GSMA Intelligence

RADAR

Digital transformation in a post-pandemic future: private 5G, eSIM, cloud and edge in vogue

Giesecke+Devrient
Creating Confidence

pod group
A Giesecke+Devrient Company

Kigen

GSMA Intelligence

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry, and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at gsma.com

Follow the GSMA on Twitter: @GSMA

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

Published June 2022

Authors
Tim Hatt, Head of Research and Consulting
Pablo Iacopino, Head of Research and Commercial Content
Peter Jarich, Head of GSMA Intelligence

This report was conducted by GSMA Intelligence and supported by G+D, Pod Group and Kigen.

Contents

Executive summary

Digitisation continues in spite of (and sometimes because of) Covid-19

The broader trend of digitisation across industries that underpins investment in cloud compute, 5G, AI and analytics was set in motion before the pandemic, so the gathering pace of recovery should be seen as a resumption of activity after a 'pause' rather than something wholly new. As one key measure, the impending growth in IoT connections to 37 billion by 2030 (a more than 2× rise on the current deployment count) underlines the economic value that companies, governments and government agencies (such as transport authorities) place on 'smart' operations.

The fundamental rationale for digitisation of companies in different enterprise verticals remains the same, which includes:

- allowing productivity gains from use of data analytics and more efficient operations
- enabling cost savings
- opening (or speeding access to) new revenue streams
- redeploying labour to higher-value functions.

Our purpose in this report is to strip away shorter-term effects from economic and political instability and focus on the longer-term implications from digitisation and the technology enablers that will power it. This applies to business and operating models of vertical sector companies and, just as importantly, to telecoms operators, vendors and cloud groups competing to enable and service this business.

A nexus of technologies will drive the story

Three broad technology 'families' sit at the intersection of the telecoms and cloud industries, and are the key infrastructure underpinnings for digitisation, especially for enterprises. These are:

- private networks (PNs)
- IoT devices, including eSIM and provisioning
- cloud and edge compute.

These families house the key tools being used across different industries for digital transformation: ultra-high-speed and low-latency connectivity; flexibility for device provisioning; and compute infrastructure to run AI-driven analytics to optimise operations and efficiency. The value chains that provide the products in each area are somewhat disparate but have become increasingly interconnected.

Private networks

Digitisation and the need for secure, low-latency connectivity on premises is the main change factor that has brought PNs back into focus. The expansion of 5G standalone (SA) networks is a further enabler. Unlike non-standalone (NSA), SA networks can deliver on the ultra-low latency requirements of many industrial clients, which a guaranteed QoS through a PN reinforces. SA networks are still the minority, with only 22 live installations, which translates to around 10% of operators with a 5G network.

Indications from operator reporting suggest this is changing. China was the only majority SA country from the outset in the 5G era. However, the US and most three- and four-player markets in Europe – France and Italy being notable exceptions – are in a situation now where over half of operators have publicly announced plans for 5G SA.

Despite their renewed focus, PNs are an LTE-era creation and the number of PNs has yet to go beyond the hundreds. The majority are LTE (approximately 60%), with around 20% being 5G and the rest having both capabilities. The pace of future adoption will be influenced by licensed spectrum availability (particularly in the mid-band), return on investment (RoI) proof points from successful deployments and the balance between competition and co-opetition with cloud majors.

eSIM

eSIM adoption in IoT vertical use cases is growing, but it's fair to say that eSIM has yet to reach critical mass. To a large extent this is expected, as ecosystem reconfiguration takes time. The ongoing period of transition from SIM to eSIM is much needed as companies gain eSIM experience and adjust to new manufacturing and logistical processes. Global, rather than proprietary, specifications and sector-wide deployments will be key to future success. Future eSIM deployments at scale will also depend on IoT companies having a clear eSIM strategy alongside their main IoT proposition.

Edge compute

While edge was a minor part of the 5G enterprise message in 2021, it's expected to be the top value proposition as we go into 2023 and beyond. As operators build out their 5G and edge capabilities, it is understood that edge will need to be a critical part of the 5G enterprise and digital transformation message.

Though the value of edge and IoT may not be in question, both operators and enterprises agree that internal challenges remain a real risk to executing on them: 40% of enterprises cited internal resistance as a challenge to IoT deployment, while unclear internal ownership and lack of internal expertise together represent the top edge networking deployment challenge for half of all operators. The good news is that internal challenges are ones that operators and enterprises should be able to address, as they are within the control of the organisation. The bad news is that unless they are dealt with, the risk could be greater than stalled IoT and edge deployments – a lack of internal coordination or internal will could result in sub-par deployments, jeopardising anything from solution performance to security and, ultimately, customer experience.

How should we think about implications? Co-opetition is king

The benefits of digitisation for enterprise are clear, although not always communicated well. The risks are mostly operational, even if RoI payback periods may go beyond five years. Implementing new technology and swapping out legacy IT systems is a common pain point. Supplier diversification is a good thing when it plays to comparative advantages; it can, however, also present challenges if suppliers are spread geographically. Finally, many businesses lack internal expertise and know-how – even in the CTO or CTIO offices – to adequately assess what solutions would best fit their objectives, which then carries into supplier selection and ongoing evaluation. We mention these not to highlight them as insurmountable problems but to pre-empt challenges that may delay or frustrate progress on an otherwise sound investment platform.

The competitive implications in the supply chain are more complex and varied. This is in part because technology is still being developed and innovated on, and even more so because of co-opetition.

For mobile operators, the key goal is to grow B2B revenues (which now encompass a wide range of their total business (15–40%)) to monetise 5G network and spectrum investments, and diversify the overall revenue base. The risk is competition with vendors and cloud groups and, in the case of PNs, spectrum carve-outs for enterprise. Shrewd partnerships with the aforementioned segments and a shift in culture towards an IT consultancy will be key to achieving success.

Technology vendors have the same goal as operators, although it is even more pronounced since services revenues are a smaller share of the legacy networks business for groups such as Ericsson and Nokia. Vendors have established an early mover advantage with products in IoT and edge compute. The risk is in balancing new revenues with navigating co-opetition relationships with their main clients (the operators). Systems integrators and providers that manage remote device provisioning can act as a 'glue' between operators, vendors, cloud groups and enterprise clients.

Giesecke+Devrient
Creating Confidence

pod group
A Giesecke+Devrient Company

Digitizing enterprise IoT connectivity

ENO ONE

Simple Scalable Secure

- Simple deployment “as a Service”
- Simple management and billing via ONE platform
- Scalable globally through leading operator agreements
- Scalable as a white label service
- Scalable with ONE SKU* for all your devices
- Secure and remotely configurable
- Secure global IoT connectivity via ONE eSIM

** Stock keeping unit*

Discover what ENO ONE can do for your enterprise
https://podgroup.com/iot-esim-solutions-eno-one/
sales@podgroup.com

1

Enterprise spend rebounding as pandemic recedes

Fast versus slow lanes

Enterprise digitisation spend on new IT, network and technology projects spans multiple industries. While it can be difficult to measure and quantify 'digitisation', one of the indicators we use to gauge scale is IoT volume forecasts, as shown in Figure 1. Because of pandemic-related economic restrictions and IT project delays, we downgraded our near-term outlook during 2020, but raised expectations for the long term to 2030 such that volumes will more than double to 37.4 billion connections from 15.1 billion in 2021.

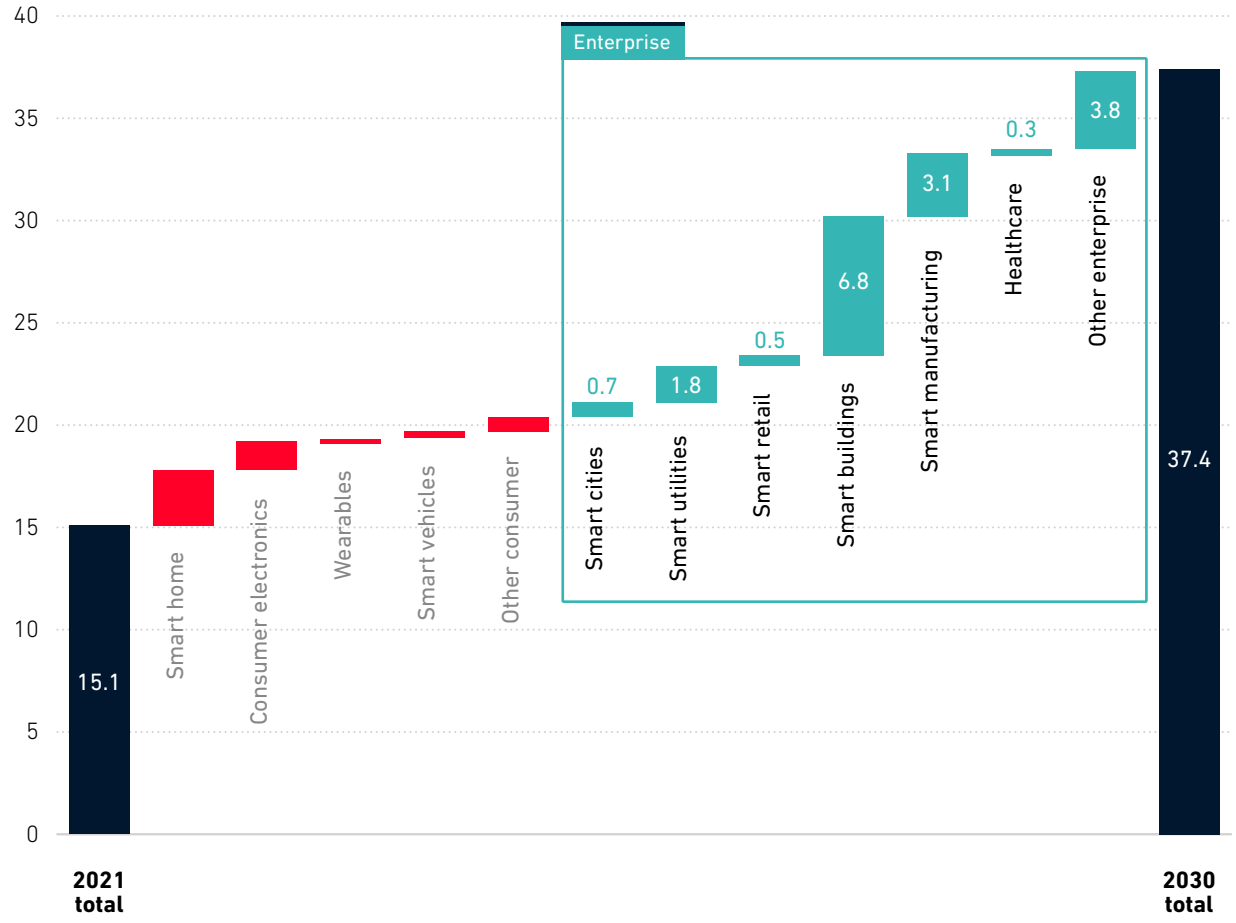
Two things stand out from this picture. First, the impending growth for total IoT connections underlines the economic value that companies, governments and government agencies (such as transport authorities) place on 'smart' operations. Second, while there will be some movement in consumer use cases, much of this has already occurred – for example, the promise of the smart home has tempered with subdued consumer interest. The majority of new/incremental IoT deployments will come from enterprise verticals. The range of deployments is diverse, with some examples listed below:

- **Manufacturing:** A broad category that includes smart factories and warehouses, typically fitted out with IoT sensors and cloud-based analytics to monitor production. This may also include private LTE or 5G networks.
- **Automotive (smart vehicles) and logistics (consolidated as part of 'other enterprise'):** These include passenger vehicle telematics and commercial logistics with, for example, driver and fuel monitoring systems. (Note that other transportation verticals such as shipping and aviation are consolidated in our 'other enterprise' segment in Figure 1.)
- **Buildings:** This includes upgraded heating and cooling systems to maximise energy efficiency, HVAC systems (combined heating, ventilation and air-conditioning) and dynamic climate control as occupancy changes.
- **Utilities:** While much of this in volume terms will come from government-mandated smart electricity and gas meters on residential premises, the largest investments will come from power grid operators and renewable energy providers as part of joined-up smart energy systems.
- **Healthcare:** This includes telemedicine, remote diagnostics, IT upgrades in hospitals and clinics, and AI-based predictive analytics.

