Kaleido Intelligence

CELLULAR IOT

ENTERPRISE DEMANDS & OPPORTUNITIES

2024 SURVEY REPORT

SPONSORED BY

Giesecke+Devrient
Creating Confidence

Kigen

wireless logic

TABLE OF CONTENTS

Introduction 03

Complexity 11

Roaming 21

eSIM 27

Security 35

Value-Added Services 43

About the Authors 47

03

Introduction

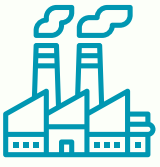
Cellular IoT has seen remarkable growth since the onset of the COVID-19 pandemic in 2020. By the end of 2023, over 3 billion connections were deployed for IoT use cases globally, with connection volumes growing, on average, by 24% annually. Cellular technology can address use cases ranging from very high throughput, low latency applications to those transmitting only a few bytes per day. This means that few other technologies exist on the market that can address such a wide variety of enterprise customer requirements.

As the industry continues to mature, it is important to understand where key challenges continue to exist in the industry. Since 2022, Kaleido Intelligence has been conducting annual surveys of enterprises, with the specific aim of uncovering sentiment surrounding cellular IoT connectivity among both adopters as well as non-adopters of the technology.

In this year's survey programme, some 1,000 enterprises responded to various questions concerning ecosystem challenges, service provider expectations as well as deployment intentions and needs. As in previous years, responses have been collected from enterprises whose primary activity is focused around one of the following verticals:

Transportation & logistics

Healthcare



Industrial & manufacturing

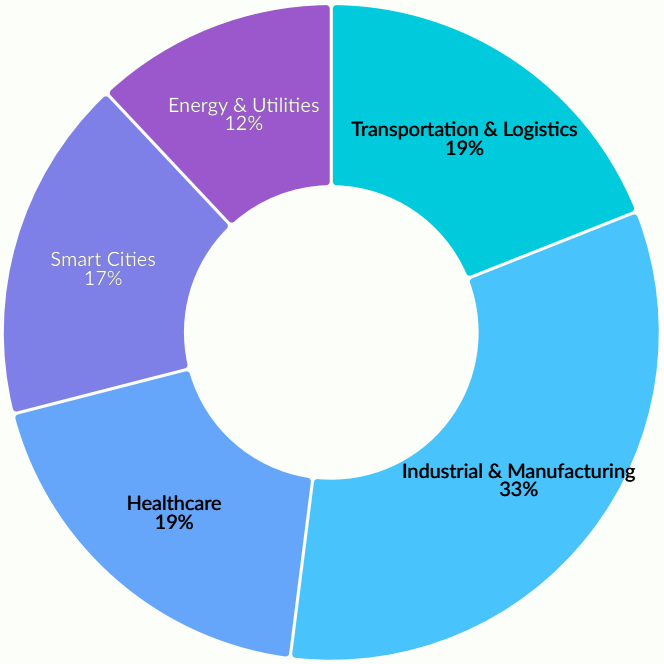
Enrergy & utilities

Smart Cities

04

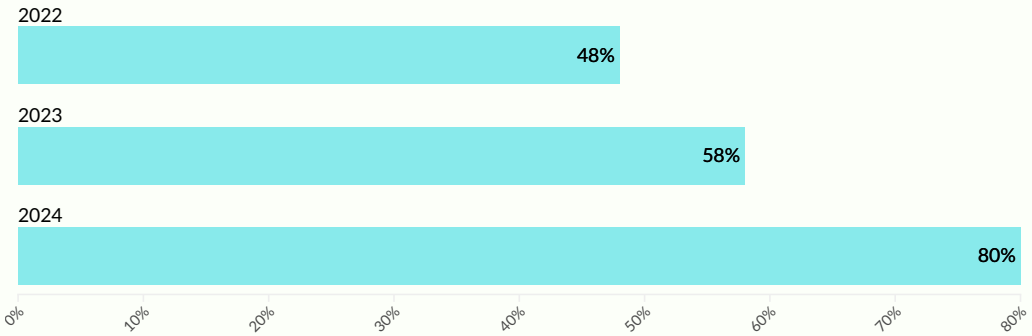
All respondents were decision-makers at managerial level or higher within their organisation, in addition to having a good knowledge of the cellular IoT ecosystem.

In what market segment does your business unit primarily operate?



A significant proportion of respondents, at around 80% of survey participants, reported that they have an active cellular IoT programme in the field. While this proportion may not reflect the absolute state of adoption of cellular IoT among enterprises globally, it does serve to highlight that growth in IoT programmes has been strong over the past 3 years: in 2022's survey, 48% of enterprises reported they were among cellular IoT adopters.

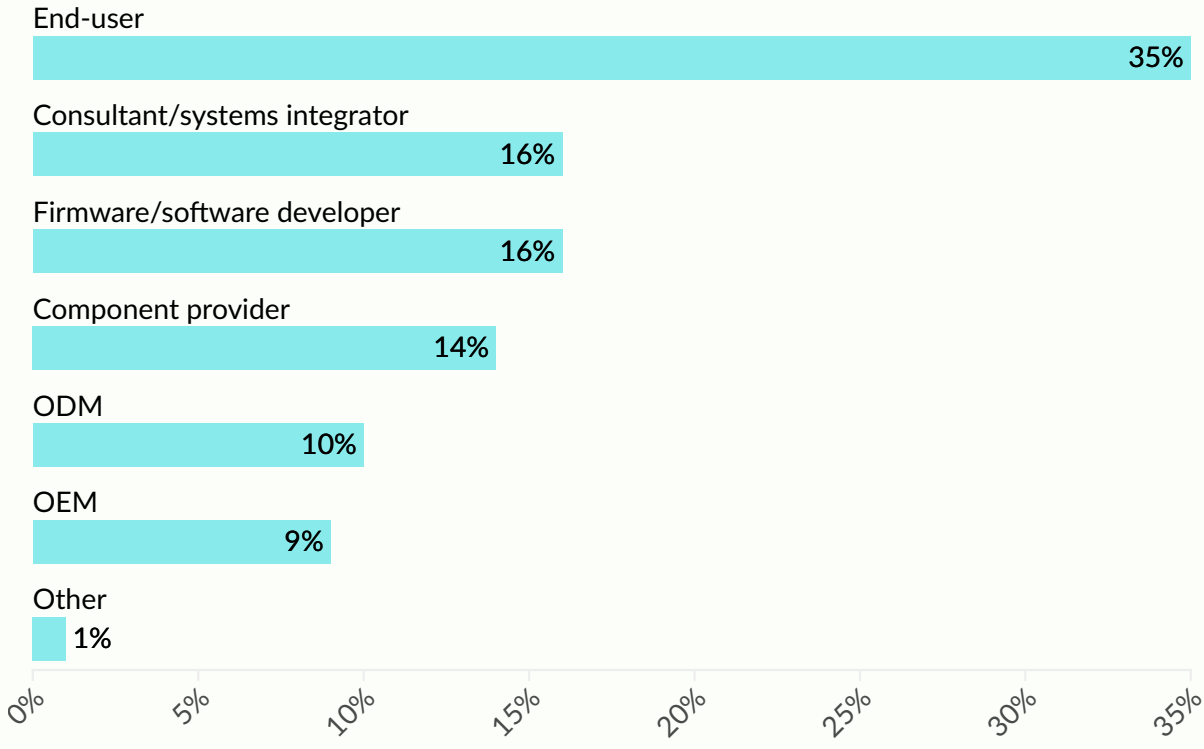
What is your organisation's current status in regard to IoT? (Proportion of Cellular IoT Adopters)



05

With the sunset of legacy 2G and 3G networks acerating across the globe, it is pertinent to understand the technologies that cellular IoT adopters are currently using. As we can observe from the figure below, some 10% of adopters have SIM estates using only legacy technology, while 12% of adopters are using a mix of 2G, 3G and newer cellular radio technologies. As such, we can infer that a significant proportion of cellular IoT adopters have challenges ahead of them, should they be located in countries where support for circuit switched network technology is due to be shutdown over the coming years. For those that wish to continue deploying IoT for the same applications, there will be questions to answer over which LTE or 5G based solutions will be suited to their application – as well as if their preferred technology matches up to requirements in terms of coverage support and module or device pricing.

How would you describe your organisation's position within the IoT value chain?



As in previous years of this survey report, there are notable themes that emerge from the data:

Complexity

Despite the fact that cellular technology is highly versatile and designed to meet a wide range of IoT application requirements, these benefits are delivered through a large ecosystem of devices, service providers and mobile networks. To a significant degree, the industry remains fragmented with no guarantee of support for specific requirements via simple plug-and-play approaches.

True global coverage for devices is largely absent from the industry, given the nature of roaming agreements and coverage footprints. Often, connectivity service providers specialise in delivering connectivity within targeted regions.

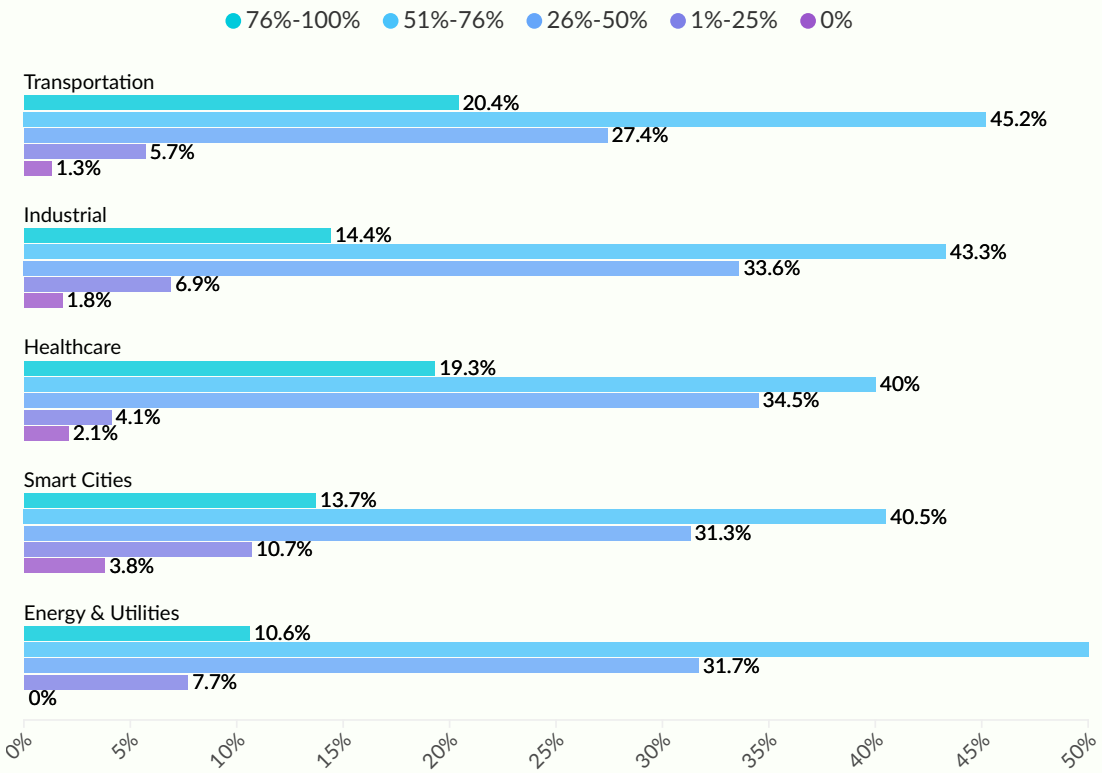
Just 2% of enterprises require domestic connectivity support only

With IoT very much an international endeavour, best-in-class solutions must deliver the most seamless route to market for customers, while additionally providing critical expertise and customer support for device deployments across the desired footprint. This is no easy feat, and depends as much on the quality of wholesale agreements between connectivity partners as it does on the underlying technology that is deployed to support operations and optimise configurations based on customer requirements.

Roaming

As a result of the international nature of IoT, roaming connectivity is fundamental to support connectivity in the case of multi-country deployments. In the vast majority of cases, these SIMs will rely on service providers' roaming agreements with international partners. Wholesale contracts in this context do not extend to the average lifecycle of IoT devices (often 10 years or longer).

What proportion of your organisation's cellular IoT device fleet requires international or multi-regional connectivity?

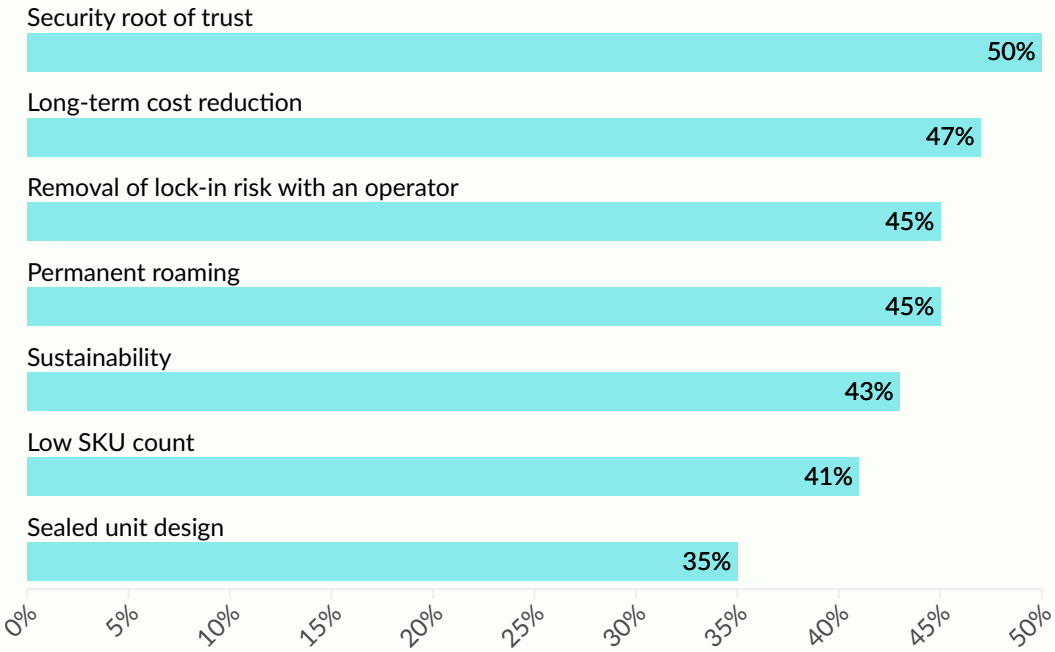


With long-term roaming frequently required, restrictions related to permanent roaming is a growing concern among enterprises. On average, the need to overcome challenges related to regulatory and commercial restrictions for roaming was ranked 2.9 out of 5, while 41% of enterprises ranked permanent roaming as a top 5 issue causing challenges when scaling IoT up.

eSIM

eSIM is a critical technology for IoT projects, in that it enables long-term flexibility in connectivity choice and availability. New standards have been developed and published by the GSMA, which addresses many of the concerns related to previous architectural implementations of the technology.

