Serving the Enterprise: The Cellular IoT Connectivity Opportunity

A Kaleido Intelligence Survey Report Sponsored By

Table of Contents

Introduction to the survey

Introduction

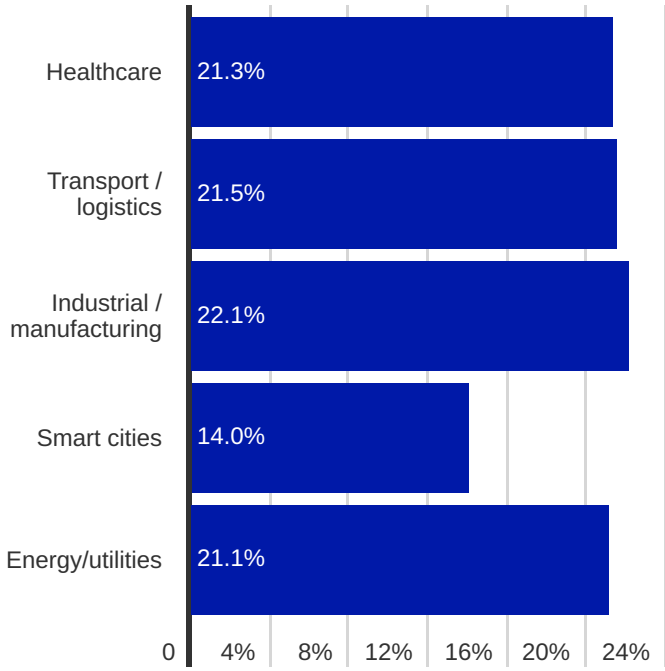
Approximately a decade ago, several large technology firms anticipated that cellular technology would form the natural basis for the majority of IoT connectivity. However, as of 2022, this has not yet happened: there were just over 2 billion cellular IoT connections by the end of 2021, while the broader IoT market ended the year with approximately 12 billion. Thus, cellular connectivity accounts for around 16% of the IoT market by connection volume.

Cellular technology has numerous advantages over other connectivity technologies that helped drive the assumptions made between 2010 and 2012: its inherent flexibility allows it to cater to high- and low-bandwidth requirements, standards have been developed to account for low-power scenarios, while the 5G standard is particularly suited to mission-critical applications that require ultra-low latency response times or Gigabit throughput. The fact that cellular technology is wireless and operates in licenced spectrum, while offering a robust security model, only serves to bolster the business case for using it as part of the IoT connectivity ecosystem.

It is a fact that IoT projects cannot succeed unless the devices are able to properly and securely transmit their data to any software ingestion point for processing. As we shall see, this is easier said than done. Moreover, the success of IoT depends on the capability of the customer to scale connected devices up as projects expand in scope, with this scaling frequently happening on an international scale. Those customers require a relatively high level of efficiency to manage those connected devices, particularly as the cost of engaging with IoT at any sort of scale is not trivial.

With this in mind, Kaleido Intelligence has set out to understand the root of many enterprise pain points in regard to IoT connectivity **through a survey that saw some 759 individual respondents across 5 industry verticals** give their perceptions on the current status quo. Respondents were typically decision-makers within their organisations, with a fair or good knowledge of the IoT connectivity ecosystem, responding on behalf of companies specialising in healthcare, transport and logistics, manufacturing and industrial, smart cities, and the energy and utilities segments.

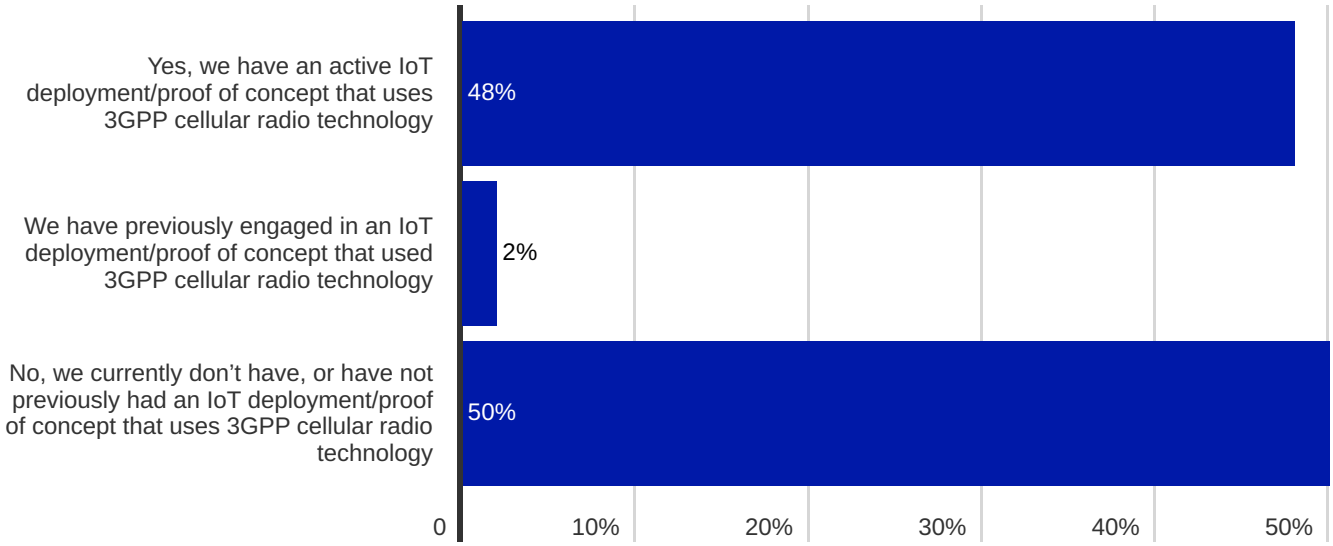
In what market segment does your business unit primarily operate?



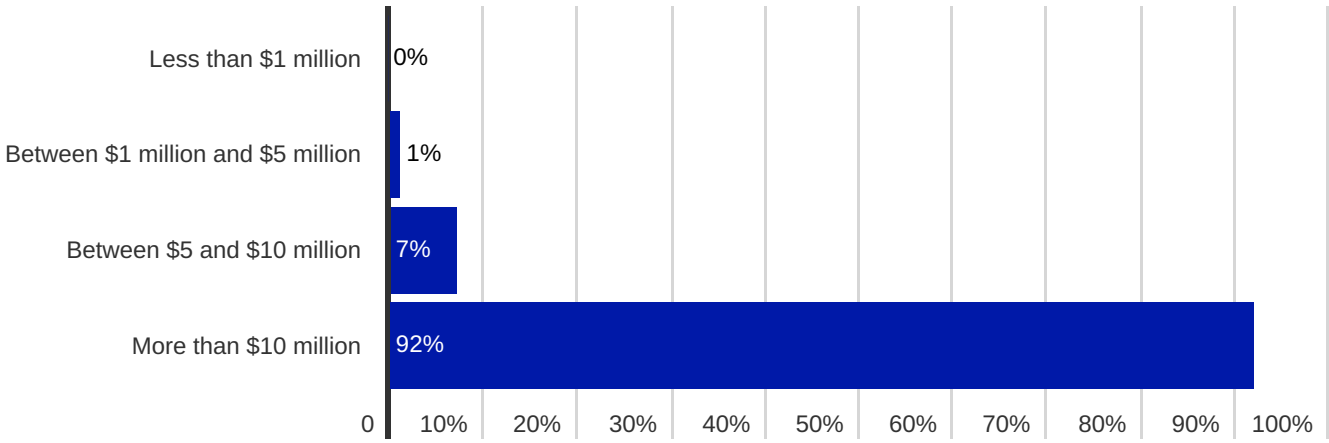
While this study is primarily concerned with cellular IoT connectivity, in order to understand a broad picture of perceptions, respondents included companies that had adopted cellular connectivity for IoT, in addition to those that had not. The differences, as well as the consensuses in perceptions among these groups and industry verticals,

are among the key goals of the study in terms of understanding where the industry can improve and where opportunities to accelerate the adoption of cellular technology for IoT lie.

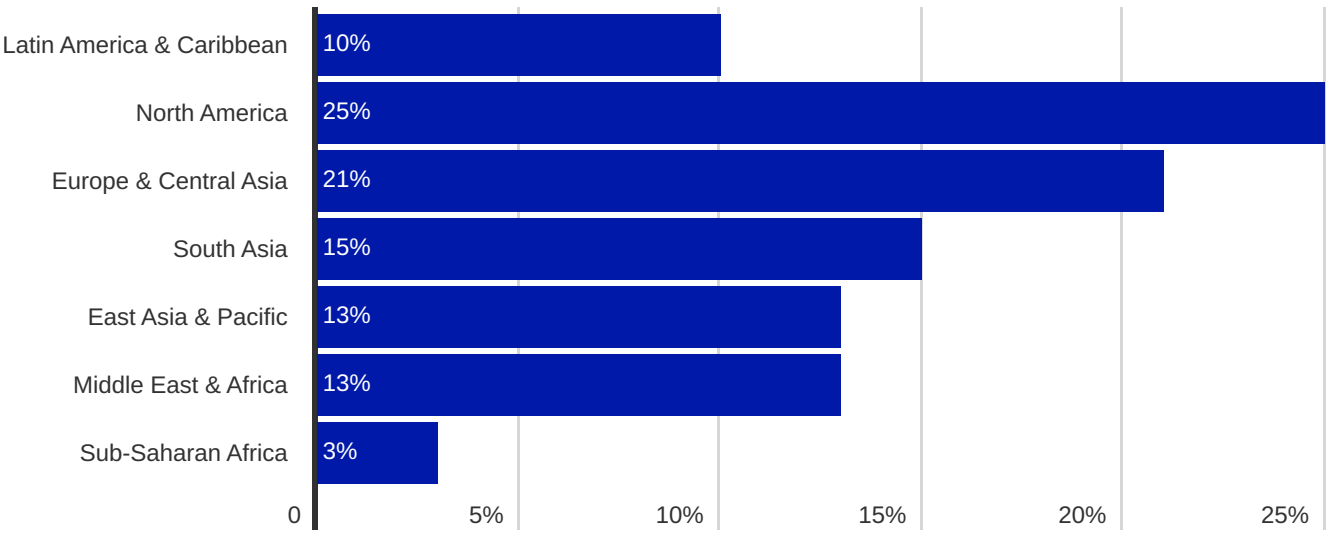
Does your business unit currently have an IoT deployment or proof-of-concept underway that uses 3GPP cellular radio technology (2G/3G/LTE/5G)?



What was your organisation's turnover in 2021?



Where is your business unit based?



Survey Themes

Kaleido Intelligence

The survey analysis allows us to identify several themes among the respondent base, surrounding:

Complexity

Costs, time-to-market, commercial and regulatory barriers, in addition to enterprise understanding of IoT requirements and goals all play a role in the success of IoT projects. Service providers must position themselves as both problem solvers as well as experts in the field here in order to help enterprise customers launch and maintain successful IoT deployments.

Roaming

IoT devices provisioned with cellular connectivity often operate across several countries worldwide. Inevitably, this means that roaming, the technical and commercial arrangement that allows cellular devices to access networks in visited countries, is required. Coverage, costs, performance and support are of fundamental concern to enterprises here.

Security

IoT data is only valuable to enterprises if is not compromised in any manner. With IoT offering cybercriminals a significant attack surface, appropriate measures at several levels are required in order to minimise the risk of disruption.

eSIM

eSIM enables a paradigm shift in how cellular connectivity can be provisioned and managed. Its reprogrammability over-the-air makes it a highly flexible solution to achieve various goals, and is increasingly considered a must-have for cellular IoT connectivity.

Private LTE/5G

Private cellular networks offer enterprises significant enhancements over traditional communications solutions, and suffer from few technical compromises. The ecosystem is complex, however, and a significant level of expertise is required to aid in choosing an appropriate deployment.

IoT Connectivity Challenges & Opportunities: All IoT Verticals

eseye iBASIS KORE TRUPHONE flo. LIVE

Complexity - All Verticals

Kaleido Intelligence

It is apparent from the results that perceptions of complexity where cellular IoT connectivity is concerned continue to plague the industry. When non-cellular IoT adopters were asked to rank the top 5 challenges of cellular IoT, they overwhelmingly reported that hardware design poses the most significant challenge to any potential undertaking, with 84% of respondents choosing this element as their number one challenge.

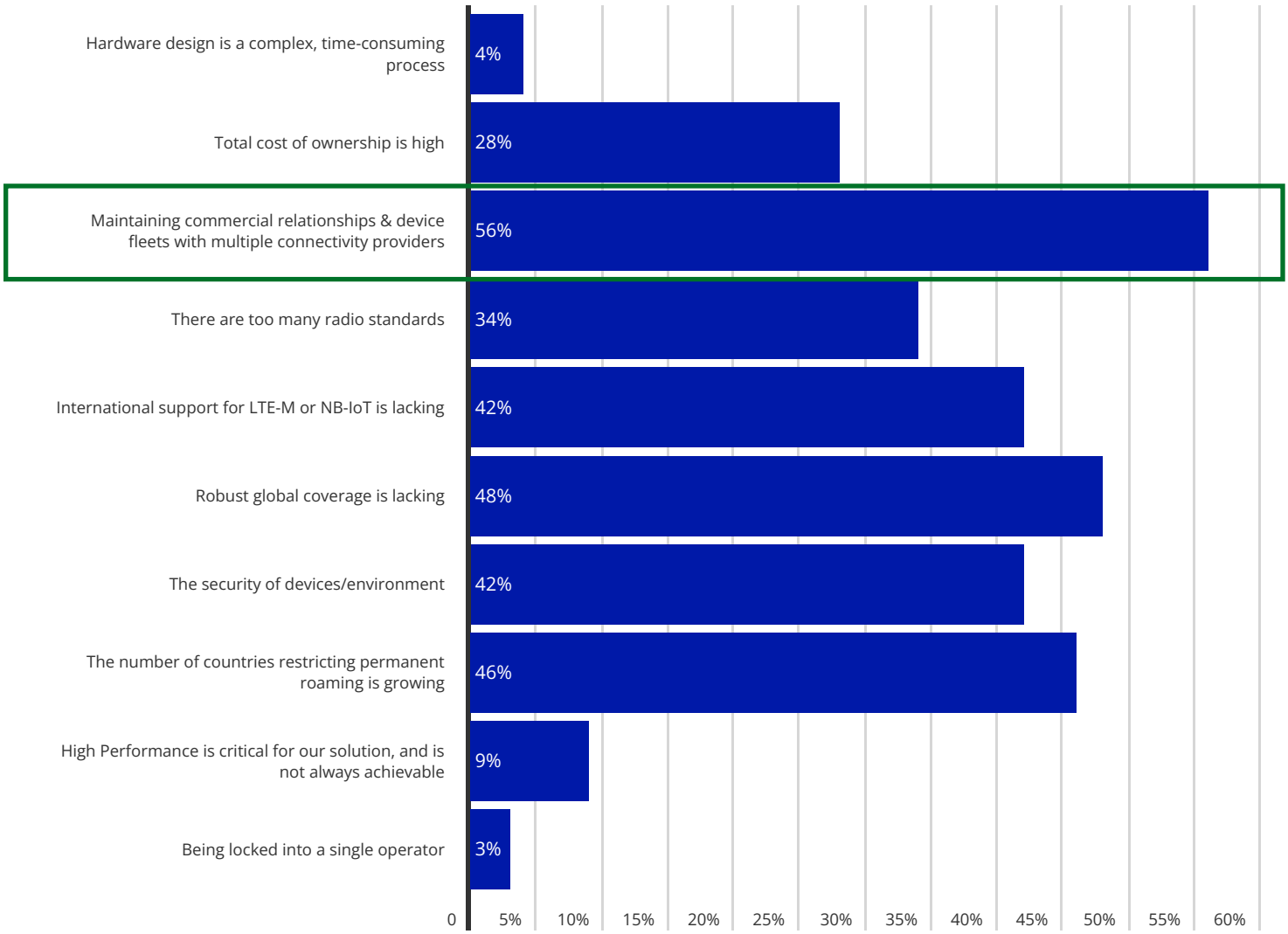
Hardware design ranked as a leading challenge by 84% cellular IoT non-adopters

Unlike the consumer smartphone industry, the IoT industry is not built around plug-and-play concepts. This means that customers are rarely able to procure off-the-shelf products with the expectation that they will meet their business requirements, much less be optimised for the project in question. Building hardware from the ground up is an arduous, costly process that, if it is built from the base components up, requires that radio hardware is certified for all the regions in which it operates. This can often result in very high costs that leave little margin for profit unless extremely high deployment volumes are expected. Cellular modules can solve this issue to an extent, in that chipsets are pre-certified for various regions and countries, while support can be offered by the module OEM for configuration and technical issues. Nevertheless, many companies are not familiar with 3GPP radio technologies in terms of the standards available on the market, in addition to the protocols in use. Without third-party expertise to guide them on their journey, selection, configuration and testing hardware solutions for cellular IoT can become a painful process.

Once an IoT project is underway, it frequently becomes an international endeavour, with products manufactured in one country and then shipped and operated in another, or even many others. This is simply the nature of global supply chains and global customer channels today. Once again, the lack of a plug-and-play model comes into play here: while large MNOs are capable of offering a broad international footprint for cellular connectivity, this footprint is often limited in terms of the number of available roaming partner networks in any given country, while costs for roaming can vary considerably; particularly when devices operate outside of the ‘core’ footprint. In some instances, the supporting MNO will be unable, either due to regulatory or commercial reasons, to offer connectivity in certain countries for devices that roam in foreign networks for long periods of time (usually over 90 days; this is known as permanent roaming). The result of this is that enterprise customers must often establish several contracts with connectivity suppliers in various markets in an effort to optimise costs, performance and support for their IoT devices. In addition to having to manage several connectivity contracts, devices must typically be managed across a number of different Connectivity Management Platforms (CMPs), making it difficult to achieve a holistic view of the device fleet and to consolidate data in an effective manner.

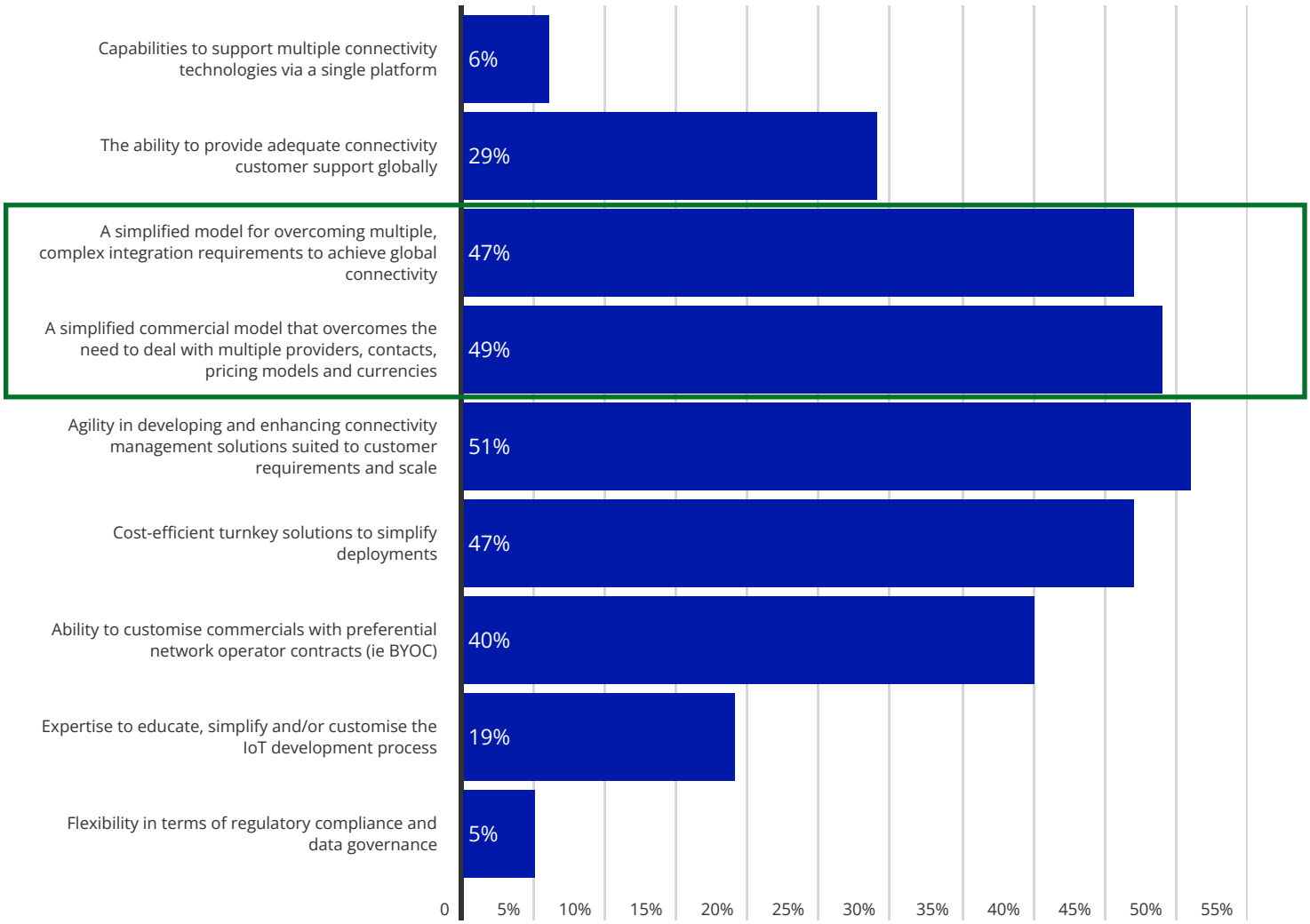
When examining the same theme from the viewpoint of cellular IoT adopters, the situation becomes slightly different. **Interestingly, hardware design complexity no longer factors as one of the main challenges associated with cellular IoT, with only 4% of respondents seeing this as a key factor.** This suggests that hardware design for cellular IoT is a challenge that can be overcome with experience: and underlines the need for service providers to offer hardware consulting services for customers, with a heavy focus on education and guidance for newcomers to cellular IoT. Nevertheless, **a significant proportion of cellular IoT adopter respondents still consider the issue of multiple contractual relationships with connectivity suppliers to be a critical issue, with 56% of the respondent base believing this to be the case.** This is a rather interesting statistic, considering the state of cellular IoT connectivity today. Indeed, while MNOs continue to dominate the number of cellular IoT connections under management today, with 1.8 billion connections at the end of 2021, IoT MVNOs now account for 11% of the market, registering 233 million connections in the same year. Historically, IoT MVNOs have focused on differentiation points such as customer service and flexibility, and as part of this have offered large, global multi-network footprints capable of being managed from a single portal or API interface. This undoubtedly highlights that while there are options on the market to alleviate some of the concerns enterprises have over complex multi-national deployments, efforts to market these differentiation points must be doubled down upon.