Figure 1

IoT will reach 37 billion connections by 2030, with enterprise sectors driving growth

IoT connections base (million)



Other enterprise includes agriculture, shipping, logistics, heavy industries (e.g. oil and gas) and a range of smaller segments. Other consumer includes a range of small-volume categories.
Source: GSMA Intelligence

Where does this leave the digitisation trend?

The digitisation trend in the long term is positive, albeit with near-term uncertainty. The fundamental rationale for digitisation of companies in different enterprise verticals remains the same, which includes:

- allowing productivity gains from the use of data analytics and more efficient operations
- enabling cost savings
- opening (or speeding access to) new revenue streams
- redeploying labour to higher-value functions.

Such rationales have always been the reasons that digitisation became a structural trend across the economy – just as electrification did over 150 years ago.

There is, though, uncertainty about how this will play out moving forwards given the re-emergence of inflationary pressures, supply-chain risks and geopolitical instability from the war in Ukraine. Supply-chain impacts on chipsets, rare earth metals and other raw materials exacerbate an already fragile situation from the ongoing US/China trade frictions.

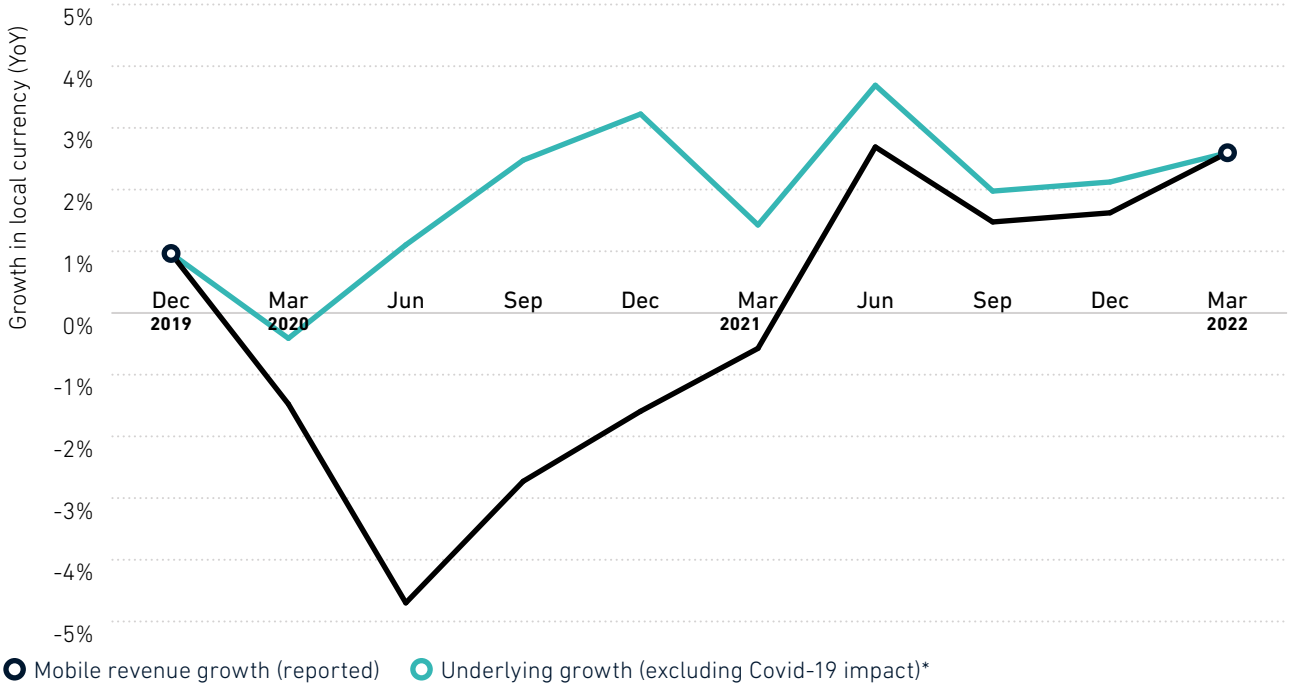
There is also the enduring impact of Covid-19, even though that is easing. The telecoms sector absorbed a financial impact from the pandemic equivalent to taking 4–5 pp off overall mobile revenue growth. This impact can be seen in Figure 2 as the gap between reported revenue growth and the notional value of what growth would have been if the pandemic had not happened (we refer to this as underlying growth).

Mobile operators reported that B2B and IoT spend (which they tend to consolidate under 'enterprise' revenue) was one of the main revenue streams affected in 2020/21, alongside their roaming and retail trade. The large-scale nature of these corporate investments made some vulnerable to delay, although others actually accelerated because of the evident changes that Covid-19 would have to long-term operating models (retail store numbers and experiences being a good example).

Figure 2

The Covid-19 pandemic took 4–5 pp off mobile revenue growth

Average of US, UK, Spain and Brazil



*Refers to what growth would have been without the impact of the pandemic. For example, in June 2020, the average pandemic impact was 5.8% for the mobile operators in the four countries, meaning that revenue growth on an underlying basis would have been -4.7% + 5.8% = 1.1%
Source: GSMA Intelligence

The broader trend of digitisation across industries that underpins investment in cloud compute, 5G, AI and analytics was set in motion before the pandemic, so the gathering pace of recovery should be seen as a resumption of activity after a 'pause' rather than something wholly new.

Our purpose in this report is to strip away shorter-term effects from economic and political instability and focus on the longer-term implications from digitisation and the technology enablers that will power it. This applies to business and operating models of vertical sector companies and, just as importantly, to telecoms operators, vendors and cloud groups competing to enable and service this business.

2 Tech enablers

Three broad technology 'families' sit at the intersection of the telecoms and cloud industries, and are the key infrastructure underpinnings for digitisation, especially for enterprises. These are:

- private networks (PNs)
- IoT devices, including eSIM and provisioning
- cloud and edge compute.

These three families house the key tools being used across different industries for digital transformation. Together, they provide the fundamental underpinnings of ultra-high-speed and low-latency connectivity, flexibility for device provisioning, and compute infrastructure to run AI-driven analytics to optimise operations and efficiency. The value chains that provide the products in each area are somewhat disparate but increasingly interconnected.

The next three chapters provide a deep dive into these enablers using a mix of analysis and examples of deployments on the ground. Each section follows a common format to ease interpretation.

It is important to qualify we are not covering each area in its entirety. Cloud compute is, for example, an industry in itself with separate competitive dynamics to the telecoms sector even though these two groups (cloud companies and telcos) do have some overlap. Instead, our focus is on a subset of key technology streams within these broad families: for PNs we mostly focus on cellular PNs running on LTE or 5G; for IoT we focus on eSIM; and for cloud we focus on edge compute.

We have incorporated commercial examples from a selection of industries, including manufacturing, automotive (passenger vehicles and commercial logistics) and energy. These sectors are at the leading edge of digital deployments, helping to illustrate, for example, implementation strategies and RoI benefits. These industries help show the economic and competitive implications of enterprise digitisation for other industries, such as media, sports and financial services.

3 Advanced connectivity: private networks

Private networks: what, why and why now?

Private networks (PNs) are point installations that provide dedicated connectivity to a paying corporate or public sector client at one or more defined locations. PNs usually draw on licensed spectrum holdings from a mobile operator or those purchased directly via auction (such as CBRS priority access licenses in the US).

By erecting a new 'mini network' PNs do not need to be in areas where mobile coverage already exists – hence their attractiveness in dense and rural areas. While PNs are seen by telcos and their vendor suppliers as a means for monetising 5G in enterprise settings, they have been around for many years using LTE. However, take-up levels have remained fairly low, with contributions to telco B2B revenues being minimal.

Digitisation and the need for secure, low-latency connectivity on premises is the main change that has brought PNs back into focus. To a certain extent, dedicated spectrum carve-outs for direct use by verticals have also played a role in countries where permitted, mostly Germany and the US. Overall, three main developments have driven momentum in 5G PNs over the last 12 months:

- **Increased digital IT investment in the manufacturing sector:** Industrial premises in the form of factories and warehouses are natural settings for dedicated networks given the need for precision operations and data analytics that run across a densely linked network of localised assets (e.g. car manufacturing or cold-chain food logistics and processing). While reported data from operators is limited, we can infer the progress of adoption of PNs in manufacturing based on estimates from the Global mobile Suppliers

Association (GSA) (manufacturing is the largest industry for PNs, accounting for 12% of PNs) and our own survey of operators. Even in the midst of the pandemic in 2020, 86% of operators said they had launched or planned to launch PNs with at least one enterprise customer (many will have been LTE), while 80% cited manufacturing industries as among the top three sectors for expected B2B revenues to 2025, according to our survey.

- **Expanded range of 5G standalone (SA) networks:** This is a key supply-side factor. Except for in China, most mobile operators have run a tethered network strategy for 5G rollouts in which 5G radios are anchored on LTE masts using an LTE core (so-called non-standalone (NSA) networks). This works for consumer smartphones but is trickier for industrial use cases that demand ultra-low latency, which would need a slice. 5G SA (i.e. greenfield) is needed for the latter. The growth of SA is, fortunately, reflected in the data: our tracking suggests that of the 180 operators with a live 5G network as of March 2022, 10% have launched 5G SA and over 50% have publicly announced plans for it. This means that over 100 operators have launched, or are in the process of building, 5G SA networks. The number of 5G SA networks will likely expand incrementally starting in specific locations where revenues are most likely (i.e. business premises).
- **Supplier diversification:** Conventional wisdom would suggest that telecoms operators, as the owners/gatekeepers of the vast majority of spectrum, be the primary suppliers of PNs to enterprises. The fact that Nokia, Ericsson, Huawei, Cisco and other vendors are operators' main suppliers may suggest it would be unwise for them to go into direct competition with operators for big-ticket B2B technology spend. However, this type of co-opetition is growing. Examples that point toward this trend include Lufthansa using twin but separate PNs supplied by Vodafone and Nokia for aircraft maintenance and testing in Germany, and Cisco's neutral host for the 2022 Super Bowl. The implication is that enterprise buyers have gained buying leverage amidst a larger range of suppliers and more price-competitive marketplace.

Adoption so far and where we're headed

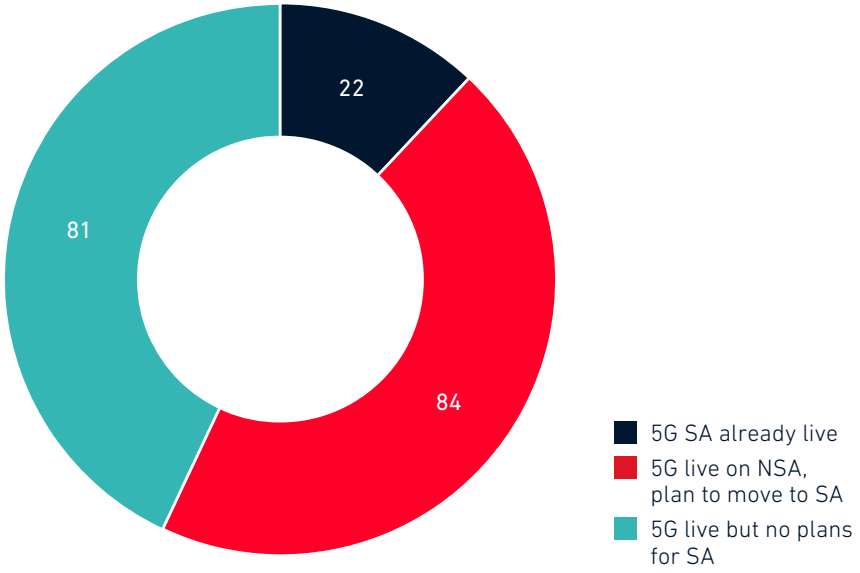
Depending on the estimate taken, PNs total in the hundreds rather than thousands.[1] The majority of these are LTE (approximately 60%), with around 20% being 5G and the rest having both capabilities. The true number of PNs may be higher given that the above estimates only track publicly announced networks. Even if the true count is higher, there is a big gap between the current reality and the theoretical potential. Nokia has estimated an overall addressable universe of 15 million locations for PNs, though this is a highly unrealistic figure, as almost 95% of these sites are factories or warehouses, of which most are in China, India, Vietnam and other industrialising Asian countries. While this estimate assumes any factory is in the addressable market, current adoption levels indicate the potential to be much lower. Less than 1% of factories in the world have so far been made 'smart' (i.e. production and maintenance tracked and adjusted via cloud analytics), with Scandinavian countries, Germany, the UK and the US being the main centres for pilots and deployments.

