenues. N=100.



Source: GSMA Intelligence Operators in Focus Survey 2021

Enhancing network security with 5G

- **Network security is a key consideration.** Enterprises moving from wired connections (which have a level of physical protection) to wireless connections have to consider new risks to their IT and OT networks. Anything that is connected can be hacked – and the growing number of connected devices within systems increases the potential attack surface.
- **5G standard facilitates a base level of security**. The 5G network uses data encryption and integrity protection mechanisms to safeguard data transmitted by the enterprise, prevent information leakage and enhance data security for the enterprise.

5G security controls outlined in 3GPP Release 15

Subscriber protection	Radio protection	Core protection
• Subscriber permanent identifier (SUPI) – a unique identifier for the subscriber • Dual authentication and key agreement (AKA) • Anchor key is used to identify and authenticate UE. The key is used to create secure access throughout the 5G infrastructure • X509 certificates and PKI are used to protect various non-UE devices	• Encryption keys are used to demonstrate the integrity of signalling data • Authentication when moving from 3GPP to non-3GPP networks • Security anchor function (SEAF) allows re-authentication of the UE when it moves between different network access points	• The home network carries out the original authentication based on the home profile (home control) • Encryption keys will be based on IP network protocols and IPSec • Security edge protection proxy (SEPP) protects the home network edge • 5G separates control and data plane traffic

Source: 5G IoT Private & Dedicated Networks for Industry 4.0

5G security needs to complement the OT security toolbox

- **Different security needs.** As OT and IT security objectives often differ, so do the security mechanisms and network design principles. In IT, the security fundamentals are confidentiality, integrity and availability. In the case of OT – the requirements of which are driving the need for private networks – asset availability and integrity could be prioritised depending on a risk assessment. To maintain continuity of industrial operations, changes could also apply to safety, reliability and performance (latency) requirements. These are important considerations for 5G network implementations. The OT security toolbox already contains features addressing security requirements at layers above the network layer.

- **Another level of complexity**. 5G private networks have a larger potential attack surface because of IoT exposure, physical mobility of devices and the interplay between enterprises, mobile operators, manufacturers, IT/OT vendors and suppliers.

Security and privacy characteristics of OT networks and corresponding 5G network needs

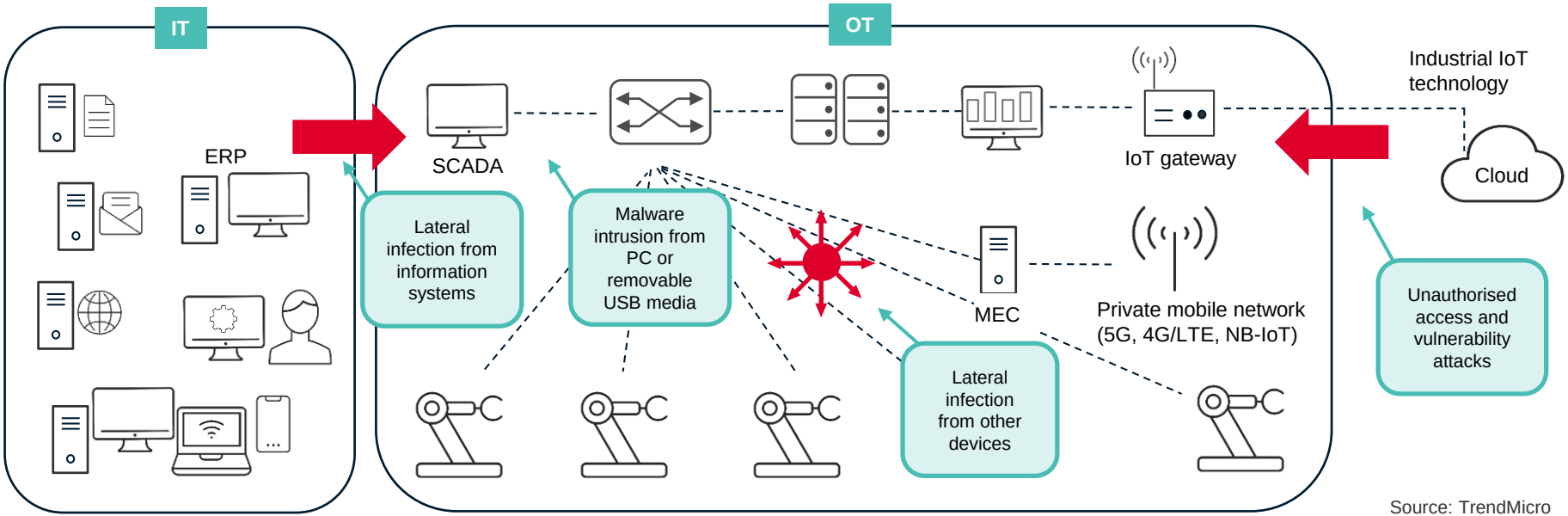
	Physical isolation	A single trust domain	Device authentication	Regulatory compliance
OT	• Perimeter protection and access control to protect processes, operational data, users and equipment confidentiality. • Controlled access from outside, including restricted access operational data flows.	• Third parties are not allowed within the perimeter, except for certain remote maintenance tasks that do not impact real-time operations.	• Physical perimeter security in the OT environment. No need for authentication, hardware security and credential storage.	• Regulatory compliance and related certifications are a business priority, as is ensuring compliance continuity, and protecting data confidentiality and integrity in line with regulations.
5G	• Physical isolation is no longer maintained. Need for logical isolation mechanisms and physical radio layer protections (jamming protection).	• Need for additional end-to-end encryption and integrity protection mechanisms. Data ownership poses a challenge.	• Need for strict authentication mechanisms, secure credential storage and processing is addressed by UICC (3GPP approved).	• 5G security features and functions need to support industry-specific requirements for compliance.