What do you perceive to be the main challenges where cellular IoT connectivity is concerned? (Cellular IoT adopter responses)



International cellular IoT complexity comes not only in the form of the potential number of commercial relationships with connectivity providers but also in the form of different commercial regulations and rules around the world. This is evidently observable through the results shown below:

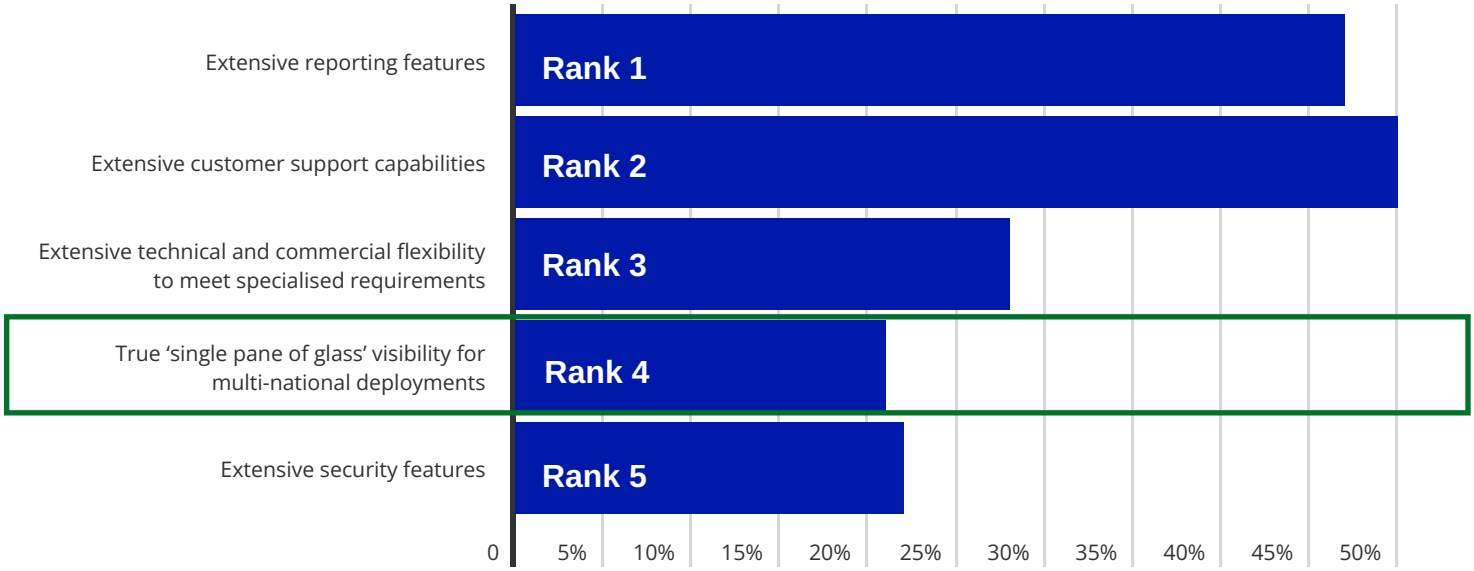
What do you perceive to be the main challenges where cellular IoT connectivity is concerned? (Cellular IoT non-adopter responses)



In the first instance, **49% of cellular IoT non-adopters believe that a simplified commercial model for international IoT connectivity is lacking**, due to the various relationships involved, the different currencies applicable in various countries, as well as the different taxation rules applied. Once again, it is clear that the onus is on service providers to demonstrate that their platforms are capable of circumventing these types of issues, by applying logic in the backend to conform to regulations and offer the customer a consistent billing experience. **Meanwhile, 47% of the same respondents believe that a simplified commercial model to overcome complex integration requirements for global connectivity is lacking.** This is a question of technical capability: as we shall examine in the next section, integrations between service provider partners are fundamental to providing best-in-class service. Moreover, if the service provider has already achieved many of the required integrations, they are able to present their platform under a 'single pane of glass' concept, enabling the customer to integrate once with their platform in order to manage a diverse fleet of devices across multiple countries.

Nevertheless, the very fact that the ‘single pane of glass’ concept has only recently risen as a differentiation point among connectivity service providers highlights that many enterprise customers are still unaware that service providers exist with this type of capability. Its importance is underlined by the fact that cellular IoT adopters view this as the number 4 top priority for cellular IoT:

What are the top 5 factors that you look for in an IoT connectivity partner’s product? (Cellular IoT adopter responses)



Roaming - All Verticals

Kaleido Intelligence

IoT roaming continues to form the basis for cellular IoT connectivity on an international scale. Here, devices that are provisioned with connectivity in one country and then operate in another are allowed to connect to visited mobile networks by virtue of a series of inter-operator agreements and technical processes that facilitate communications and data exchange between the 'home' and the 'visited' operator. Historically, this was achieved using the same agreements and routes as consumer cellular devices, although increasingly, dedicated agreements are being set up at the wholesale level to accommodate the enormous differences in behaviour and data consumption between consumer mobile handsets, which frequently make use of high-bandwidth video, messaging and voice services and connected machines, which vary from simple telemetry and sensing devices to advanced robotics and remotely operated unmanned vehicles that require exceptional Quality-of-Service (QoS) performance.

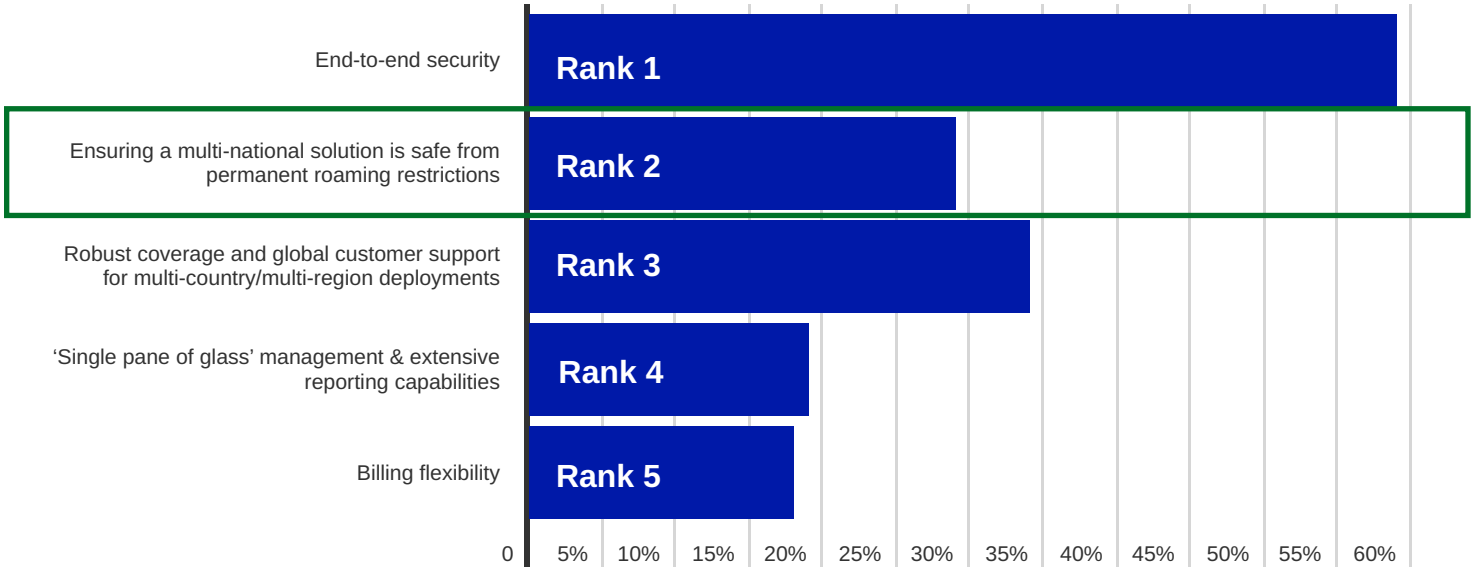
Over the years, the industry has seen an increasing level of concern over the impact of IoT roaming. Traditional roaming agreements were built around the predictability of short-term roaming service usage for tourism or business travel which, as a general rule, results in roaming service provision for a period of fewer than 90 days. The case for IoT roaming is quite different. Not only are data consumption patterns highly variable depending on the deployment type in question, but IoT is almost always a long-term endeavour, with devices in the field for many years. Inevitably, this means that many roaming IoT devices are operating in the visited network for periods well over the 90-day threshold commonly seen in the handset space. This so-called 'permanent roaming' has given rise to perceived issues, such as:

- There is a common perception that, given the high growth in cellular IoT devices, the volume of connections operating in a 'foreign' country may lead to network capacity and performance issues.
- IoT devices frequently consume low levels of data traffic while still consuming a high level of signalling resources. This can create challenges with traditional roaming business models based on traffic consumption and negatively impact the bottom line.
- MNOs have invariably focused on serving their domestic footprint over international enterprise needs. They are thus likely to view the permanent use of foreign SIMs as a threat to their domestic business.
- Regulators in some countries do not take a favourable view towards cross-border data transit for IoT devices. In these cases, permanent roaming clearly presents issues.

The net result is that National Regulatory Authorities (NRAs), as well as MNOs, are, in some instances, taking an increasingly hostile view towards permanent roaming. In several countries, such as Brazil, China, Turkey and Singapore, permanent roaming is prohibited by the regulator. Meanwhile, in countries such as Canada, the US, and Australia, MNOs have actively taken a commercially hostile approach to permanent roaming, limiting the ability of service providers to support permanent roaming.

This issue is clearly of considerable concern for enterprise customers: **after end-to-end security, the ability to ensure that a cellular IoT deployment is safe from permanent roaming restrictions was ranked as a top priority by cellular adopter respondents, who clearly see this as a potential barrier towards expanding the scope of the IoT deployments internationally.**

What are the top 5 factors that you look for in an IoT connectivity partner's product? (Cellular IoT adopter responses)



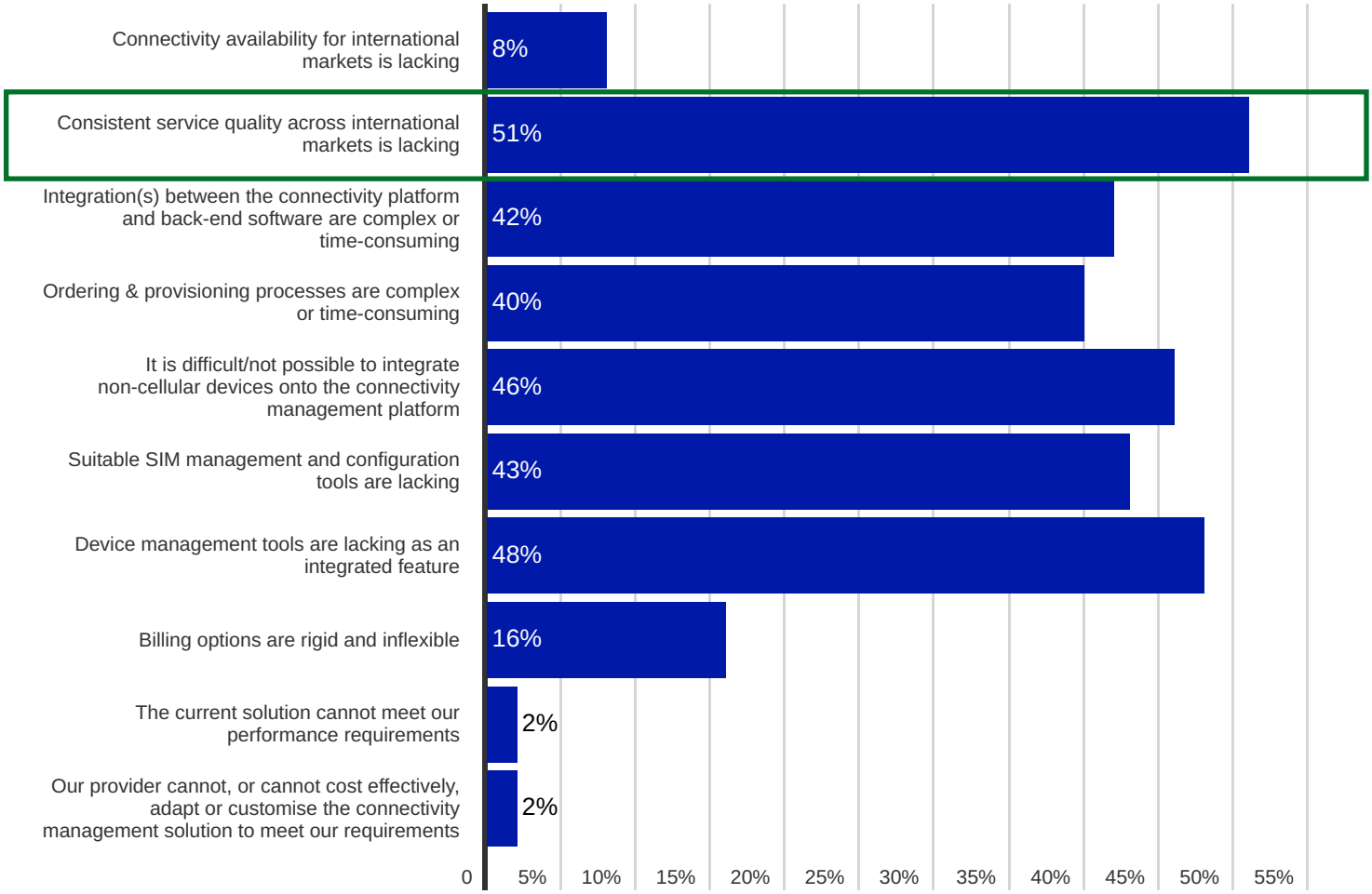
Permanent roaming is equally viewed as a key challenge among non-cellular IoT adopters, with the growing number of countries prohibiting or limiting permanent roaming ranking as the 4th top challenge related to cellular IoT.

Permanent roaming restrictions key for 21% non-cellular IoT adopters

The fact that permanent roaming may be difficult from a commercial or regulatory perspective does not mean that it is impossible for connectivity service providers to support devices in those countries or regions. Indeed, some Connectivity Service Providers (CSPs) have sufficient market power to enable them to reach commercial agreements with other operators around the globe to ensure that devices may roam permanently on their networks. Additionally, there are technical solutions available on the market in the form of eSIM or multi-IMSI SIM cards whereby local operator profiles, International Mobile Subscriber Identity (IMSI) translation, or donated local IMSI ranges can avoid the registration of a foreign IMSI on a network and thus avoid roaming on a technical basis. Today, it is certainly the case that an innovative CSP will apply at least one of these methods alongside traditional roaming capabilities to ensure that regulatory or commercial restrictions can be avoided. As we shall examine in a later section, eSIM is now increasingly deployed as a means to guarantee the longevity of device connectivity availability and is often supplemented alongside some form of multi-IMSI implementation to deliver an optimal customer experience from a cost or performance perspective.

Additional challenges with roaming IoT deployments can arise when it comes to visibility and support of devices. We have already discussed the challenges arising from many enterprises expressing concern over the need to engage with multiple operators; however, those that are able to engage with a single provider to secure connectivity in multiple countries may also see issues in another form. This is exemplified through the survey in that **over 50% of cellular IoT adopters reported that their current IoT connectivity solution was unable to deliver a consistent service quality across international markets.**

What are your biggest issues with your current cellular IoT connectivity solution? (Cellular IoT adopter responses)



One main reason behind this is that the mobile core networks of the home and visited operators are not typically integrated in any fashion. This makes the home operator reliant on the visited operator to ensure that support and performance KPIs are maintained at a high level. Nevertheless, it is almost always the case that the visited operator places a higher priority on serving its domestic customers: after all, the retail value of connectivity revenue is considerably higher than the revenue potential of roaming connections, which are monetised at the wholesale level. This means that obtaining support for roaming IoT devices can be a protracted process, with the visited operator placing a lower emphasis on resolving issues as quickly as possible. Additionally, there may be a number of different touchpoints for customers to engage with before being able to take a step towards problem resolution.

In recent years, several connectivity providers have not only launched their own dedicated core networks for IoT services (thus being able to optimise many aspects of the service delivery, rather than relying on a general-purpose core network suited to mobile handsets), but they have also integrated the core network with those of their roaming partners. This allows for a much greater level of visibility in the context of the device fleet and often enables the home operator to understand and resolve any issues in a much more efficient way than was previously possible. It is thus not surprising to see that **cellular IoT adopters ranked the ability of service providers to offer both robust coverage as well as support for international deployments as number 3 in importance, after end-to-end security and insurance against permanent roaming risks.**

Robust international coverage & support a top 3 concern among 34% cellular IoT adopters

Security - All Verticals

Kaleido Intelligence

Security frequently appears at the top of surveys investigating IoT challenges, and the results in this study are no different. Historically, few IoT devices have been produced with security built-in from the ground up, while countless devices have been shipped with default, easy-to-guess administration passwords, making them highly susceptible to mischievous action by cybercriminals. It is, therefore, of little surprise to see that nearly 60% of cellular IoT adopters ranked end-to-end security as the most important factor where cellular IoT connectivity is concerned.

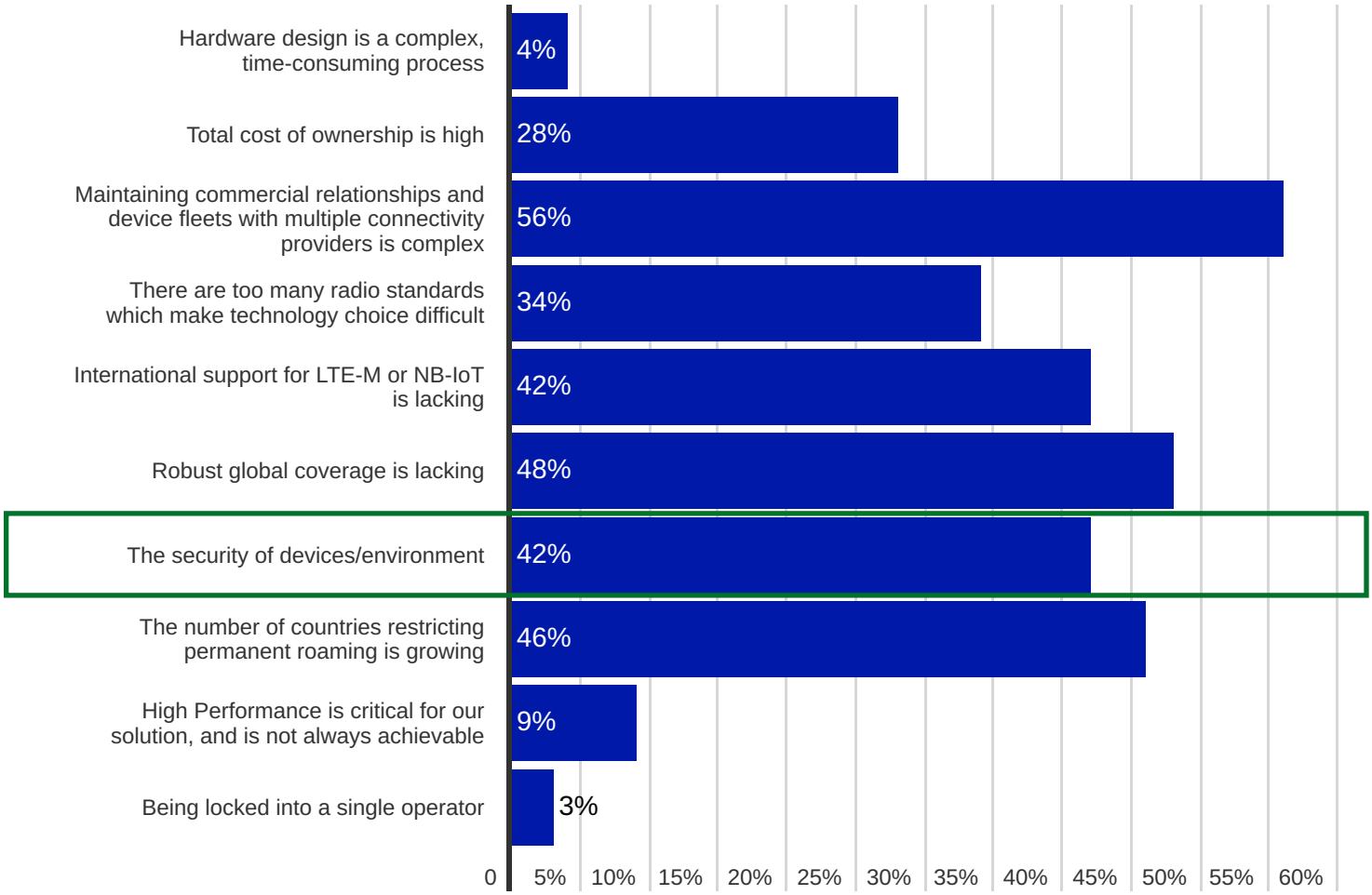
59% cellular IoT adopters ranked end-to-end security as their #1 priority

Cellular technology has the benefit of a robust security framework built-in from the ground up. Unlike other technologies, such as Wi-Fi, authentication on the network is not governed by a secret username and password given to any applicable user but rather a unique mobile identity and secret cryptographic key embedded on the SIM card. This means that authentication is device-based rather than user-based and offers a significant step-up in terms of security strength: it is not trivial to steal SIM authentication keys, owing to the certified, secure production process applied by SIM vendors. Conversely, a username and password that is known to an individual is susceptible to being stolen through social engineering.

More recently, the GSM Association (GSMA) has recognised the need for elevated security for IoT, and in collaboration with a number of industry actors, has developed the IoT SIM Applet For Secure End-2-End Communication (IoT SAFE), which provides a common framework and standardised API to increase security in SIM-based IoT devices. The basis for IoT SAFE is the SIM itself which, in any form factor, serves as a Secure Element to store various secrets. As discussed earlier, the processes which SIM vendors must undertake to deliver certified products to customers means that SIMs are delivered through a highly secure supply chain, making them an ideal piece of hardware for security applications. While IoT SAFE can be leveraged to support a number of security-based applications, a commonly applied use case is to ensure the end-to-end security of communications with cloud-based services. In this context, IoT SAFE is used to mutually authenticate both the device that is sending any data as well as the cloud service that the data is being sent to. The capabilities of cybercriminals to break this chain of custody is dependent not only on finding some form of weakness in the SIM security but also in the cloud service that is being communicated with. This makes it a highly reliable solution for achieving secure end-to-end communications.

In spite of this, **some 42% of cellular IoT adopters believe that the security of devices or the environment is lacking.** It is important to note at this stage that adoption of IoT SAFE remains relatively constrained, with around 10% of CSP customers having adopted it. Nevertheless, a significant number of players were promoting their IoT SAFE implementations at 2022's Mobile World Congress, highlighting that robust security is now being emphasised by innovative players.

What do you perceive to be the main challenges where cellular IoT connectivity is concerned? (Cellular IoT adopter responses)

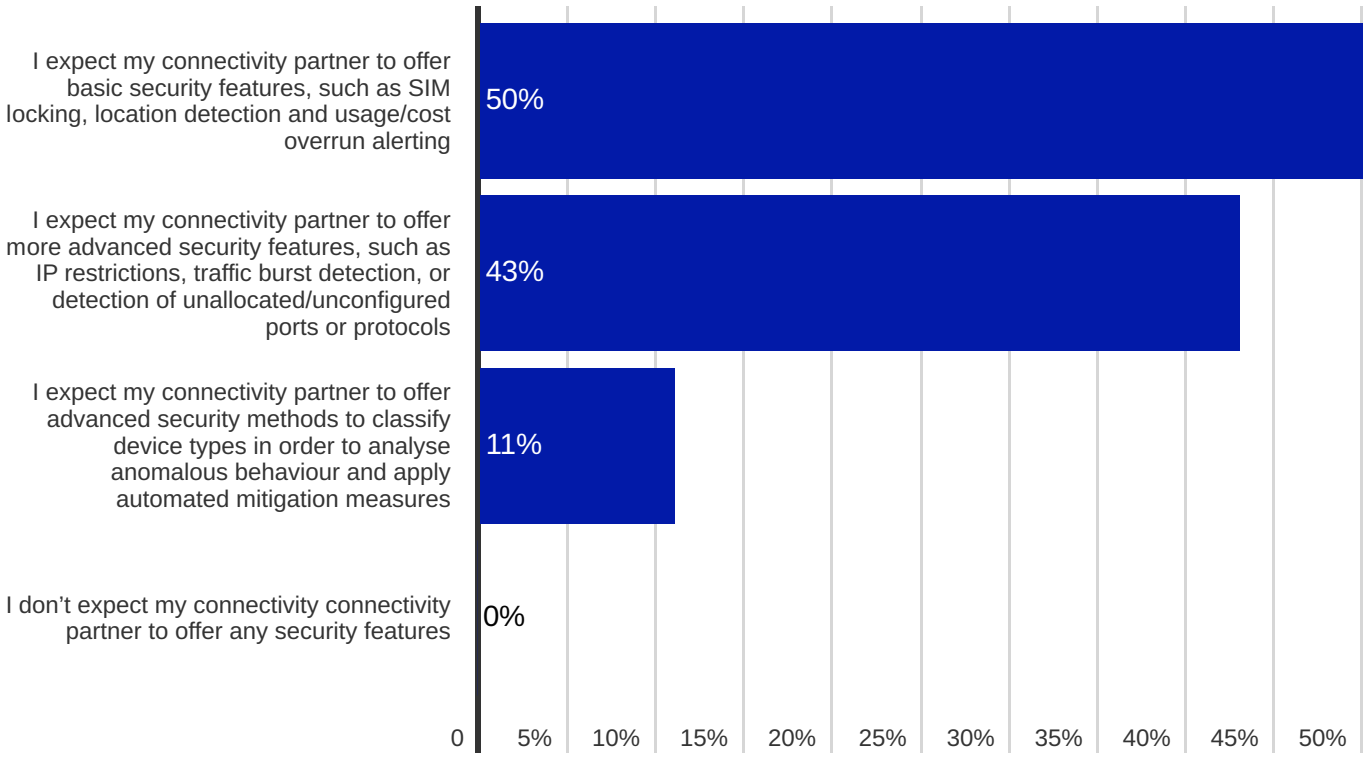


The security of IoT communications and data can be addressed by many actors in the value chain but, undoubtedly, CSPs have an important role to play in this context.