The expansion of 5G SA networks is likely to drive the number of PNs up. SA networks can deliver the ultra-low-latency requirements that many industrial clients need, which a guaranteed QoS through a ringfenced (i.e. not open to competing uses) PN reinforces. SA networks are still in the minority, with only 22 live installations, which translates to around 10% of operators with a 5G network (see Figure 3). Indications from operator reporting suggest this is changing. China was the only majority SA country from the outset in the 5G era (see Figure 4); however, the US and most three- and four-player markets in Europe – France and Italy being notable exceptions – are in a situation now where over half of operators have publicly announced plans for 5G SA. Spectrum release, demand from industrial clients and refarming of 2G and 3G spectrum have all helped. This does not mean 5G NSA will be fully replaced, at least not at first, more that there will be a phased expansion of SA such that the two network topologies will coexist and serve different parts of a given country.

1 The GSA counts around 650 companies and organisations (February 2022), while analyst group Berg estimates 300.

Figure 3

SA is a prerequisite for industrial 5G, but only 10% of telcos with a live 5G network have deployed it

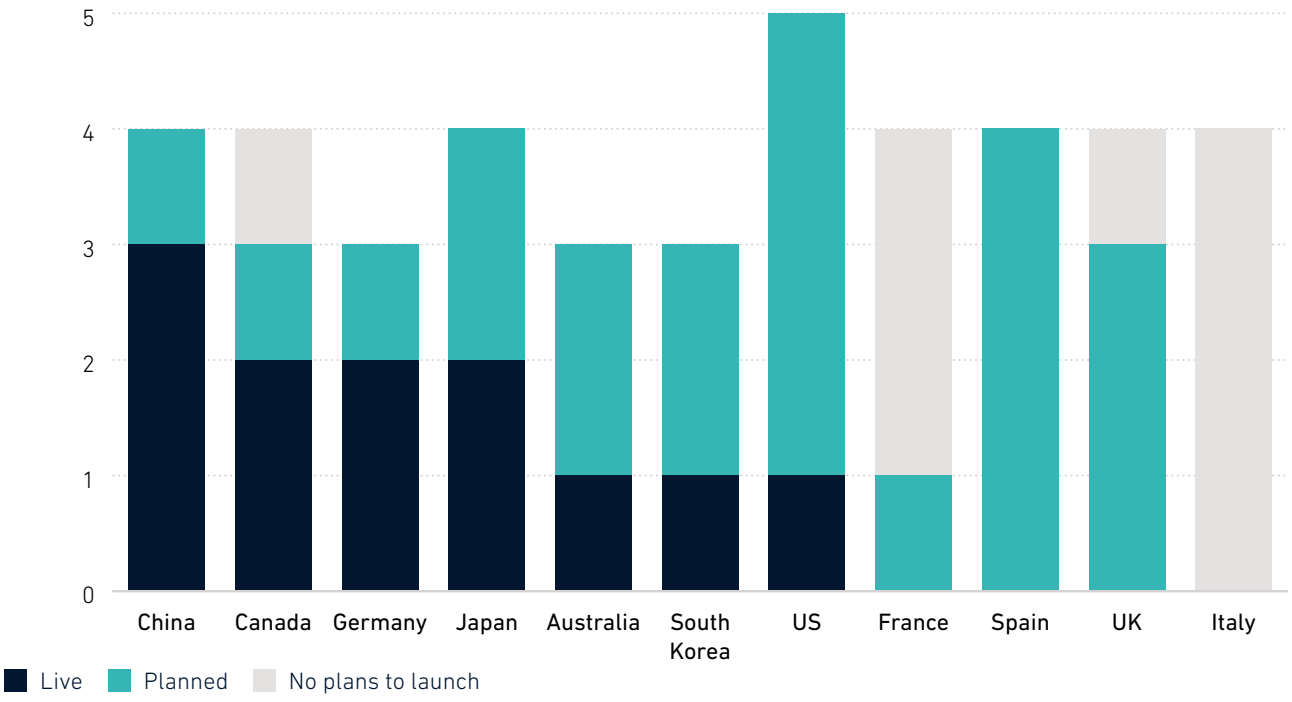


Figures represent the number of mobile operators, split by their 5G SA network status and publicly stated intentions. Data as of March 2022.
Source: GSMA Intelligence

Figure 4

China remains the only majority 5G SA country, although others are moving towards this

Number of operators with a 5G SA network



Data as of March 2022.
Source: GSMA Intelligence

CASE STUDY

Europe's largest highly innovative 5G multifunctional campus

Efficient connectivity management for sustainable IoT devices

CUSTOMER
Deutsche Messe, Hannover (based in Germany)

PROVIDER
Giesecke+Devrient (G+D)

OTHER COMPANIES INVOLVED
Pod Group, SODAQ, TUK

Context and pain points

- 4G and 5G enable a vast number of new IoT use cases, such as in manufacturing or logistics. To unleash their full potential trusted connectivity and data are essential. Private networks contribute to this and provide significant benefits, especially for enterprises.
- Initiatives such as Deutsche Messe's 5G Smart Venue are crucial to enable enterprises to conduct test scenarios and field trials for their 5G product development. Within these environments secure and convenient onboarding, tracking, roaming and life cycle management of devices are mission-critical activities for the digitisation of enterprises.

Deployment strategy

- The cooperation between Deutsche Messe and G+D includes the deployment of security and authentication solutions for the 5G Smart Venue. This creates an important prerequisite for secure lifecycle management of devices and systems while they are within the dedicated private network of Deutsche Messe. The 5G Smart Venue was launched during the leading international exhibition Hanover Messe in May 2022.
- G+D provides a remote provisioning system (G+D AirOn) for the multitudes of eSIM-enabled devices on premises. eSIMs are equipped with a local profile assistant such that each device can connect and seamlessly switch between private networks depending on the location and functionality it demands. A simple, fast and fully digital way for eSIM-enabled devices to be logged into a private or public network via QR code is enabled by G+D's eSIM management solution AirOn.
- Pod IoT Suite uses the G+D eSIM management to download and activate the different profiles. At the manufacturing stage, a Pod ENO ONE SIM is embedded into an eSIM device. It includes a bootstrap profile, which enables zero touch provisioning as well as the connection to the desired network.
- SODAQ, a partner of G+D, offers an end-to-end solution for tracking valuable goods along the entire supply chain. The Track Solar device is the ideal sustainable solution for the logistics and manufacturing industry.
- TUK is a research institute pioneering the use of advanced networking solutions to improve operational efficiency in industrial settings. TUK uses the 5G Smart Venue to move eSIM-enabled autonomous robots seamlessly between public and private networks.

Benefits

- Deutsche Messe offers Europe's largest highly innovative 5G multifunctional campus on an area of 1.5 million square meters. Here, future intelligence technologies are made visible and tangible. G+D and partners implement components of mission-critical activities for the digitisation of enterprises.
- The customised nature of a private network combined with eSIM management provides flexibility to enterprise buyers, something particularly attractive when working with hundreds or thousands of devices on premises or in remote locations inaccessible (or highly expensive) for staff call-outs.
- The solutions underline the importance of convenience and security in IoT. They are realised by using sustainable hardware and system components, which play a significant role in large-scale deployments and are a competitive advantage.

Executing on the promise: risks to address

Beyond the availability of SA networks, the eventual success or failure of 5G PNs will depend on several factors:

- **Spectrum availability:** PNs require sufficient spectrum to operate, regardless of whether they are controlled by a telco or enterprise vertical. mmWave spectrum may be suitable for defined area networks such as a manufacturing plant, although this is primarily a US phenomenon for now. Other countries/regions will rely on mid-bands, some of which have been released and some of which have not and remains pending assignment. The regulatory attractiveness of carving out spectrum for the exclusive use of industrial companies directly is based on reducing the barriers to entry for running advanced networks. There are, however, several problems with this, including a lack of internal expertise, the cost to deploy a network and potential interference issues without priority rights. Providing increased licensed spectrum that can be used by operators and their vendor partners for running campus networks is a far more economical and sensible approach.
- **RoI proof points:** 5G PNs will be weighed against the overall investment cost for IT transformational upgrades, such as for a smart factory, port or city. The risk here is companies demanding a short payback period (five years or less), when it is likely to be more gradual. This means that factors besides new revenues must also be pushed, particularly cost savings associated with reduced energy, lower carbon emissions in line with a higher share of renewables and the ability to redeploy labour to higher-yielding functions.
- **PNs versus cloud:** Another factor is the extent to which a PN is needed as data-centre capacity moves closer to the edge of the public access cellular network and replicates some of the same functions. This last point is perhaps most sensitive now that most cloud majors have products doing just that (e.g. AWS Greengrass). As cloud capacity expands, so too does the window of opportunity for operators close. For this reason, many telcos have gone into partnership with webscalers either to lease cloud capacity or as joint bidders for enterprise contracts. The recent partnership expansion between Deutsche Telekom and Google Cloud is a good example, as is AT&T's collaboration with Microsoft.

Kigen

Supercharging towards secure and trusted IoT

The present day IoT is complicated and fragmented. We can do better.

Kigen's Open IoT SAFE enables enterprises to take advantage of chip-to-cloud security and scalability to make most of their eSIM adoption. No matter what vertical, a security-first approach gives you the advantage.

Discover the scalable solutions with Kigen eSIM OS with OPEN IoT SAFE today.

› kigen.com/esim

Recognized as eSIM enablement "specialist" global leader for 2021 by Counterpoint Technology Research

4

IoT devices: eSIM

eSIM for vertical sectors: what, why and why now?

eSIM technology has long been seen as a substantial enabler and accelerator of IoT deployments across vertical sectors such as automotive (e.g. connected vehicles), utilities (e.g. smart meters and smart grids), logistics (e.g. tracking systems) and agriculture (e.g. farm monitors). It's not a coincidence that mobile ecosystem collaboration for setting up eSIM global specifications started with IoT, culminating in the first release of the GSMA eSIM specifications for connecting M2M devices in 2013. Since then, eSIM specifications have been continually updated or upgraded to reflect new IoT requirements, capabilities and market demands, including work on integrated SIM (iSIM) technology (integrated eUICC).

The connection between IoT deployments and digital transformation is clear and robust. Our research, based on a global survey of around 2,900 enterprises across most vertical sectors in 18 major countries, shows that IoT deployments are part of a wider digital transformation agenda for 63% of enterprises (IoT deployments are standalone initiatives for 37% of enterprises). That means eSIM deployments in IoT are eSIM deployments for digital transformation.

eSIM benefits for IoT vertical sectors span multiple areas. An eSIM provides considerable space reduction in an IoT device compared to traditional removable SIMs and can be updated remotely using over-the-air (OTA) technology, significantly increasing the range and nature of IoT devices that can be connected. This is a significant benefit, for example, for companies with fleets of connected machines in inaccessible remote locations that need to operate for long periods without human intervention. Also, eSIM reduces logistical and manufacturing costs compared to a traditional removable SIM (while maintaining the same function) and offers a single stock-keeping unit (SKU) and best-in-class security (a must for all IoT solutions).

From a service perspective, the add-on model enabled by eSIM is fit for purpose; the multi-country connectivity and roaming functionalities is built in during the manufacturing process of the IoT devices (including cars), and then delivered locally to IoT applications and services, in a zero-touch process enabled by bootstrap technology. This allows IoT companies to leverage eSIM to enhance their global propositions and solutions. Different solutions to ensure truly global connectivity (and global roaming) while giving enterprises access to all the network profiles they need to scale are being deployed and commercially launched, including solutions that leverage multi-IMSI and eSIM technologies for both public and private networks (e.g. the recent ENO ONE solution developed by Pod Group).