What factors made you choose eSIM (eUICC)?



Notably, 46% of enterprises reporting that they have used eSIM as part of their IoT deployment cite the fact that it enables a long-term cost reduction, while 49% indicated it as a useful technology to deliver security benefits as a root of trust. This indicates both a maturation of the technology, and signals that from a customer perspective, understanding over the technology is improving.

Security

The importance of security for IoT has never been more apparent than in this year's survey. Likely this is driven not only by the fact that the industry is starting to mature, with more sophisticated enterprise customers aware of the risks with larger device estates, but also by the fact that the regulatory landscape is imposing greater pressure on IoT users and service providers to ensure that compliance requirements are met.

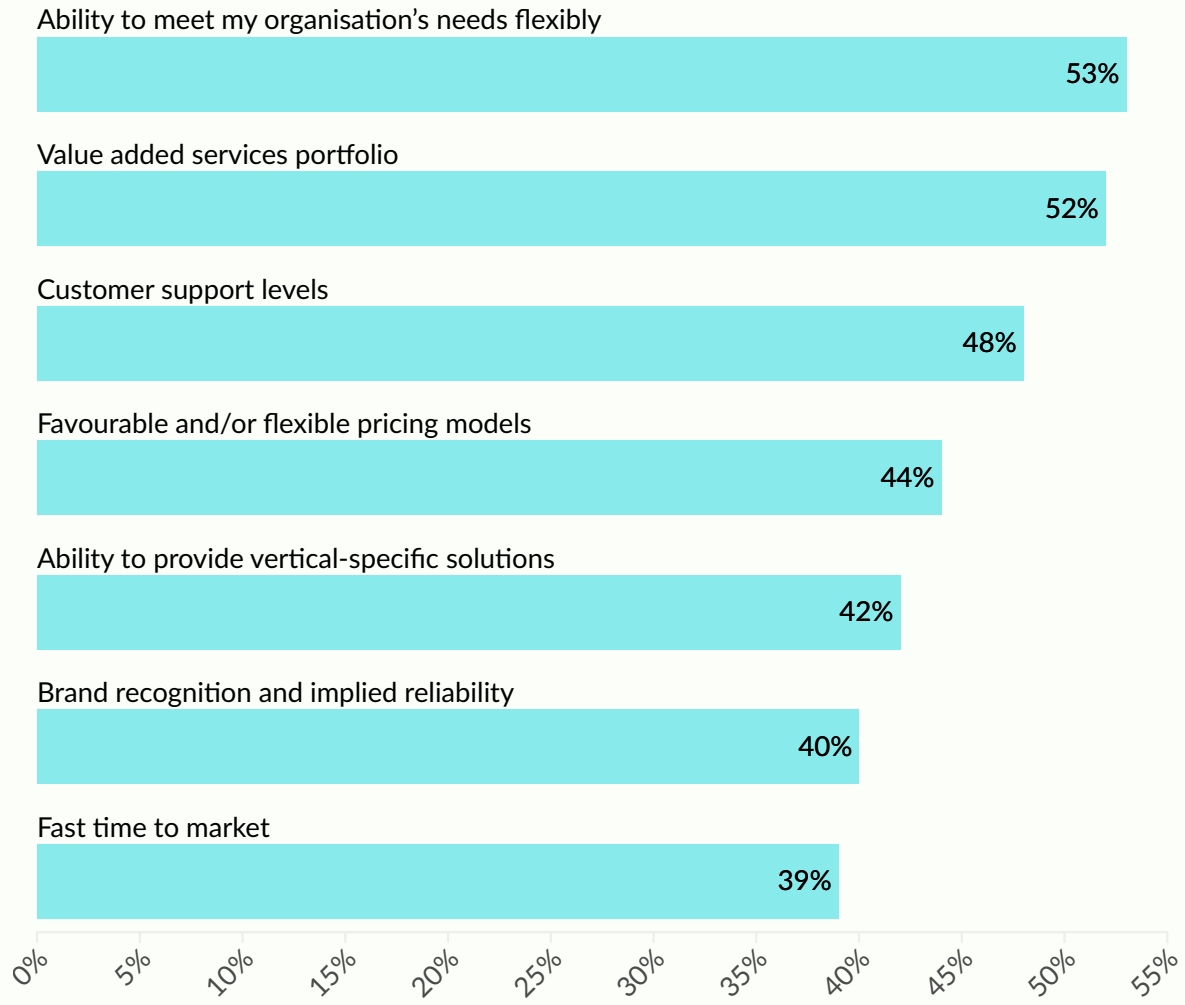
What are the top 5 factors that you look for/would look for in an IoT connectivity partner's product? (Average rank)

Ensuring end-to-end security was ranked as the most important factor for IoT connectivity among all respondents, while 60% of respondents require their service provider to offer extensive security features.

Value-Added Services

In line with the concept of complexity reduction being a driving factor behind service innovation, it is apparent that the notion of a connectivity service provider simply offering connectivity alone is antiquated. Certainly from the perspective of survey respondents, cellular IoT adopters reported VAS (Value-Added Services) as the second highest non-technical factor behind purchase decisions.

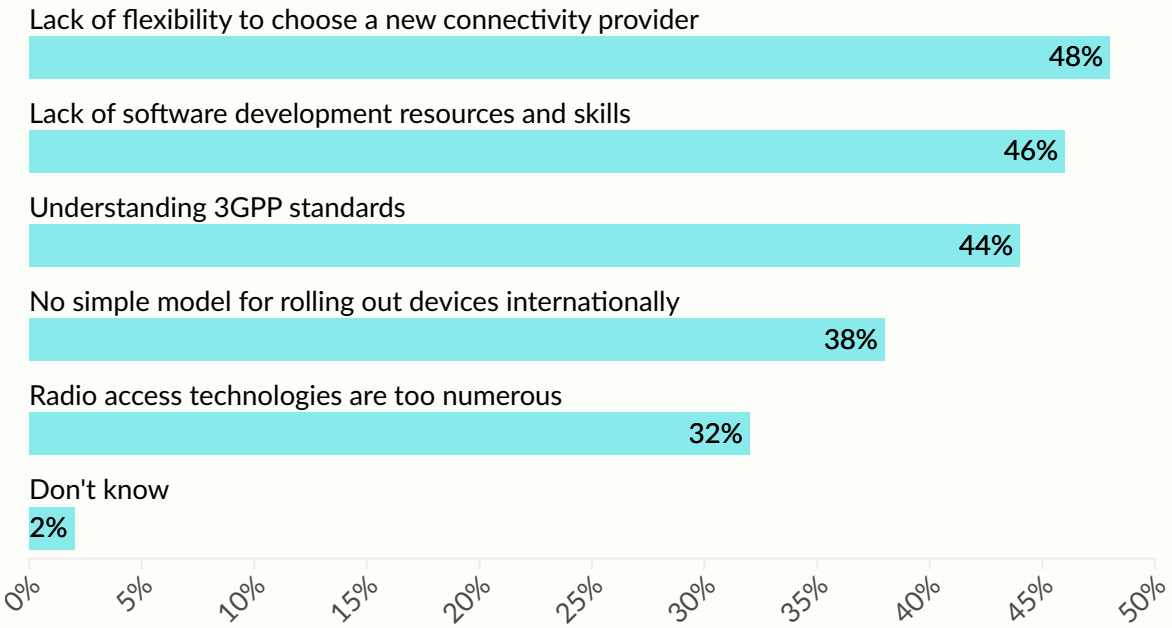
What non-technical/commercial factors influenced your organisation in choosing a cellular IoT connectivity provider?



Complexity

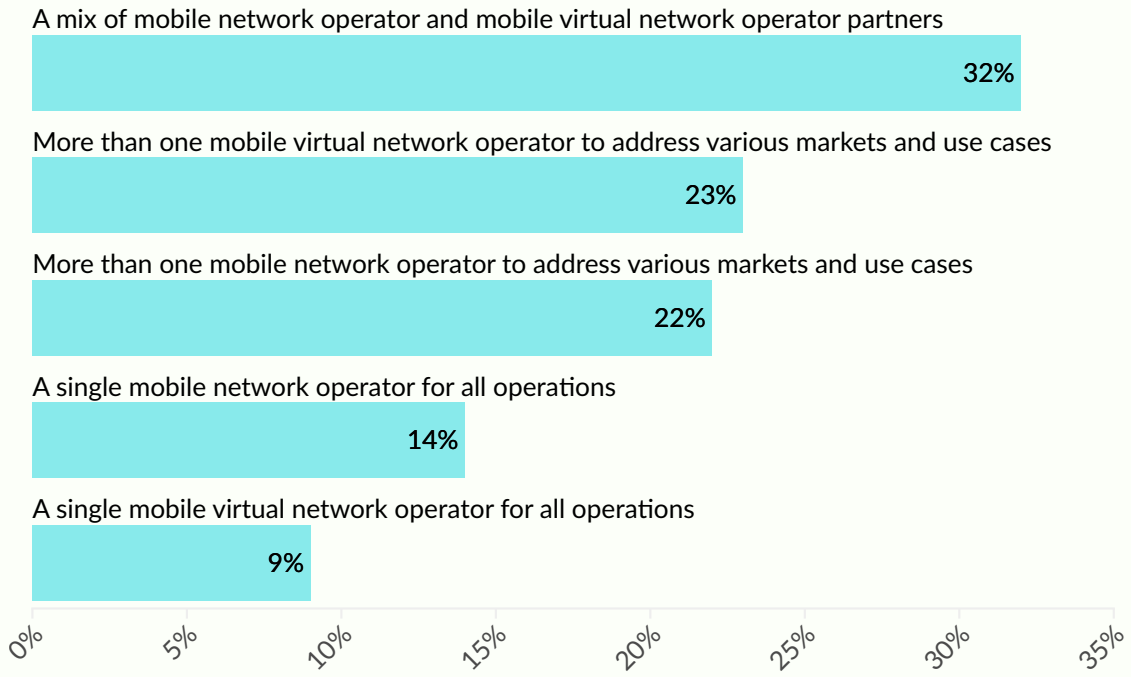
Complexity has been a consistent theme across each of Kaleido's enterprise IoT connectivity surveys. The nature of the industry means that each company's requirements are changeable in terms of outcomes required, in addition to the tools needed to achieve desired outcomes. Over the years, cellular technology has advanced from relatively simple-to-understand capabilities (from an end-user perspective) in the form of 2G and 3G to an increasingly complex ecosystem of RAT (Radio Access Technology) options through various flavours of LTE and 5G. This, coupled with the fact that organisations are often less familiar with cellular technology and development around this type of communications technology, creates a challenging environment. Here, lack of software development resources and skills (cited by 46% of respondents) in addition to understanding of 3GPP standards in the context of software or firmware (reported by 44% of respondents) highlights how application development for cellular IoT is viewed as a challenging process.

What do you perceive as the main challenges for organisations wishing to leverage cellular technology for IoT connectivity for the first time?



Notably, 48% of the survey cohort perceive the main challenge for first-time entrants into the cellular IoT market to be the fact that it is difficult to migrate from one connectivity provider to another. However, this sentiment is unlikely to be one that will change in future: by nature, service-level agreements, technological integrations and migration and onboarding processes will vary between different providers. This means that, even with the proliferation of technologies such as eSIM that enable the remote switching of connectivity from one service provider to another, the lack of standardised platforms, capabilities and APIs made available by providers means that there will always be an inherent difficulty in device estate migration.

What type of connectivity service provider have you chosen to engage with for your cellular IoT deployment? (Cellular IoT Adopters)

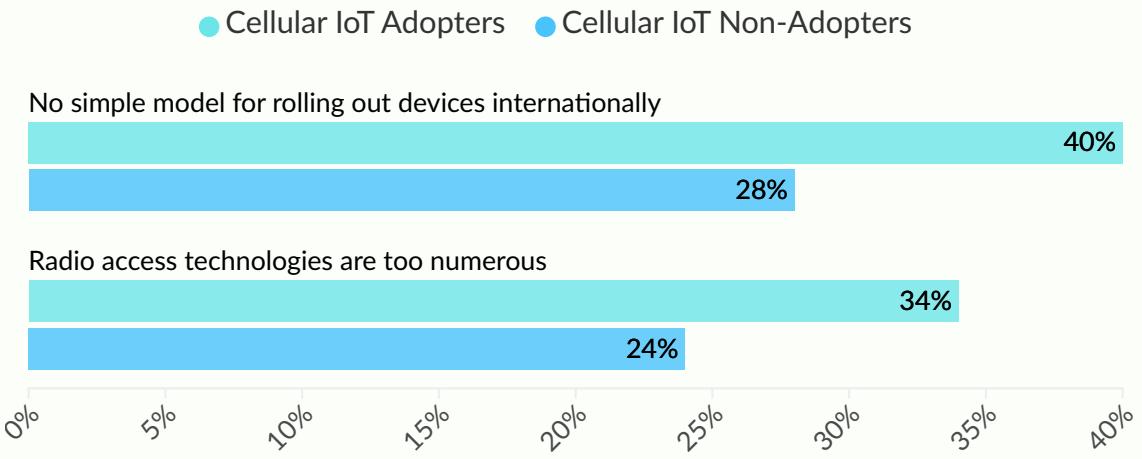


Meanwhile, and as in previous years, these challenges are compounded by the fact that among cellular IoT adopters, 77% of enterprises have engaged with more than one CSP (Connectivity Service Provider) for connectivity.

As such, enterprises must often deal with multiple contracts and SLAs (Service Level Agreements), in addition to managing connectivity across more than one platform. The resource drain here inevitably means that migration to a preferred partner is perhaps more challenging than it should be.

Looking a little more closely into the data, it is apparent that non-adopters do not perceive the challenges in international deployments for cellular IoT as acutely as existing adopters. Here, 40% of cellular IoT adopters cited this as an issue, with only 28% of non-adopters reporting the same. Meanwhile, 34% of cellular IoT adopters feel that the abundance of cellular IoT RATs cause complexity in the industry, compared with only 24% of those that have not yet adopted cellular IoT. It is natural that IoT focused companies that have not yet had real-world experience of cellular IoT deployments do not feel pain points in the industry in the same manner as those who have already undertaken cellular IoT projects. Nevertheless, these results highlight the importance of industry education, particularly for customers new to the ecosystem, and indicates a strong need for nuanced IoT expertise among CSP sales teams.