Traditionally, almost all cellular connectivity providers have offered customers the capability to disable SIMs from the network if, for example, the customer is alerted that the International Mobile Equipment Identity (IMEI) has been changed (effectively that the SIM has been moved to another device), or if unexpectedly high data consumption has taken place. The scope of this capability varies, with some providers allowing customers to configure specific automated actions based on events such as IMEI changes or unwanted data attach requests in specific countries. Increasingly, this type of capability has become table stakes, with some connectivity providers aiming to offer a more robust security model for connections under management.

More advanced players are now adding more advanced security features into their connectivity management solutions, allowing customers to detect unusual activity, such as traffic bursts, attempts to use unusual ports or protocols in addition to IP address monitoring alongside more basic features. **50% of cellular IoT adopters believe that connectivity service providers should offer basic security features as described above, with some 43% believing that these providers should offer more advanced features. Interestingly, only 11% of respondents believe that highly advanced security features,** such as device and behavioural classification tools used to identify anomalous behaviour and autonomously take action upon detection are necessary to be supplied by the CSP.

What security features do you expect your cellular IoT connectivity partner to provide? (Cellular IoT adopter responses)



While the data shows clearly that both adopters and non-adopters of cellular IoT are highly concerned with end-to-end security for IoT connectivity, it is apparent that enterprises do not necessarily view the CSP as the provider of the most advanced security features. This is likely due to the fact that CSPs are not traditionally viewed as security experts, and thus the expectation is that a third party will assume the role of the security gatekeeper. Indeed, some CSPs are not establishing partnerships with expert security services providers or moving to acquire or invest in in-house capabilities as a means of offering Value-Added Services (VAS).

eSIM - All Verticals

Kaleido Intelligence

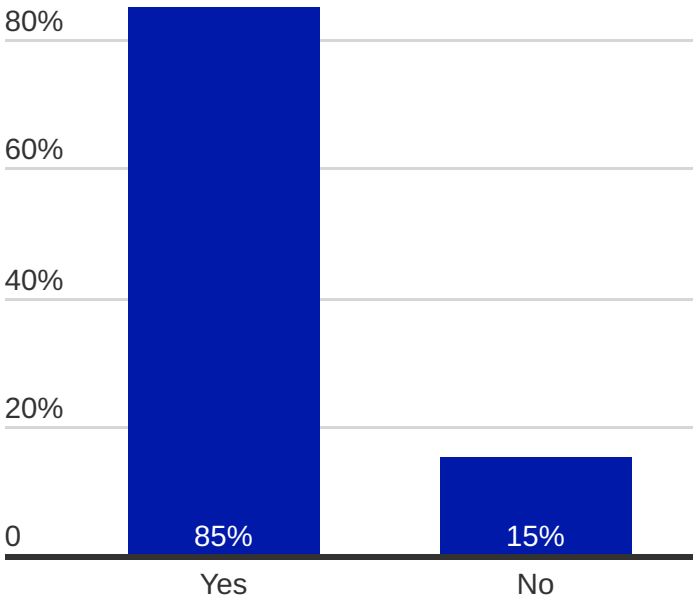
The GSMA's publication of the first interoperable embedded SIM (eSIM) specification in 2016 set the stage for a transformation in how cellular IoT connectivity can be provisioned. eSIM essentially decouples ownership of the SIM card and connectivity from the operator and the enterprise customer in the sense that eSIMs are capable of storing digital operator profiles that are remotely updatable over-the-air (OTA). In simple terms, this means that a single chip can be used as a proxy for any number of SIM cards without the need to physically swap between them, as was traditionally the case. Despite the name suggesting eSIM is only applicable to embedded (soldered) SIM cards, the remote management software architecture can actually be used for eSIMs in any form factor, as long as the SIM card carries an appropriate OS and is linked to a certified Remote SIM Provisioning (RSP) management platform; this makes eSIM a potentially useful tool across any number of IoT use cases and applications.

The business case behind eSIM use for IoT, when eSIM is maximised to its full potential, is overwhelming. The capability to update operator profiles OTA can enable enterprise customers, for example, to avoid the significant costs involved in having to physically swap SIM cards in instances where the commercial relationship with the original connectivity provider breaks down or where regulatory action may prohibit permanent roaming mid-lifecycle. The industry has already observed cases where enterprise customers were told that their devices would no longer be able to access the mobile network due to one of these reasons.

As device volumes in the field grow in number, the cost avoidance capability that eSIM offers becomes significant, often running into millions of dollars of saved expenses.

The fact that **85% of cellular IoT adopters have chosen eSIM as part of their deployment** is thus not surprising.

Have you decided to use eSIM (eUICC) as part of your IoT deployment? (Cellular IoT adopter responses)

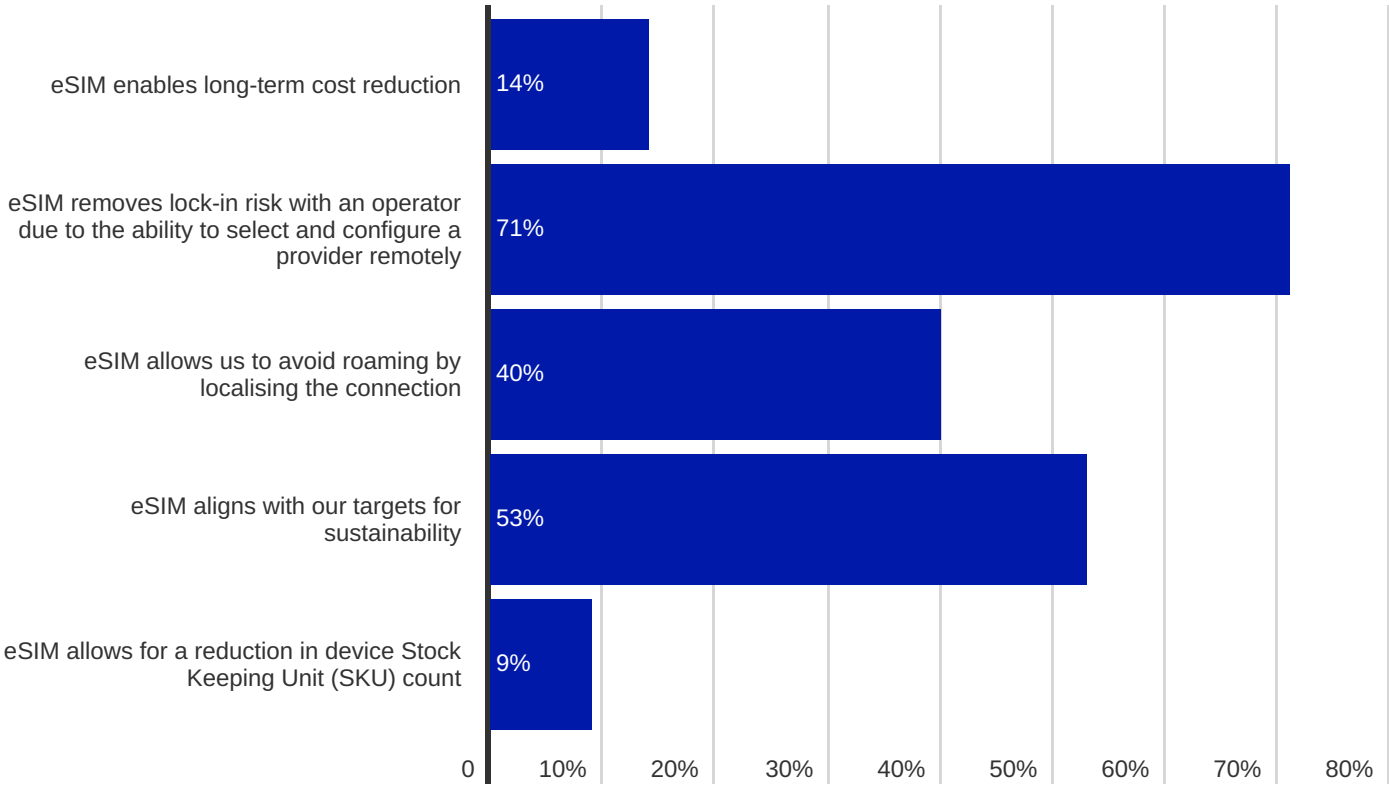


Today's M2M eSIM specification for IoT products incorporates a highly complex and challenging technical architecture, which often introduces legal, business process, and technical hurdles for those wishing to switch operator profiles OTA. The result of this is that IoT eSIMs are predominantly used for insurance purposes; switching operator profiles only in unavoidable situations; rather than using the technology as a means to regularly optimise costs and performance.

Nevertheless, the long-term project viability that eSIM offers means that **71% of eSIM adopters see it as an important tool to avoid the lock-in risks associated with legacy SIM deployments.**

An often-overlooked advantage associated with eSIM is the fact that a single component can potentially replace multiple SIM cards. Not only is this important from a long-term cost perspective, as we have seen earlier, but also from an environmental perspective. As more profiles are associated with and used with an eSIM, the savings in terms of energy use and materials consumption becomes exponentially greater. As sustainability and environmental protection is now increasingly at the top of countries' and organisations' strategic goals, the benefits that eSIM can offer in this context are becoming increasingly important. Here, **53% of eSIM adopters stated that the technology's environmental sustainability was an important factor behind their decision to use eSIM.**

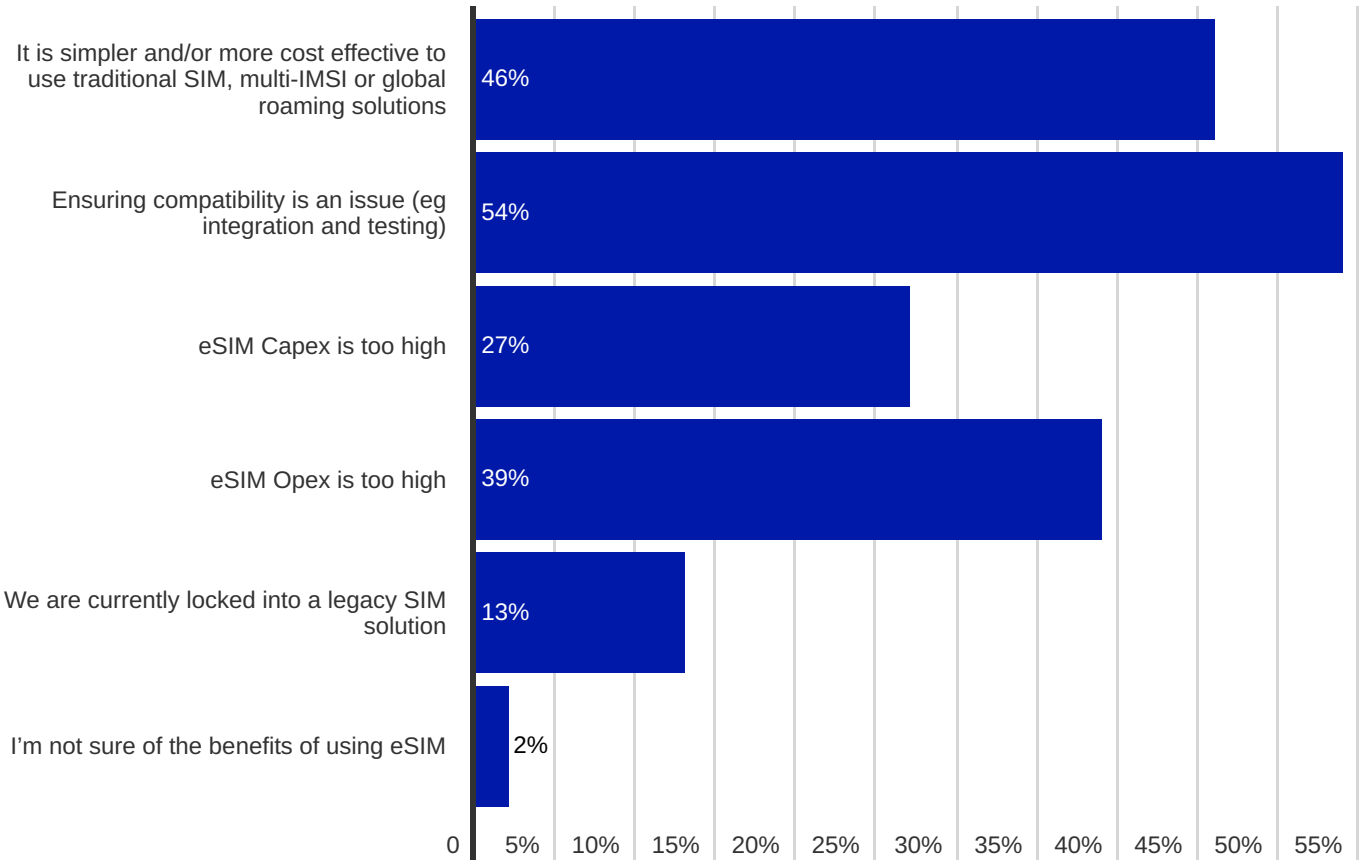
What factors made you choose eSIM (eUICC)? (Cellular IoT adopter responses)



Although eSIM offers great potential in many areas, the ecosystem has not yet fully matured to the point that other connectivity solutions have become irrelevant. As stated earlier, the technical architecture of the M2M eSIM specification creates several barriers that can raise costs and complexity when OTA changes to the operator profile are required. Meanwhile, each OTA operation executed via the RSP platform incurs a charge in order for RSP providers to achieve a return on investment in the eSIM software support environment. As such, it was important to understand why some respondents are not using eSIM, and what sort of challenges are experienced by those using it, in order to identify opportunities to increase adoption and maximise eSIM potential.

Significantly, **54% of eSIM non-adopters stated that integration and testing requirements to ensure compatibility between devices and eSIMs were a key reason not to use the technology, while an important 46% of the respondent base stated that other SIM solutions, such as global roaming SIMs, multi-IMSI technology and traditional SIMs were simpler or more cost-effective to deploy.** It should be understood at this juncture that SIM operating systems and the manner by which they communicate with device components are not fully standardised: indeed, this is rarely the case with low-level interfaces. It is thus imperative that devices are tested before being deployed at scale in the field to ensure that connectivity is maintained when various commands are issued to the device, and that uptime is maintained across various networks and operator profiles in use. This is certainly an area where CSPs can engage with enterprise customers as part of support services to ensure that unexpected headaches are not encountered later when several hundred thousand devices may be in the field.

Why have you chosen not to use eSIM (eUICC)? (Cellular IoT adopter responses)

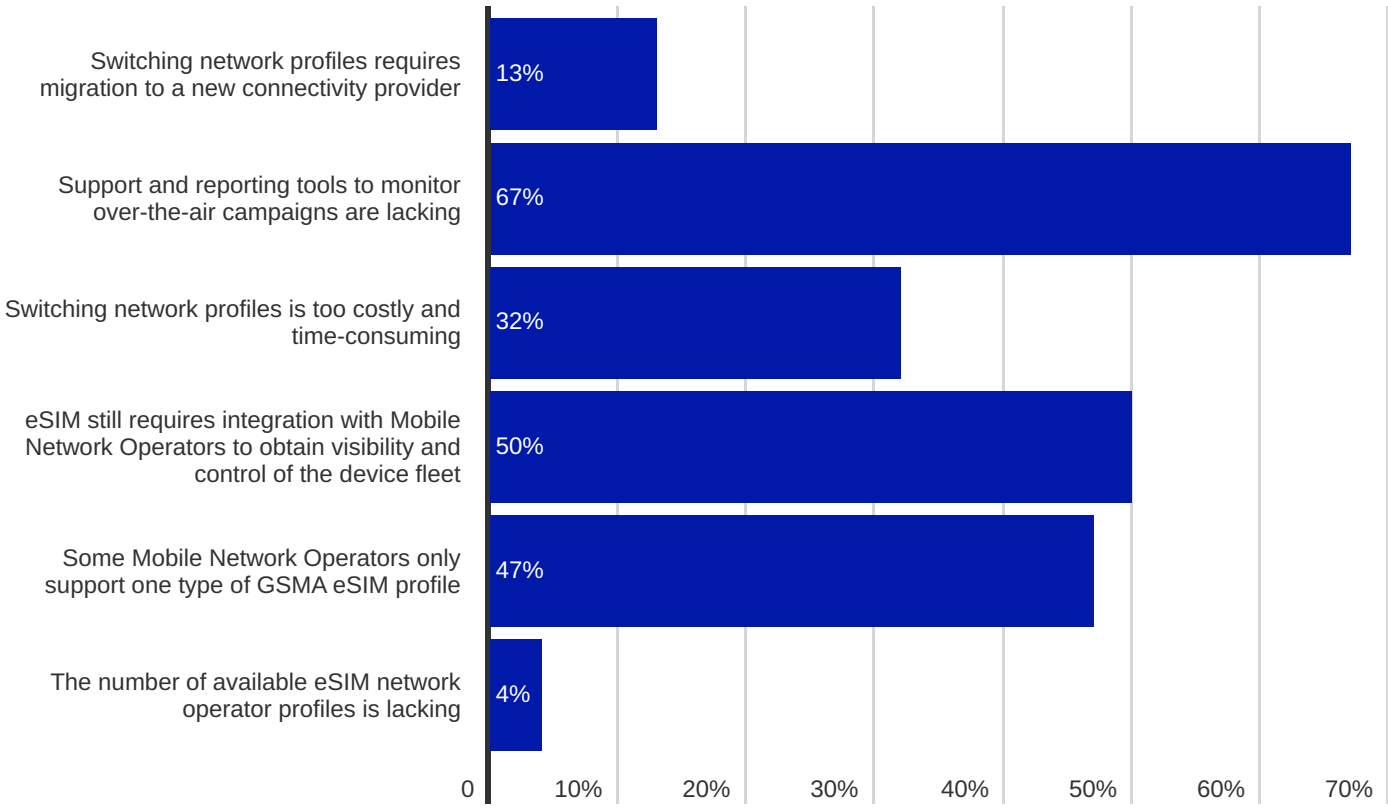


It is interesting to note that 'legacy' SIM solutions remain, in some cases, as a preferred means to enable connectivity over eSIM. Traditional roaming SIM solutions do not offer long-term risk mitigation against the threat permanent roaming issues; they do, however, offer a relatively simple route to market for enterprise customers given the generous roaming footprint offered by many providers, which reduces the need to establish multiple local contracts with operators for deployments that are spread across several countries or regions. However, these solutions are dependent on the the CSP to ensure that long-term inter-operator agreements can be established to enable permanent roaming, but it must be stated that the length of these contracts

does not typically come close to the number of years that IoT devices spend in the field on average.

Several IoT MVNO players now offer a combination of standardised eSIM solutions coupled with multi-IMSI technology. In this context, eSIM OTA capability is normally used as an insurance option to ensure that the customer can switch away from the MVNO, although in many instances, these MVNOs have access to eSIM operator profiles, and are integrated with relevant RSP architectures, to allow customers to localise connectivity for compliance, cost, or performance reasons while maintaining device visibility via the same, original MVNO's CMP. Presently, this offers a highly flexible solution that allows customers to optimise connectivity based on costs or performance using multi-IMSI in the first instance (and avoiding the OTA costs involved with operator profile switching), with eSIM OTA functionality called upon for specific use cases. This operational strategy is partly reflected in the results, which highlight the main issues that eSIM adopters have with their solution: **32% of respondents feel that switching eSIM network profiles is too costly and time-consuming.**

What are your main issues with your current eSIM (eUICC) solution? (Cellular IoT adopter responses)



The results above highlight that there are other areas where the industry can improve however, and this is likely to become even more important as the eSIM specification is developed. **67% of respondents felt that support and reporting tools to monitor OTA campaigns are lacking with their current solution**, indicating that visibility in terms of campaign successes, failures and retry attempts is not being delivered to the level that is expected. **Readers will recall that 'single pane of glass' management and reporting was among the top 5 requirements for cellular IoT customers**

and underlines the need to provide a high level of transparency over fleet activities to the customer. As stated earlier, this will only become more important in the future: the GSMA is in the process of developing its IoT specification for eSIM, which is aimed at greatly simplifying the technical and legal barriers to operator profile switching. If it succeeds in this endeavour, it is likely that more enterprise customers will wish to use eSIM to optimise their device fleet via OTA switching, which will make transparency and reporting increasingly important. This is especially the case for devices using radio technologies such as LTE-M and NB-IoT, where devices frequently enter sleep or power-saving modes and thus will often not be immediately reachable by any management platform.

iBASIS
POWERED BY TOFANE

BE THERE FIRST

REACT MOBILE + iBASIS

IoT Connectivity Powering Reach to Panic Buttons Around the Globe

REACT mobile

React Mobile is a global leader in providing panic button solutions for hotels utilizing an open and flexible platform enabling management to deploy response resources to the exact location of an emergency within seconds of an alert.

They required a mature, proven global IoT connectivity solution with global reach and extensive operator relationships to ensure the automatic selection of optimal connectivity to support panic devices throughout all areas of large facilities including hotels, convention centers, hospitals and schools.

iBASIS IoT eSIM solution enables dynamic selection of mobile communications carriers in the cloud to achieve the strongest signal to reach its devices anywhere on or off property.

RESULTS

- With over 50,000 panic buttons deployed, the solution is powering global reach to enhance employee safety around the world
- iBASIS eSIM dynamic carrier selection offers the most effective device connectivity to remotely monitor and manage devices
- React Mobile is now able to offer a standalone LTE version of its panic button that no longer needs a smartphone to connect to the cellular network.
- React devices leverage integrated iBASIS eSIMs and Nordic Semiconductors for easy implementation and automatic connectivity through a single provider
- Seamless integration of pre-activated SIM cards into devices and leveraging of pooled data to ensure that SIM cards stay active and do not require 'refills' or maintenance
- Flexibility to transition between carriers and bands ensures robust fallbacks with ready access to migrate to an alternate network without intervention or configuration
- Easy-to-use platform for tools, testing, and internal support

> "We needed a truly global partner with a mature service offering and dynamic capabilities to select carriers for the best reach everywhere our devices are deployed. iBASIS offers unification through one provider with access to superior networks and seamless entry to all global markets.
>
> The knowledge that Nordic Semiconductor selected iBASIS as the single global connectivity provider to be included in all their cellular modem development kits, and that iBASIS is actively testing LTE-M connectivity around the world, gave us complete confidence to select iBASIS as our global connectivity supplier."

Riley Eller
CTO, React Mobile

ABOUT iBASIS

iBASIS is the leading communications solutions provider enabling operators and digital players worldwide to perform and transform. Powered by Tofane Global, the new iBASIS is the first independent communications specialist, ranking third largest global wholesale voice operator and Top 3 LTE IPX vendor with 660+ LTE destinations. With the integration of Tofane's acquisition of the Altice Europe N.V. international voice carrier business in France, Portugal, and the Dominican Republic, iBASIS today serves 1,000+ customers across 18 offices worldwide.

iBASIS provides the end-to-end Global Access for Things™ connectivity solution, delivering single source cellular IoT access (LTE, LTE-M, and NB-IoT) worldwide provisioned through GSMA-standard eSIM/eUICC technology. The solution simplifies IoT device connection through one unified platform for seamless, remote, programmable, and secure communication. For more information, please visit www.iBASIS.com.