Over the last decade, leading providers of eSIM technology have been vocal about the benefits of eSIM for IoT use cases and for enterprises. But what do enterprises think of eSIM, and what do they expect from it? GSMA Intelligence research, based on the abovementioned enterprise survey, reveals important insights. First, awareness of eSIM is high among enterprises – only 2% of respondents said they are not familiar with eSIM technology.

Second, 83% of enterprises said that eSIM is important to achieving success in their IoT deployments. That means there is an opportunity for operators and other providers of eSIM and IoT solutions to fulfil unmet enterprise demands.

Third, enterprises of all sizes consider best-in-class security and scalability as the top eSIM benefits (see Figure 5). More specifically, device-to-cloud or chip-to-cloud security is seen as the most important eSIM benefit for IoT deployments, to ensure data is secured throughout the entire path, from where the data is generated to where it is processed. This is one of the drivers behind the rise of partnerships between eSIM vendors and cloud companies and the growing collaboration around global security initiatives such as the GSMA's IoT SAFE. Importantly, for enterprises, security is not only a must-have backend requisite – our research shows that a majority of enterprises that have changed their security practices as a result of their IoT deployments or the Covid-19 pandemic have done so with the aim of adopting a security-first approach as a competitive advantage.

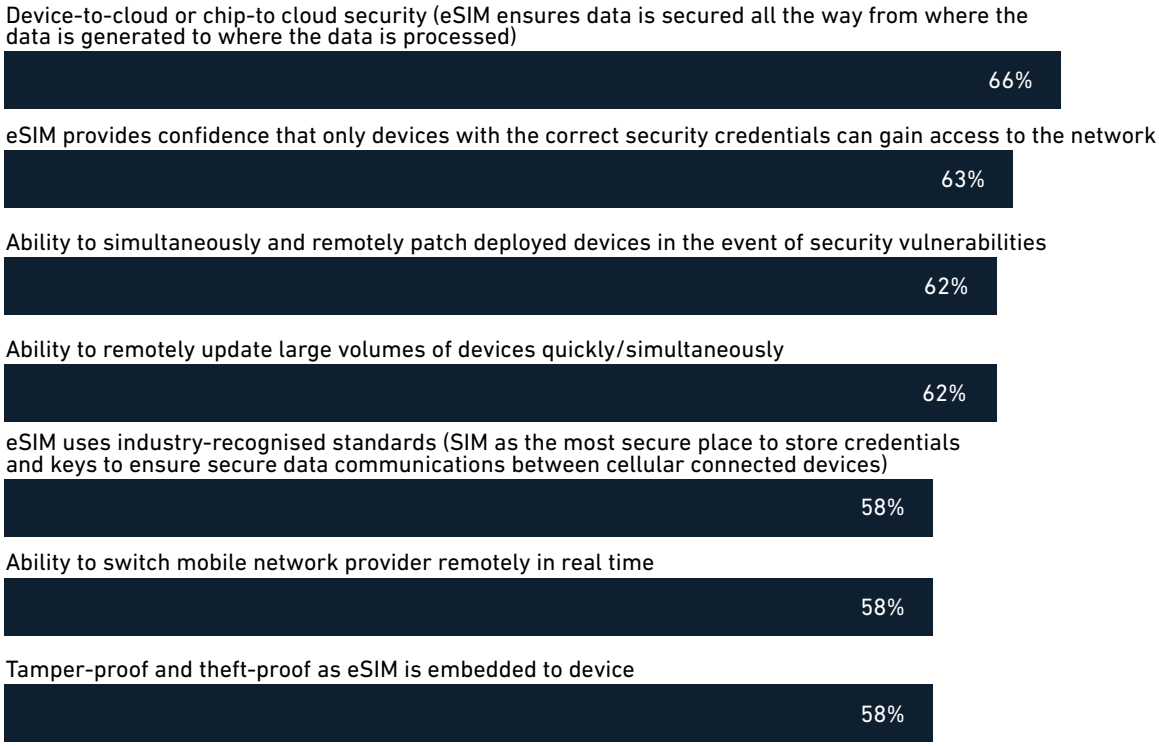
eSIM builds on the well-established reputation of the SIM as a leading route of trust for secure authentication and data protection (underpinned by a mix of hardware and software cryptographic algorithms and by the adoption of industry standards, based on the experience of more than three decades of using pluggable SIMs across all consumer and enterprise verticals). It also adds further security benefits (e.g. tamper-proof, theft-proof) that are extremely useful in some IoT scenarios (e.g. remote locations), and the flexibility for enterprises to control devices offered as a service (e.g. for roaming).

Scalability also ranks highly. The ability to remotely update large volumes of devices quickly and simultaneously is a key benefit that enterprises expect (and need) from eSIM. This comes as no surprise, given that the average IoT deployment size continues to grow. Very small deployments (fewer than 50 devices) now constitute less than 20% of total deployments, compared to a third in 2018. Finally, cost efficiency is boosted by having a choice of public native and roaming profiles in addition to customised SIM applets to enhance security, provisioning and device management.

Figure 5

Importance of eSIM benefits to the success of enterprise IoT deployment

How important is each of the following eSIM benefits to the success of your IoT deployments? (Percentage of respondents who said "very important")



Base: Enterprises that consider eSIM important to achieve success in their IoT deployments (N=c2400)
Source: GSMA Intelligence Enterprise in Focus Survey 2020 (global survey of c2900 enterprises across most vertical sectors)

Over the last 12–24 months, we have seen important eSIM advancements spanning multiple areas:

- **Moving beyond connected vehicles:** Automotive (consumer, light and heavy vehicles) is the leading sector, apart from consumer devices, in terms of eSIM deployments, accounting for a significant share of eSIM activations. eSIM functionality is available in a growing share of new cars (for both vehicle and driver/passenger features), and collaboration between operators, eSIM vendors and auto manufacturers is on the rise. Regulation (especially for eCall) is also driving eSIM deployments. Beyond automotive, we are seeing eSIM deployments in other vertical sectors. Today, eSIM technology is commercially available across a range of use cases including bikes, smart meters, drones, security cameras, healthcare, aircraft and smart tracking for micro-mobility in smart cities.
- **eSIM making its debut in private mobile networks:** Private networks represent an incremental market for eSIM. We have seen some trials or initial deployments already, led by major eSIM vendors such as G+D and Thales. For example, in 2021, the Technical University of Kaiserslautern completed a deployment test of eSIMs in a private network using network solutions from MECSware and eSIM technology from G+D. VITES and G+D have also teamed up to provide eSIM-based solutions for cellular connectivity in disaster recovery scenarios.
- **eSIM supporting the green imperative:** Sustainability has moved from the realms of corporate social responsibility to a core strategic priority for businesses in all sectors. The eSIM ecosystem is increasingly committed to sustainability. eSIM provides a more sustainable approach to connectivity, as it requires less plastic and less transport and produces less general waste. As enterprise IoT decision-makers become increasingly aware of sustainable initiatives and increasingly conscious about the environmental impacts of their purchase decisions, the green proposition will be a further factor driving eSIM adoption.

Adoption so far and where we're headed

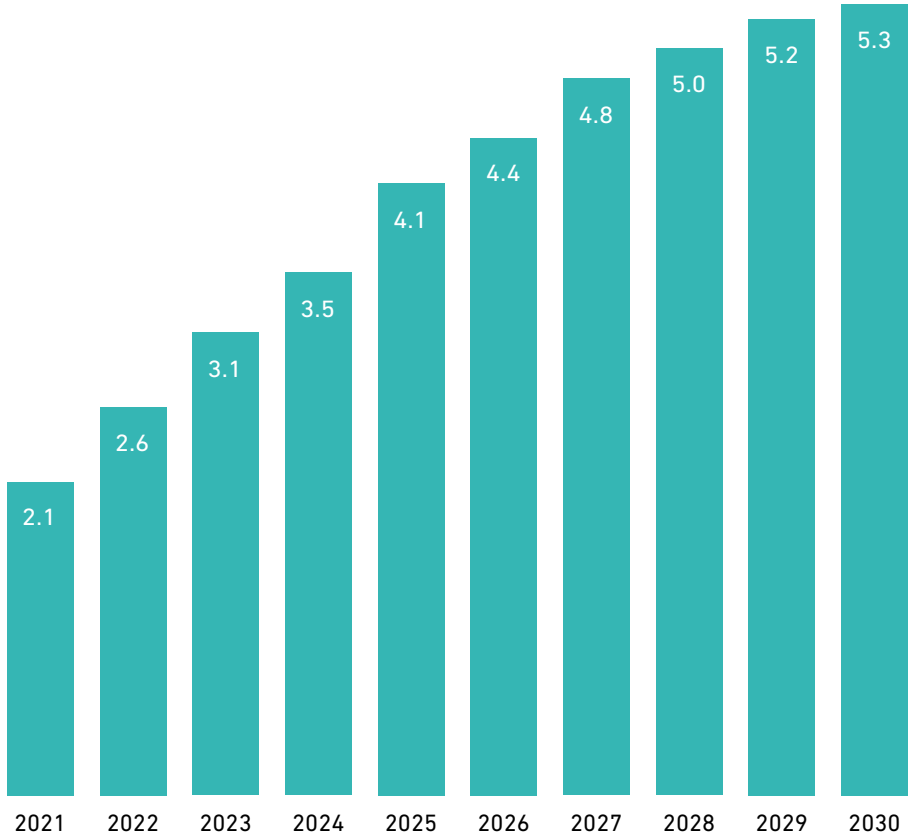
GSMA Intelligence forecasts that the number of IoT connections (enterprise and consumer) will reach 37.4 billion globally by 2030, up from 15.1 billion in 2021. Enterprise IoT will be the main driver of growth, accounting for 76% of the increase over the forecast period. Indeed, enterprise will surpass consumer in connections in 2024. Cellular networks currently serve 14% of total IoT connections (consumer and enterprise), with adoption of eSIM-enabled connections (a subset of cellular IoT connections) on the rise. The latest figures reported by the Trusted Connectivity Alliance (TCA) shows that the adoption of eSIM continues to grow in the IoT market. TCA members reported 38% growth in M2M eSIM shipments in 2021, driven by automotive and other IoT vertical use cases. That's an encouraging growth rate considering the chip shortages and supply-chain disruptions.

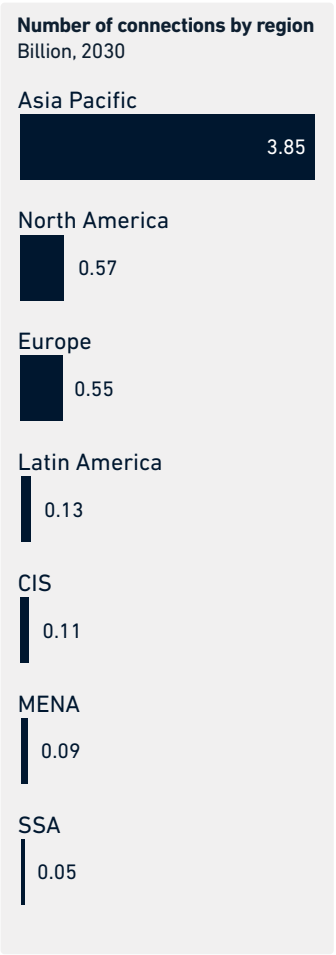
Looking to the future, the addressable market for eSIM in IoT is sizeable. GSMA Intelligence forecasts that the number of licensed cellular IoT connections will reach 5.3 billion globally by 2030, up from 2.1 billion in 2021 (11% CAGR), with China by far the largest market (3.5 billion). Cellular M2M will continue to support IoT devices that require mobility and higher data transfer speeds, with licensed LPWA coming of age to support devices previously served by legacy cellular networks (2G/3G). eSIM (and iSIM) is targeting an increasing share of cellular IoT connections.