Source: 5G ACIA

The attack surface grows with IT/OT convergence to drive digital transformation

- **Industry 4.0 comes at a cost.** Covid-19 has proved to be a catalyst for Industry 4.0; it has exacerbated existing challenges and pain points for manufacturers and accelerated the need for smart connectivity and digital transformation. The move to digital brings numerous benefits but also introduces cybersecurity risks as it removes the physical separation (different networks). These include internally generated threats (e.g. malware infection caused by laptops brought into a factory) and external threats (e.g. lateral movement from the IT network, illegal access and vulnerability attacks from the internet).

Cyber risks in factory settings – attack triggers from IT, OT networks and the internet



Source: TrendMicro

With 5G security, one size doesn't fit all

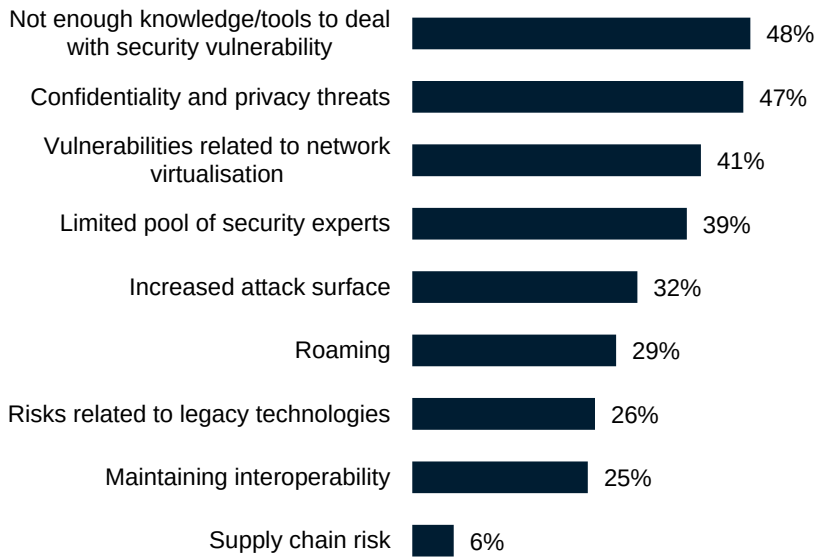
- **Lack of resources.** In the 5G era, security risks are greater than before because of the combination of cloud, data and IoT security threats. The pandemic has intensified ransomware attacks and cybercrime in general. Against this backdrop, operators see not having enough knowledge or tools to discover and solve upcoming security vulnerabilities as a top challenge (48% of surveyed operators), further exacerbated by a limited pool of security experts (39%).

- **Blame IoT.** 63% of enterprises have deployed IoT as part of their digital transformation. Operators need to get ready to address the challenges IoT brings. Yet, 47% of operators see confidentiality and privacy threats which are related to critical IoT as a key challenge to offering a 5G-based solution, while 32% see an increased attack surface (related to massive IoT).