CORPORATE HEADQUARTERS

10 Maguire Road, Building 3
Lexington, MA 02421

T +1 781 430 7500
F +1 781 430 7300
E info@iBASIS.net

iBASIS.COM

Truphone connects MachineMax's entire fleet in moments

MACHINEMAX

"With the support of Truphone, we are confident we can continue our rapid global expansion whilst providing seamless global connectivity."

Amit Rai, CEO, MachineMax

The company produces sensors designed specifically for off-highway heavy equipment—tractors, dumper trucks, excavators, diggers of any brand and any model—and ships them globally. Its customers use the sensors to track their machines and receive efficiency, productivity and fuel-cost insights to help them maximise profitability and reduce emissions.

But while MachineMax could offer revolutionary wireless telematics to its customers, it didn't have a way to simplify connectivity for their vehicle fleets.

That was, until it partnered with Truphone.

How eSIM has changed the Machine Max offer

Truphone's commitment to eSIM (embedded SIM) technology has given MachineMax a huge competitive advantage, and its customers a simple solution for getting their off-highway vehicles connected.

By implementing Truphone's state-of-the-art eSIM technology in its devices—and thanks to Truphone's network which supports 2G, 3G, 4G and CAT-M1/LTE-M networks worldwide—MachineMax is now able to offer connectivity straight out of the box, wherever in the world the device is deployed.

TRUPHONE

What's more, every eSIM profile in customers' fleets can now be updated and connected remotely and at scale from the Truphone for Things platform. Users have the ability to deploy and manage connectivity for thousands of devices via a simple-yet-powerful interface, at their fingertips.

MachineMax's connected-device offer provides the company's customers with complete confidence that their fleet of devices can be tracked, 24/7, no matter the site size or manufacturer.

But it also provides MachineMax's CEO, Amit Rai, with belief. "With the support of Truphone, we are confident we can continue our rapid global expansion whilst providing seamless global connectivity."

A one-stop shop for IoT connectivity

Truphone for Things joins together previously fragmented elements of the Internet of Things (IoT) ecosystem to provide a **'one-stop shop' for IoT connectivity.**

The company's global mobile network is leveraged to connect devices anywhere—via a range of low-and high-power networks—and full control is provided via an easy-to-use management platform.

So it's little wonder new partnerships such as the one with MachineMax are forming continually as manufacturers seek to unlock the potential of the Internet of Things for their customers.

TRUPHONE

Private LTE/5G - All Verticals

Kaleido Intelligence

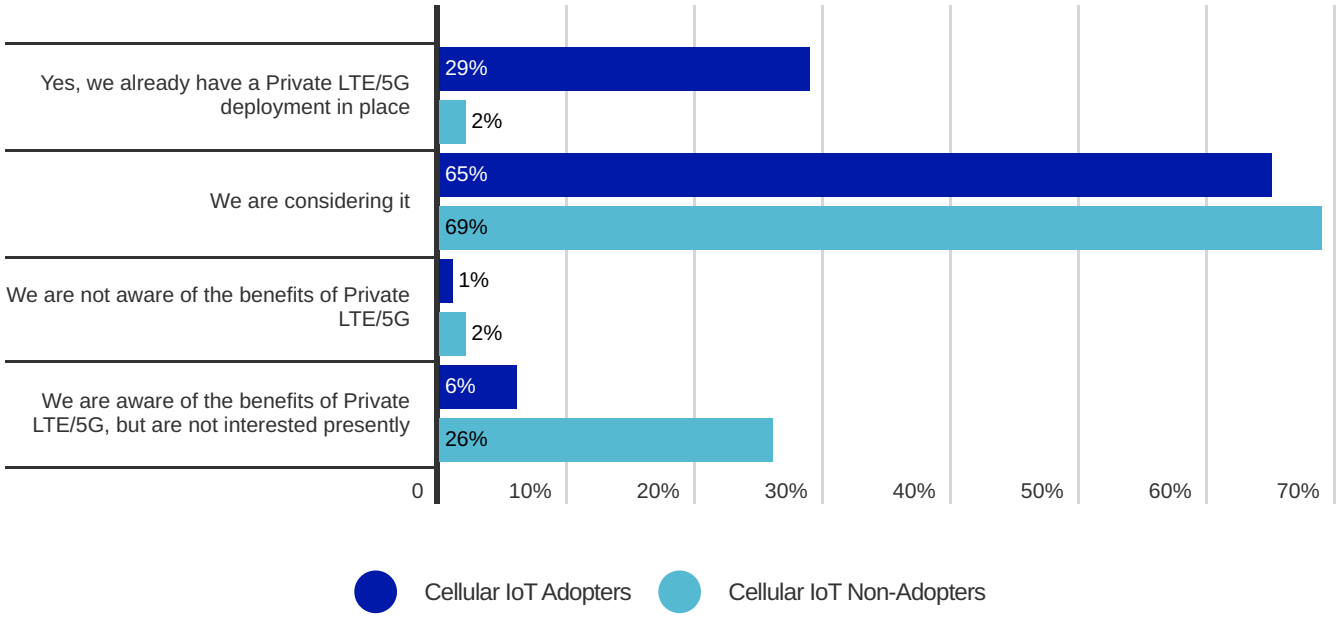
Today, most enterprises around the world make use of some form of private network, whether that is supported by Wi-Fi, Ethernet or even TETRA. While these technologies have been invaluable in supporting business objectives, they are frequently hampered by compromises such as unreliability, high costs, or a lack of available bandwidth to support more advanced applications.

In recent years, the use of cellular technology to support private networks has come to the forefront of discussions. In part, this is due to the fact that LTE or 5G are, in many instances, able to match or exceed the performance and reliability provided by expensive wired communications technologies, while benefitting from the flexibility of Wi-Fi. Additionally, regulators across several countries in the world have assigned dedicated spectrum ranges to support Private LTE or 5G and opened processes to allow enterprises to access this spectrum either directly, or through a third-party. The benefits of using LTE or 5G for a private network are numerous, and as such present a powerful business case:

- Cellular technology offers significant coverage improvement over Wi-Fi, while its use of dedicated spectrum minimises the impact of interference, which Wi-Fi frequently suffers from.
- Gigabit speeds can be achieved with cellular technology, which at least matches the performance of Ethernet. Meanwhile, this throughput is possible without the need to install miles of expensive cable, while the physical network design can be altered without having to move and reinstall a substantial amount of cabling.
- The capability to address a multitude of applications and scenarios, ranging from national private networks to smaller campus areas, while supporting a range of QoS requirements, including ultra-low latency applications and high connection density.
- The significant security upgrade in terms of device authentication over Wi-Fi user authentication, as discussed earlier.

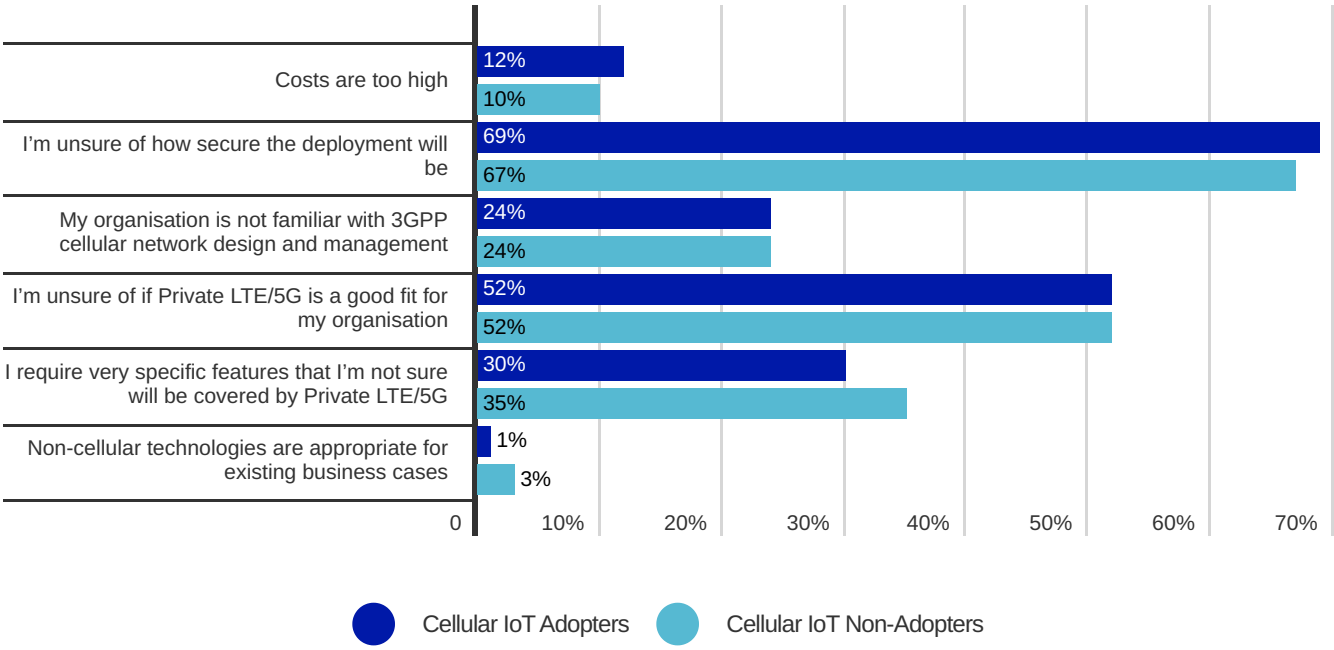
These factors have undoubtedly generated significant interest in private LTE or 5G: **among non-adopters of cellular IoT, 69% of respondents reported they were considering using the technology, while 65% of cellular IoT adopters reported the same.** Thus, it is evident that industry actors have succeeded in generating interest in private cellular network solutions across a very broad range of enterprise players. Overall adoption remains at a relatively low level, however: **some 29% of cellular IoT adopters have a private LTE or 5G deployment in place, while 2% of cellular IoT non-adopters have a solution in place.** Evidently, this latter tranche of enterprises are using private LTE or 5G to connect workers rather than assets and thus do not consider their deployment as IoT.

Does your business unit have an interest in Private LTE/5G to enhance business operations? (All responses)



Across the spectrum of cellular IoT adopters and non-adopters, enterprises remain unsure of the security of private LTE or 5G, with 69% of the former group reporting concerns over security, compared with 67% of the latter group. This is a very revealing result, particularly when considering that one of the benefits of any private network is the security of communications from outside sources and highlights a lack of understanding of the private LTE and 5G ecosystem as a whole. It is important to note that private cellular networks can be architected to conform to different levels of security requirements, in addition to different levels of flexibility and cost entry points.

What are your main concerns over a potential Private LTE/5G deployment? (All responses)



For the most part, this is dependent on where the mobile core network and radio components are located:

- Traditional private LTE deployments saw all network components located on-site, resulting in a fully isolated network with no data egress. This type of architecture is generally expensive, and limits the growth of the market to enterprises with high entry capital.
- More recently, private cellular networks have been offered using a hybrid architecture, with radio components on-site but with core network software off-site in virtualised environments. This moves some of the spend to operational, as-a-service costs, thus lowering the barrier to entry for enterprises. Security here is dependent on service providers' capability to separate user plane data (data generated by devices) from control plane data (signalling messages used to manage the network and control authentication and billing), with control plane data being sent to the virtualised core, and user plane data kept inside the enterprise private network site.
- In some cases, where the private network is to be deployed nationally, such as might be the case for utilities companies or transportation use cases, the public mobile network radio might be used. In 5G, this is possible by logically separating a portion of radio resource into a slice, which is dedicated to an enterprise customer. Typically, a virtualised core network will be used to support control plane functions as described above.

These deployment architectures are not simple for enterprises to understand, given that, in all likelihood, they are not familiar with 3GPP cellular technology nuances. Indeed, the corporate IT department is likely to be most familiar with Wi-Fi or Ethernet, which is not only deployed in a different manner, but also managed in a different way. It is certainly the case that at this stage of private LTE or 5G market maturity, enterprises must receive considerable guidance in how they might leverage and deploy a private cellular network.

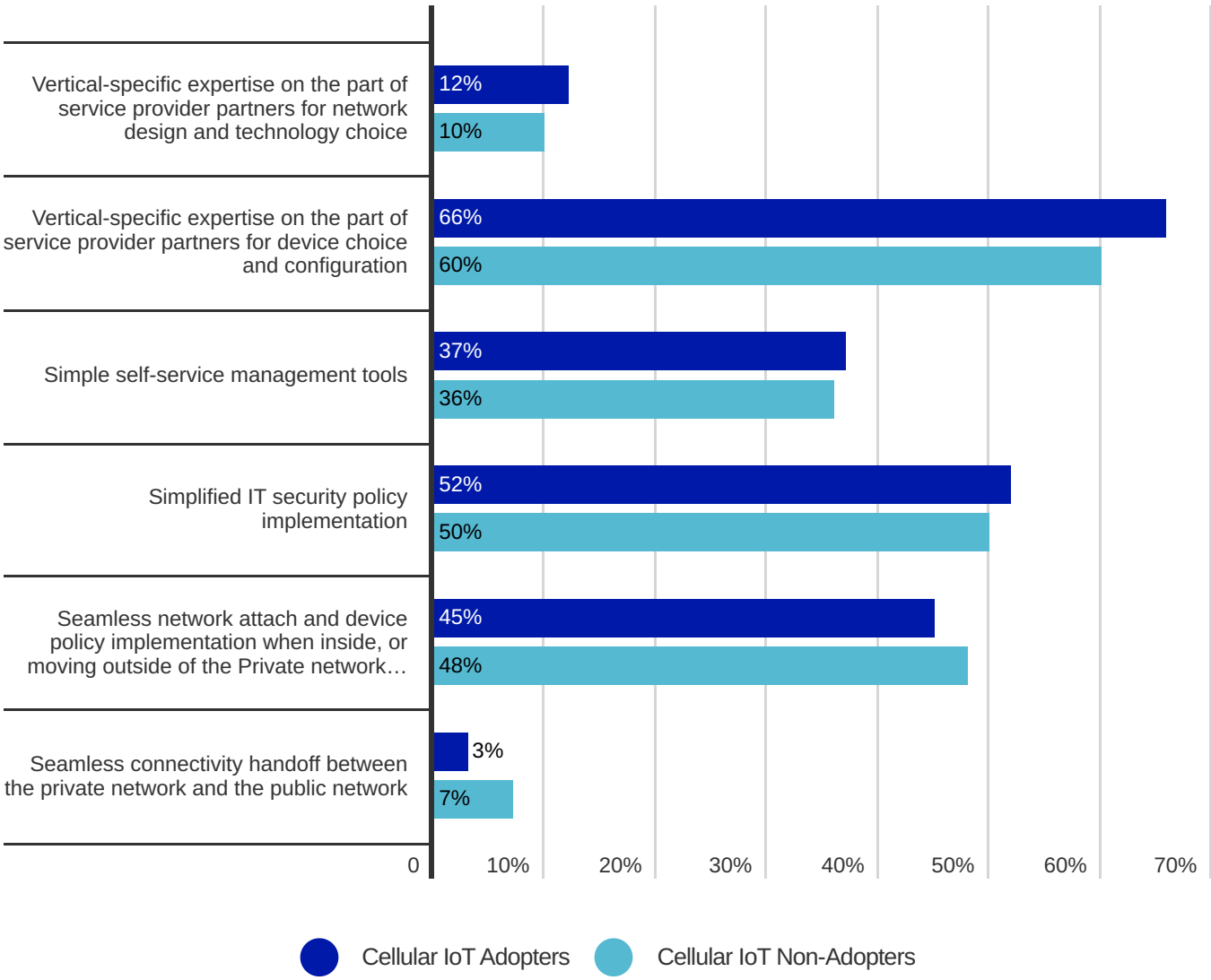
This is further underlined by the fact that **among cellular IoT adopters as well as cellular IoT non-adopters, 52% of respondents reported that they were unsure if private LTE or 5G would be a good fit for their organisations, while 35% and 30% respectively reported being unsure if a private cellular network solution is capable of addressing specific features for the enterprise strategy.**

Further evidence that enterprises require a significant level of expertise in the private LTE or 5G journey can be found in the survey results showing that 60% of cellular IoT non-adopters and 66% of cellular IoT adopters believe that they require vertical-specific expertise to help them choose devices and configure them. This speaks back to results that were examined earlier in the context of hardware design complexity, which is evidently an area of unfamiliarity on the part of all types of potential enterprise IoT clients. It is a well-known fact that Operations Technology (OT) and IT convergence has posed significant challenges to enterprises owing to the fact that OT systems have typically been isolated from IT systems, with the meshing of the two giving rise to concerns over security as well as uptime. Meanwhile, OT device development and management has historically taken a different path to IT systems development, which creates additional challenges in terms of harmonisation. This is particularly impactful in the private cellular network space, due to the unfamiliarity with 3GPP network design and

protocols, and suggests that hardware and development expertise is even more critical to address enterprise concerns.

It is evident from the results that significant concerns also lie in other areas. **52% of cellular IoT adopters believe a simplified IT security policy implementation is required, while 50% of cellular IoT non-adopters believe the same. Meanwhile, 45% of the former group raised concerns over network attach and policy implementation when crossing between private and public networks, closely matched by 48% of respondents in the latter group.** These results highlight that, in the first instance, maintaining security is a critical perceived challenge by all groups of enterprises, while on the other hand, many enterprises recognise the need to ensure connectivity continuity for assets and workers that traverse between private and public network coverage areas. This latter use case is likely to become highly important in verticals such as manufacturing, in addition to transportation, owing to the movement of people and assets to various private network sites around the world, while support, tracking and maintenance requirements will undoubtedly drive the need to ensure that objects can connect to public and private networks, wherever in the world they are.

What are the most important factors for consideration where Private LTE/5G is concerned? (All responses)

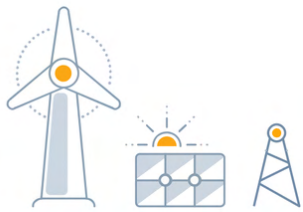


PRIVATE NETWORKS FOR UTILITY COMPANIES

WHAT MATTERS TO THEM

Smart Meters

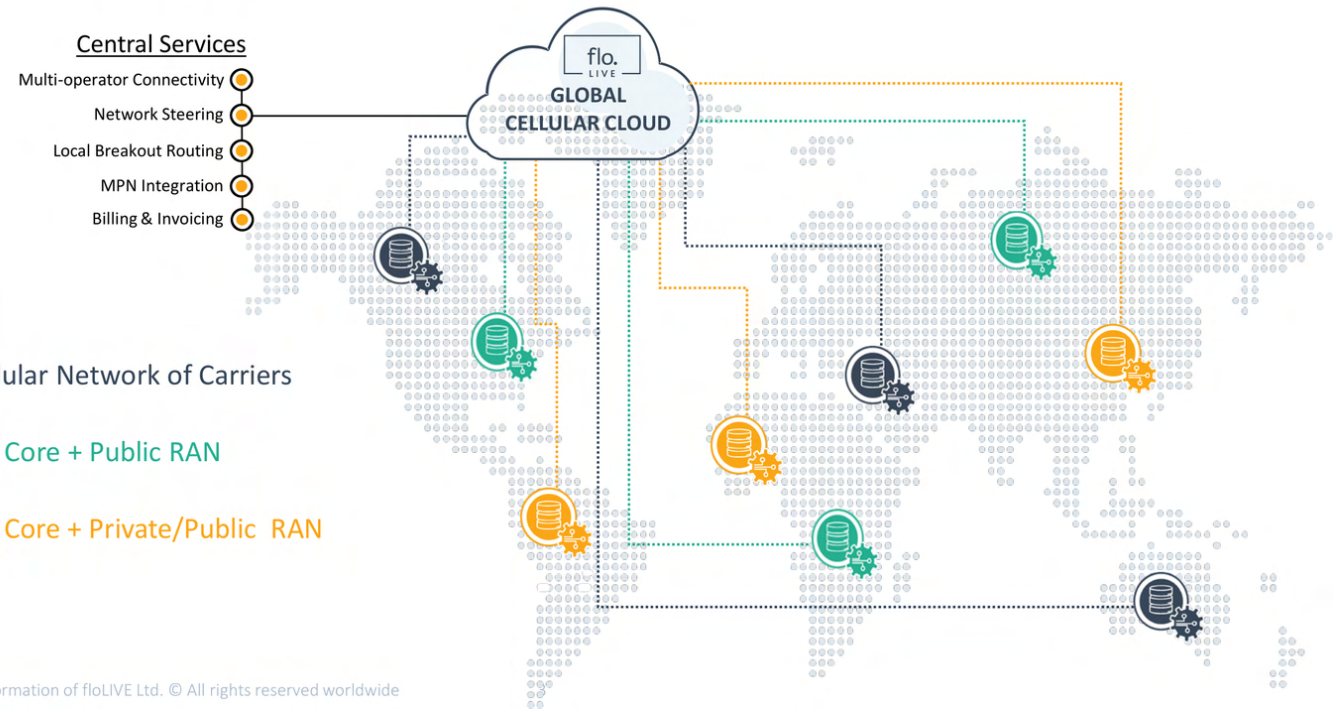
- Private Core
- Utilizing the carriers' public RAN
- Tight Integration into their IT environment
- Multi-carrier (multi-IMSI) with automatic steering



Operational/Technical Fleet

- Private Core
- Deploy their own private RAN
- Tight Integration into their IT environment
- Autonomous Failover to the public network

OUR GLOBAL CELLULAR CLOUD



The Concept

- Global Cellular Network of Carriers
- Private 5G Core + Public RAN
- Private 5G Core + Private/Public RAN