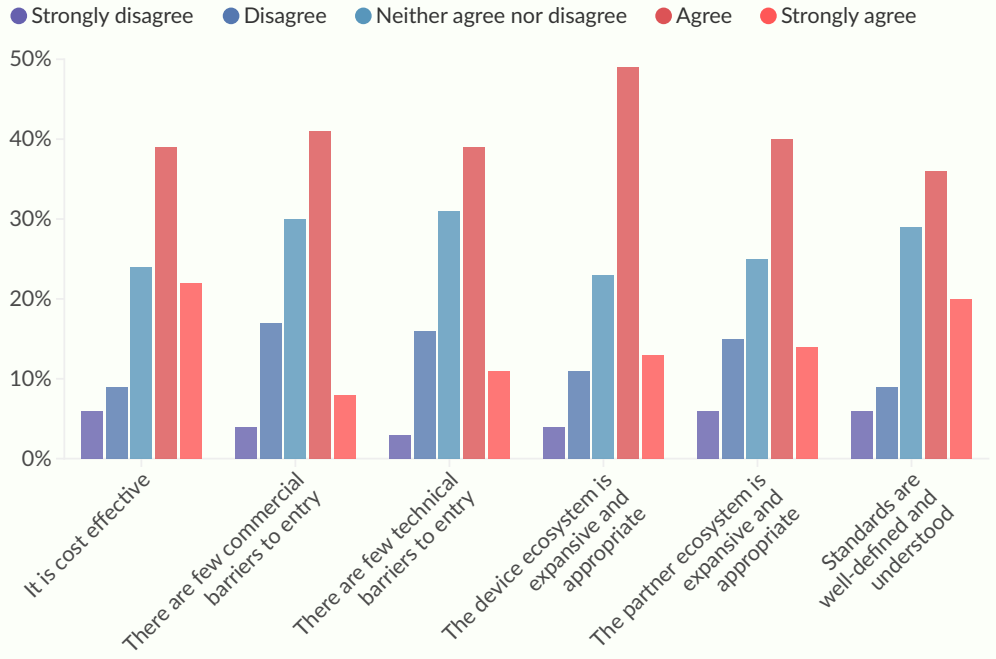
What do you perceive as the main challenges for organisations wishing to leverage cellular technology for IoT connectivity for the first time? (Split by Adopters & Non-Adopters)



Looking purely from a non-adopter perspective towards cellular IoT, it is evident that the technology is viewed as a key enabler of IoT connectivity. In this context, 62% of cellular IoT non-adopters believe that cellular IoT is the most viable WAN (Wide Area Network) technology for IoT.

In contrast, only 13% of the same respondents believe the same for LoRaWAN. Despite a growing popularity for deployment of the latter technology, projects thus far have largely revolved around private network initiatives, while throughput and latency is naturally restricted by the technology itself, making it less flexible than the overall cellular IoT ecosystem. Examining this sentiment more closely, the survey shows that cellular IoT non-adopters believe both in the cost-effectiveness of cellular IoT, in addition to the well-developed device ecosystem available to customers: these form 60% and 62% of the respondent base, respectively, when positive sentiment responses are summed.

How far would you agree with the following statements about cellular IoT connectivity as applied to your use cases? (Cellular IoT Non-Adopters)

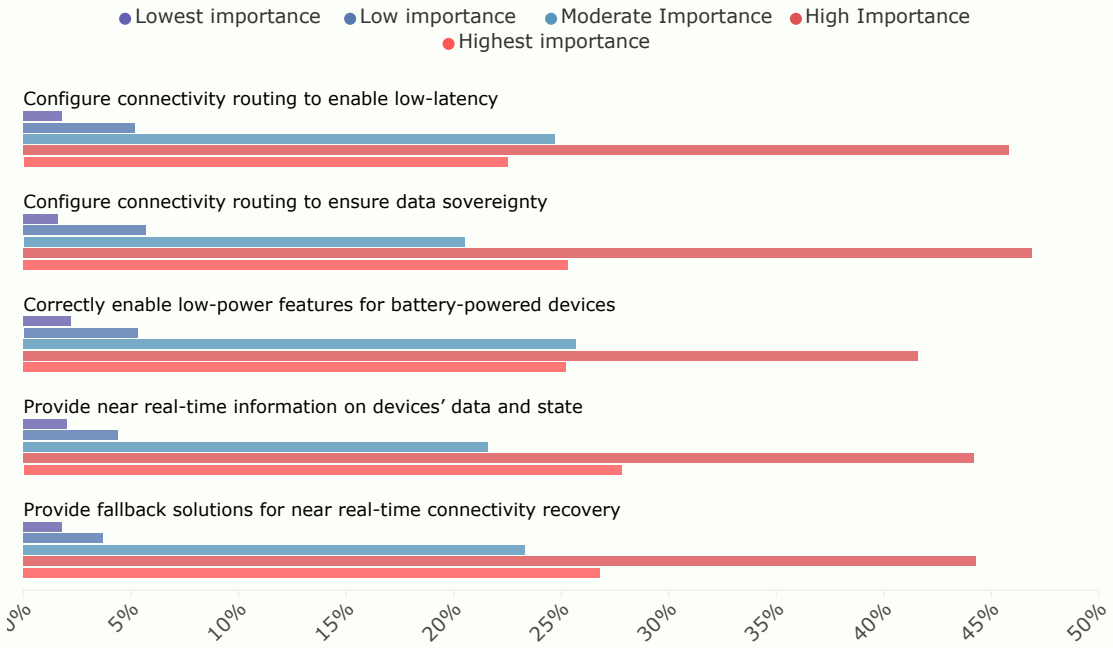


Nevertheless, it is also important to examine where the most notable negative sentiment arises. In this case, commercial barriers and partner ecosystem realise the highest proportion of responses, each with 21% of survey respondents reporting challenges in these areas. This evidently forms somewhat of a juxtaposition: on the one hand, cellular IoT is viewed as cost-effective, likely due to the relatively low cost of connectivity and capability to meet varied requirements, while on the other hand, underlying commercial challenges mean that the path towards deployment is not as seamless as it should be. This hypothesis ties in with the idea that the partner ecosystem still requires

development, where a lack of network access, or unexpected commercial complexity mean that the business case is damaged. Overall, this underlines the fact that the industry is far from a 'plug and play' concept, as well as the fact that potential customers are increasingly sophisticated in their understanding of the underlying wholesale ecosystem.

Complexity is often seen in the form of customer demands. As the IoT industry matures, enterprise requirements become more varied, while customers themselves become increasingly aware of the challenges of IoT that result from regulation as well as traditional approaches to connectivity.

How important is it that your connectivity service provider is able to provide the following? (Cellular IoT Adopters)

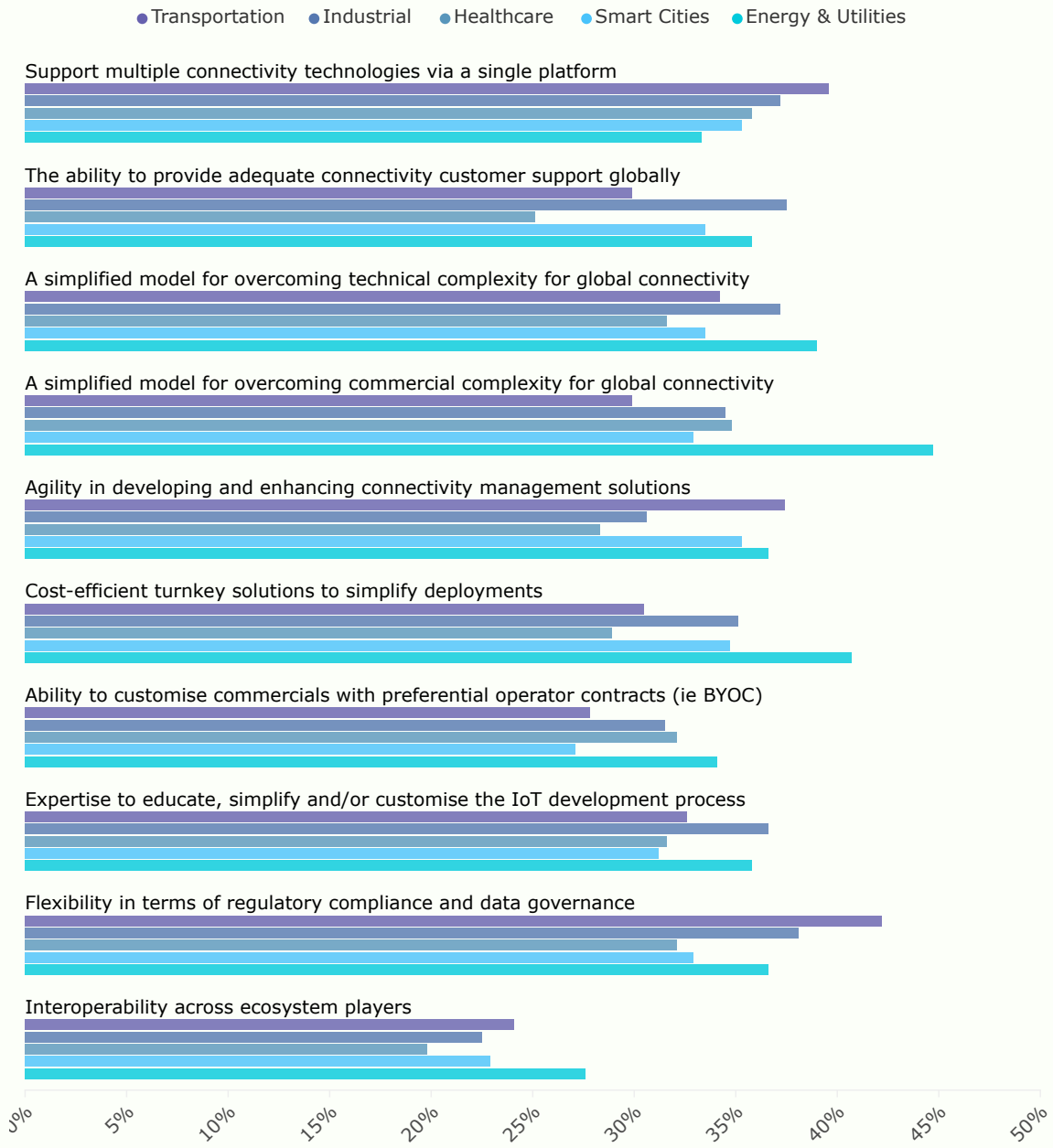


This type of complexity is notable when examining how cellular IoT adopters expect their CSP to address various requirements: the ability to provide real-time information on SIM estates, configure connectivity routing to meet data sovereignty in addition to the capability to offer near-real-time solutions for connectivity failover were reported as either high or highest importance by over 70% of respondents. This particular part of the survey underlines the importance of infrastructure ownership and control: where providers are reliant on others' infrastructure and integrations, this type of advanced network control and visibility is not always possible.

Notably, the ability of service providers to offer real-time information on SIMs' data consumption and network status was viewed as the most important of all items, with 28% of respondents reporting this under 'highest importance.' This naturally ties in with the need to ensure that high availability is maintained across the deployment; thus, it is not surprising that 27% of respondents cite the ability to recover from network incidents as an item of highest importance.

Sector Focus

What do you perceive as lacking in the present IoT connectivity ecosystem? (All respondents)



The challenges that cellular IoT connectivity CSPs face is evident when questioned over what is perceived as lacking in the ecosystem. All verticals save for energy & utilies cited a lack of capabilities to support multiple connectivity technologies across a single platform within the top 3 highest selected items, with healthcare and smart cities respondents reporting this as their top issue. Meanwhile, a lack of flexibility in terms of regulatory compliance and data governance was among the top 3 selected items for transportation, industrial and healthcare respondents, but not smart cities and energy & utilities respondents.

On the one hand, this means that providers looking to service the market from a horizontal perspective may not have the desired tools for certain vertical requirements, and leads to the idea of vertical specialisation. On the other hand, it is of course necessary to balance the investment required to achieve this with the volume of anticipated customers and connection volumes. From a multi-technology management standpoint, development of relevant partnerships and integrations seems a reasonable step forward, if investment is not directed towards in-house solutions. In Kaleido's 2023 Connectivity Vendor Hub analysis examining cellular IoT CMPs (Connectivity Management Platforms), around 65% of platform vendors reported that they do not include either Wi-Fi, satellite, LoRa or Sigfox connectivity management support. Meanwhile, among those that did, less than half of those platforms integrated that management into the same management portal as the primary tools for cellular IoT connectivity management.

Meanwhile, with only 2% of cellular IoT adopters reporting that they only require connectivity in a single country, it is clear that the capability to ensure data sovereignty and compliance requires control over data routing, which in turn brings the discussion back to infrastructure. While the vast majority of leading IoT connectivity service providers operate their own core network infrastructure with accompanying packet gateway elements, the build out of this infrastructure continues to be highly varied, largely as a result of investment and customer requirements. For many players, it will be important to formulate a concrete strategy to this end moving forward, if they wish to address connectivity for certain vertical industries.

Giesecke+Devrient

Case study

Enhanced Container Tracking Solutions by Wackler, Cargoline Network, & Giesecke+Devrient

The challenge

In today's dynamic global marketplace, efficient logistics management is paramount for businesses aiming to stay competitive and meet customer demands effectively. One of the critical components of streamlined logistics operations is container tracking solutions. These innovative technologies leverage advanced tracking mechanisms, including GPS, up-to-date connectivity and IoT sensors, to provide real-time visibility and insights into the movement, status of the freight and productivity of the container fleet throughout the intermodal supply chain.

The transport of cargo/goods tends to rely on a complex, intermodal network of roads, rails, air and sea, interacting on a frequent basis with various stakeholders. The biggest challenges include operational inefficiencies (calling drivers for whereabouts, need for frequent inventory checks etc.) and lack of visibility in the value chain (the movements of the goods).

Wackler, a partner of Cargoline, was facing such challenges. One major issue was the lack of visibility of shipments being transported by trucks carrying pallets of dry containers, mostly loaded with palleted goods of various types, and reefer containers carrying temperature-sensitive and time-critical goods, like chemicals that need specific temperature conditions.

WACKLER
Spedition & Logistik

Wackler is a transport and logistics company with a wide portfolio ranging from warehousing to full-service logistics and e-commerce solutions. Since 1993, Wackler has been one of the 50 members of the Cargoline alliance.