- **Hacking 5G.** The 5G network core will be based on software-defined networking (SDN) and network function virtualisation (NFV). SDN and NFV make heavy use of the HTTP and REST API protocols. These protocols are well known and widely used on the internet, and are thus hackable. It isn't surprising that 41% of operators highlight vulnerabilities related to network virtualisation.

- **Don't ignore legacy**. In reality, only a minority of 5G private networks will be greenfield; most will have to integrate and interoperate with existing (legacy) technologies. Only a quarter of surveyed operators see this as a challenge.

What security challenges are you facing/ will you face when offering 5G-based services?
Percentage of respondents. N=100.



Source: GSMA Intelligence Operators in Focus Survey 2021

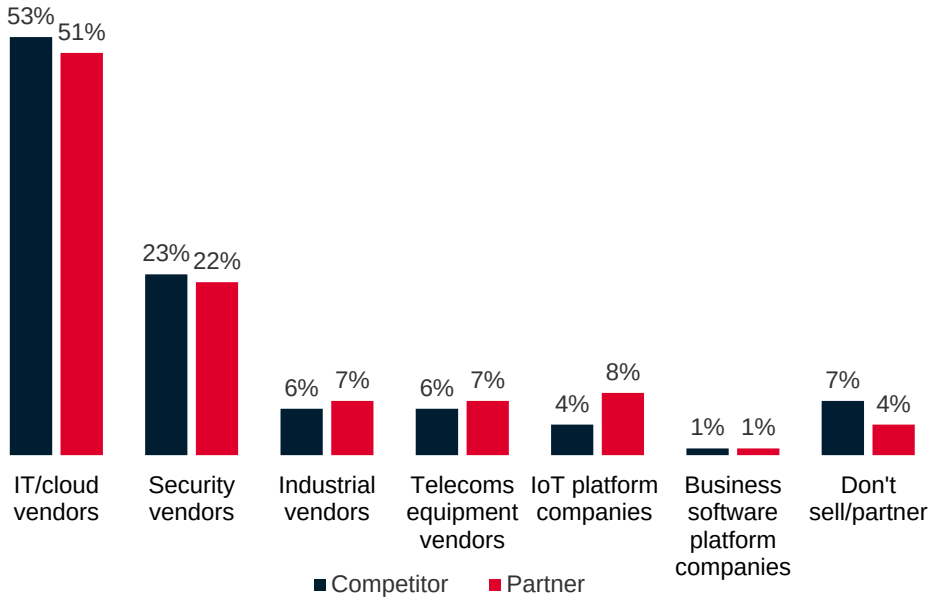
Coopetition with IT/cloud vendors ahead of security vendors for private network security

- **Investing in security for success**. In 2021, 45% of operators consider it extremely important to invest in security to help them achieve a long-term enterprise revenue goal (versus 22% in 2020). This came second to understanding customers' business needs in order to achieve a long-term enterprise revenue goal (49%). As the M&A route is only available to a few operators that have the financial muscle, entering into collaboration and resale agreements with competitors is an alternative.

- **IT/cloud vendors come first.** Operators are most likely to see these as competitors and partners for private network security. This isn't surprising, considering enterprises trust cloud vendors the most to secure their IoT deployments, according to our Enterprise in Focus Survey. Enterprises tend to work with what they know, and are already familiar with AWS and Azure environments, for example.

- **Security vendors a distant second**. Despite having strong credentials and being less direct competitors to operators, security vendors are not front of operators' minds to work with to provide private network security. With security built into the 5G standard, there is less of a perceived need to look for additional security.

Who do you view as your most formidable competitor/partner, besides your telecoms peers, for private network security?
Percentage of respondents. N=100.