IoT Connectivity Challenges & Opportunities: Transport / Logistics

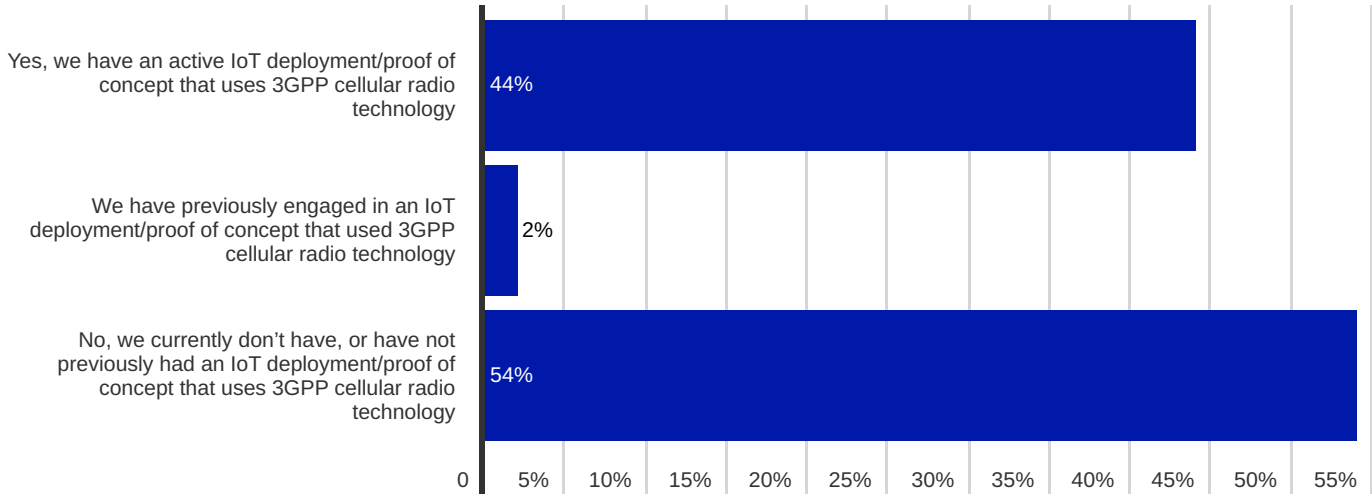
eseye iBASIS KORE TRUPHONE flo. LIVE

State of IoT - Transport/Logistics

Kaleido Intelligence

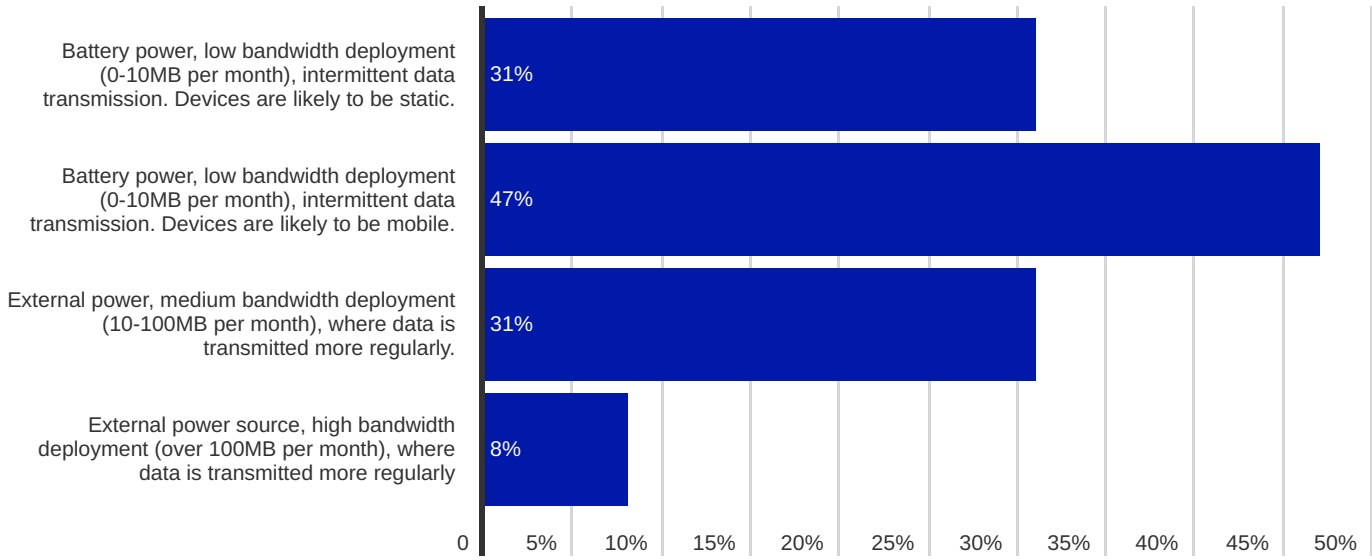
The survey results show that this particular vertical is relatively well-engaged with cellular IoT, with **46% of respondents either having a current or previous cellular IoT deployment. 54% of the respondent base reported that they had never deployed cellular IoT; of those respondents, 41% intend to deploy the technology for their IoT strategy within the next 12-24 months.**

Does your business unit currently have an IoT deployment or proof-of-concept underway that uses 3GPP cellular radio technology (2G/3G/LTE/5G)? (All responses)



41% intend to deploy cellular IoT in the next 12-24 months

What type of cellular IoT deployment is this likely to be? (Cellular IoT non-adopter responses)

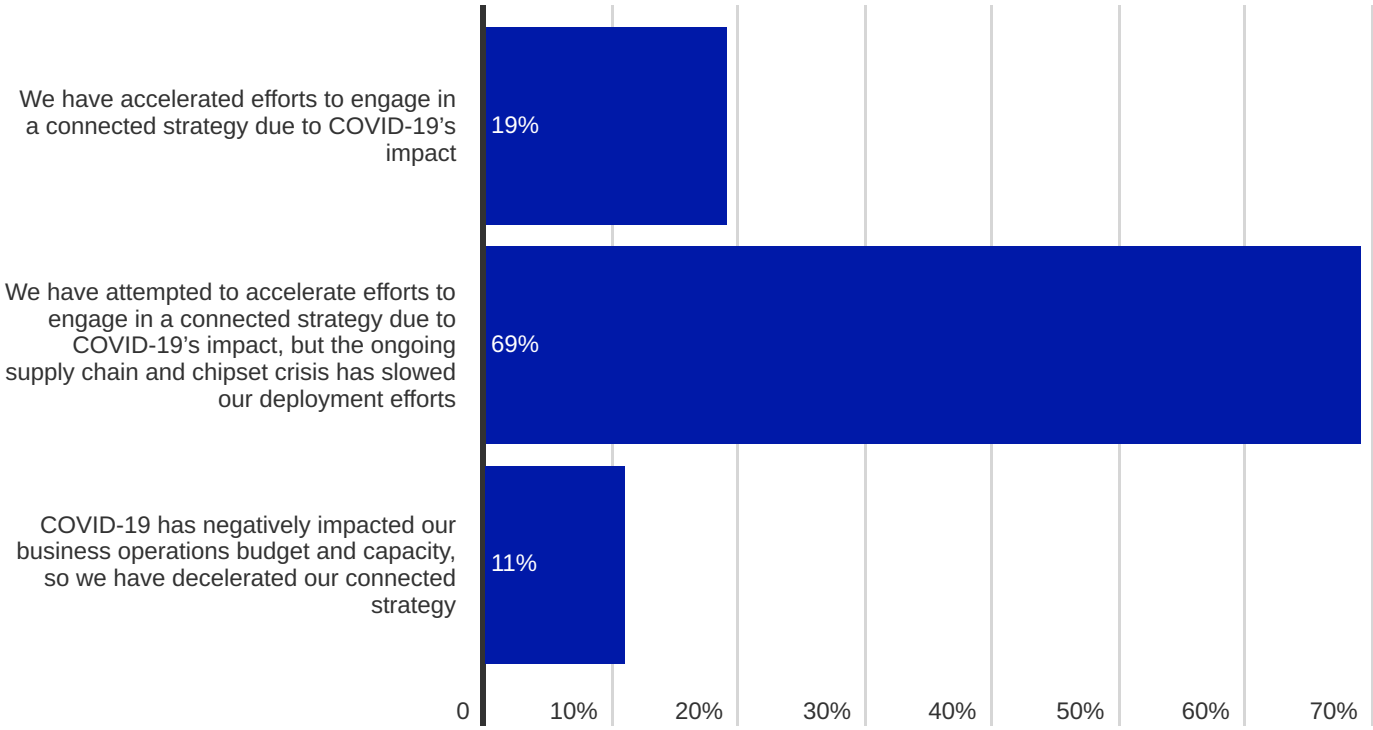


eseye iBASIS KORE TRUPHONE flo. LIVE

Some **78% of those intending to deploy cellular IoT in the near future stated that they would likely use some form of low bandwidth, battery-based connectivity.** This allows us to infer that the majority of deployments will involve either LTE-M, NB-IoT or, in a potentially smaller number of cases, LTE Cat1/Cat1bis. In the majority of cases, these technologies will be used for monitoring and telemetry purposes, with the intermittent data transmission desired likely pointing to simple state monitoring devices. It is likely that the impact of COVID-19 has increased demand for these types of applications, owing to a greater need to monitor goods along logistics supply chains, the desire to track assets globally in addition to a desire to monitor various static and mobile objects for maintenance purposes.

Only **39% of respondents stated a desire to deploy IoT devices using more regular data transmission with higher bandwidth requirements and a need for an external power source.** This suggests that while the desire to increase vehicle telematics and infotainment applications remains relatively strong, a higher emphasis is now being placed on monitoring assets that are transported by vehicles rather than the vehicles themselves, which can supply an ongoing power source.

How has COVID-19 impacted your organisation's IoT strategy? (Cellular IoT non-adopter responses)



It is interesting to note that this vertical has been most heavily impacted by COVID-19 out of all of the verticals that were analysed in this particular study: some **69% of respondents stated that supply chain constraints and chipset component availability had impacted their ability to roll out IoT solutions.** This may partly explain the lower level of demand for higher bandwidth devices, on account of the fact that devices with high-end requirements, such as larger memory, screen interfaces, and so on, have seen a heavy impact as a result of the ongoing chipset crisis.

Complexity - Transport/Logistics

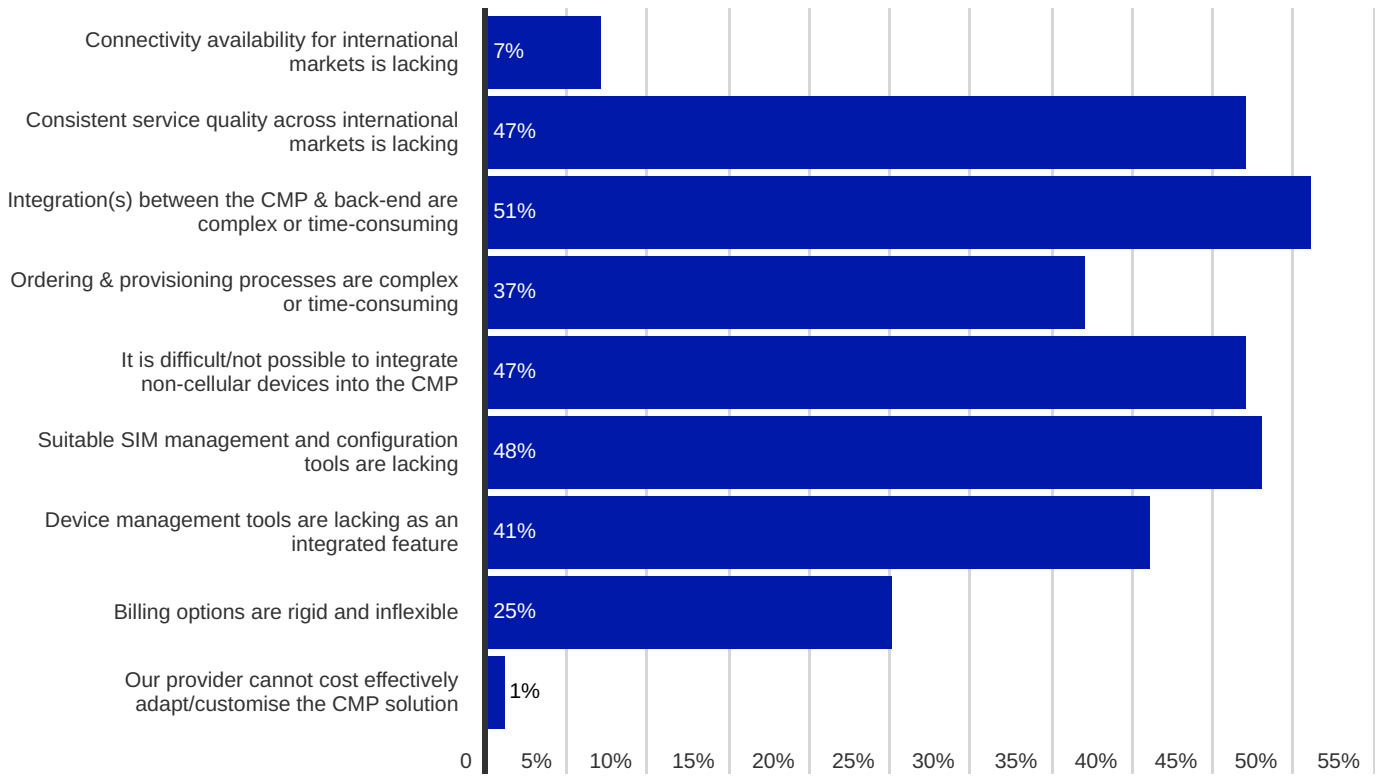
Kaleido Intelligence

For the transportation and logistics industry, being able to offer a consistent experience is paramount. This is especially true for automotive applications, where OEMs have a strong desire to harmonise vehicle features and services no matter where the vehicle is sold. This desire is highlighted by the fact that **72% of cellular IoT non-adopters stated that the need for CSPs to have an extensive network of mobile operator partners for their connectivity footprint was their top priority in terms of a CSP's capabilities, while 56% of the same respondent base reported that the ability to provide extensive customer support was the number two priority in the context of a connectivity partner's product.** Being able to cater to these requirements will result in a high level of uptime while additionally minimising the number of disparate relationships required for customers have to deliver their products worldwide. As we have seen earlier, this is a critical factor across the enterprise landscape as a means of reducing complexity for global IoT solutions.

Extensive MNO partnerships are a #1 priority for 72% cellular IoT non-adopters

Extensive customer support is a #2 priority for 56% cellular IoT non-adopters

What are your biggest issues with your current cellular IoT connectivity solution? (Cellular IoT adopter responses)



eseye iBASIS KORE TRUPHONE flo. LIVE

Nevertheless, there is evidently a perception that the issues described above have not yet been solved. **51% of cellular IoT adopters in this vertical stated that maintaining multiple connectivity relationships with providers continues to be a significant challenge, while 51% of the same respondent base reported that integrations between the connectivity platform and back-end software are complex or time-consuming**.

Undoubtedly, the majority of these challenges could be solved in instances where a single provider is capable of delivering a highly robust global footprint alongside a substantial number of integrations with connectivity partners' core network architectures. Minimising the pain points: contractual relationships in addition to the amount of time required to integrate CMPs with back-end software is clearly highly valued by customers within this vertical.

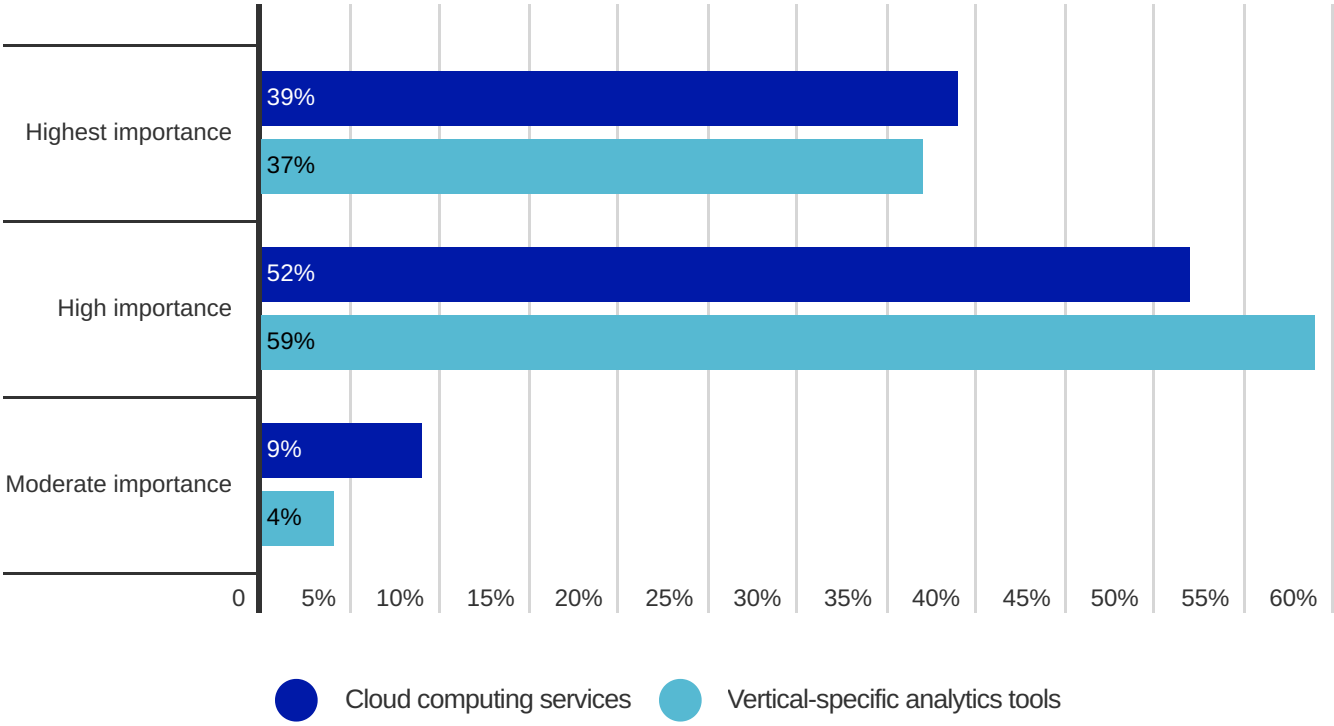
Further opportunities for reducing complexity lie within the relationship between device, and device connectivity. **47% of cellular IoT non-adopters stated that it is important for a connectivity provider to offer a consolidated hardware and connectivity offering, while 41% of cellular IoT adopters reported that suitable device management tools as a feature integrated with the connectivity solution were lacking**. This speaks to the need to more closely intertwine device and connectivity management, with the latter offering capabilities such as device software and firmware updates, and non-SIM monitoring capabilities. The fact is that in the transportation space, the ability to launch new products and services OTA has largely been lacking from the industry, with this capability only having emerged in recent years. The ability for connectivity service providers to bundle this type of offering alongside the connectivity service would once again allow the enterprise customer to reduce the number of support touchpoints required to develop their IoT solution, and offer a point of differentiation. In addition to this, the ability to bring hardware expertise to the table alongside connectivity is an important factor, given the testing involved when launching an IoT product, and the inevitable in-field support requirements involved when deploying at scale.

47% cellular IoT non-adopters rank hardware & connectivity bundles as #2 priority

41% cellular IoT adopters wish to see device management tools integrated into the connectivity management solution

The survey also highlights that transport and logistics customers place a high emphasis on 'out-of-the-box' integration of cloud services and vertical analysis tools. **91% of cellular IoT adopters stated that they wished to see connectivity providers offering cloud services integration as a high priority, while an even greater 96% of respondents stated the same for vertical-specific analytics tools.**

How important is it that your cellular connectivity solution provider offers integration with the following tools/services out-of-the-box? (Cellular IoT adopter responses)



The results emphasise the fact that CSPs must quickly establish partnerships in the ecosystem to deliver a broad number of inbuilt services for customers within this vertical, which are evidently anxious to generate value from their deployments with as minimum fuss as possible.

Roaming - Transport/Logistics

Kaleido Intelligence

The globally distributed nature of the transportation and logistics industry makes roaming for cellular IoT inevitable. This raises understandable concerns in the context or permanent roaming where, although assets are often mobile in nature, they frequently operate in various countries for long periods of time. It is thus not surprising to see that **27% of cellular IoT adopters view permanent roaming and the ability to minimise risk against it as the number two priority for cellular IoT connectivity; meanwhile 36% of cellular IoT non-adopters view this as the second-highest priority item where cellular IoT connectivity is concerned.**

27% cellular IoT adopters & 36% non-adopters ranked the ability to minimise permanent roaming risks as their #2 priority

With the transportation and logistics segment having driven a substantial proportion of the overall cellular IoT connection base, it is important to understand that deployments at scale are ongoing. As such, the risks of devices losing the ability to attach to mobile networks around the world are substantial, and could result in a significant cost penalty to enterprises that encounter commercial or regulatory challenges to devices that are permanently roaming. It is therefore imperative that connectivity partners have measures in place to guard against these risks, either in the form of inter-operator agreements that allow connections to roam permanently, or through technical solutions such as eSIM or access to local IMSI ranges that enable devices to localise the connection and avoid roaming altogether. Given the fact that **cellular IoT non-adopters ranked CSP coverage in countries with permanent roaming restrictions as rank number 5 in terms of connectivity partner capability priorities** it is evident that while guarding against risk is important, the ability to offer technical solutions against it is of greater importance than agreements at the commercial level. This is likely an issue of long-term risk mitigation, rather than settling for short- to mid-term connectivity availability, and is especially important given the long lifecycle (over 10 years) of devices used in automotive and transportation applications.

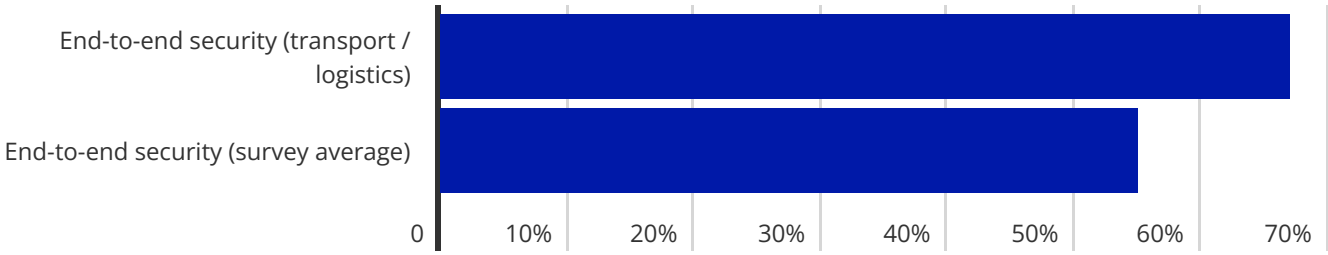
26% cellular IoT non-adopters stated that a CSP must have coverage in countries with permanent roaming restrictions as a top 5 priority

Security - Transport/Logistics

Kaleido Intelligence

In parallel with all other verticals, **end-to-end security was the top priority for transport and logistics enterprises that have not yet adopted cellular IoT. Interestingly, this vertical achieved the highest proportion of votes for this element in the top rank, with 67% of the respondent base selecting it, compared to 55% on average.**

What are your top 5 factors that are most important where IoT connectivity is concerned? (Rank 1, cellular IoT non-adopter responses)



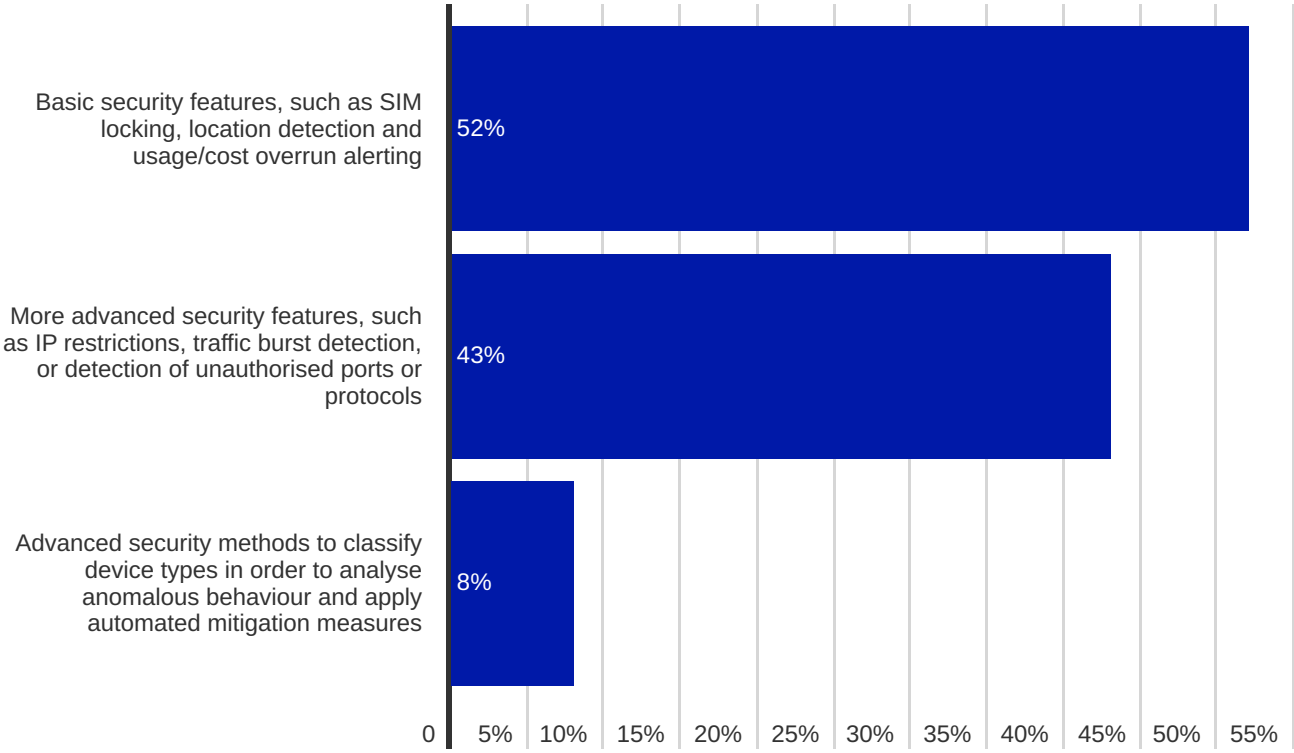
This result underlines the fact that data security is a fundamental aspect for consideration where transport and logistics applications are concerned. In many instances, highly sensitive data may be involved requiring protection from confidentiality breaches, while in other instances, the data transmitted may be related to the very safety of the application itself.