Figure 6

Licensed cellular IoT connections (consumer and enterprise)

Number of connections globally (billion)





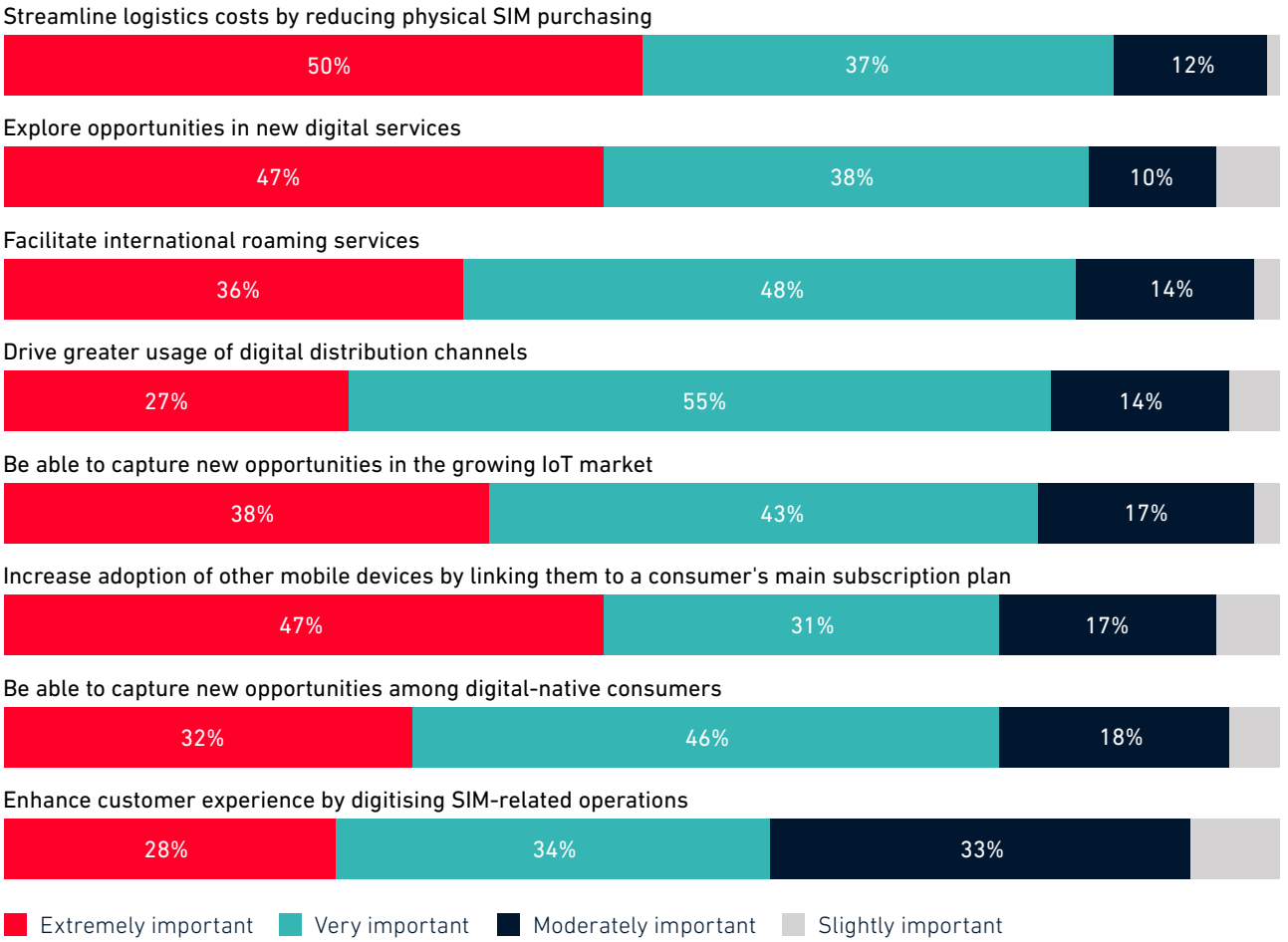
Source: GSMA Intelligence

MNOs and MVNOs have a big role to play in driving eSIM adoption across IoT vertical sectors. Our research shows that 81% of operators see eSIM as "extremely" or "very" important to be able to capture new opportunities in the growing cellular IoT market (see Figure 7). While it's difficult to track how many operators have launched commercial eSIM services for enterprise use cases, the pace of eSIM launches in the smartphone market provides an important reference. As of 2021, 232 mobile service providers (MNOs and MVNOs) had launched commercial eSIM service for smartphones across 82 countries. Discussions with eSIM vendors indicate that these figures are probably higher now. With 88% of operators planning to offer eSIM service for smartphones by 2023, momentum will build in 2022 and 2023.

Figure 7

The importance of potential benefits associated with eSIM

Rate the following potential benefits associated with eSIM based on how important they are to your business (Percentage of respondents)



Source: GSMA Intelligence Operators in Focus Survey 2021 (global survey of 100 operators)

eSIM in practice

There is no shortage of successful and innovative deployments of eSIM technology across IoT vertical use cases. All eSIM vendors are successfully externalising their achievements, innovative solutions and new partnerships, which certainly helps drive eSIM momentum. In this section, we focus on energy, a sector that is undergoing unprecedented digital transformation driven by changing regulations, sustainability efforts and the need to modernise legacy energy infrastructure in an IoT world. Data is a fundamental asset in smart grids as it allows more efficient energy resource management while ensuring smarter coordination between supply and demand of energy across all use cases, where it is needed and at any time. The shift in automotive, enabled by electrification of vehicles, also brings new IoT assets into the energy mix as well as new and high-volume IoT data into smart grids.

Kigen has been driving innovation and developments in smart grids, leveraging eSIM and IoT SAFE technologies. Key projects include KORE, Kigen and EnergyWeb working together to develop a smart grid application that provides secure data to IoT providers and Kigen working with Iskraemeco for eSIM-enabled smart metering (the following case study).

In 2021, Iskraemeco (a global smart metering solution provider with 100 million meters installed) turned to Kigen as it began trials of its next generation eSIM-enabled meters with multiple utility companies.

CASE STUDY

eSIM in smart meters

Digital transformation of energy grids through eSIM-enabled smart metering infrastructure

CUSTOMER
Iskraemeco

PROVIDER OF ESIM TECHNOLOGY
Kigen

Context and pain points

- Smart meters are moving beyond their original use cases, forming the foundation of truly interoperable systems that enable seamless data flows and smooth upgrades for new smart grid and smart home applications. Regulation is a key driver, as is the need to modernise outdated smart meter infrastructure that currently hinders the ability of energy companies to unlock the potential of data insights.
- Connectivity is an essential enabler across long service lifespans. However, using the traditional, removable SIM has some limitations. SIM procurement, handling, testing and distribution adds significant overheads and cost. Also, in harsh field conditions contacts can corrode over time and SIM cards may then operate intermittently or fail. For this reason Iskraemeco decided to shift to eSIM, which enables both factory over-the-air meter testing and out-of-the-box global connectivity. eSIMs can survive extreme temperatures, humidity, corrosion and vibrations, and because they are more difficult to remove, their physical security is also better than that of traditional SIMs.

Deployment strategy

- Iskraemeco manufactures the smart meter and embeds the eSIM. The smart meter can be deployed anywhere in the world and, thanks to the global connectivity bootstrap profile contained in eSIM, it can connect to any available network. Iskraemeco decides which profile will be downloaded and enabled on the meter based on criteria such as location.
- Kigen's remote SIM provisioning (RSP) server delivers the selected operator profile to the smart meter and requests profile enablement, with no need for physical access to the device. The smart meter connects to the desired network with the newly activated profile. eSIM cards run Kigen's eSIM OS.
- Iskraemeco aggregates data flowing from its smart meters. Small and medium utilities typically adopt Iskraemeco's meter management software, while larger utilities usually have their own software, integrating Iskraemeco's data stream.

Benefits

- Integrating Iskraemeco's meter management software with the Kigen RSP server's APIs offers the opportunity to create a unified data workflow for utility companies, which can then provide value-added services to their consumer and enterprise customers, such as dynamic pricing, real-time billing, real-time access to connected devices for remote monitoring, analysis and usage control.
- When coverage is patchy, networks can be switched quickly and easily to ensure continuity of service. Interoperability across mobile operator profiles, as well as modular subsystems, removes hurdles for utilities when integrating mobile technology for large-scale, cost-sensitive smart meter deployments.

Executing on the promise: risks to address

eSIM adoption in IoT vertical use cases is growing, but it's fair to say that eSIM has yet to reach critical mass. To a large extent this is expected, as ecosystem reconfiguration takes time. The ongoing period of transition from SIM to eSIM is much needed as companies gain eSIM experience and adjust to new manufacturing and logistical processes.

To fully leverage the potential of eSIM for enterprise digital transformation, and scale market adoption, various challenges need to be addressed at the ecosystem level in the coming years:

- **Proprietary solutions versus global specifications:** There is widespread agreement within the mobile ecosystem that adopting a single approach on global standards and specifications is key to driving eSIM to scale. The GSMA eSIM specifications are seen as the most viable and widely implemented option considering their international recognition and benefits in terms of security and compatibility. However, there are still proprietary solutions out there. Full alignment on the adoption of standard and global specifications would ensure that smaller operators, OEMs and providers of IoT services continue to have equal access to market opportunities while helping tackle some of the challenges around cost, integration and interoperability of different IoT solutions and platforms.
- **Selling technology versus solving enterprise pain points:** Across all businesses, people in charge of making digital transformation investment decisions are interested in the expected RoI rather than the underlying technology. This involves evaluating how a new solution will help them reduce the total cost of ownership of managing IoT while getting more analytics and ultimately gain a competitive edge. To reach critical mass, eSIM solutions need to help address some of the top challenges that enterprises face when deploying IoT solutions, such as integration with existing technology and legacy systems, data security concerns and cost of implementation (the top three challenges according to our research). Also, given the multitude of new features and applications that enterprises need for their digital transformation, developing end-to-end solutions that integrate those features in a seamless and cost-efficient way is increasingly key to lower entry barriers, especially for SMEs.
- **Single initiatives versus sector-wide deployments:** While individual initiatives (e.g. those seen in smart energy or disaster response) help build momentum for eSIM in vertical sectors, sector-wide deployments (e.g. those seen in connected cars) are needed to scale eSIM adoption. But how do we get there? Covid-19 and 5G are important factors to leverage. The pandemic has accelerated the digital transformation of vertical industries, fuelling demand for connectivity and value-added services, including IoT, cloud and security. Similarly, the success of eSIM in the enterprise IoT market is to some extent linked to the future adoption of 5G in vertical sectors, which requires product/service innovation and the ability to match 5G benefits with enterprise requirements. Solving today's challenges of permanent international roaming (regulation is a factor) is also important, as discussed in our Roaming in a post-Covid world report.
- **eSIM versus iSIM:** While the mobile ecosystem is currently focused on the implementation and adoption of eSIM, iSIM technology is also being explored both as integrated eUICC and integrated UICC. The first builds on eSIM progress, going a step further to embed the eSIM functionality into the device's main processor while still using trusted hardware that passes all the security checks applied to traditional SIM cards and eSIM chips. eSIM versus iSIM is not an either-or scenario and there is overlap (e.g. integrated eUICC). Both are valid options that will continue to coexist to meet the requirements of the varied IoT use cases. However, the IoT ecosystem shouldn't let the technology (eSIM or iSIM) determine the future direction of enterprise IoT. Beyond the form factor, there are important developments needed for operating systems, backend performance systems, onboarding and applications that will support the adoption of enterprise IoT use cases at larger scale.
- **Strategy versus implementation:** Beyond the technology factors (implementation), future eSIM deployments at scale will also depend on IoT companies having a clear eSIM strategy alongside their main IoT proposition. Many major companies in the wider IoT ecosystem believe that eSIM is crucial to driving enterprise IoT developments, but few have a clear eSIM strategy. Embracing eSIM at scale undoubtedly takes time, but it's an important requisite to fully realise the eSIM benefits for enterprise digital transformation.