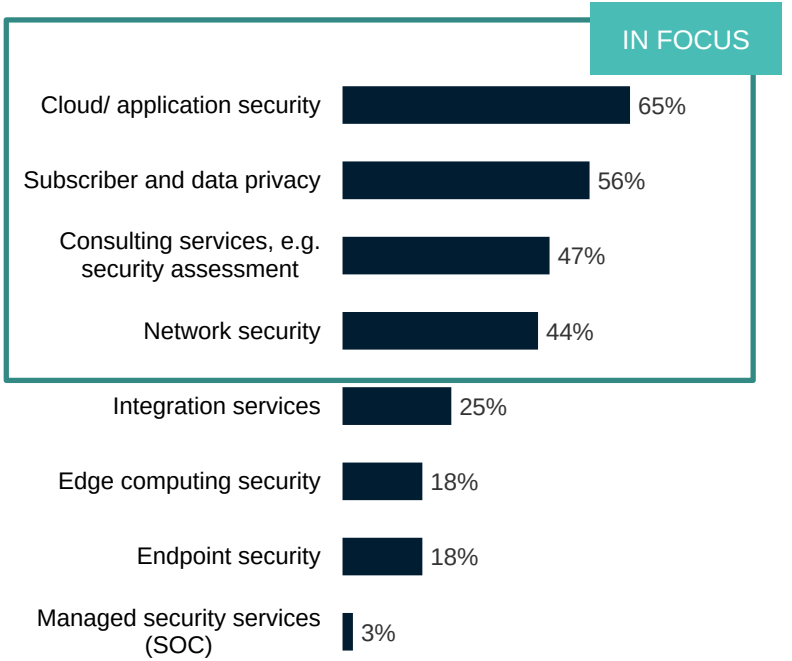


Source: GSMA Intelligence Operators in Focus Survey 2021

Operators view cloud/application security as integral to their private network security offering

- **Commitment to cloud/application security.** The majority of operators' offerings comprise cloud/application security. They have already been deploying their cloud offerings to address enterprise security risks, typically with multiple cloud vendors operating across multiple sites.
- **Protecting privacy.** 56% of operators see protecting privacy as a key component of their offering. 5G presents an opportunity for operators to address key privacy concerns, and protect personal data using subscription concealed identifier (SUCI) to encrypt the subscriber identity number (part of the international mobile subscriber identity or IMSI). However, this could be a less relevant feature for private networks as more machines than people are connected.

Which of the following forms your private wireless security solution offer?
Of those that plan to offer private network security. N=77.

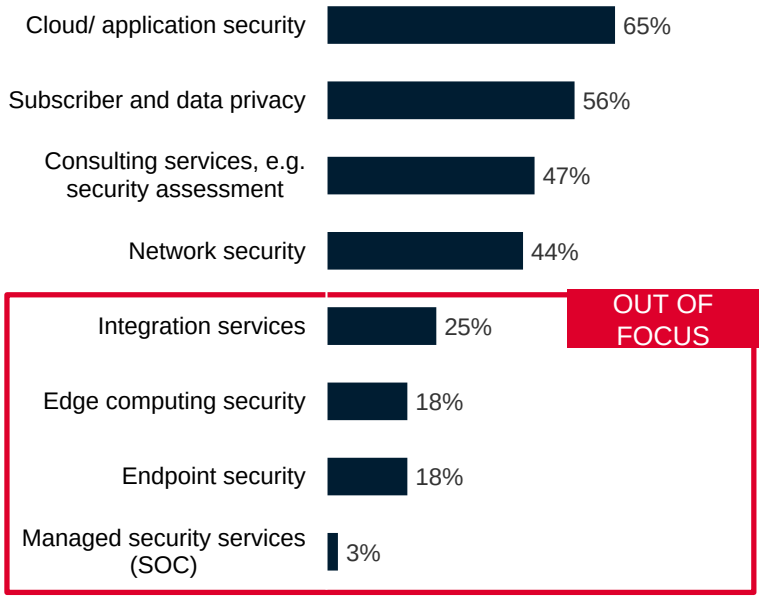


Source: GSMA Intelligence Operators in Focus Survey 2021

Operators need to fine-tune their private network security offerings

- **Lending a hand.** 47% of operators include consulting services and a further 25% integration services as part of their private security solutions. Through consultancy services, operators can assess enterprises' existing solutions to determine security gaps and perform threat analysis to ensure regulatory requirements are met and that they adhere to best practices and security standards.
- **Edge and endpoint security under the radar.** Edge computing is an important part of 5G private networks, as is ensuring endpoint security. However, only 18% of surveyed operators have these in their security solution portfolios for private networks, as they are still assessing how to make these part of their offering. To futureproof their investments, it is important to include MEC and endpoint protection (for securing enterprise data) in 5G private networks from the start (proof of concept).
- **Overlooking SOC?** To protect customer data, security operations and security zoning concepts are essential to understand anomalies in traffic and minimise damage in the event of a problem. Especially for private 5G for enterprise applications, it will be necessary to take an enterprise-wide view of integration with SOC.