This latter observation is evident across the automotive and transportation industry, where regulation and a desire to offer differentiated connected features are resulting in an increased number of safety-related features, such as cabin monitoring, road hazard detection, lane departure warning systems, in addition to monitoring roadside or railroad assets. The disruption or manipulation of the data chain of custody in this context can potentially lead to accidents that may harm public safety, or cause issues with insurance claims where connectivity is used to support insurance applications.

Despite this need for high security, only 8% of cellular IoT adopters in this segment stated that they expected their connectivity provider to offer highly advanced security features, such as automated device classification and behavioural monitoring tools while those who had not adopted cellular IoT ranked the need for the connectivity partner to provide extensive security features as rank 5 out of their top 5 priorities for a partner's product.

CSPs able to offer extensive security features is a top 5 priority for 17% cellular IoT non-adopters

What security features do you expect your cellular IoT connectivity partner to provide? (Cellular IoT adopter responses)



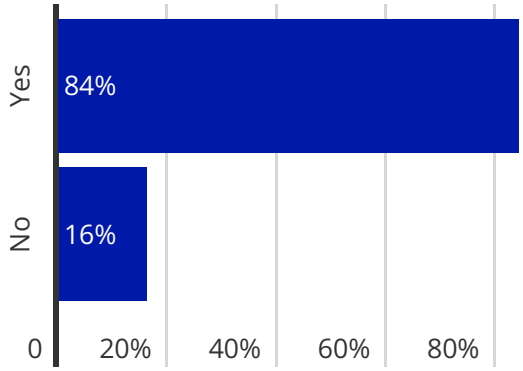
From the results shown above, it should be understood that the majority of transport and logistics enterprises expect to rely on third-party expertise for their security monitoring solutions, with the connectivity partner expected, for the most part, to offer basic to mid-level security features to enhance the security of the connectivity itself. This is understandable, given the very high emphasis placed on the need for end-to-end security, in that customers are willing to forgo some of the simplification associated with out-of-the-box security solutions in order to ensure a best-in-class service is selected for their deployments.

eSIM - Transport/Logistics

Kaleido Intelligence

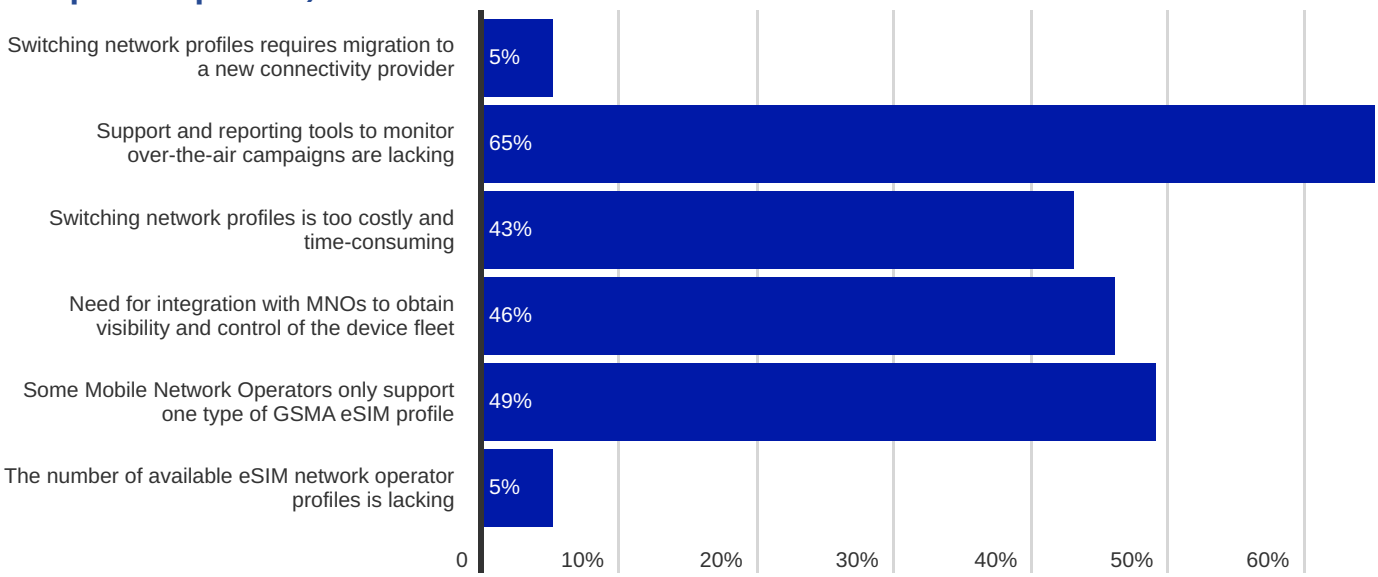
With the automotive segment in part responsible for the development of the original interoperable eSIM specification, it is not surprising to see that **84% of cellular IoT adopters stated that they are using the technology for their IoT deployments.**

Have you decided to use eSIM (eUICC) as part of your IoT deployment? (Cellular IoT adopter responses)



The ability to offer a consistent customer service experience across global deployments is a fundamental aspect of automotive OEM success, with eSIM offering a technical solution to enable that and de-risk long-term IoT deployments. Furthermore, emergency calling (eCall) regulations; particularly in the EU; have led to the de facto use of eSIM in an attempt to ensure that, in the event of a traffic accident, the vehicle can connect to emergency services to report the incident no matter if it is in the original connectivity partner's coverage footprint or not. Nevertheless, this vertical was notable in the fact that **43% of eSIM adopters stated that network operator profile switching was too costly and time-consuming** and refers here to the technically and commercially complex M2M specification in common use for transportation applications. It is often an enormous challenge to ensure that eSIM profiles are downloaded and activated away from the original network profile at scale, and is one of the reasons why network profile switching has rarely been observed in this vertical. This presents a clear opportunity for IoT MVNOs that have extensively tested their eSIM connectivity solution and capabilities, but also have secured partnerships with a broad number of MNOs to use their digital profiles.

What are your main issues with your current eSIM (eUICC) solution? (Cellular IoT adopter responses)



In addition to the above, transport and logistics enterprises were significantly concerned with the type of eSIM profiles available at their disposal. Presently, eSIM profiles conform to one of two specifications: one developed for M2M applications, with another for consumer-orientated applications. With many connected services, such as infotainment and navigation, in the transportation segment delivered via the vehicle's head unit in addition to services that monitor and report on metrics related to the vehicle or asset itself in the headless domain (ie without any user interface), relatively high demand for a mixture of eSIM profile types has arisen in this segment in order to cater for the diversity of applications in use. However, the survey results highlight that **49% of transportation and logistics customers have observed a lack of compatibility on the part of the connectivity provider with both profile types**, which has the net result of the customer being forced to seek disparate connectivity relationships with partners in order to service applications in their fleet that require a mix of eSIM profile types.

With the latest IoT eSIM specification likely to be delivered as an extension of the existing consumer eSIM specification, with support for remote management of IoT eSIM requirements, the ecosystem is on the way to resolving some of the issues described above. Nevertheless, development of the specification is not expected to be completed until the end of this year, while commercial rollouts and support are only likely to gather traction several months beyond that. Additionally, the transportation segment is infamous for long lead times in product development, meaning that demand for 'legacy' consumer and M2M eSIM profile types is likely to continue for at least 2 years. It is thus important for CSPs to take this into consideration in the context of their future eSIM support strategy, and may present an opportunity for innovative IoT connectivity service providers to capture market share from MNOs, which may be more risk-averse to eSIM in general in the first instance, while also reluctant to cater to specific market niches.

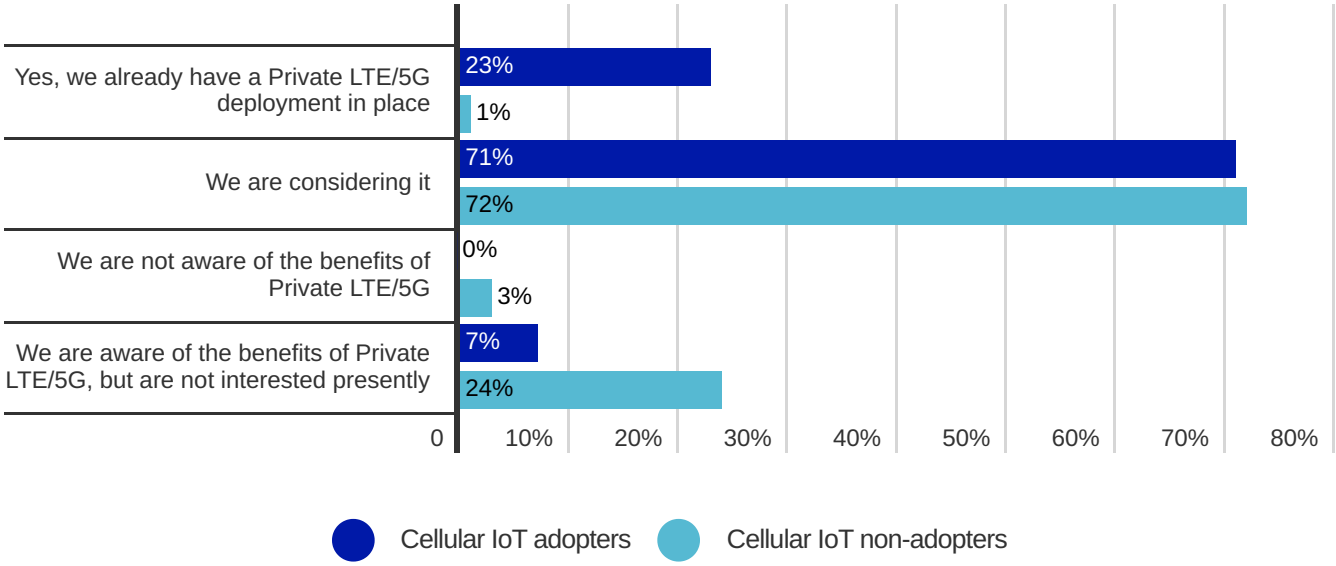
49% of cellular IoT adopters observed a lack of support for both consumer & M2M eSIM profile types

Private LTE/5G - Transport/Logistics

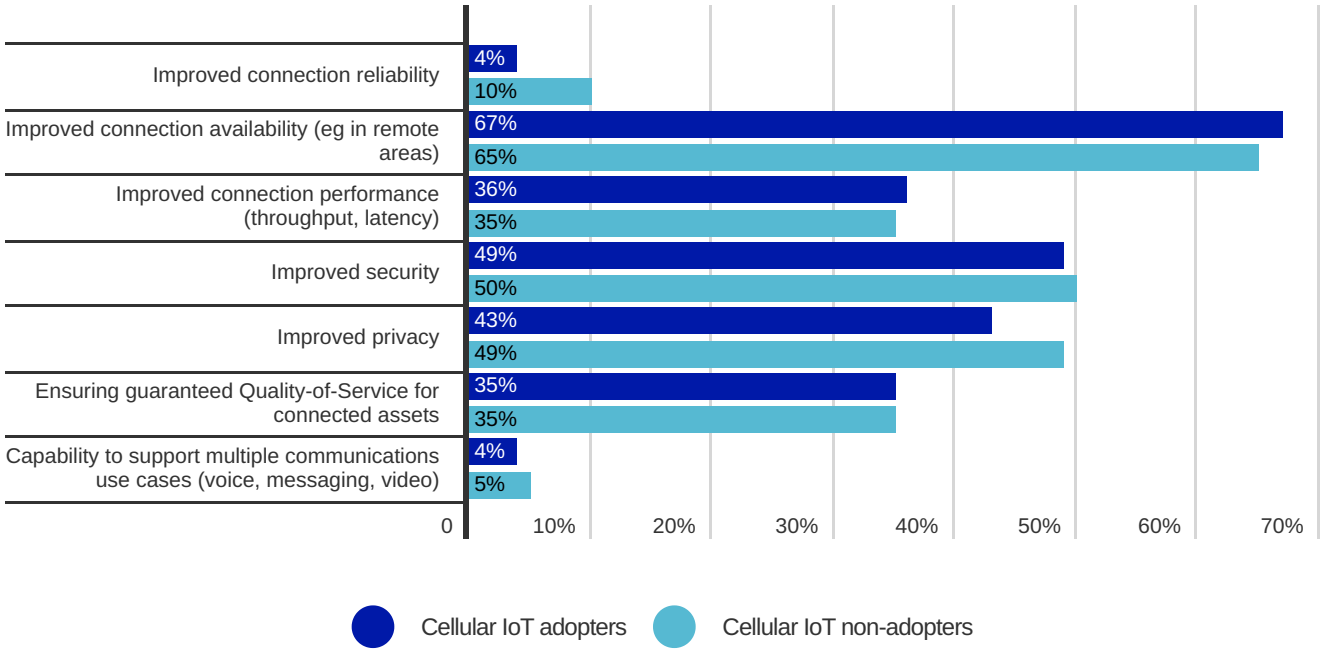
Kaleido Intelligence

The transportation and logistics segment can be counted as one of the early adopters of private LTE solutions, with transport hubs and warehouses in particular suited to dedicated, reliable connectivity for operations. It is therefore not surprising to see that **71% of cellular IoT adopters are considering either private LTE or 5G to enhance business operations, compared with the survey average of 65%; meanwhile, 72% of cellular IoT non-adopters are also considering a private network deployment using LTE or 5G technology.**

Does your business unit have an interest in Private LTE/5G to enhance business operations? (All respondents)



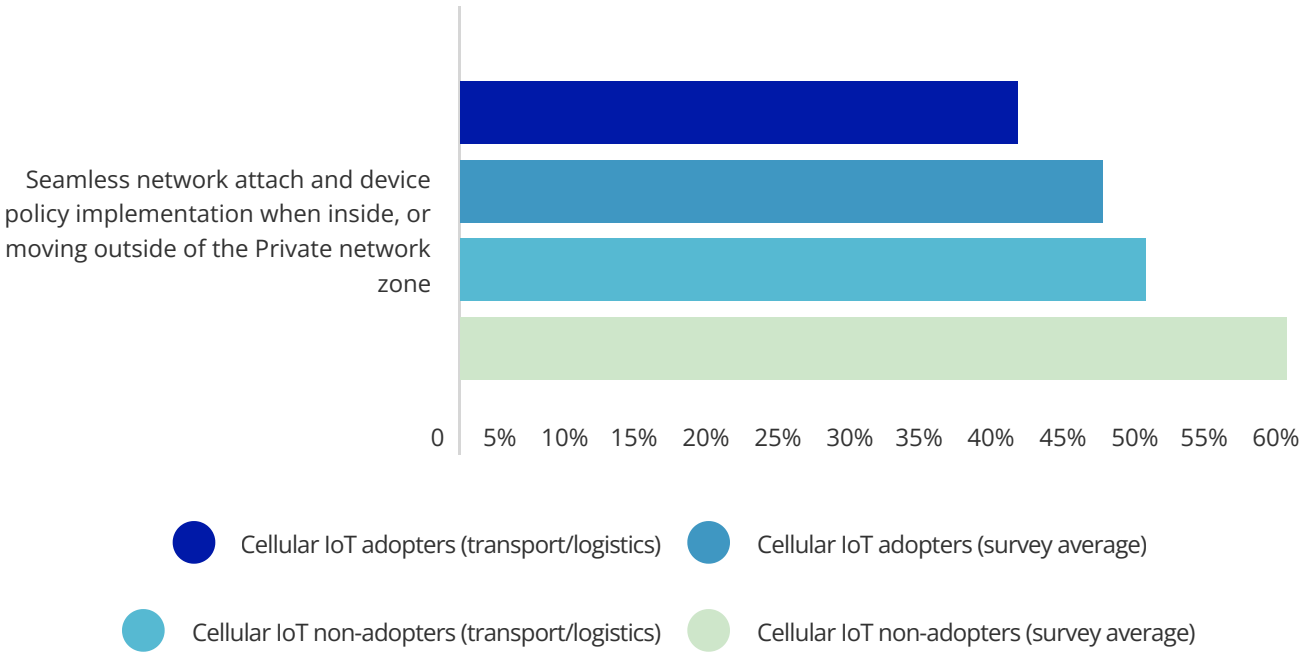
What do you perceive to be the main benefits of a Private LTE/5G solution? (All respondents)



Wi-Fi has typically been deployed by enterprises in this segment to deliver connectivity for workers and assets, although a common complaint is that Wi-Fi coverage and QoS have not been as reliable as was desired. This is one of the drivers, for example, for airports to upgrade to LTE or 5G radio technology, and is supported by the fact that **65% and 67% of cellular IoT non-adopters and adopters respectively stated that the main benefit to private LTE or 5G was improved connectivity availability**. It is certainly the case that Wi-Fi requires significant effort to achieve a broad coverage footprint, while the fact that it operates in unlicenced frequency bands makes it highly susceptible to interference which may, in turn, lead to connection dropouts.

It is interesting to note that there is a disparity in perceived requirements for private LTE and 5G where cellular IoT adopters and non-adopters are concerned. **Seamless network attach capabilities and policy implementation when assets or workers 'roam' between private and public networks was viewed as above average importance by cellular IoT non-adopters (58% of transportation and logistics enterprises vs. 48% of the overall survey base). However, when cellular IoT adopters were asked the same question, only 38% of respondents viewed this as important, vs. 45% of the overall survey base.** While it is clear that, in general, fewer cellular IoT adopters are concerned with this capability, it is important to note an increased divergence from the average among cellular IoT non-adopters, which may indicate an opportunity for CSPs to promote 'roam in, roam out' capabilities as part of their private LTE or 5G offering. Nevertheless, it is important to note that the disparities between cellular IoT adopters and cellular IoT non-adopters are reversed when considering IT security policy implementation: 64% of IoT adopters view this as an important factor vs. only 41% of non-adopters. Evidently, this points to a mismatch in understanding of cellular IoT challenges in the private network domain and leads to the assumption that, in line with comments earlier, enterprises require considerable guidance in the context of choosing private LTE or 5G deployment types and connectivity requirements.

What are the most important factors for consideration where Private LTE/5G is concerned? (All respondents)



IoT Connectivity Challenges & Opportunities: Energy / Utilities

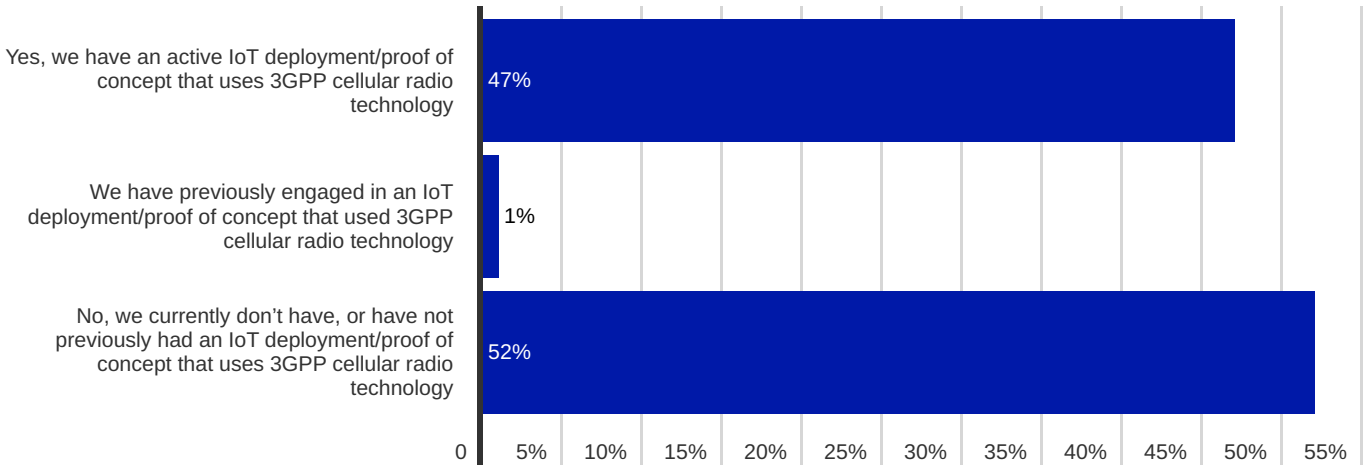
eseye iBASIS KORE TRUPHONE flo. LIVE

State of IoT - Energy/Utilities

Kaleido Intelligence

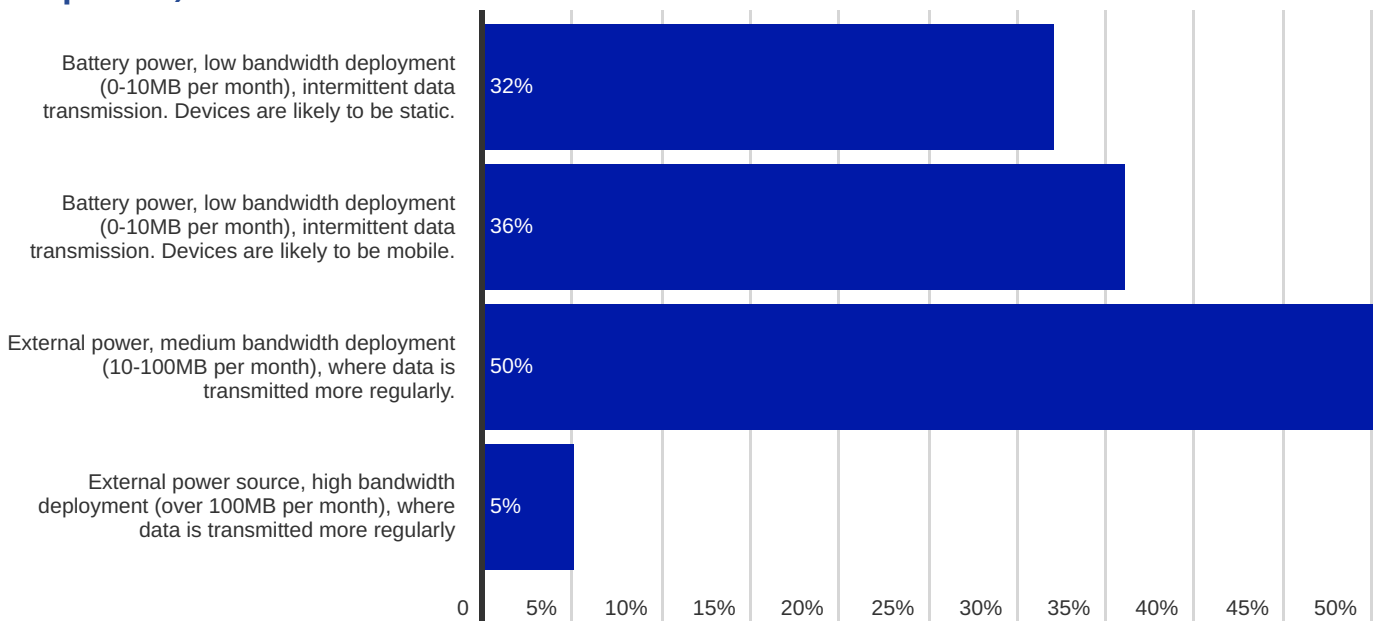
Cellular IoT adoption in this vertical is relatively high, with some **48% of survey respondents stating that they had an active or previously active cellular IoT deployment in the field**. However, it should be noted that near-term intentions to deploy cellular IoT among those who had not adopted yet was low relative to the survey average, with **only 27% of respondents stating that they intended to deploy cellular IoT in the next 12-24 months, compared with 35% of the overall survey respondent base.**

Does your business unit currently have an IoT deployment or proof-of-concept underway that uses 3GPP cellular radio technology (2G/3G/LTE/5G)? (All responses)



27% intend to deploy cellular IoT in the next 12-24 months

What type of cellular IoT deployment is this likely to be? (Cellular IoT non-adopter responses)



eseye iBASIS KORE TRUPHONE flo. LIVE

Connectivity technology choice in this particular segment has historically been diverse, with some regions and countries favouring cellular technology, and others preferring solutions such as Power Line Communications in addition to other communications technologies. Cellular technology has, in part, been hampered by the ongoing shutdowns of 2G and 3G radio networks, which offer good signal propagation for indoor or underground monitoring systems. Standards such as NB-IoT or LTE-M are intended to replace those, particularly in smart metering applications, although a relative lack of global coverage and support has meant that expected levels of traction for devices using these technologies has not been achieved yet.