5 Cloud: edge compute and analytics

Edge computing: what, why and why now?

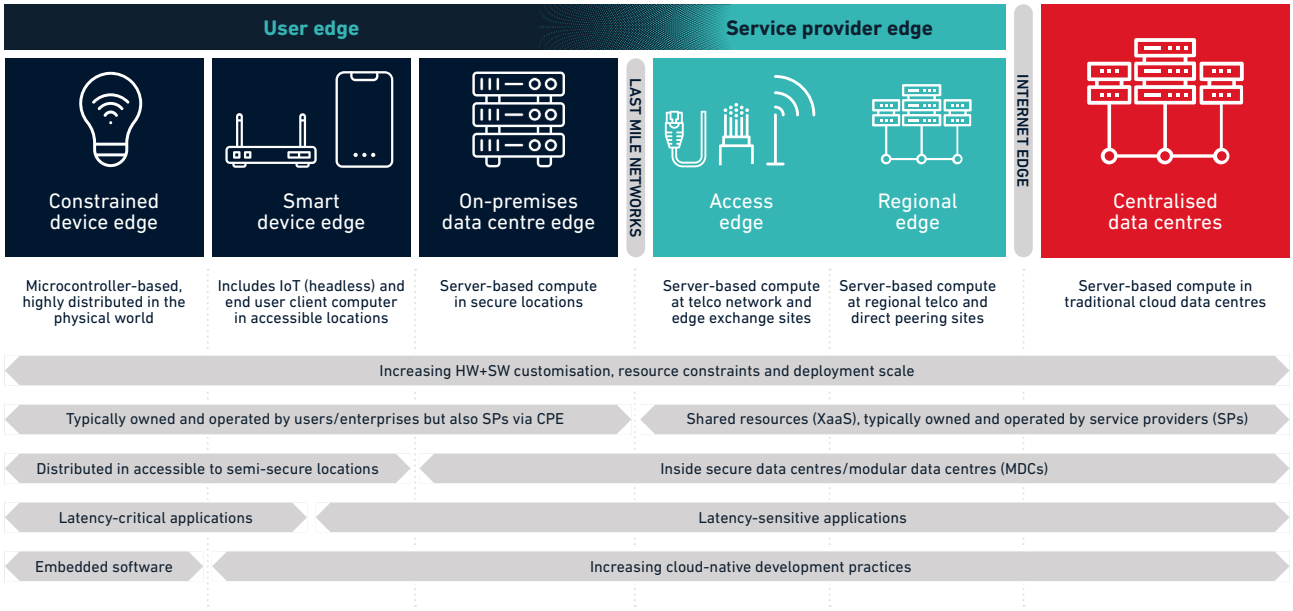
Edge computing discussions and debates predate the arrival of 5G. The commercialisation of 5G, however, pushed edge into the spotlight – a position it continues to maintain as operators and enterprises alike look to leverage 5G in support of digital transformation priorities.

The great expectations surrounding edge technologies can partly be explained by a broad view of how to define edge computing and where the 'edge' lives: in an operator's network; in the public cloud; at a customer premises; at a 4G/5G base station; an IoT gateway; or an IoT device.

While this doubtlessly contributes to confusion around edge computing use cases and deployment strategies, the reality is that the edge simply represents a continuum of models that place computing power closer to the end-user application than a traditional centralised core. These models range from regional data centres to lightweight, highly distributed devices, depending on application requirements (latency, reliability, data security/sovereignty). Each model implies technical, deployment and even business model trade-offs (e.g. ownership and management of edge devices).

Figure 8

How far can the edge go?



Source: The Linux Foundation

Definitions and use cases aside, what's not in question is the linkage between edge computing, 5G and enterprise digital transformation. Put simply, operators are looking for 5G to deliver new B2B revenues: 83% of operator CEOs in a GSMA survey highlighted enterprise and government verticals as the top opportunity for 5G revenue upside. Edge computing, in turn, is seen as a necessity for executing on key enterprise demands for a number of reasons:

- **Latency and reliability:** 5G promises low-latency connectivity, but placing computing power at the edge of the network – on the enterprise premises or potentially in an IoT device itself – enables latency-sensitive use cases while ensuring that applications can keep running regardless of the state of connectivity out to the edge.
- **Security and control:** IoT is about collecting, processing and making use of data. In many cases that data will be sensitive and even subject to privacy regulations. Keeping that data on-site and within the direct control of the enterprise helps to provide assurances over the integrity and sovereignty of that data, regardless of any latency or reliability requirements of an edge application.
- **Cost containment:** Cloud resources are making it increasingly easy to process data efficiently, inexpensively and with familiar, easy-to-use tools. Transporting data up to the cloud, however, can quickly become expensive, particularly for data-intensive use cases touching many endpoints. Processing data at the edge obviates the need to do so, making many use cases cost-effective that would otherwise not be.

The development of edge computing solutions and applications has been a work in progress for years, and that work continues. Beyond the theory of edge computing as an enabler of enterprise digital transformation, recent events and market developments point to the market's continued confidence in the promise of edge computing:

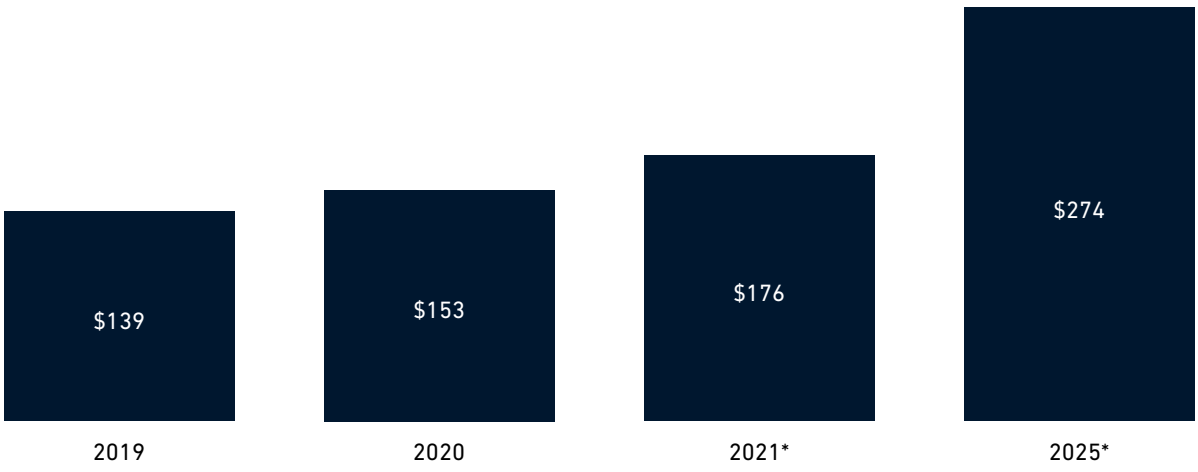
- **Cloud swallows the edge:** Earlier this year, AWS announced an expansion of its Local Zones programme, pushing its services out towards the network edge, in line with moves underway in edge from rivals Google and Microsoft. More recently, the acquisition of telco edge specialist MobiledgeX by Google highlights the continuing intersection of the cloud and edge industries, with hyperscalers looking to deliver the cloud wherever it's needed.
- **Edge fills out the vertical portfolio:** IT infrastructure suppliers have included edge solutions in their portfolios for years. Dell Technologies CEO Michael Dell leveraged his keynote at Dell Technologies World this year to talk about edge as "the next frontier, where data becomes a competitive advantage immediately at the point of creation". This wasn't a particularly new message, but when combined with Qualcomm CEO Cristiano Amon leveraging the company's 5G Summit to talk up the "intelligent connected edge" as central to its aspirations in automotive and industrial IoT markets, it is clear that the message isn't waning.
- **Operators and edge innovation:** Edge remains central to the enterprise and private wireless offerings from most operators. With 64% of operators stating edge is important to their success in the enterprise, as per GSMA Intelligence research, this shouldn't be a surprise. Yet, Vodafone's launch of its Edge Innovation Programme 2.0 – aiming "to inspire the creation of innovative and futuristic services, products and applications" with edge and 5G – signalled that operators still see themselves having a role to play in edge beyond simply executing on today's demands.

Adoption so far and where we're headed

Taking into account the multitude of use cases, solution components and solution owners, it's not difficult to see how the value of the global edge computing ecosystem could quickly grow into an immense market.

Figure 9

Edge computing market value, 2019–2025
Billion



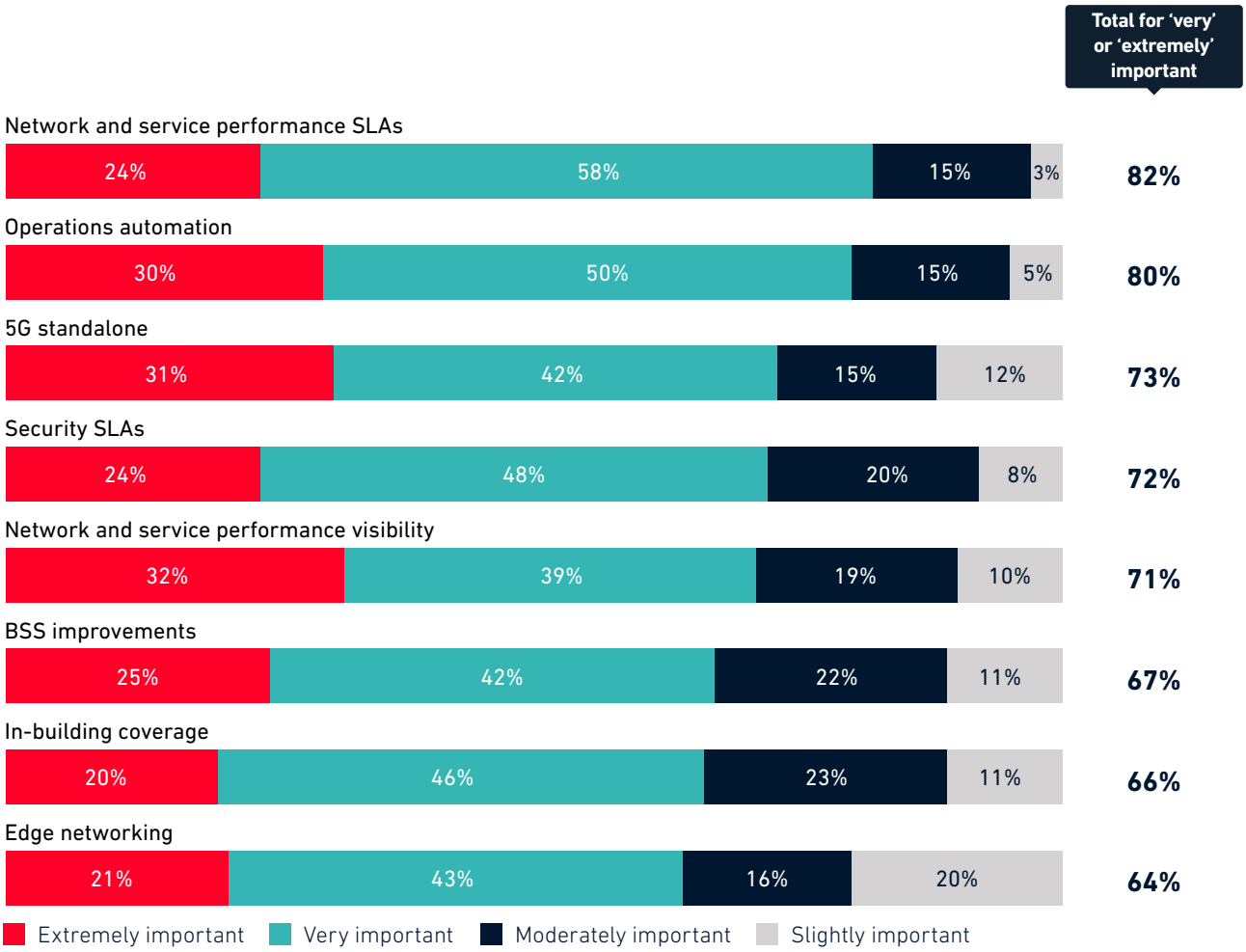
*Figures for 2021 and 2025 are forecasts
Source: Statista

The larger point is that the edge computing market opportunity is expected to grow sharply because edge delivers on enterprise demands and on operator interest in tapping those demands.