Which of the following forms your private wireless security solution offer?
Of those that plan to offer private network security. N=77.

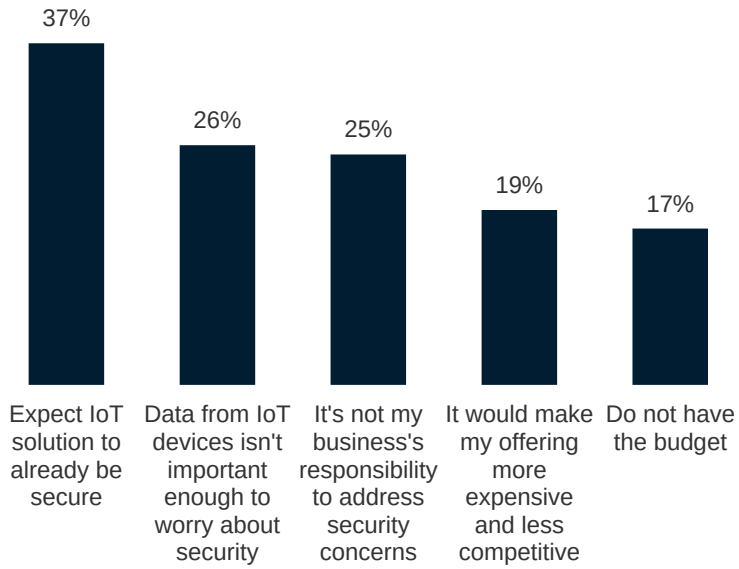


Source: GSMA Intelligence Operators in Focus Survey 2021

Many enterprises are risking the cost of inaction

- **Security awareness isn't uniform.** 85% of enterprises with IoT deployments have amended their security practices, primarily to establish a "security-first" strategy as their company's unique selling point, according to our Enterprise in Focus Survey. Yet, 15% haven't.
- **Security basics don't go away.** Many enterprises, especially smaller ones, fall victim to basic attacks because they lack the baseline protection and a minimum level of digital hygiene. 37% of those that haven't amended security practices expect IoT solutions to already be secure. Risk assessments are a must to understand an organisation's security risk tolerance; operators can help determine this.
- **Protect the data.** 5G private networks have a bigger attack surface as they focus more on IoT, connecting more devices. Disturbingly, some enterprises still don't regard data from IoT devices as important.
- **Everyone's responsibility.** 5G SA is more secure than any previous network generation. However, as the attack surface expands and convergence of IT/OT and IoT continues, any security breach has a company-wide impact. Yet, 3% of enterprises overall don't see addressing security concerns as their responsibility.
- **Use AI.** Machine learning models capable of detecting unknown threats will grow in importance. Security by design, which includes automation and is able to dynamically apply security policies, will be able to keep up with the speed of 5G networks

What are the main reasons why you have not implemented changes to your security as a result of your IoT deployment?
Percentage of those that have not amended security practice. N=381.