The biggest problems included excessive standstill times, late arrivals, damages to the cool chain cargo, and resulting penalties that Wackler had to assume.

Moreover, the arrival of containers for unloading and loading was not coordinated, causing sudden traffic jams on the dock station and leading to delays in dispatch and arrivals. The only way to get information about the location and condition of the shipments was for the supervisors to make phone calls to their fleet drivers, resulting in poor management of the dock occupancy (loading and unloading docks).

How do Giesecke+Devrient solutions help?

The main goal was to better control the swap body inventory of Wackler assets within the Cargoline network. mecSOLAR GPS-tracking devices provide the perfect solution, granting short-cycled movement tracking of container assets and 24/7 monitoring thanks to self-sustaining devices via solar charging and state-of-the-art global connectivity in combination with the mecFLEET platform, which allows for central management of location and status (ETA timing, cargo safety and customer visibility).

mecSOLAR devices can be attached hassle-free on the swap body unit (in as little as 5 minutes) and withstand harsh weather conditions such as in the Arabian desert and the cold winds of Scandinavia while covered with snow for weeks.

mecSOLAR modules can detect the conditions of cargo using sensor tags, such as monitoring the temperatures of Wackler's swap body containers, and display such data analytics in real-time in the form of comprehensive reports, which can be easily accessed and exported by supply chain managers within the mecFLEET platform.

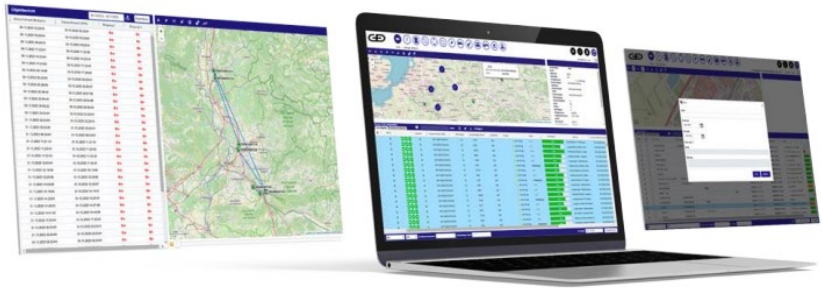
Furthermore, the ability to set up alert notifications and generate instant reports broken down per individual units is one of mecFLEET's most acclaimed features utilized by the supply chain team. This is especially useful for responding immediately in cases where the temperature of the goods fell below a certain threshold. Data showing excessive stationary periods that have occurred is also immediately available instead of having to wait for the driver card to be reviewed.

The main application of G+D solutions which this case utilized is the **mecSOLAR iot with wired temperature sensor and mecFLEET telematics portal**, is the ability to manage the bookings of swap bodies, track entry/exit events, which generate information about estimated time of arrival and thus allow for accurate yard and loading dock occupation management.

In addition, mecFLEET allows for registering damages to incoming swap bodies, providing evidence to link the damage to the liable party. It can also generate reports of standstill times, entry and exit events, standstill times in transit, and instances where temperature exceeds set limits. All of this is managed easily within the mecFLEET platform.

Completing the full user experience circle, in-field actions are also supported for reporting problems on the go using a mobile phone.

The fleet drivers were able to take photos and register damage while en route. The main inspection date control and pairing of devices can be done via the mecTRACE app and are immediately updated in the mecFLEET platform.



mecFLEET telematic portal

mecSOLAR iot tracking device

The result

Using mecSOLAR in combination with mecFLEET gave Wackler real-time visibility and control to act on incidents immediately, resulting in significantly reduced costs and optimized asset allocation.

Having access to real-time data on the location and status of individual units provides valuable insights about the distance and time traveled between places using an interactive map within the mecFLEET platform. Real-time visibility allows Wackler to react quickly in situations of unexpected standstill times, when there is increased risk of the cargo being damaged or stolen.

A semi-annual inventory of the fleet is no longer necessary as mecSOLAR devices provide daily inventory pings.

Making phone calls to fleet drivers also became obsolete, significantly reducing their daily workload and allowing them to react much faster to disruptions.

A significant reduction in labor cost was achieved by giving stakeholders (operators/customers) real time visibility of their asset whereabouts using the shared link functionalities of mecFLEET. On time delivery can now be validated using evidence from the GPS position with a timestamp from the customer's side, thus avoiding potential penalties.

Finally, yard management was streamlined by guiding incoming assets to the correct loading docks, since Wackler was provided the necessary tracking information about expected departure and arrival times, giving priority to critical shipments.

With the ability to make better-informed decisions, and thanks to G+D's innovative solutions, Wackler, as partner of the Cargoline network, was able to optimize its supply chain management, save costs and increase its asset utilization.

Lastly, utilitizing mecSOLAR devices enabled Cargoline to reduce its environmental footprint, by optimizing fleet deployment and maintenance of the solar powered battery (without changes needed for over 10 years). This is of increasing importance in today's global climate.

Benefits summarized

- Ability to optimize number of vehicles deployed and routes travelled (time and distance)
- Quick reaction on unexpected standstill times (especially with sensitive cargo) to prevent loss of cargo
- Ability to provide detailed route visibility using shared link functions within the platform
- Ability to verify on time delivery
- Improved loading dock occupancy management
- Simplified inventory management

> "By using the mecSOLAR modules, we have taken another step towards digitalization."
>
> **Andre Apelt (Wackler, Transport & Logistics)**

Giesecke+Devrient

Giesecke+Devrient Mobile Security GmbH
Prinzregentenstrasse 161
81677 Munich
Germany

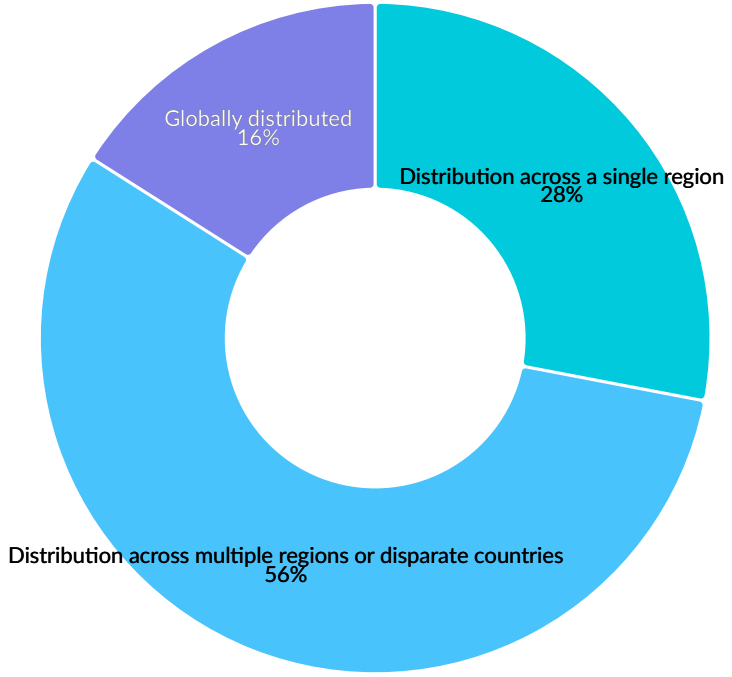
www.gi-de.com
connectivity@gi-de.com

Follow us on:

Roaming

The international nature of cellular IoT has never been more apparent than in this year's survey cohort. Where 8% of cellular IoT adopters reported requiring only domestic connectivity in 2023's survey, this year that figure has reduced to 2%. On average, 54% of cellular IoT adopters' SIM estates are reported as requiring connectivity across more than one country. Nonetheless, the results highlight that deployments are largely based either within a single or multiple regions: only 16% of enterprises with international connectivity requirements reported that their devices were being utlilised on a global basis.

What is the nature of your organisation's international cellular IoT connectivity footprint requirement? (Cellular IoT Adopters)

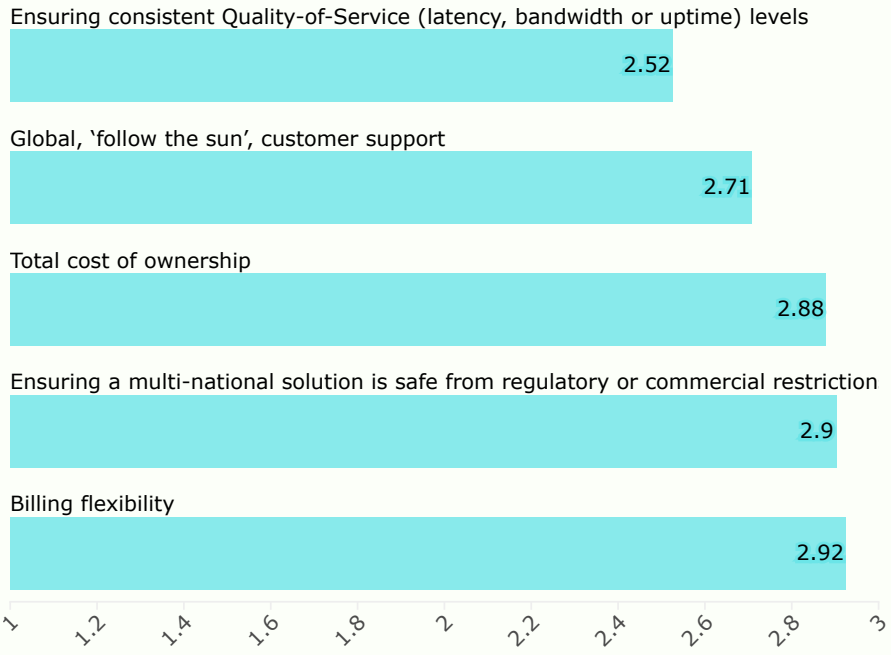


When examining the top 5 factors that are most important where IoT connectivity is concerned, it is pertinent to note that 3 out of the 5 factors are related to international connectivity when ranks are averaged across the response base. Most importantly, enterprises value consistent QoS (Quality-of-Service) for their devices, where likely the most valuable aspect is the assurance of high connectivity uptime levels.

This means that providers must have mechanisms in place to overcome the inevitable problems that arise when relying on various partners' networks across the globe. The 'resilience' concept appears to be a growing trend among some providers, with technology enabling SIMs to automatically register with a backup network should the primary roaming or local connectivity fail. While touted as a novel concept via 'rSIM,' it should be noted that several providers have offered similar technology for several years.

Meanwhile, there are important tools to consider at the backend. Is roaming connectivity being monitored for uptime and quality, and are service providers transparent and proactive in communicating issues with customers, as well as establishing processes to maximise customers' connectivity uptime? Part of this is dependent on the relationship with wholesale partners, but also in the underlying technology to monitor quality – not only on the network, but also on the platforms themselves.

What are your top 5 factors that are most important where IoT connectivity is concerned? (All respondents, average rank)



The issue of permanent roaming reared its head once again in this year's survey, with an average rank of 2.9 out of 5, and was selected as the fourth most important factor. This represents a slight fall from last year's survey, where challenges related to commercial or regulatory restrictions was top-of-mind among enterprises. The ability to address long-term roaming IoT connectivity in markets where either incumbent MNOs or national regulators impose restrictions on the level of inbound roaming that is allowed to take place has traditionally been the strength of specialised IoT MVNOs. This is largely in part due to a willingness to embrace and develop solutions around multi-IMSI and eSIM technology, in addition to the capability to aggregate the connectivity footprint around several partners under a single solution. However, this is now shifting to a degree, with MNOs undertaking initiatives to smooth the path to deployment – either via the establishment of MVNO entities or through platform layer abstraction for connectivity management.

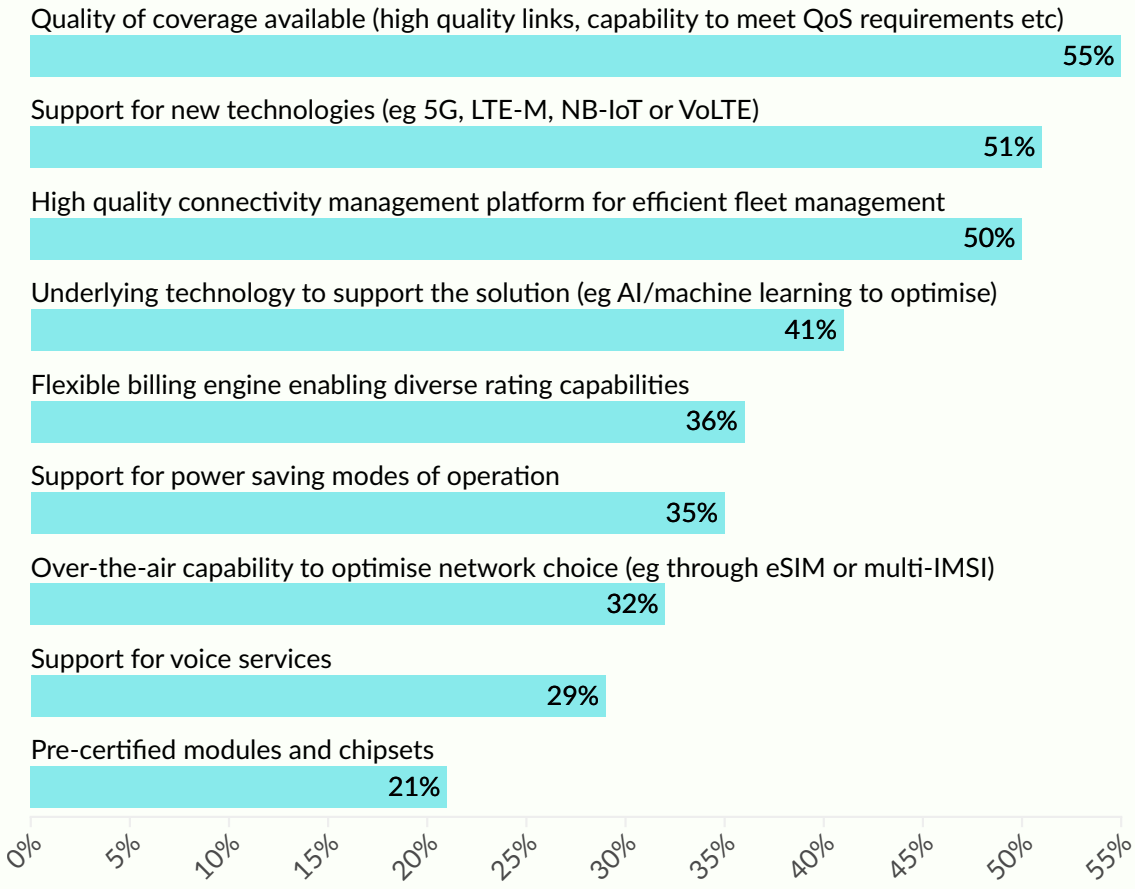
While roaming and interconnect has established arguably the most seamless option for multi-country connectivity when cellular is compared with other wide-area technologies, the industry has struggled to optimise the ecosystem for IoT connectivity. In the consumer handset market, travellers consistently expect to consume relatively high volumes of data, which realises a simple profitable solution for wholesale roaming deals. This is not the case in IoT, where device data consumption per month can range from several Gigabytes, to mere Kilobytes per month. With many IoT applications being sensor-based, upload-centric data consumers, key factors behind investment in IoT are often predicated on low-cost and, high-availability high-reliability. However, this can in turn create challenges where wholesale monetisation is concerned and means that the necessary support, commercials or availability may not always be at the desired level. This sentiment is reflected by the survey cohort when considering scaling IoT up: when asked to rank the top 5 challenges in this domain, 3 out of the top 5 average ranked items were concerned with roaming connectivity.