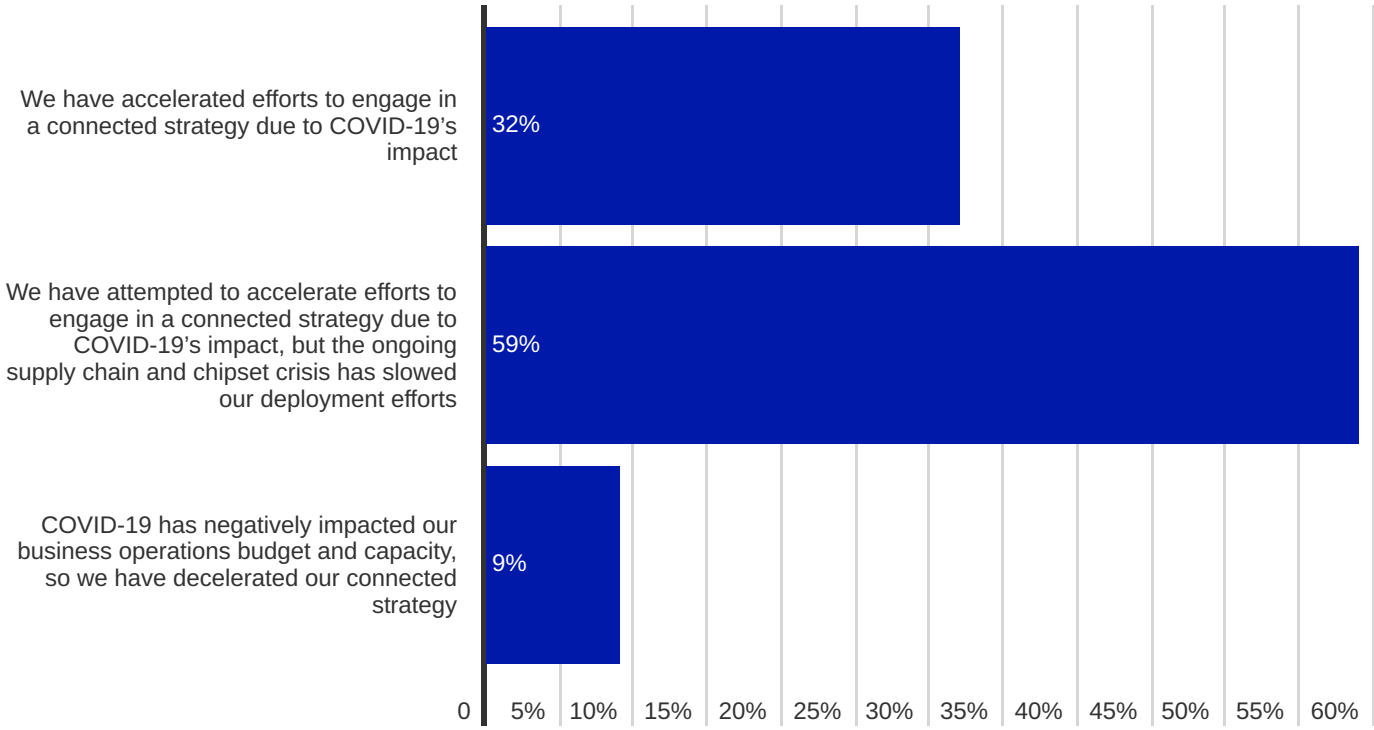
IoT applications in this particular vertical are predominantly centred around smart metering for electricity, gas, and water, while an increasing number of countries have developed strategies to deploy smart grid automation technologies. Here, metrics such as real-time demand in addition to fault and leakage are intended to generate efficiencies, cost reductions, and proactive business processes to streamline operations. Smart metering is additionally intended to ensure accurate billing, reduce theft and fraud, while also providing an endpoint monitoring solution to allow visibility of demand and enable a more diversified supply of renewable and non-renewable energy sources. In addition to this, energy generators are increasingly adopting 'industry 4.0' initiatives to monitor the state of turbines and other assets at the generation site in order to generate cost savings through proactive maintenance and reduced downtime.

When asked about the nature of future intended cellular IoT deployments, some **50% of respondents reported that deployments are likely to consist of medium bandwidth devices that are coupled to an external power source, with fewer than average respondents stating that very low bandwidth devices will be desirable.**

These results suggest a highly diverse range of forthcoming deployment types, with **68% of enterprise customers likely to require either LTE-M or NB-IoT connectivity to support smart metering applications, alongside a considerable proportion of enterprises aiming to develop IoT solutions to support generation side or grid automation activities.** It should be noted at this juncture that smart meters are commonly supplied with external power regardless of cellular radio technology used and as such, the emphasis on battery power for these types of devices, as opposed to bandwidth consumption and communications regularity, should be viewed as lower here.

The impact of COVID-19 on IoT deployments in this vertical is roughly in line with the overall average: some **32% of respondents stated that the pandemic had accelerated efforts to engage with an IoT strategy, while 59% reported that the ongoing supply chain and chipset crisis had slowed deployment efforts.** It can certainly be said that worldwide restrictions on social mixing created a notable impact on energy and water suppliers' ability to visit customers' premises to take meter readings, although it is evident that the pandemic has had a notable impact on enterprises' capabilities to roll out solutions.

How has COVID-19 impacted your organisation's IoT strategy? (Cellular IoT non-adopter responses)



Complexity - Energy/Utilities

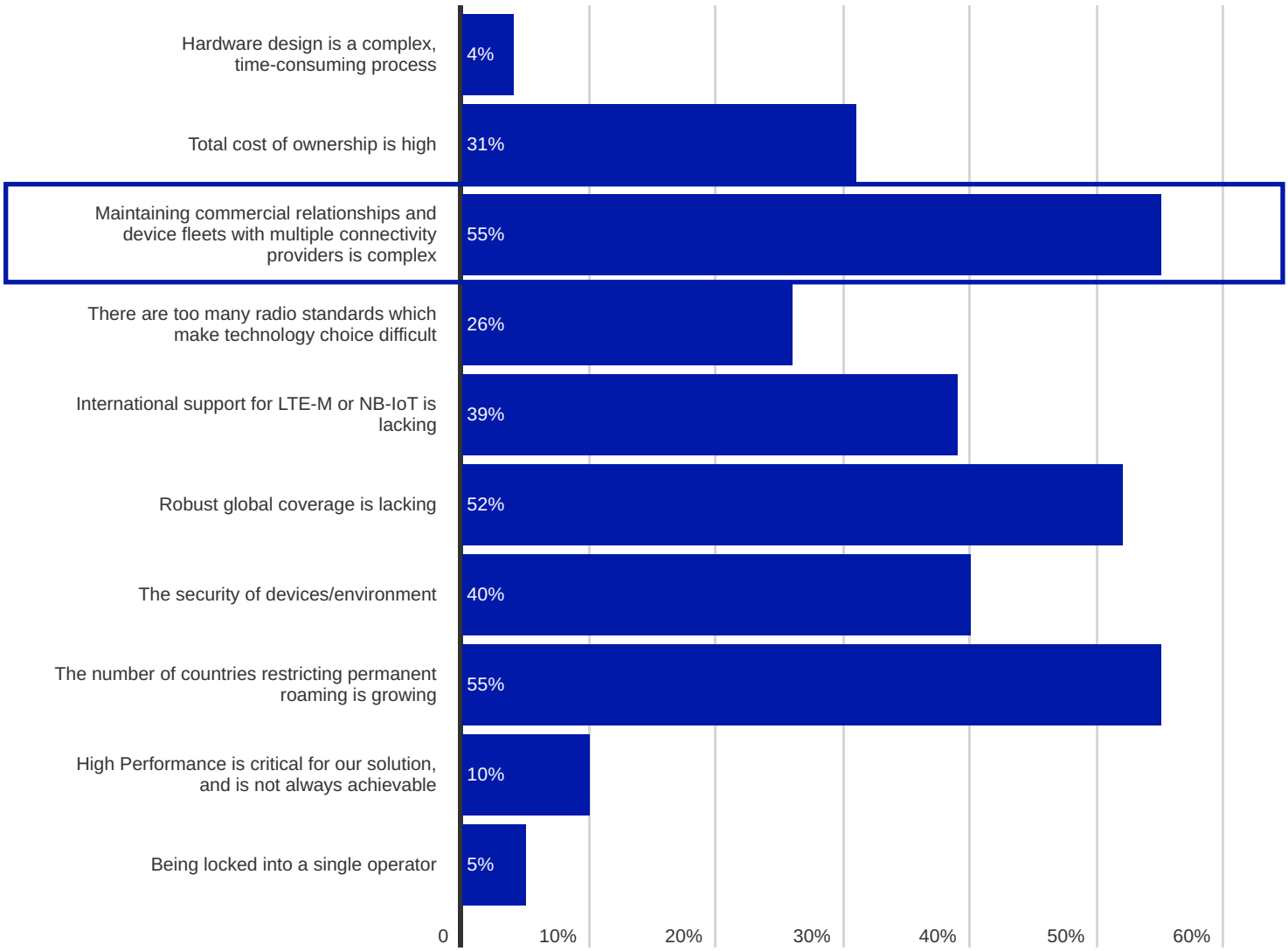
Kaleido Intelligence

While deployments in the smart metering domain have often focused on local contract engagements, demand for international connectivity support from meter and energy suppliers is growing, which means that many enterprises within this segment will increasingly be looking to streamline connectivity solutions across their international sales footprint. Evidently, the fact that the ecosystem is broadly able to cater to requirements of a minimal number of connectivity contracts has not yet resonated with a significant number of companies within this segment: **some 64% of cellular IoT non-adopters ranked the challenge of maintaining commercial relationships and device fleets with multiple connectivity providers as their second most prominent issue when considering cellular IoT connectivity; this proportion is significantly higher than the overall survey average of 51% of respondents.**

64% Cellular IoT non-adopters state multiple commercial connectivity contracts is their #2 issue

While industry education on the part of cellular IoT non-adopters can in part explain this result, it is also important to note that many customers in the smart metering segment are likely to demand LTE-M or NB-IoT radio access. The present lack of a substantial number of international roaming agreements for these technologies has meant that most deployments thus far across the industry have been domestic in nature and often require a contractual relationship with a relevant operator in each country of operation. It is thus likely that this issue has led to an increase in the challenges described above: it is down to the CSP community to build up international roaming agreements as rapidly as possible to support broader rollouts of LTE-M and NB-IoT, particularly as 2G and 3G networks are being phased out across the globe. This hypothesis is supported by the fact that **among cellular IoT adopters, 55% of respondents believe that maintaining commercial relationships and device fleets with multiple connectivity providers is complex.**

What do you perceive to be the main challenges where cellular IoT connectivity is concerned? (Cellular IoT adopters)



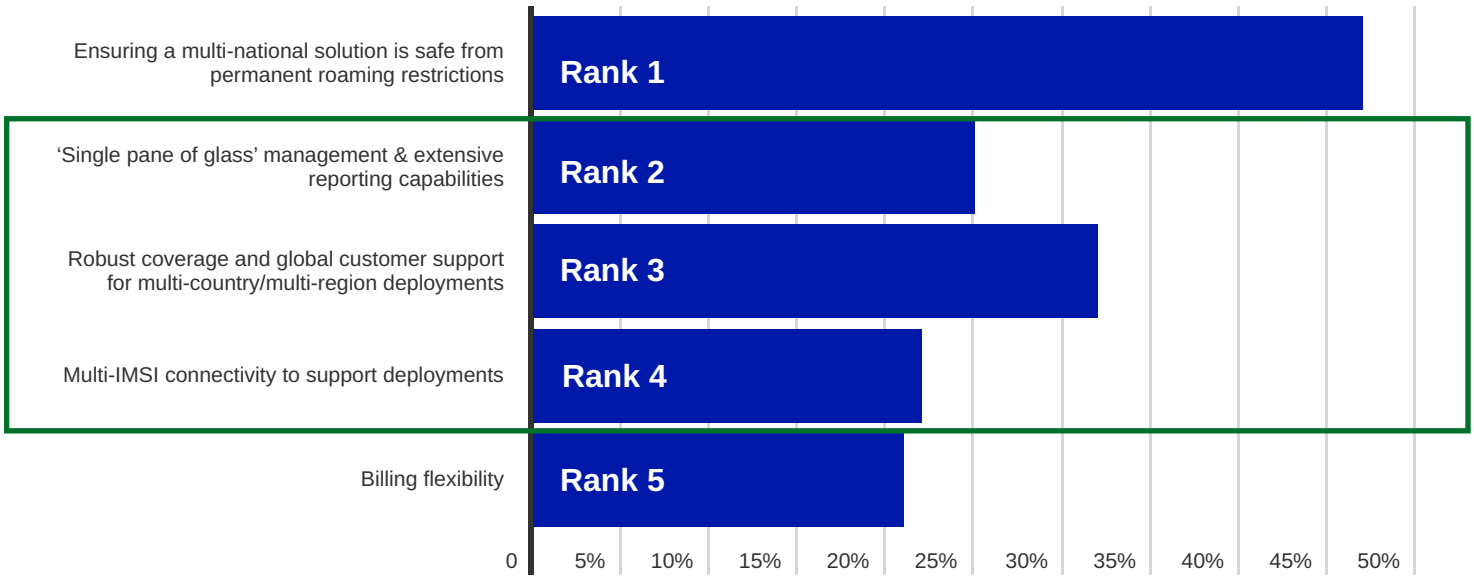
It is notable that energy and utilities enterprises ranked the numerous radio standards available in the cellular ecosystem as a challenge towards deployments, with 32% of respondents ranking this as the fifth top challenge to cellular IoT, compared with the survey average of 26% believing the same. It is apparent that the availability of 2G, 3G, LTE-M and NB-IoT radio standards are causing cellular IoT non-adopters uncertainty where device development is concerned, and means that expertise will be required to understand the scope of any future deployments, in addition to the performance and cost requirements of those deployments.

32% cellular IoT non-adopters ranked multiple radio standards as a top 5 issue

With **55% of cellular IoT adopters in this segment stating that consistent service quality across international markets is lacking**, it is apparent that the connectivity partners that these enterprises have engaged with are not offering the level of support that is expected.

The second, third and fourth highest priority for cellular IoT suggests that current connectivity providers have been slow, or unable to enable customers to streamline their international operations via these solutions.

What are your top 5 factors that are most important where cellular IoT connectivity is concerned? (Cellular IoT adopter responses)



An important question raised over the complexity of a cellular IoT connectivity solution is how the deployment should be managed. In some instances, enterprises are willing to invest time to develop expertise to enable them to configure services, develop customised rulesets for alerting or automated event triggers as well as optimise the device fleet themselves. Many others however, prefer to have the connectivity solution managed on their behalf in order to abstract complexity away and allow the enterprise to focus on other elements of value generation in the deployment. By and large, this is the case with energy and utilities enterprises: some **68% of cellular IoT adopters stated that they preferred a fully managed service, although noted that costs are an issue towards this. Meanwhile, 23% stated the same, but noted that costs are not an issue. The picture among cellular IoT non-adopters is rather different, with only 42% of respondents preferring a fully managed service.**

This disparity highlights a dramatic shift in opinion for enterprises that do eventually deploy cellular IoT, and underlines the need for CSPs to offer managed connectivity services in this vertical. Although this type of offering inevitably raises costs for the customer, it is evident that customer loyalty may be increased if a fully managed service is provided; therefore, some short-term discounting or trial phases may be worth considering, in order to demonstrate the value of managed services to newcomers to cellular IoT, leading to upsell opportunities later down the line.

Roaming - Energy/Utilities

Kaleido Intelligence

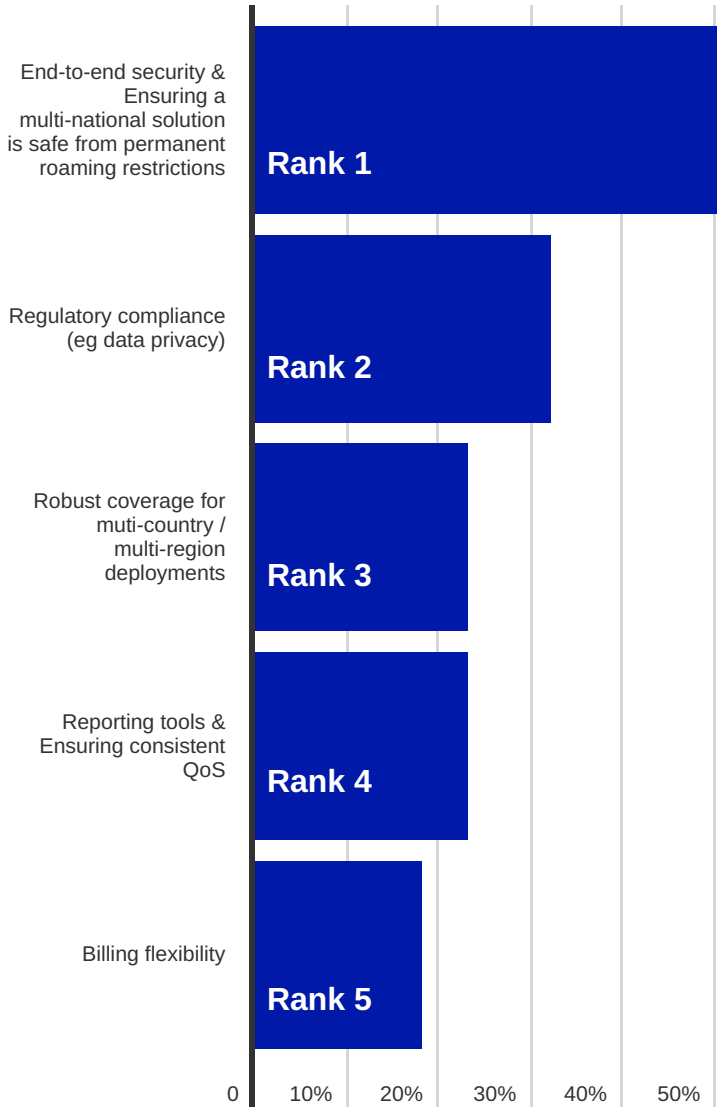
Challenges associated with roaming are clearly of top concern among enterprise energy and utilities customers, with this being the only vertical to rank capabilities to mitigate permanent roaming risks as the top priority: **50% of cellular IoT non-adopters ranked this as the most important factor where IoT connectivity is concerned. Meanwhile, 47% of cellular IoT adopters ranked this as their top priority for cellular IoT connectivity**, underlining that this is a concern across the industry where cellular IoT is concerned.

50% cellular IoT adopters ranked the ability to minimise permanent roaming risks as their #1 priority

Meanwhile **32% of cellular IoT non-adopters ranked the ability to deliver against regulatory compliance requirements, such as data privacy, as the number 2 priority for IoT connectivity**.

This raises an important point where roaming is concerned, in that the traditional technical architecture for roaming means that data is 'tromboned' between the visited operator and home network operator. In simple terms, roaming normally operates using a 'home routed' architecture, which means that data must travel from the visited operator, to the home operator and back again before being delivered to the device. This raises concerns over the cross-border traversal of data, with some countries prohibiting it and others imposing strict regulations around the processing and storage of such data. Since the advent of LTE, technical solutions known as local breakout and regional breakout have been developed to, in part, address this issue, in addition to offering the ability to improve connection performance on account of reduced latency. However, it has rarely been deployed in practice.

What are your top 5 factors that are most important where cellular IoT connectivity is concerned? (Cellular IoT non- adopter responses)



eseye iBASIS KORE TRUPHONE flo. LIVE

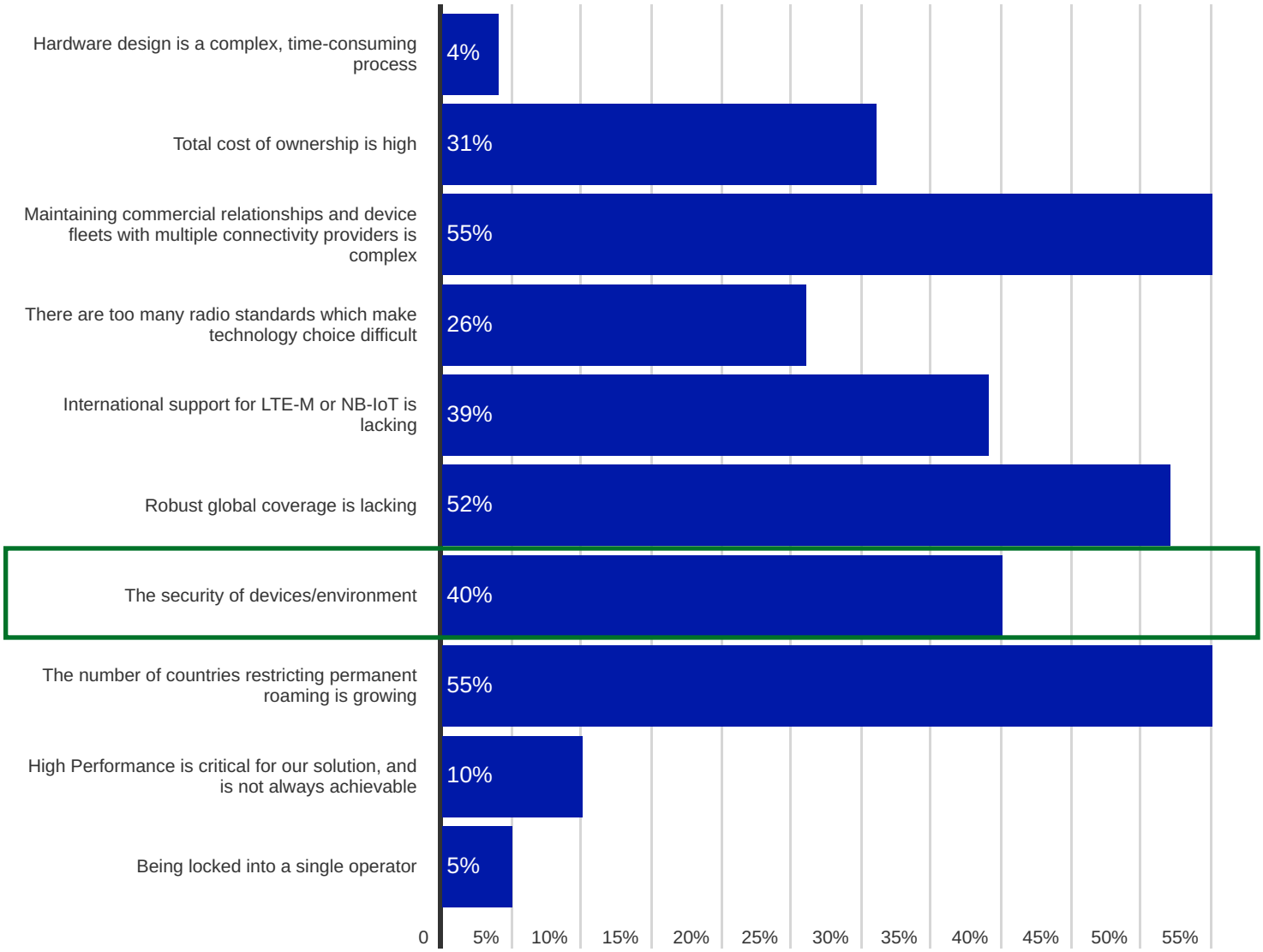
Security - Energy/Utilities

Kaleido Intelligence

The issue of security where cellular IoT adopters and non-adopters are concerned shows considerable variance, particularly when placed in the context of cellular IoT connectivity priorities. For example, while **50% of non-adopters ranked end-to-end security as their top priority for connectivity, only 26% of cellular IoT adopters reported the same.** While this may seem as if security is not a priority for cellular IoT adopters, this hypothesis is countered by the fact that adopters consider the security of devices and the environment a key connectivity challenge.