Source: GSMA Intelligence Enterprise in Focus Survey 2020

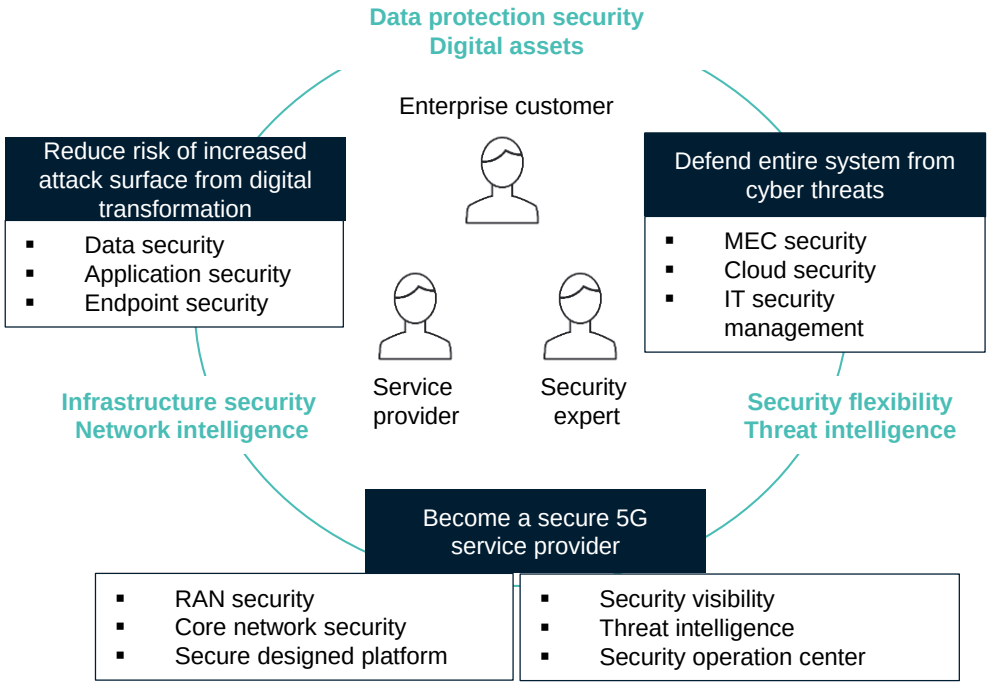
Securing 5G is a shared responsibility

- **Is 5G secure?** 5G networks are designed to be more secure than previous technology generations but no network technology provides end-to-end security. It provides physical and link layer protection to prevent eavesdropping and tampering of data in transit. However, enterprises deciding to deploy 5G networks will be moving away from an OT-based network with physical isolation. Operators will need to offer logical isolation mechanisms and physical radio layer protections (jamming protection). To fulfil the requirements for a single trust domain, additional end-to-end encryption and integrity protection mechanisms need to be in place.

- **Shared security responsibility.** With 5G, enterprises and providers can be jointly responsible for security. End-to-end security requires vendor collaboration, but enterprise customers have a role to play too. They have work to do in ensuring their data is protected as they are in charge of their own devices and the data generated by them, regardless of where it is stored. To take on the role of a secure service provider, an operator has to either broaden its credentials or partner with a SI, cloud vendor and/or IT vendor.

- **The call for zero trust.** A zero trust architecture alleviates both the risk of an external attacker getting into the network and the risk of lateral movement in the event of a security breach. 5G specifications are aligned with zero trust creeds.