What do you perceive to be the top 5 challenges where scaling up cellular IoT connectivity deployments is concerned? (All respondents, average rank)

Notably, a lack of available NB-IoT or LTE-M support internationally was ranked as a top 3 concern for enterprises. Indeed, in Kaleido's own analysis of the roaming market for these technologies, a mere 13% of networks globally that support traditional LTE roaming also support either NB-IoT or LTE-M inbound roaming. This means that for constrained device applications where either of these technologies is ideal for deployment, coverage is far from ubiquitous at a global level. In large part, this has to do with the monetisation opportunities available to network owners at the wholesale level, where the opportunity for profitability is perceived as low. On the other hand, a reluctance to support the ecosystem is naturally damaging to the industry at large. Recently, network access-based charging as a means of monetising connectivity has been somewhat of a trend in the wholesale market, but this may pose challenges on the retail side of the market when customers expect pricing for connectivity to be extremely low. As yet, there is no clear solution to reconciling these challenges, although an increase in connectivity localisation through multi-IMSI or eSIM may present opportunities for CSPs that have adopted such strategies.

Availability of high performance connectivity and availability of robust coverage were cited overall within respondents' top 4 and 5 concerns of scaling IoT operations up, respectively. The fact that both high performance demands in addition to NB-IoT or LTE-M coverage both rank among the top concerns underlines the diversity of IoT applications, and the need for service providers to develop capabilities to address these. Most IoT roaming connectivity is based on architectures and routing that raise latency levels; standardised solutions to reduce latency (such as local breakout) have been available for many years, but have seen limited traction on the market due to inter-operator trust concerns over roaming session management and visibility. Nevertheless, many providers are now capable of offering regional breakout solutions, often using public cloud instances to spin up gateway infrastructure, which offer considerable enhancements over traditional roaming solutions. Evidently, education on the market is still required to make enterprises aware of such solutions.

What technical factors influenced your organisation in choosing a cellular IoT connectivity provider? (Cellular IoT Adopters)

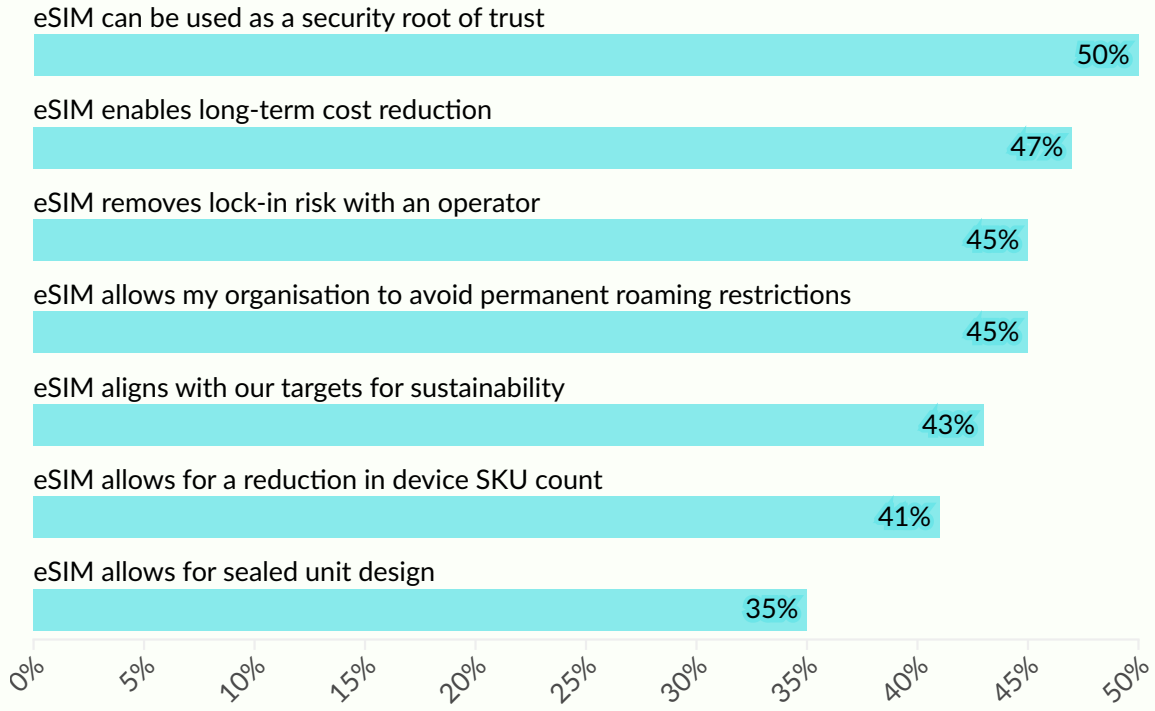


Looking towards cellular IoT adopters, it is perhaps pertinent that the top 2 technical factors behind choosing a cellular IoT CSP were reported as quality of coverage and support for new technologies such as 5G, NB-IoT and LTE-M. Availability, both in the sense of reliability as well as choice, are evidently major concerns among this year's enterprise survey cohort.

eSIM

The emergence of eSIM as a technology to facilitate greater flexibility and choice of mobile operator has been one of the biggest changes to the cellular IoT landscape in recent years. There was a high reported incidence of eSIM usage among respondents, with 78% reporting they used the technology. However, this will be in relatively small numbers in each deployment, with active eSIMs making up a small proportion of the overall cellular IoT connections base. This is likely to have been an early adopter phenomenon, with buying processes driven by more forward-looking departments (like R&D and product development) being slightly more likely to use eSIM. This attitude is also reflected in the preferences of non-users, who are significantly more likely to want trusted and proven technology from their connectivity provider, while eSIMs are relatively new. A shift in the mindset of these users is likely needed to increase penetration of the technology much further.

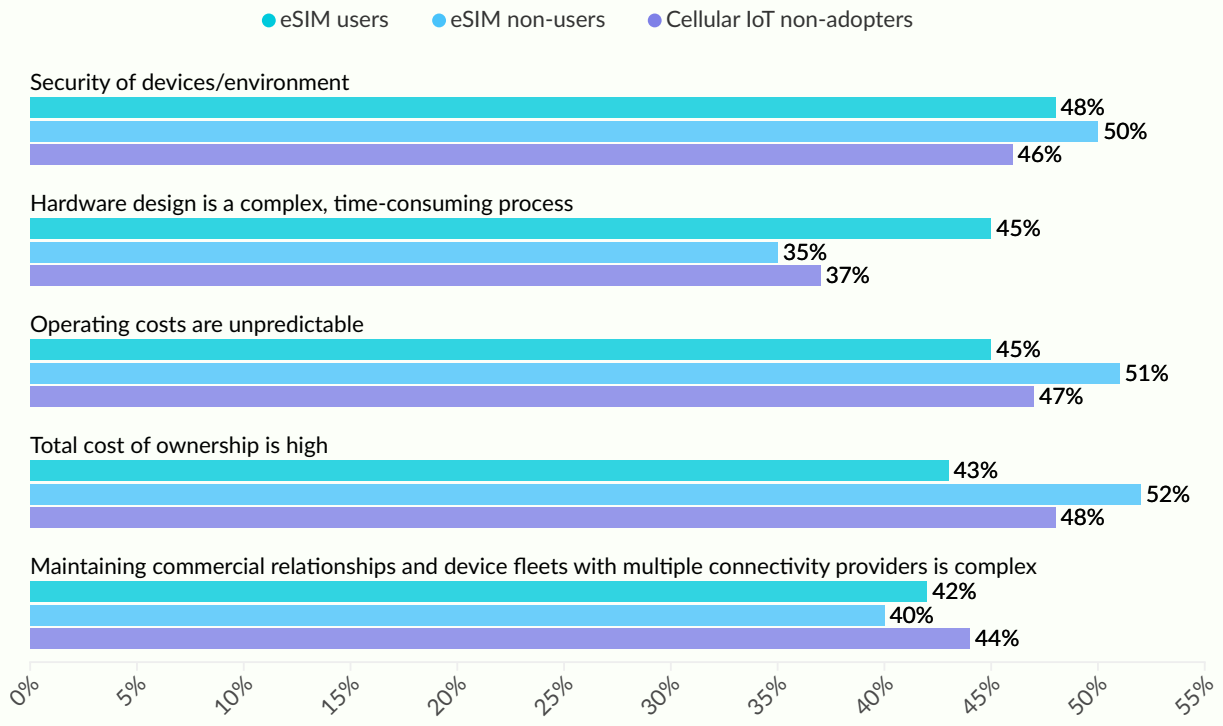
What factors made you choose eSIM (eUICC)? (Cellular IoT Adopters)



The ability to change operator at need without having to change a physical SIM card can bring greater operational efficiency and uptime, particularly for mobile assets. This flexibility is appealing to cellular IoT users, with 32% reporting that the ability to perform OTA (Over-the-Air) optimisation of connectivity is a factor influencing their choice of connectivity provider. This is already a well-known benefit of eSIM, with only 5% of those who wanted that ability reporting not using eSIM, and 45% of eSIM users selecting the technology explicitly for this reason.

However, this is only one of several key reasons to use eSIM, with only sealed unit design being noticeably different from the other drivers. However, the drivers have different appeals by vertical. The ability to reduce costs is most appealing to healthcare users, while smart cities and transportation are more likely to use eSIM because they believe the technology aligns with their sustainability targets. This shows that flexibility in operator choice is not necessarily the silver bullet solution to drive eSIM adoption, although it should also be noted that another commonly-cited benefit, avoiding permanent roaming restrictions, is not much more appealing than others in this category, save for smart cities users, where over half of eSIM users reported it as a benefit.

What do you perceive to be the top 5 challenges where scaling up cellular IoT connectivity deployments is concerned? (eSIM users, eSIM non-users, Cellular IoT non-Adopters; proportion ranking items within their top 5)

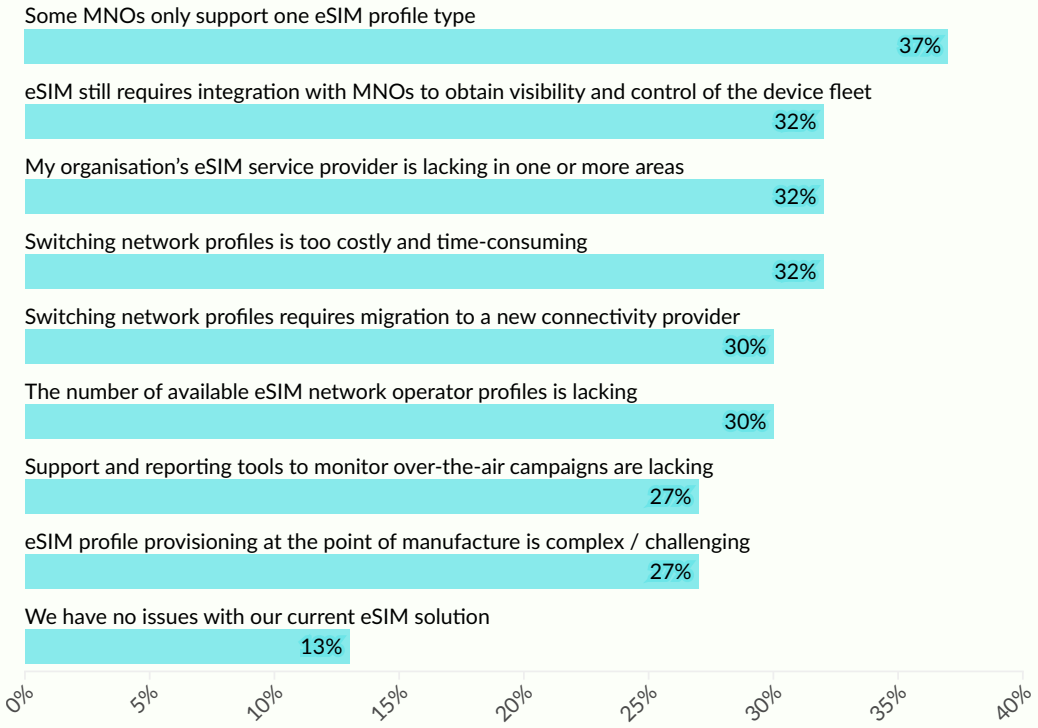


These varied benefits indicate that eSIM providers need to be ready to cater to many different use cases if they want to appeal to a broad range of industries, with markedly different appeal. Those who found the 'traditional' eSIM benefits most appealing were healthcare, energy and utilities and smart cities. eSIM users were slightly more likely to consider roaming restrictions a challenge to scaling IoT than non-users, but this did not reach the level of statistical significance.

When considering challenges for the IoT more broadly, eSIM users do not have many specific differences from cellular IoT users who go in for other SIM technologies. The only significant differences between the groups were that a higher number of eSIM users reported hardware problems in their top 5 challenges, while being significantly less concerned about total cost of ownership than other cellular IoT users. As eSIMs are hardware solutions, it is clear that there is still some problems with fully integrating eSIMs into the desired devices. As such, providing a consultative service to fully integrate the solutions into devices and infrastructure will be appealing to eSIM users, and provide opportunities for VAS selling. However, there is little explicit acknowledgement of this need, as eSIM users are only slightly more likely to look for device consulting services than non-users, with 50% of eSIM users putting consulting services in the top 5 capabilities they want a connectivity provider to have.