Figure 10

Technological capabilities aiding success with enterprises

How important is each of the following technology capabilities in helping you to achieve success with enterprises? (Percentage of respondents)



Source: GSMA Intelligence Operators in Focus: Enterprise Opportunity Survey 2021

With so many different priorities for operators in terms of monetising the enterprise digital transformation opportunity, the role of edge might not always be completely clear.

As mentioned previously, 64% of operators believe that edge networking as a technology is important to their success with enterprises. While this might seem impressive, edge networking is only one of many technologies operators acknowledge they need when trying to meet enterprise demands – in fact, it's seen as less important than many others.

However, when revealing the value operators will be delivering to enterprise customers via 5G – today and in the future – the role of edge becomes much clearer. While edge was a minor part of the 5G enterprise message in 2021, it's expected to be the top value proposition as we go into 2023 and beyond. As operators build out their 5G and edge capabilities, it is understood that edge will need to be a critical part of the 5G enterprise and digital transformation message.

The logic here is easy to follow. Operators see themselves playing a role in supporting digital transformation across the entire breadth of enterprise verticals. But four verticals stand out: financial services, retail, manufacturing and transportation. These are seen as the greatest potential revenue sources (connectivity and value-added services) in the 2020 to 2025 period. The role of edge in supporting their digital transformation is well understood:

- **Financial services:** Like many customer-facing industries, hyper-personalisation in support of improved customer experience is a focus for financial services. Edge-based computing underpins data analytics applications for security and fraud detection while keeping sensitive customer details secure.
- **Retail:** Hyper-personalisation and contextual marketing are goals for the broader retail industry. At their most ambitious these may involve immersive in-store experiences, which can only be made possible with edge compute. While more mundane, operational support for customer traffic management and inventory management also benefit from the edge value proposition.
- **Manufacturing:** Latency-sensitive applications dominate the discussion of edge computing in support of manufacturing and smart factories. Machine vision, machine control and automated guided vehicles all require the low-latency connectivity enabled by edge.
- **Transportation:** By putting edge compute devices in vehicles a wide variety of uses cases are opened up, from predictive maintenance and driver/pilot analytics to video analytics and even passenger-facing applications. By keeping data on the vehicle, connectivity costs can be kept in check, while reliability can be improved.

Edge in practice

The growing value of the edge computing market would not be possible if edge solutions were not being increasingly deployed and profited from. Investigating a recent example of edge being put to use in support of pandemic-related priorities helps to provide context for the edge value proposition through the lens of the transportation (and smart city) vertical.

CASE STUDY

Edge data processing for transport efficiency

CUSTOMER
Transport for New South Wales (TfNSW)

PROVIDER
Cisco

Linking IoT and edge infrastructure

Context and pain points

- TfNSW is the transport and roads agency in New South Wales, Australia, responsible for the country's largest metropolitan area, Sydney, as well as other areas.
- Across the diverse assets it is responsible for – rail, ferry, tram and bus – TfNSW had three priorities it needed to execute on: understand the real-time and historical performance status of the vehicles in support of improved maintenance; accurately track passenger loads in order to avoid congestion; and keep solution costs in check.

Deployment strategy

- Working with Cisco, IoT gateways were deployed on TfNSW assets, which supported integration with vehicle diagnostic ports and sensor functions such as GPS and accelerometer tracking.
- Cisco Meraki Smart Cameras were deployed to provide visual passenger counts, while a Wi-Fi analytics solution sourced from partner Cohda Wireless provided additional detail on passenger loads.
- LTE links provided connectivity from the vehicles and IoT gateways up to TfNSW's dashboard system.

Benefits

- The value proposition here was processing data at the network edge – on the vehicle.
- By performing video analytics and Wi-Fi device analytics on the vehicle, potentially sensitive user identity information did not need to be transferred to TfNSW's systems; only user counts were conveyed.
- At the same time, by only using the mobile broadband link to send user counts and vehicle diagnostic triggers – instead of a mass of raw data – mobile broadband usage was minimised, keeping data costs in check.

Executing on the promise: risks to address

- **Edge and cloud thinking:** In early 2018, GSMA Intelligence investigated a nascent edge computing market as part of the Radar series. Dedicated edge research followed later that year, and a major message across this work was the potential rivalry between telcos and cloud players as each looked to leverage their strengths to dominate the edge computing opportunity. By the middle of 2022, we still see cloud players and telcos focused on their respective assets, but with a larger degree of cooperation than competition. Even if the dynamic between telcos and cloud players has become more nuanced, there still remains the risk of the market viewing the cloud and edge as distinct rivals, with decisions made focusing on one versus the other. The edge represents a wide array of options, each of which serves its own role, alongside the use of centralised cloud assets. All of these assets and deployment locations, however, will need to work together and be planned for in a holistic way. Otherwise, the whole may well be less than the sum of its parts.
- **Internal roadblocks:** Across telcos and enterprises, the value of digital transformation, IoT and edge computing are not in question. In our 2021 enterprise survey we looked at the state of the IoT market through the lens of more than 2,800 enterprise decision-makers and found "unclear RoI" was an IoT deployment challenge for only 27% of enterprises. This matches operator thinking on edge networking: our 2021 research on operators identified RoI as the top edge computing deployment challenge for a meagre 1% of operators. Though the value of edge and IoT may not be in question, both telcos and enterprises agree that internal challenges remain a real risk to executing on them. 40% of enterprises cited internal resistance as a challenge to IoT deployment, while unclear internal ownership and lack of internal expertise together represent the top edge networking deployment challenge for half of all operators. The good news here is that internal challenges are ones that operators and enterprises should be able to address, as they are within the control of the organisation. The bad news is that unless they are dealt with, the risk could be greater than stalled IoT and edge deployments: a lack of internal coordination or internal will could result in sub-par deployments, jeopardising anything from solution performance to security and, ultimately, customer experience.
- **Security at (and beyond) the edge:** In our mid-2021 network transformation survey, operators revealed that network security and end-user security had become their top network technology priorities, with around 90% of operators ranking each case as either "extremely" or "very" important. This shouldn't be surprising due to the increasingly critical workloads that 5G carries, the broader attack surface from IoT expansions and the well-documented rise in security threats during the pandemic. At the edge, the topic of security takes on a heightened degree of importance; if the value proposition of edge computing is in helping to deliver improved application performance while keeping sensitive data under tight control, any security breach at the edge could compromise its reason for being. To be sure, the need for security as a part of edge and enterprise digitisation solutions is known and being addressed.

Security solutions and services represent operators' top expected source of revenues from private network offers, with 88% of operators planning to offer them within the next year. Likewise, technologies such as eSIM and iSIM promise to help secure cellular-connected IoT devices by tightly integrating standards-compliant security into the IoT device while allowing for simplified device software updates (including security patches). The adage that 'a chain is only as strong as its weakest link' applies here; while edge security strategies must secure edge devices, they must also be crafted as part of a whole that thinks of end-to-end (cloud to edge) security

Outlook and competitive implications

The strong business rationale for digitisation supports a positive outlook for enterprise spend on digital technology and connectivity. As we stated earlier, negative financial impacts of the pandemic triggered delays in some major IT and networking upgrades. However, for many companies, the opposite is true, with the Covid-19 pandemic accelerating existing plans, particularly for industries that have historically relied on consumer-facing business models such as retail, banking, live entertainment and sports.

A recent survey by Neos in the UK affirms this point: 98% of companies surveyed indicated that digital transformation is key to their future strategy, with around half reporting that the pandemic accelerated existing plans. The building momentum in enterprise spend is therefore a resumption of a pre-existing trend, not something new.

The competitive implications and value distribution of enterprise investments in digital transformation are more complex and varied. This is in part because technology is still being developed and innovated on, and in part because of co-opetition. To help think about these issues, we have separated out the thinking for three different groups below: vertical enterprise customers (those commissioning digital transformation plans); telecoms operators; and equipment vendors. For all three groups, we present the benefits, risks, business model and investment considerations, and open questions.

Enterprise verticals

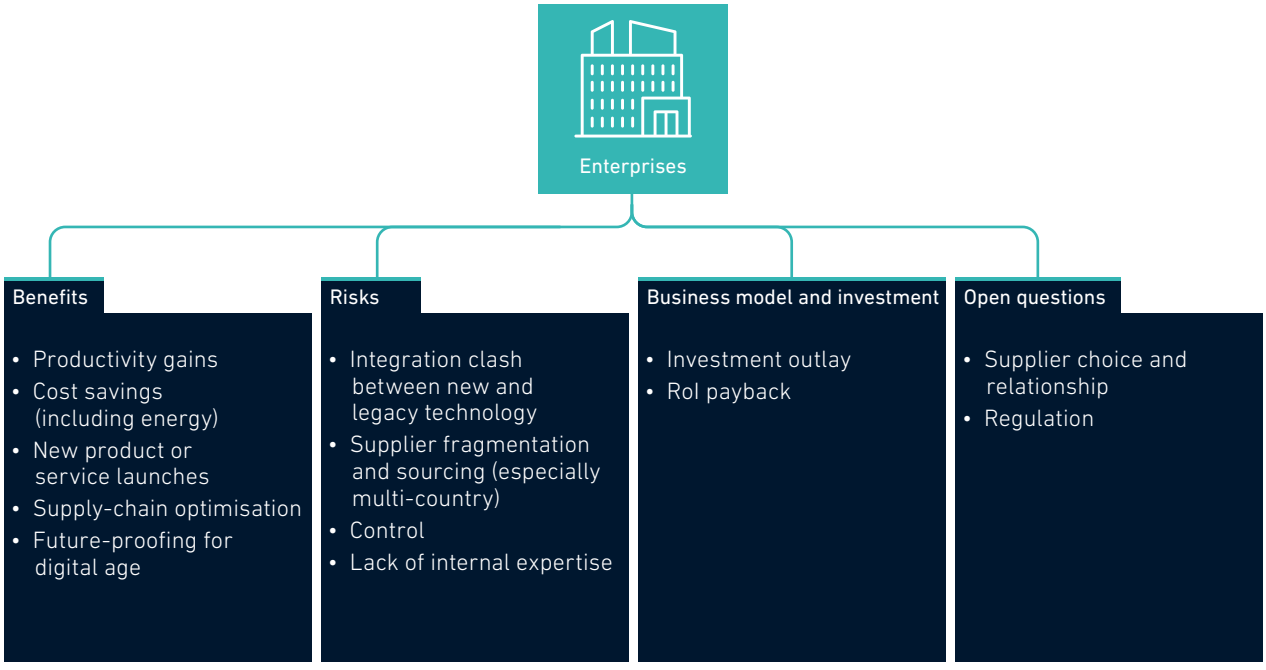
The benefits and rationale for implementing digital transformation is generally common across industries, even if projects vary in size (e.g. a smart factory versus, say, the entire London Underground network). This includes productivity gains through automation, analytics, redistribution of labour, cost savings and future-proofing operating models as more purchasing activity moves online and processing power to the cloud.

The risks are mostly operational, even if RoI payback periods may go beyond five years (though there is a need for more case studies and literature with evidence on this front). Implementing new technology and swapping out legacy IT systems is a common pain point. Supplier diversification is a positive when it plays to comparative advantages; it can, however, also present challenges if suppliers are spread geographically. Finally, many businesses lack the internal expertise and know-how – even in the CTO or CTIO offices – to adequately assess what solutions would best fit their objectives, which then carries into supplier selection and ongoing evaluation. We mention these not to highlight them as insurmountable problems but to pre-empt challenges that may delay or frustrate progress on an otherwise sound investment platform.

Open questions are less defined and harder to generalise on. Climate and environmental regulations are likely to become more commonplace as countries grapple with the 'how' of hitting net zero commitments by 2050. To the extent enterprises can use mobile network and digital technology investments to help reduce carbon emissions (alongside a shift to renewables), this will likely pay long-term dividends.