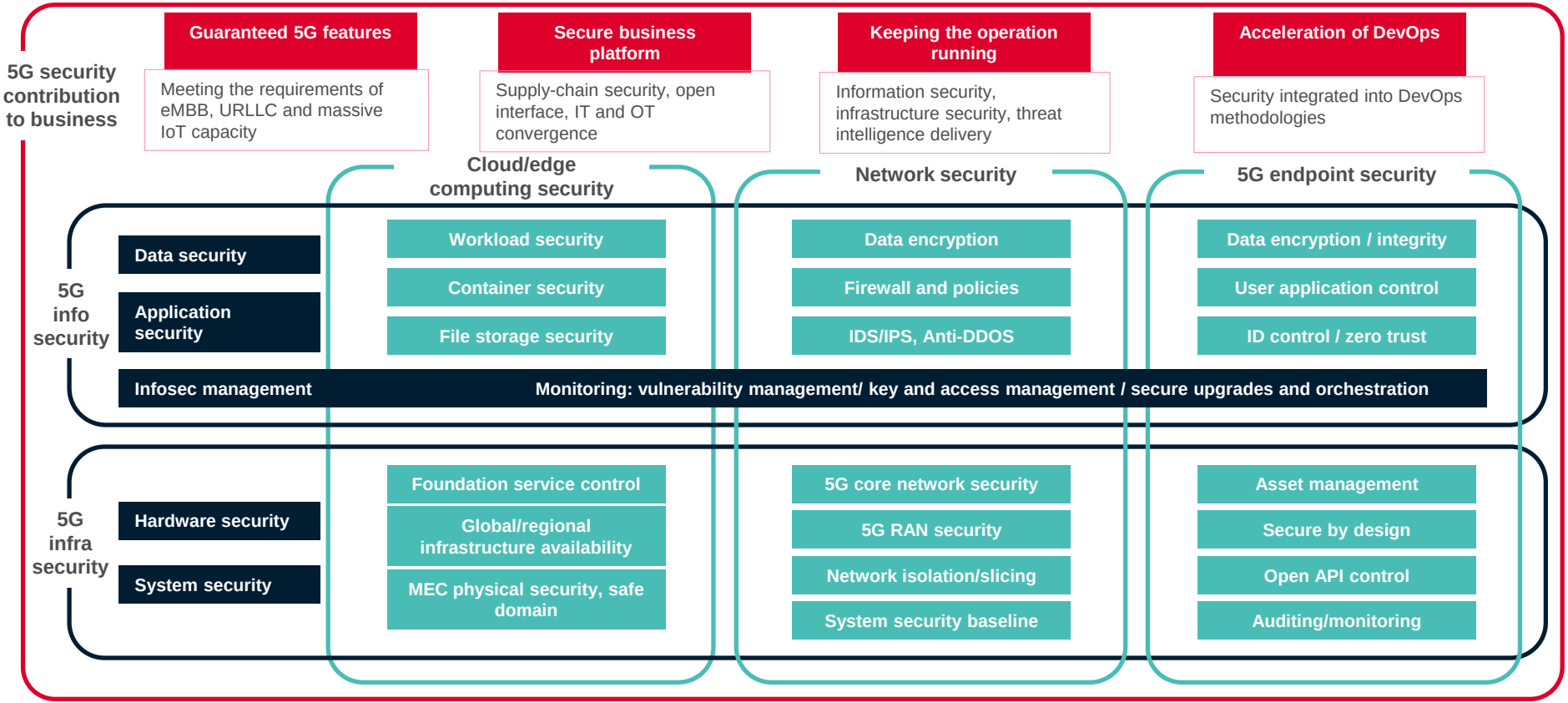
Shared responsibility in enterprise 5G



Source: TrendMicro

5G security requires a cross-functional approach

5G security for enterprises: assessment matrix



Source: TrendMicro

Research methodology

The **GSMA Intelligence Operators in Focus Survey 2021** canvassed 100 decision-makers from operators around the world to understand their views on the enterprise opportunity.

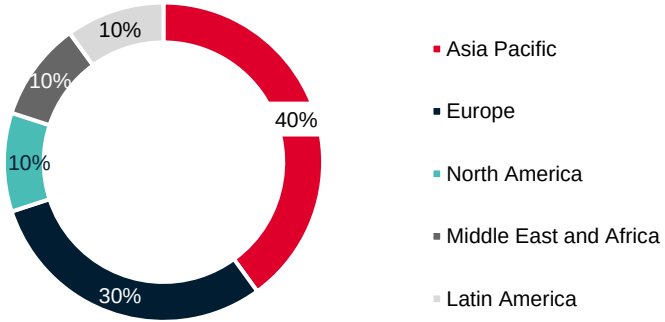
The decision-makers have a strategic role to grow enterprise revenues, selling traditional communications services (fixed and mobile) and other value-added services (cloud infrastructure and services, IoT, security, big data and analytics, application management and development services, and professional services).

All responses were confidential and are only reported in aggregate.

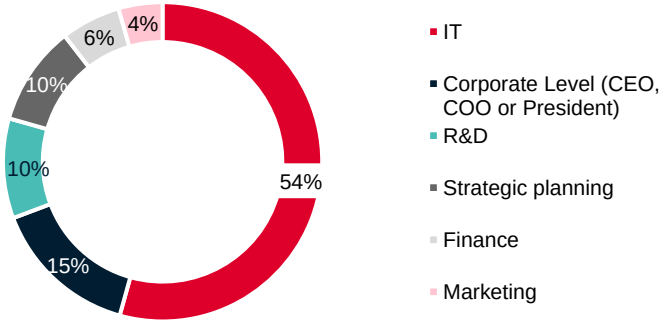
The **GSMA Intelligence Enterprise in Focus Survey 2020** spanned 2,873 companies, representing the following:

- **Eight industry verticals:** retail, utilities, transportation, healthcare, public sector, manufacturing, automotive and consumer electronics
- **Countries covered:** Argentina, Australia, Brazil, China, France, Germany, India, Indonesia, Japan, Mexico, Russia, South Africa, South Korea, Spain, Sweden, Turkey, UK and US.
- **Company sizes:** small and medium-sized companies with 20-249 employees, and large enterprises with more than 250 employees.
- **Roles:** IoT decision-makers from various departments.

Regional distribution of respondents (N=100)



Respondents by department (N=2,873)



GSMA Intelligence

gsmaintelligence.com

@GSMAi