There is no statistically significant difference between eSIM users and non-users who find dealing with multiple connectivity providers a challenge, and so this is unlikely to be a driver for eSIM usage. However, it should be noted that eSIM users are slightly more likely to use multiple CSPs, and are significantly more likely than non-users to consider interoperability and simplified commercial models to be lacking in the IoT ecosystem. However, this is likely due to the limitations of their particular eSIM platforms; 50% of eSIM users who report that MNO integration is still required also report a lack of interoperability and simplified models, while only 31% of other eSIM users think the same. There is still considerable work to be done to simplify the process overall, but the need for further MNO integration is having a clear impression. This means that the ability to apply local IMSIs will be a much-desired quality, as it can give a greater level of visibility and flexibility to eSIM connections.

What are your main issues with your current eSIM (eUICC) solution? (eSIM Users)

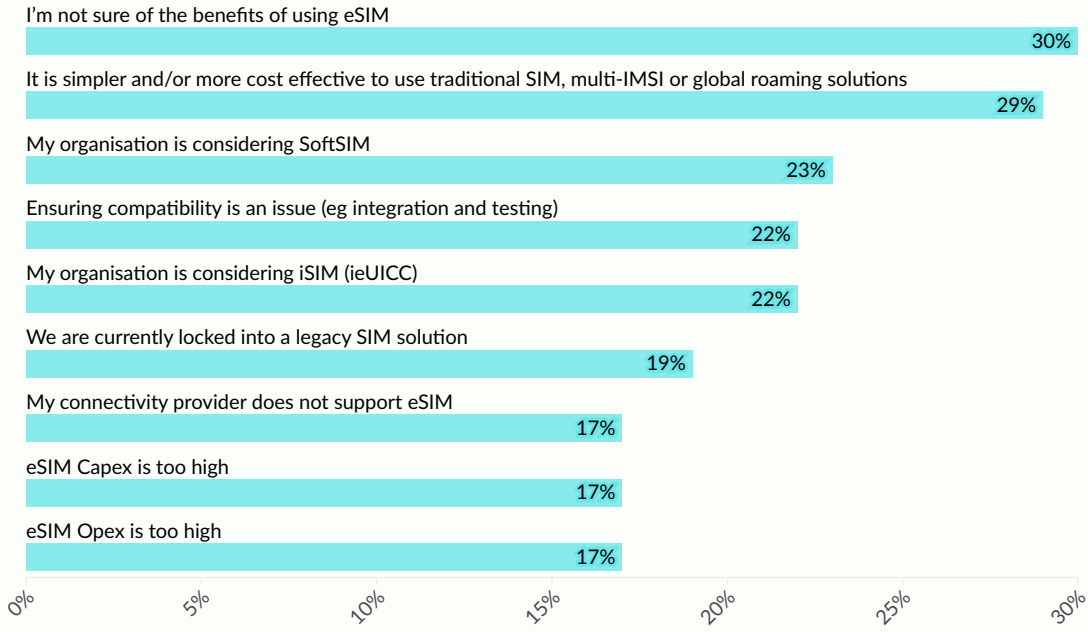


When considering what problems eSIM users have, it is clear that it is an imperfect technology, with only 13% reporting they have no issues with their solution. In general terms, a lack of flexibility is a common complaint, which manifests in multiple ways. 37% claim to have a problem with the provision of only consumer or M2M profiles, while 32% say that switching profiles is too time-consuming. 30% of users also say switching profiles means switching providers, although there is not a large overlap between those who say it is time-consuming compared to those who say they need to switch providers to switch profiles. However, this is still a large proportion of users for a technology that claims profile switching as a core benefit.

Reporting tools are a clear area of improvement, as well. 27% of eSIM users report that reporting and OTA campaign monitoring tools are lacking in the cellular IoT ecosystem, while 59% put extensive reporting in their top 5 desired product features. This area potentially requires greater localisation from eSIM providers, who should be doing more to connect with specific countries, even where there are no regulatory constraints on permanent roaming.

When considering reasons that eSIMs are not used, 30% of respondents report being unsure of the benefits of eSIM, while 29% consider alternatives to be simpler or more cost-effective. This decision is not often made in ignorance; only 15% of those who consider alternatives better also claim to be unsure of eSIMs' benefits. Nevertheless, there is still a large minority of cellular IoT users who could benefit from further education about the nature of eSIM and the benefits they can bring.

Why have you chosen not to use eSIM (eUICC)? (eSIM Non-users)



We have already noted that eSIM users potentially have a higher cost threshold than non-eSIM users, and indeed 28% of eSIM non-users consider that either Capex or Opex is too high for them to consider using the technology. However, only 8% of non-users overall think that both Capex and Opex are too high. This means that eSIM providers who can be flexible in their charging model have a larger potential market, and need to be upfront about that flexibility to appeal to users who may have restrictions in some parts of their budget but not in others. There is also a clear uncertainty for the future of eSIM, which has manifested in many places before. 40% of non-users reported not using eSIM because they are considering iSIM or SoftSIM, with relatively little overlap for both of these technologies. eSIM providers should look into incorporating these alternative form factors into their portfolio alongside eUICC. There is however little difference between verticals among the non-users who are using these, meaning that targeting these users will be quite difficult.

Britvic maximises data insights and champions sustainability with advanced connectivity from Wireless Logic

About Britvic

Britvic is a leading soft drinks business known for its iconic brands such as Robinsons, Tango and J20. Founded in the 1930s from humble beginnings in Essex, UK, the international organisation now distributes and exports to over 100 countries worldwide. Sustainability is an important part of Britvic's ethos, as it strives for resilience through the responsible use of natural resources and a reduced impact of its operations on the environment.

Accordingly, Britvic has an active programme 'Beyond the Bottle', which seeks to reduce unnecessary packaging. As part of this initiative, Britvic introduced the Aqua Libra Flavour Tap, which provides flavoured water to consumers via a digital dispenser, as an alternative to single-use plastic bottles or cans. The eco-friendly tap, which is tailored for workplaces, hospitality and retail environments, generates usage and other data which Britvic can capture and analyse, thanks to cellular IoT connectivity.

Challenge

Britvic recognised immediately that telemetry data from its installed taps provides valuable insights the company could feed into its marketing and strategic planning, as Scott MacKenzie, Director of Beyond the Bottle Platforms at Britvic, explains: “It allows us to build a really rich database of information that we can leverage to understand consumer trends, forecasting and machine capabilities.”

To get this information, Britvic connected the taps initially through a software-as-a-service model, whilst it tested the concept. However, once it had recognised the product’s market potential, it looked around for the best way to transition to a direct connection approach.

“As we look to expand, scalability and reliable connectivity are crucial,” adds Scott. “We needed a trusted connectivity partner to support our growth.”

The telemetry data Britvic receives gives it insights into the flavours that customers choose, usage data throughout the day and information about the taps themselves. Britvic recognised the potential of the IoT to deliver this detail, thereby helping the company streamline its forecasting and logistics, and be more agile in its planning.

As Britvic considered its IoT connectivity options, security was a top priority. The Aqua Libra Flavour Taps are installed onsite in customer facilities and locations, so it was crucial that the safety of the networks be assured.

Solution

Britvic conducted a robust market review of IoT connectivity providers. When approached, Wireless Logic assessed Britvic’s requirements and responded by recommending its dedicated IoT network Conexa to provide the wide coverage needed, together with the ability to change network profiles remotely in the future and a secure and sophisticated management platform.

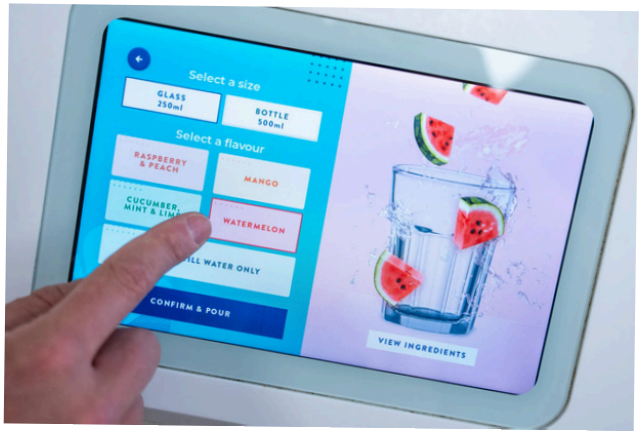
Conexa is Wireless Logic’s globally-distributed mobile core network which is dedicated to the IoT. It delivers resilient, secure and globally compliant connectivity. It can scale in line with Britvic’s global expansion plans to remotely provision the most appropriate network in the country where taps are installed. This ability to swap operator profiles remotely using a combination of eSIM and multi-IMSI technology, helps to simplify logistics, scale seamlessly and address the operational, commercial and regulatory pressures that can change over time.

SIMPro is Wireless Logic’s IoT connectivity management platform that is highly customisable. It gives Britvic visibility and control over its devices so it can perform tasks from SIM management to troubleshooting through deep network diagnostics. A comprehensive set of rest APIs and advanced alerts and rules allow Britvic to integrate SIM operations into existing workflows.

Conexa and SIMPro, together with expert onboarding support from Wireless Logic's technical team, ensured that the taps worked hand-in-hand with the connectivity solution and made Wireless Logic stand out from its competitors. Overall, it was a natural fit for Britvic's deployment.

Scott says: "With Wireless Logic as our connectivity provider, we have secure, reliable and real-time access to data on flavour preferences and consumption patterns."

Outcome



By partnering with Wireless Logic for cellular connectivity, Britvic has the visibility it needs into the Aqua Libra Flavour Taps. Insights it receives from the taps' data equip Britvic to make informed business decisions in support of its strategy and product enhancement.

"This has already revealed unexpected trends, challenging our assumptions and informing our strategic decisions," adds Scott. "By using these insights to streamline our forecasting and logistics, we've enhanced our overall agility and responsiveness, enabling us to adapt production and flavour distribution strategies based on seasonal variations and shifting consumer behaviours."

Britvic set out to reduce plastic waste and promote sustainable soft drink consumption through its solution designed for environmental good and connected using cellular IoT. As Britvic continues to explore the potential of refreshing and flavourful hydration 'beyond the bottle', it can further evolve how it uses data insights to ensure its product offerings are targeted to deliver maximum customer satisfaction. Wireless Logic's solution can scale in line with Britvic's plans, to deliver flexible, resilient connectivity when and where it is needed and data insights for continued informed decision-making.

"Security was at the forefront of our thinking right from the very start. That was part of what brought us to Wireless Logic - to have a trusted partner that had its own network."

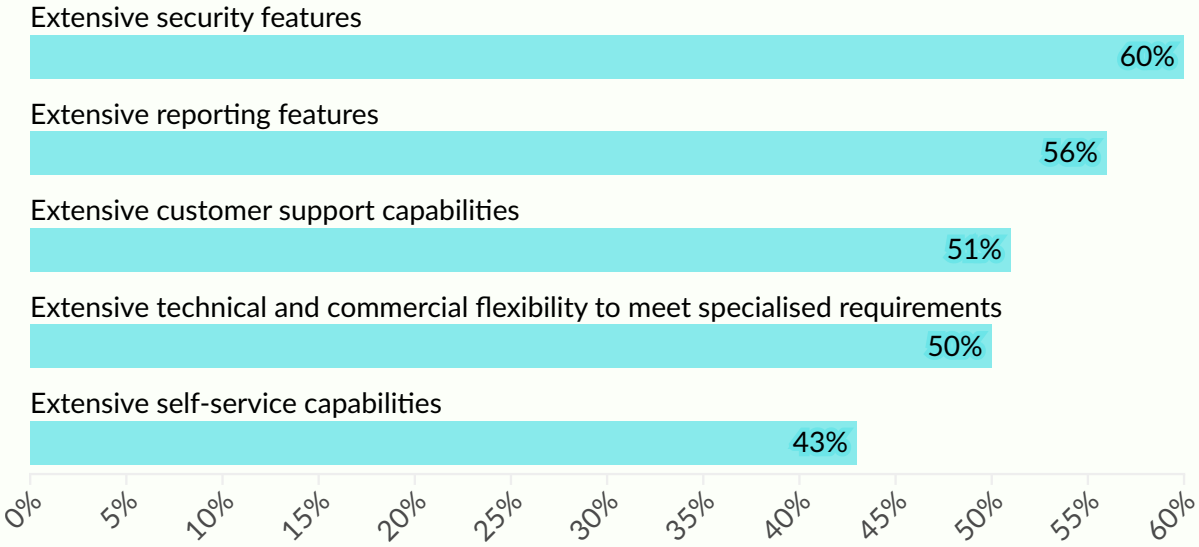
Scott MacKenzie, Director, Beyond the Bottle Platforms
Britvic

Security

With ever more connected devices and industries comes more opportunities for cybercriminals to damage enterprise infrastructure. This is a particular problem where older devices are brought into the connected world, as they will not have been built with security in mind. Despite this, there will likely be little drive to replace these devices, with concerns over ROI deciding when devices are replaced in most cases, rather than purely basing it upon security concerns.

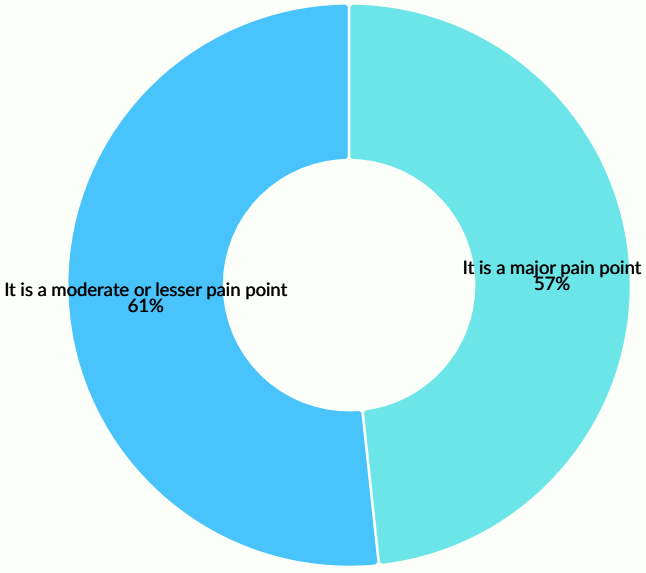
With this overall landscape, it is unsurprising that 89% of respondents report that cybersecurity breaches are a major or moderate pain point in their organisation. Despite this concern, it does not feature similarly heavily in connectivity purchase decisions, with only 48% of respondents putting the security of devices and environment in their top 5 challenges in scaling up cellular IoT, and 51% putting end-to-end security in their top 5 most important factors for IoT connectivity. It is actively sought after by a majority of users, with 60% putting extensive security features in the top 5 features they look for in an IoT CSP's product.