Figure 11

Competitive implications of digital transformation for enterprises



Source: GSMA Intelligence

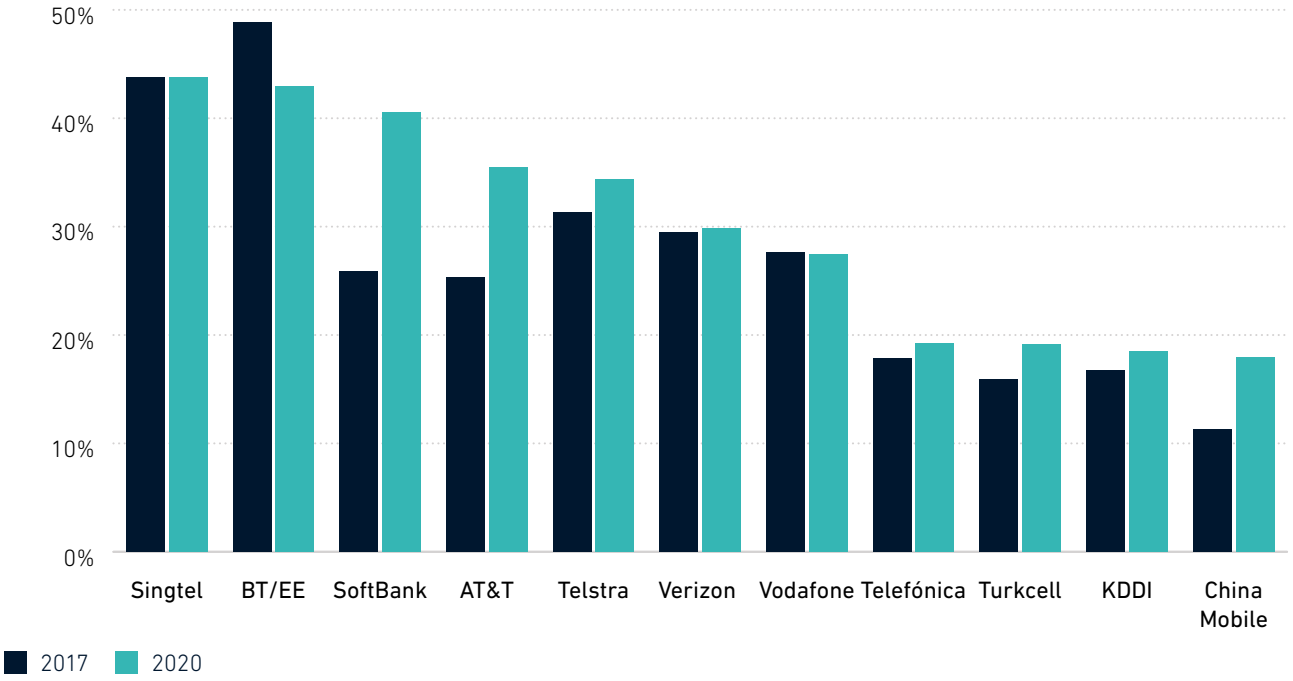
Telecoms operators

The key goal for operators is to grow B2B revenues, helping to monetise 5G network and spectrum investments, and diversify the overall revenue base. B2B accounts for around 20–40% of revenues for the largest telcos worldwide, and while that number has been rising (see Figure 12), it has not (yet) moved the needle on overall revenue growth. Disclosure on B2B uplifts from 5G connectivity and other services such as PNs has so far been minimal, suggesting it remains early days even if deployments are rising. Automotive, logistics, healthcare and manufacturing are all high-potential verticals. Risks are more competitive than operational. Amazon, Google, Microsoft and a raft of enterprise IT suppliers such as HPE and Dell are all involved in this space, primarily with cloud and edge compute. While edge data centres are not a replacement for connectivity, in environments where mobility is not crucial to operations (e.g. an airport), the lines can blur. Partnerships between operators and cloud groups can help mitigate this risk.

Figure 12

B2B contributions vary widely among major operators but much of this is legacy, leaving headroom for 5G-led growth

B2B as a percentage of overall revenue

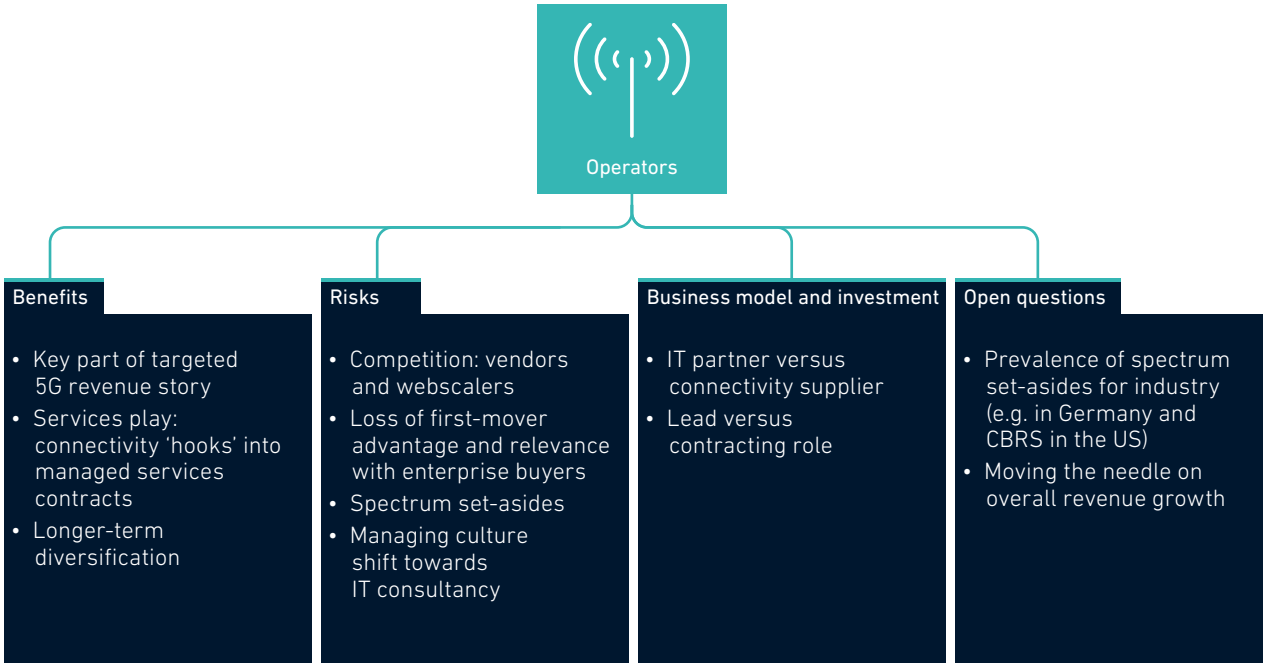


Source: GSMA Intelligence

In terms of investment and business model considerations, most of the operator risk capital is the capex for national network build-outs. Additional investments to build out PN infrastructure for dedicated clients would come as part of separate project budgets. It is important to work as an enterprise partner rather than a traditional supplier to help clients through journeys end to end. This matters and is a change from traditional enterprise telecoms sales. The main open question concerns the risk (for operators) of regulators carving out spectrum for enterprise use directly. This emulates the CBRS model in the US and carve-outs in Germany.

Figure 13

Competitive implications of digital transformation for operators



Source: GSMA Intelligence

Equipment and technology vendors

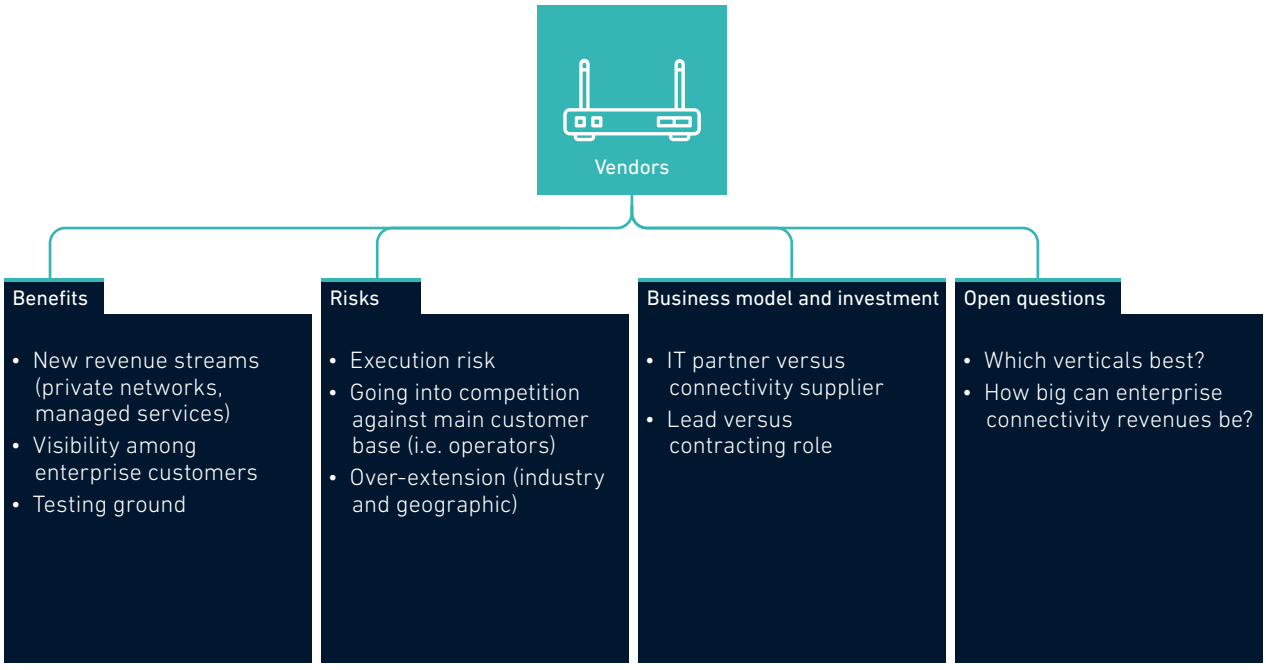
The main network equipment vendors have the same strategic rationale as operators in servicing the enterprise digitisation opportunity to increase B2B revenues. The difference is that vendors come at it from a different vantage point, being suppliers of equipment rather than owners of spectrum. This brings positives and negatives. The positive is that they can bring advanced technology to commercial deployments quickly on premises, such as at factories, hospitals or transport hubs. Good examples include Nokia working with Lufthansa on a 5G PN at its maintenance hangar in Hamburg in 2021, and Cisco's deployment at the Super Bowl in Los Angeles in February 2022. Vendors were among the earliest to deploy cloud and edge-cloud solutions in enterprise settings in 2019–2020, providing a testing ground to learn and improve upon products.

A key risk is a tactical one, as vendors are competing for enterprise business with operators (i.e. their own customers), although in practice most deployments will involve joint bids and consortiums. The 'who' in those bids may also change, with pairings between vendors and global scale IT consultancies such as Tata and Accenture as likely as with traditional telco bedfellows. The complexity of an overall enterprise technology system is underlined by the range of devices, IoT sensors and provisioning systems, low-latency connectivity requirements, and AI or ML software processed in the cloud or at the edge. Additionally, there is the question of how big enterprise connectivity revenues can be for vendors. Despite the hype, as with telcos, enterprise sales are a fraction of the legacy networks business for most vendors. Ericsson, for example, consolidates these into its emerging business segment, which accounts for only 5% of overall revenue as of its latest Q1 reporting. Clearly there is headroom to grow, but the time to do so is limited.

Finally, for other technology vendors at the device and provisioning level of the value chain, there is a 'glue-like' role to play between enterprises, operators, cloud groups and equipment vendors. The hygiene factors of security, device and life cycle management, managed connectivity and even system integration and consultancy are crucial elements of a successful digital transformation project.

Figure 14

Competitive implications of digital transformation for vendors



Source: GSMA Intelligence

gsmaintelligence.com

GSMA™
Intelligence

gsmaintelligence.com