What are the top 5 factors that you look for/would look for in an IoT connectivity partner's product? (All respondents; proportion selecting items within their top 5)



However, it appears that the prevailing attitude regarding security is one of checking a box, rather than tying it to any perception of security threat., but those who consider cybersecurity breaches a major/moderate pain point are not significantly more likely to put security in their top 5 challenges, important factors or product features. There is also little difference between those who report cybersecurity as a major or moderate pain point and those who do not in their expectation for network threat detection and mitigation services. This pattern holds for all forms of CSP, with respondents showing very little difference in attitude to security features whether they engage an MNO or MVNO. This means that all need to be able to offer security products, either through partnerships or their own in-house developments. Partnerships are probably the best model for smaller MVNOs, who may not have the requisite in-house expertise but still need to offer security VAS as an option.

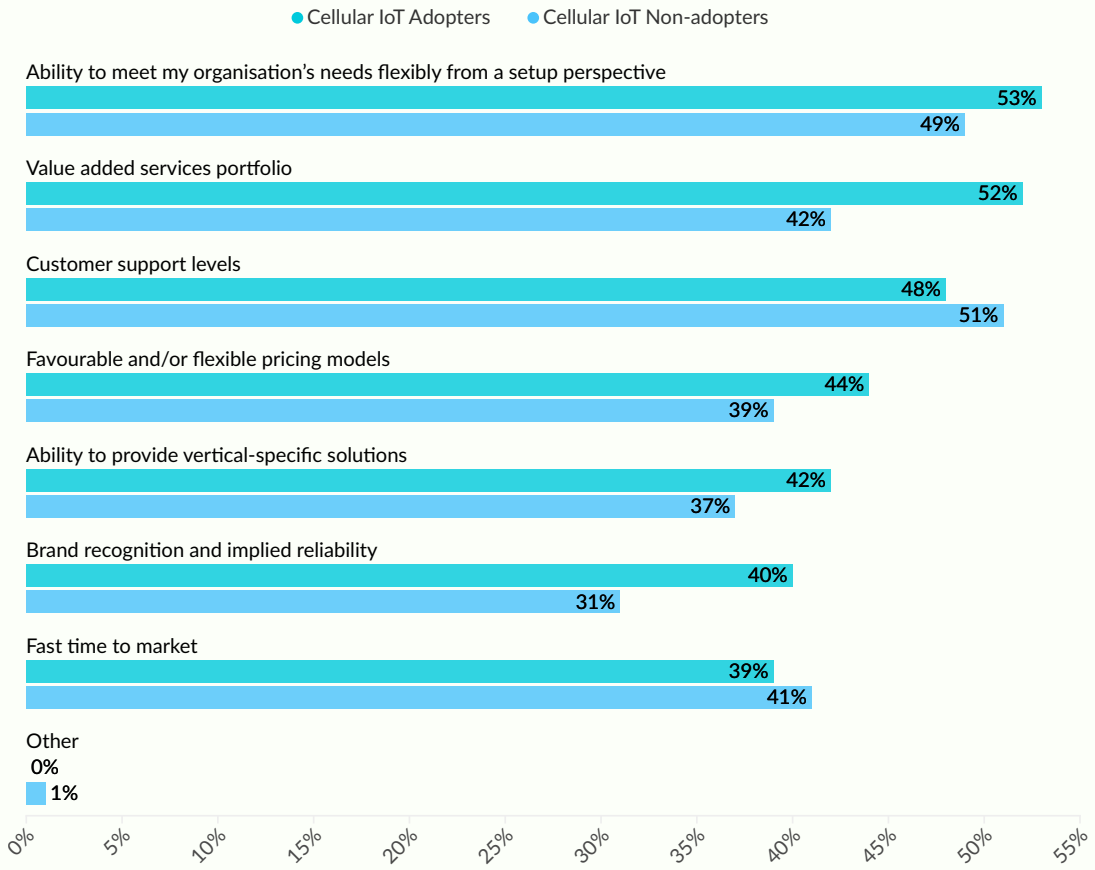
Do the threats of cybersecurity breaches or issues related to compliance as a result of cybersecurity issues represent a pain point for your organisation? (All respondents)



Given these results, there is not necessarily less concern for security among some respondents, but rather that it is considered an integral part of connectivity, without being considered a key product feature that drives purchase. However, there likely are those who will be turned away by a lack of security, so including security features as a key part of any VAS offering is vital.

This will need some explaining to those who do not currently use cellular IoT, as they are significantly less likely to consider VAS as a general driver of purchase. CSPs must refine their messaging around security to ensure they do not lose customers through a perceived lack of security in their baseline product features. Even though security is not necessarily top-of-mind for future deployments, there will be an expectation of a certain level of security, beyond what is offered as VAS.

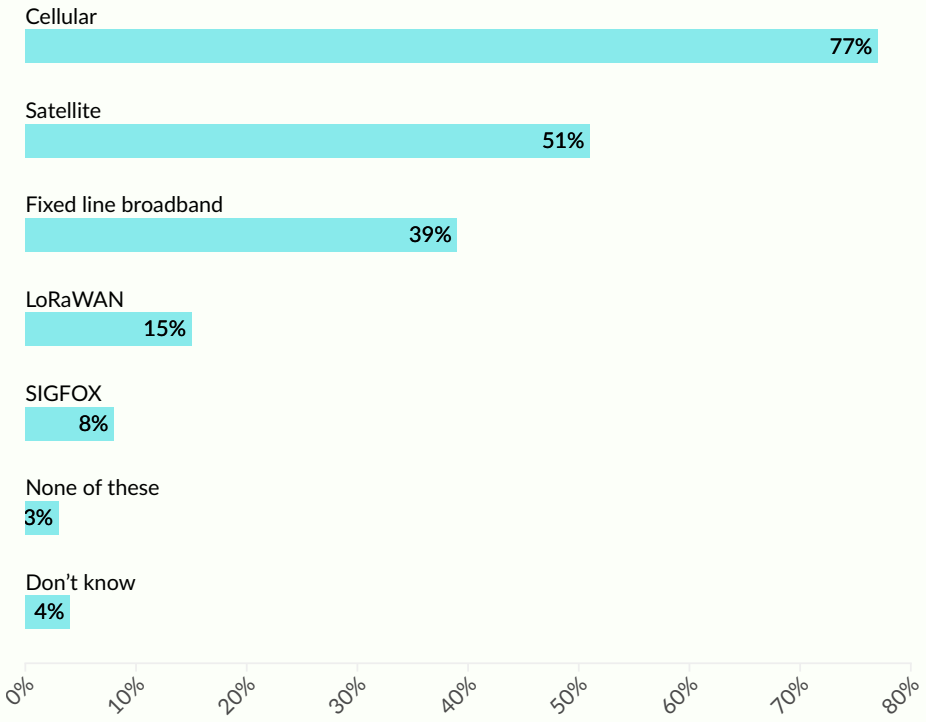
What non-technical/commercial factors influenced your organisation in choosing a cellular IoT connectivity provider? (All respondents)



Branding is of relatively little importance to security in itself, but security forms an increasingly important component of branding, at least in the negative sense – having cybersecurity incidents will reflect poorly on an organisation that has known vulnerabilities in its products. The implied reliability in branding is a component of consideration for 40% of users and 31% of non-users, and having a strong security posture forms a key part of that implied trust.

It should be noted that security can be incorporated in other ways beyond a security platform offering; 50% of eSIM users cite the ability to use an eSIM as a root of trust. This can be extended to SIMs in general, to potentially enhance the profile of cellular connectivity compared to the alternatives, which may be necessary if a CSP is exclusively cellular. However, cellular is generally more likely to be considered suitable than other technologies, so this may not be necessary.

Which technology(ies) for wide-area connectivity do you view as most viable for IoT deployments? (Cellular IoT Non-adopters)



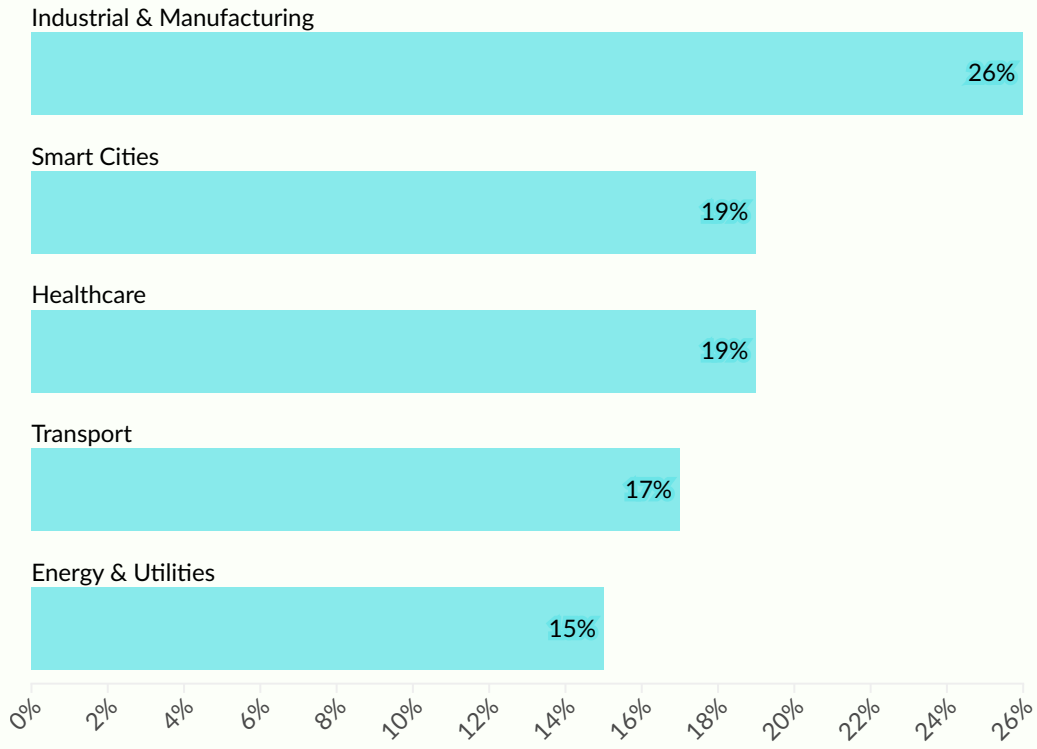
Various monitoring tools that can be used for network performance metrics can also be used for security purposes when paired with the relevant software. This is likely the case for many respondents, 88% of whom reported they expected their CSP to provide traffic metadata. Much of this can be used for security purposes, such as protection against traffic surges in a network or anomalous data indicating attempted attacks of various forms. While this kind of analysis usually requires some degree of AI or at least an underlying rules-based engine, having the data to hand through some means is at least a prerequisite to certain forms of more advanced security.

Sector Focus: Manufacturing

Manufacturing as a sector handles a lot of confidential product information, and with increasing levels of automation and digitisation, more than any other sector, is likely to feel the impact of any security breaches more severely. As a result, it is the sector most interested in security measures, although in many cases the increase here is only slight. For example, over half of manufacturing cellular IoT users report an expectation for CSPs to offer network threat detection and mitigation, compared to 45% of those in other sectors.

This is potentially because manufacturing has the highest proportion of enterprises reporting that IT or OT departments having sole decision-making power on the issue. This will put operational concerns like security to the forefront in manufacturing contexts in a way that is less likely in other industries.

How much influence do each of the departments involved in the connectivity purchase decision have? (All respondents, proportion selecting IT or Operations as Sole Arbiter)



Cellular success factors: Global, simplified and end-to-end security

Security as a strategic advantage in your IoT

Enterprises seek to derive value from the data generated by their IoT systems, devices, and sensors to enhance efficiency and deliver differentiated experiences, often across global operations. Cellular connectivity is a major factor driving this data revolution, delivering benefits of robust security, global and resilient network availability, and scalability.

Furthermore, cellular technology brings the ability to use the SIM, eSIM, or iSIM as root-of-trust to deliver end-to-end security, unlocking new waves to drive revenue with innovation.

End-to-end security with eSIM-based scalable trust

As the number of IoT devices grows, securing data throughout its lifecycle generation, transmission, and storage—has become increasingly critical. Leveraging a hardware secure element (SE) as a 'Root of Trust' to execute security services and store security credentials is an essential step in the development lifecycle to guarantee end-to-end security for IoT products and services.

Kigen

The Challenge

There are several proprietary hardware SE solutions available to deliver this root of trust, but market fragmentation introduces a key challenge.. Many IoT solutions rely on proprietary hardware SEs, creating market fragmentation and complicating the process of delivering consistent security across different devices. Enterprises now face the challenge of ensuring end-to-end security for their IoT deployments while maintaining interoperability and scalability.

As the digitalization of industries such as smart metering, transportation, logistics, and more scales, it is more urgent and important than ever before as enterprises start acting to adopt resilient IoT security features through directives such as the **EU Cyber Resilience Act**. The timing of this partnership proves vital for the Cellular IoT industry's 'hyper-growth', with some estimates putting the number of devices as **exceeding 6 billion by 2028**.

Crypto Quantique, quantum security leader for IoT and global IoT connectivity partner ZARIOT, turned to Kigen's IoT SAFE solution to lower costs in transitioning to post-quantum resistant security.

The Solution

Developed by the mobile industry, the GSMA IoT SAFE (IoT SIM Applet For Secure End-2-End Communication) standard enables IoT enterprises, device manufacturers and service providers to leverage the SIM, eSIM or iSIM as an applicative KeyStore where security keys are securely stored and dynamically managed. There is also no need for an expensive and dedicated Secure Element.

What's more, Kigen's IoT SAFE solution goes further to ease the development of integration into enterprise solution stacks to deliver greater scalability, simplicity, and trust.

Each SIM produced by Kigen is fully certified in both manufacture – GSMA Security Accreditation Scheme for UICC Production (SAS-UP), and management – GSMA Security Accreditation Scheme for Subscription Management (SAS-SM).

Combined with the industry-leading secure SIM OS, Kigen's IoT SAFE solution addresses key design hurdles, simplifying how design middleware can easily access SIM, eSIM, or iSIM services. This radically changes the way enterprises can use SIM, eSIMs or iSIMs as a viable and available solution that works in tandem with Crypto Quantique's market-leading solution to fully secure connections for authentication, encryption and service acceleration.

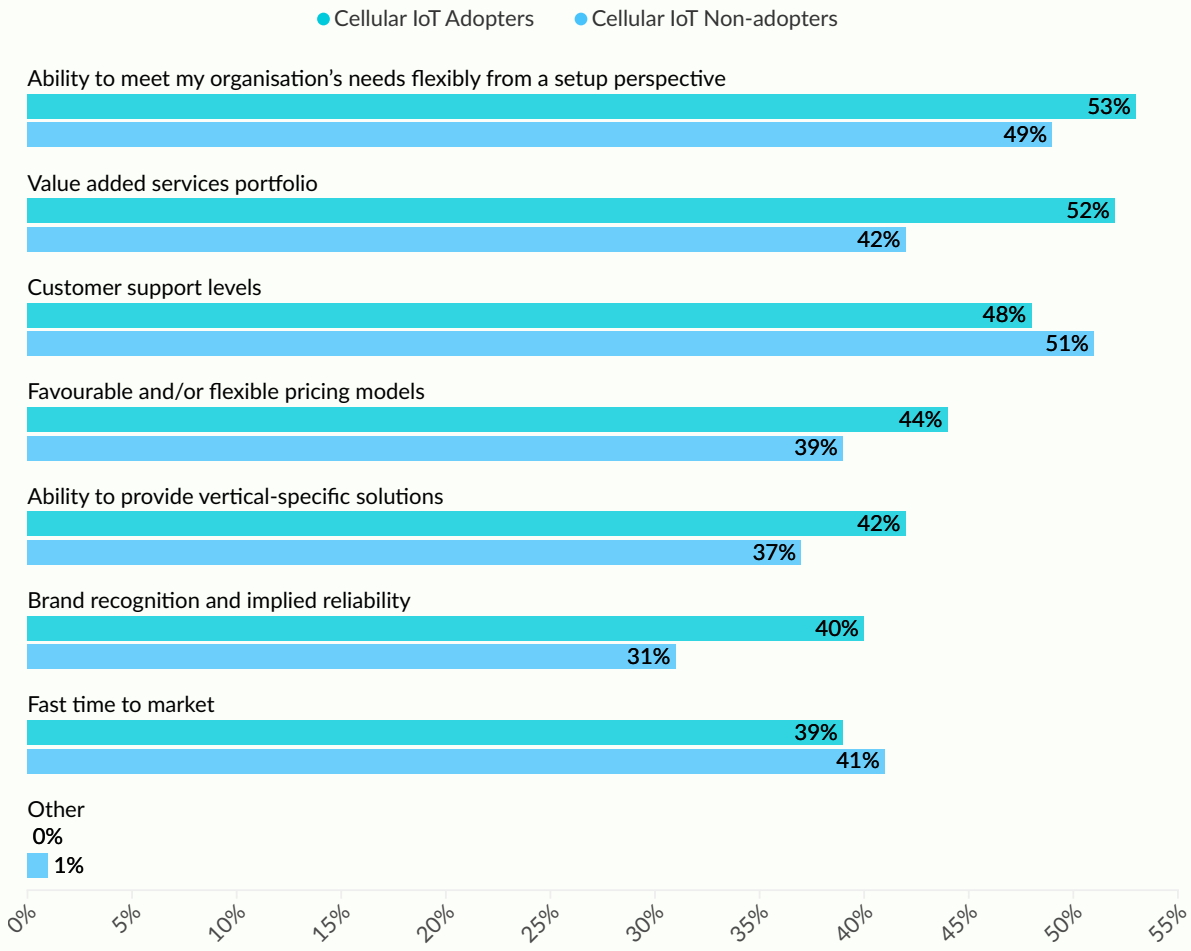
Looking ahead

As the IoT ecosystem continues to expand, Kigen's commitment to innovation ensures that enterprises can leverage scalable, secure connectivity solutions. The combination of eSIM-based security and IoT SAFE standards allows for faster, more secure IoT deployments, positioning enterprises to meet future regulatory requirements while safeguarding data at scale.

Value-Added Services

Connectivity providers are often not a 'dumb pipe' for enterprises. They can be useful partners who can offer many different services in addition to connectivity, which may not be enough to meet enterprise needs on its own; connectivity is rarely needed for its own sake. Our survey respondents recognise this, with current cellular IoT users reporting VAS (Value-Added Services) as the #2 non-technical element in their decision to use a particular CSP, while current non-users rank it as their third most important element. Overall, more than 50% of respondents consider VAS an important element in choosing a CSP.

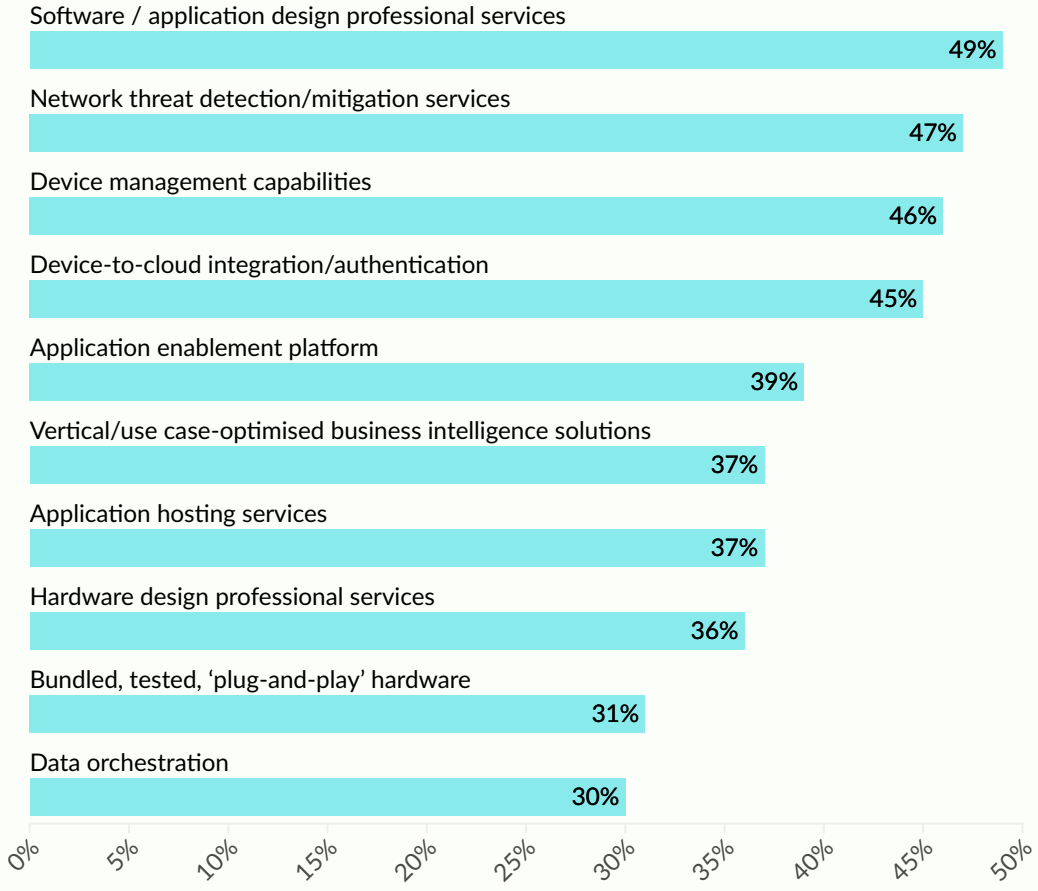
What non-technical/commercial factors influenced your organisation in choosing a cellular IoT connectivity provider? (All respondents)



There are several VAS that are key to respondents' needs, with the average cellular IoT user wanting more than 3 services, with end user organisations wanting significantly more VAS than those elsewhere in the value chain. There are still some definite differences even within the end-user cohort, with those wanting plug-and-play connectivity wanting significantly less VAS than those expecting to obtain their own connectivity. However, those expecting to source connectivity services themselves represent a larger overall group, meaning that CSPs should focus on more flexible offerings to cater to the larger market.

Respondents report a more diverse array of top-scoring VAS than in previous years. While previously device-based services were the most prominent on offer, in 2024 they have been joined by services for application design and threat detection and mitigation. These services will require CSPs to move out of their traditional comfort zones, as hardware and software services are not traditional elements of their offering, even where more advanced connectivity services are offered.

Beyond connectivity, what value-added services do you expect your cellular IoT connectivity service provider to offer? (Cellular IoT Adopters)



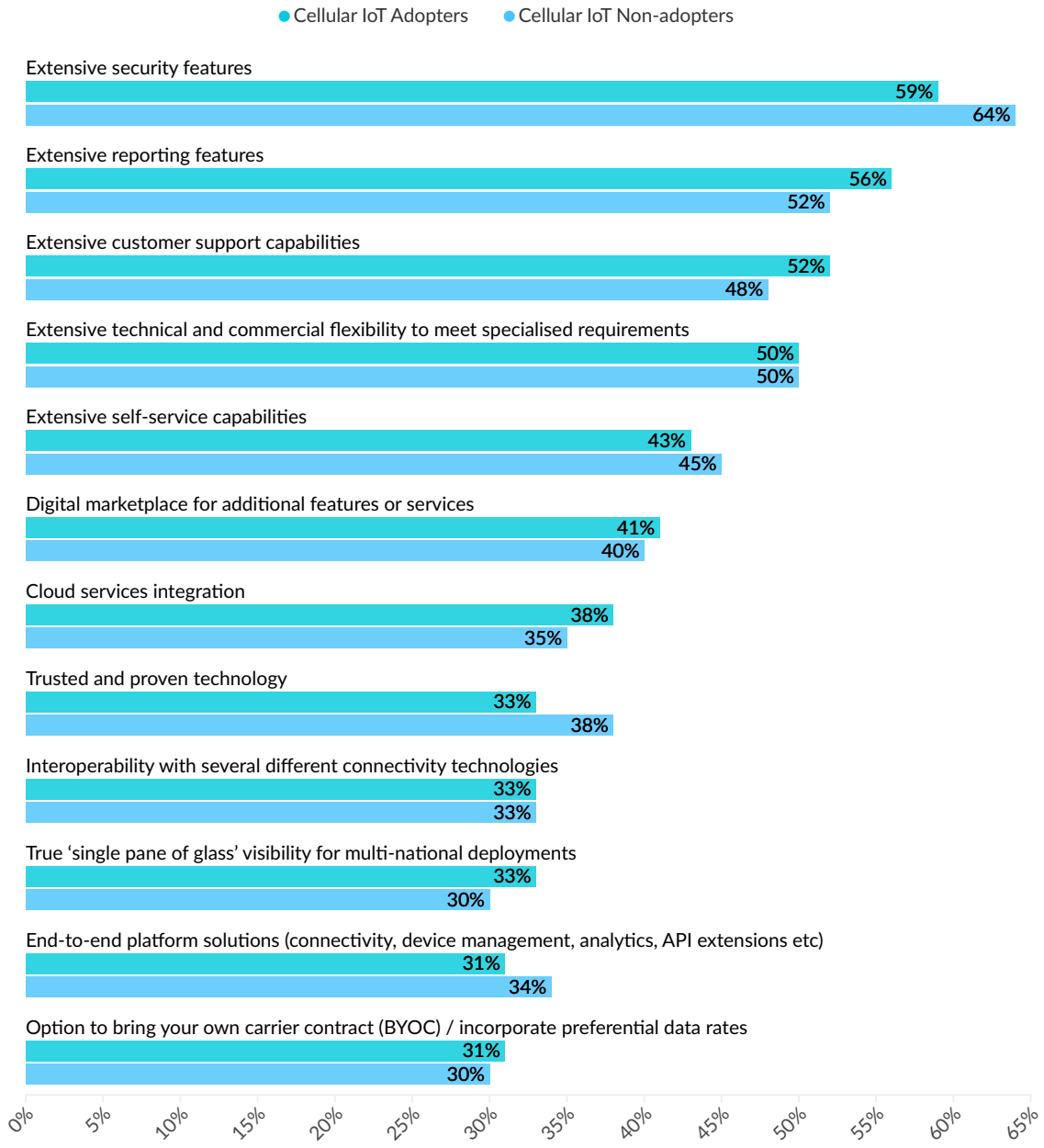
There is a clear need for advice on devices and hardware, for both end users and other portions of the value chain, although OEMs and ODMs show slightly less interest in this compared to other enterprise types. Moving into this area will allow CSPs to become more active partners for most potential customers. Even OEMs and ODMs score relatively highly on these metrics, even if it is lower than other groups; 41% of OEMs report a desire for software design professional services, for example.

Notably, only 39% want an AEP (Application Enablement Platform) as VAS, and reporting tools are in the top 5 product features most looked for according to 55% of these. In addition, 72% of current cellular IoT users reported that it was of the high or highest importance that their CSP can provide real-time information on data consumption and the network state. This combination highlights a desire for connectivity information and status from respondents, but not necessarily self-service tools.

The desire to be an active partner must be handled carefully, though; only 24% reported that they obtained services through the kind of direct channels that this kind of consultative relationship would imply. 40% of users indicating they already used a digital marketplace or eCommerce platform to purchase VAS services. This will continue in future, with 41% of all respondents reporting that a digital marketplace for additional features would be in their top 5 product features.

There is a similar level of desire for connectivity that ensures data sovereignty, offering a strong opportunity for local breakout and edge processing as additional services that can localise data in line with regulatory requirements and security concerns. This can also be linked to a desire for low-latency response connectivity, which 68% of respondents claim is of high or highest importance. While this may be an overestimation of a business' connectivity needs, it shows a receptivity to the capabilities and requirements of 5G.

What are the top 5 factors that you look for/would look for in an IoT connectivity partner's product? (All respondents; proportion selecting items in their top 5)



Several of the most desired product features can be presented as VAS to customers, with security as the most traditional VAS offering available. 50% also want flexibility as one of their top 5 product features, which a strong VAS portfolio can serve to demonstrate. This does not necessarily need to be offered through the CSP's own capabilities; while 32% of respondents reported end-to-end platform capabilities in their top 5 features, the majority are open to a less integrated approach, allowing CSPs to more easily source platform elements from partners without harm to their offering.

About the Authors

This survey report would not be possible without the support of its sponsors. Kaleido wishes to thank the sponsors of this study, who are supporting our vision of enabling business decisions across the enterprise sector through inspiring, educational and accessible insights.

Giesecke+Devrient Creating Confidence

Kigen

wireless logic

Kaleido Intelligence is a specialist consulting and market research firm with a proven track record delivering telecom research at the highest level. Kaleido provides insightful business analysis, market projections, recommendations and growth strategies for global mobile operators, telecom vendors and IoT service providers.

Kaleido covers industry-leading market intelligence and publications on IoT Roaming, eSIM, Connectivity Management Platforms, Private Cellular Networks and Mobile Telecoms Fraud & Security. Research is led by expert analysts, each with significant experience delivering insights that matter.

Publication Date: October 2024
For more information on this market study or if you have further requirements, please contact:
+44 (0)20 3983 9843| info@kaleidointelligence.com