50% cellular IoT non-adopters ranked end-to-end security as their #1 priority

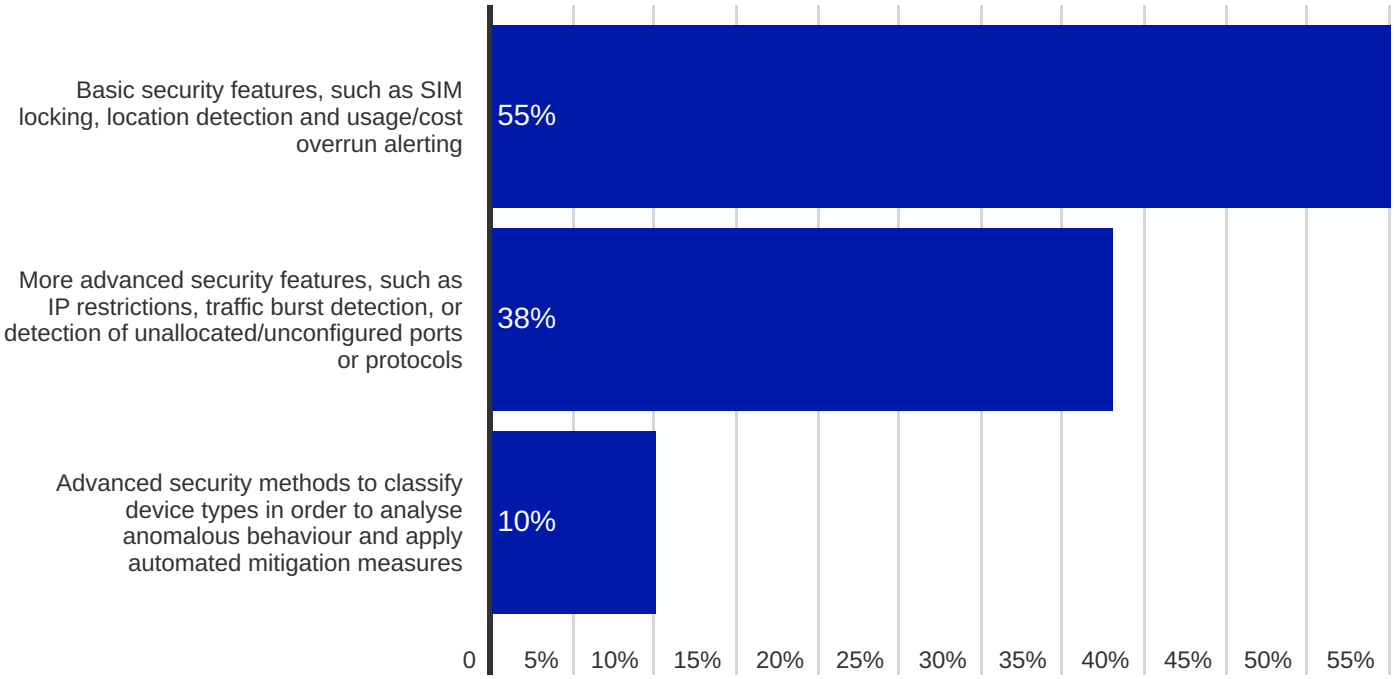
What do you perceive to be the main challenges where cellular IoT connectivity is concerned? (Cellular IoT adopter responses)



What becomes evident when looking more closely at the results is that security is not viewed as such a considerable a challenge as other factors, such as international connectivity availability and support, seamless fleet management capabilities and billing flexibility. One can therefore infer that many energy and utilities customers are experiencing challenges with the overall operation of their device fleets, with security providing an important, but diminished factor for consideration.

Moreover, it should be noted that **a higher than average (55% vs. 50%) number of cellular IoT adopters in this segment stated that their connectivity partner should only be responsible for basic security features, such as SIM locking and cost overrun prevention. 38% of respondents stated that they would prefer their connectivity partner to offer more advanced security features, which is below the survey average of 43%**. This suggests that enterprises in this segment view security less as something that must be addressed within the connectivity domain, and more something that a third-party provider should be responsible for.

What security features do you expect your cellular IoT connectivity partner to provide? (Cellular IoT adopter responses)



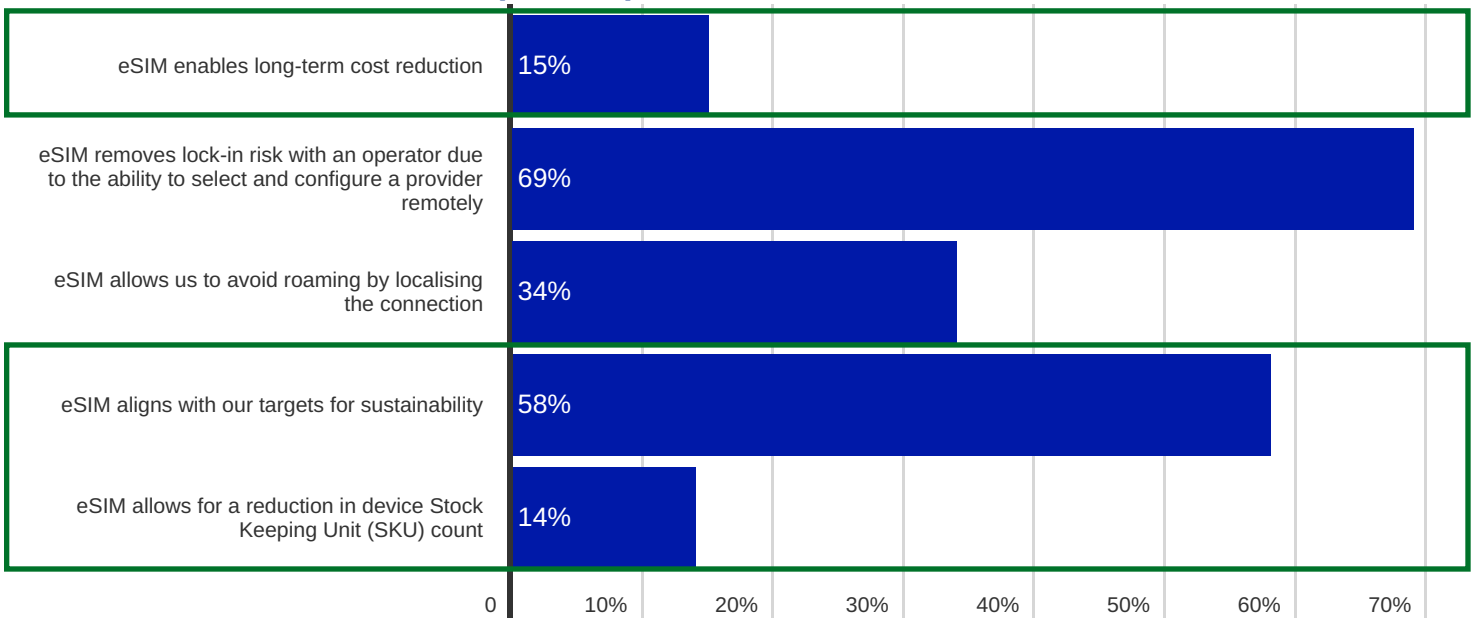
eSIM - Energy/Utilities

Kaleido Intelligence

eSIM is particularly important to the energy and utilities sector, with **92% of cellular IoT adopters stating that they count eSIM as part of their IoT deployment.** The high adoption of the technology speaks to concerns analysed in this section over coverage and roaming, and, when one considers that service lifespans for devices such as smart meters can reach 15 years, the need for eSIM to mitigate risks associated with commercial and regulatory challenges becomes evident.

The reasons for choosing eSIM are heavily skewed towards cost reduction in some form or another and are above average in this respect. For example, **when looking at cost-related benefits to eSIM; the capability to launch products via a single Stock Keeping Unit (SKU), and long-term cost reduction as a result of fewer physical SIM swaps, some 30% of the respondent base reported that this was an important factor in their decision to use eSIM, vs. a survey average of 23%**. eSIM is therefore clearly viewed as a tool to streamline both capital and operational overheads encountered during the lifecycle of the device. **An additional driver behind eSIM is sustainability, with 58% of respondents stating that the technology is aligned with enterprise sustainability goals.** This proportion was second only to those within the smart cities segment, and highlights that environmental concerns are at the forefront for enterprises.

What do you perceive to be the main challenges where cellular IoT connectivity is concerned? (Cellular IoT adopter responses)



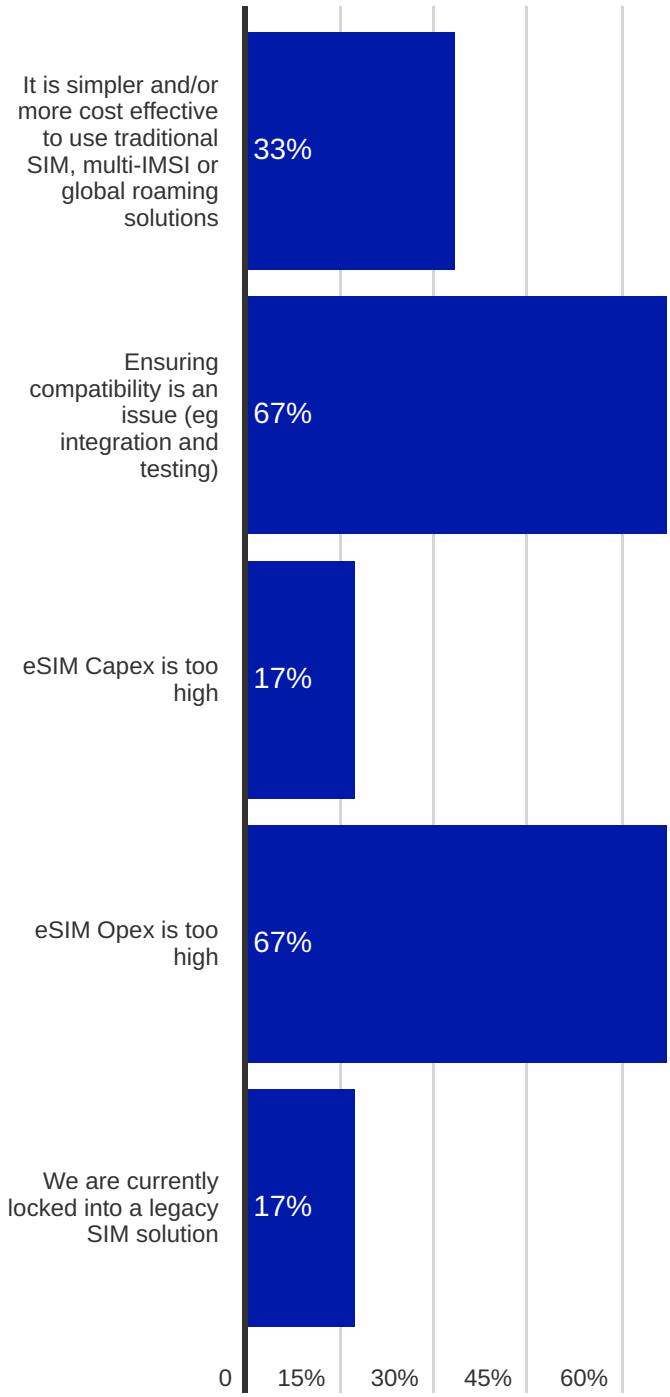
It is notable that among those who had not adopted eSIM, high Opex and challenges surrounding eSIM compatibility with devices were cited as major concerns. Indeed, **those reporting that eSIM Opex is too high (67% of respondents) are considerably higher than the survey average (39%).**

In part, this may relate back to challenges noted in terms of data regulation and compliance, which in turn may limit the ability to deploy using traditional roaming IoT architectures. While eSIM allows customers to download and install local operator profiles in order to

avoid roaming, the present state of the market does not deliver this functionality without costly overheads. Indeed, customers requiring this type of functionality can expect to spend several tens of cents per OTA transaction to execute a network operator profile swap and, when one considers that fleet deployments in this segment often run into several hundred thousand or even millions of devices, costs can very quickly accumulate. This impact may be particularly relevant for smart metering deployments, where the present high cost of wholesale energy, in addition to the investment required to replace legacy metering infrastructure, leaves relatively little room for margins where retail energy suppliers are concerned.

With 67% of respondents who had not chosen eSIM as part of their IoT deployment reporting that device compatibility in terms of integration and testing is an issue, it is apparent that an important segment of energy and utilities enterprises require additional expertise and guidance where device development is concerned. This is particularly relevant when considering radio technologies such as LTE-M and NB-IoT, with one radio technology often used as a fallback option for the other if the preferred standard is not supported in the country of operation. Testing here must ensure that the SIM can be used with different cellular radio standards to ensure connectivity availability, and allow enterprise customer to be confident that their devices will connect to mobile networks wherever they are delivered in the field.

Why have you chosen not to use eSIM (eUICC)? (Cellular IoT adopter responses)

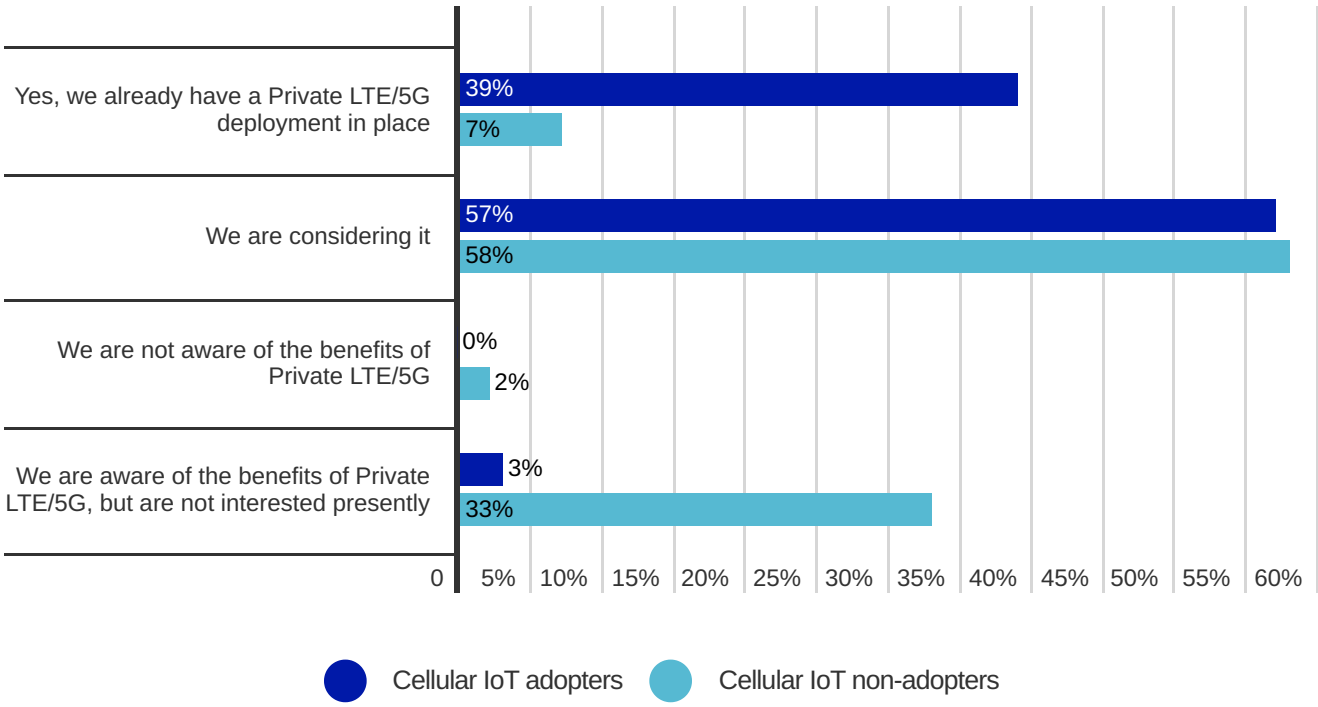


Private LTE/5G - Energy/Utilities

Kaleido Intelligence

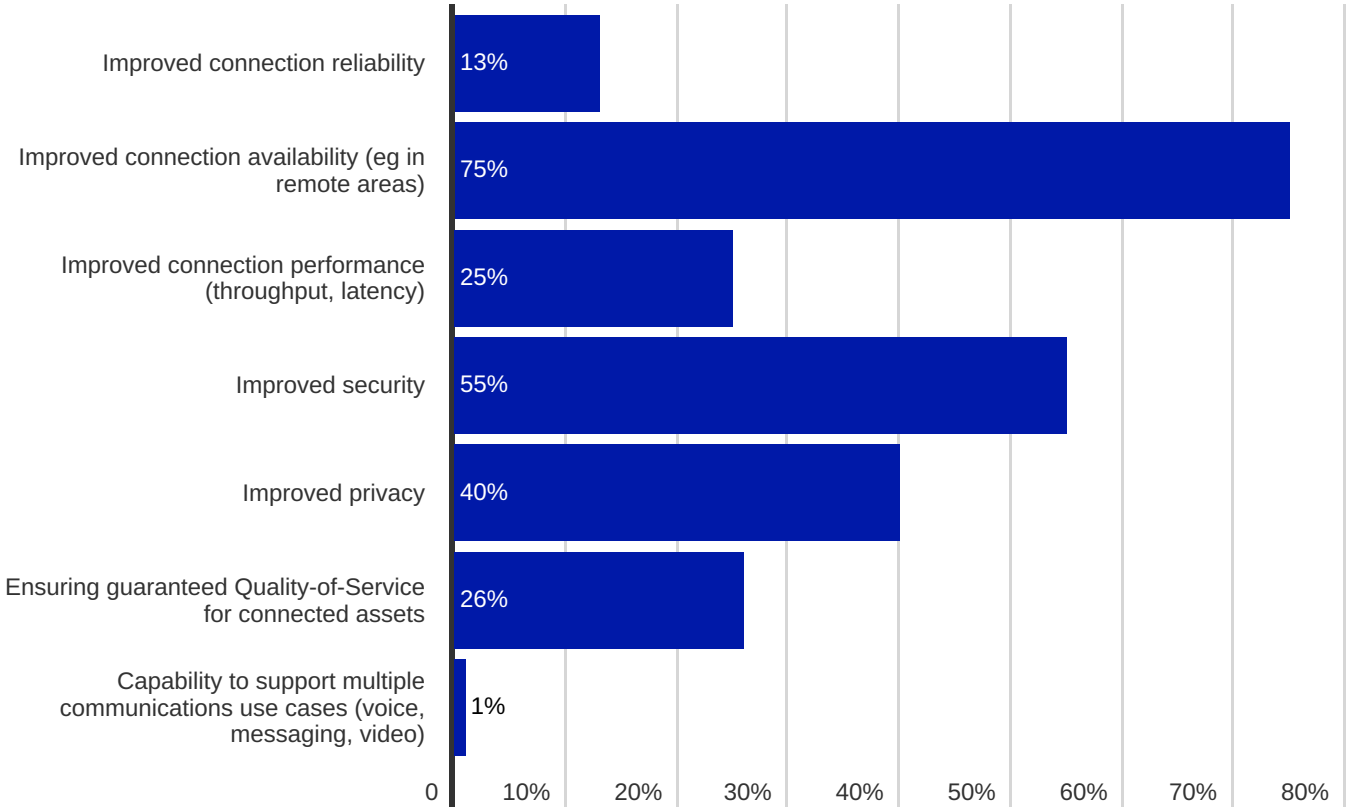
The potential for private LTE or 5G is particularly high within this segment: s**ome 96% of cellular IoT adopters either have deployed, or are considering a private LTE or 5G deployment, while 65% of cellular IoT non-adopters reported the same.** It is notable that the potential for private LTE or 5G services becomes markedly higher when cellular IoT has already been adopted and is likely related to the fact that enterprises in this sector are especially concerned with streamlining operations.

Does your business unit have an interest in Private LTE/5G to enhance business operations? (All respondents)



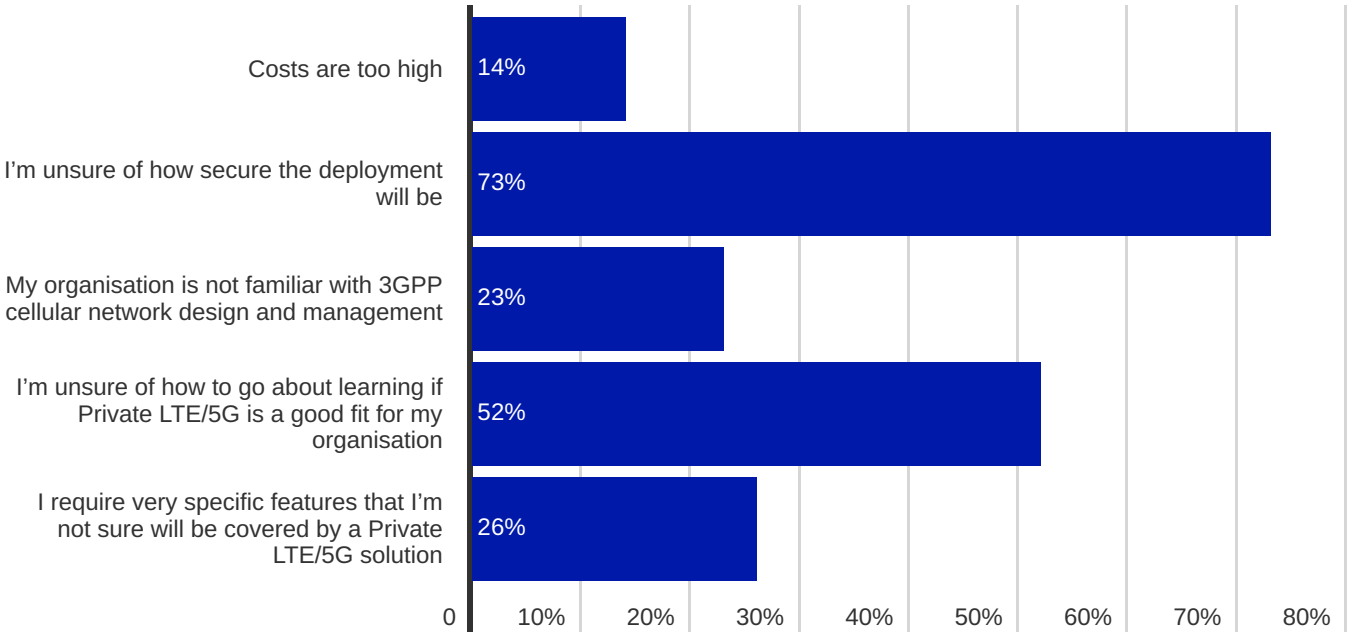
Historically, oil and gas enterprises have been counted among early adopters of private LTE and have formed a core part of the customer base requiring fully isolated private network solutions in remote locations. Increasingly, customers that have traditionally used TETRA for communications are now aiming to upgrade their connectivity solutions to LTE or 5G in order to enhance operations and support a more diverse number of applications. **The ability to provide connectivity in remote locations is particularly important in this sector, with 75% of respondents stating that this is the main perceived benefit to private LTE or 5G, compared with a survey average of 66%.** Indeed, many sites in the oil and gas sector are in locations that are poorly served, if at all, by public mobile networks. Demand for private cellular networks is now expanding into the utilities sector, where dedicated connectivity promises improved reliability for services such as smart metering and operations streamlining at energy generation sites. The potentially sensitive data generated by these applications means that security for private LTE or 5G is evidently of high concern: **73% of respondents stated that they were unsure of how secure a deployment would be.**

What do you perceive to be the main benefits of a Private LTE/5G solution? (Cellular IoT adopter respondents)



Meanwhile, **52% of the respondent base was unsure how good a fit private LTE or 5G would be for their organisation**. These results are likely due to the significant level of OT/IT convergence involved with certain types of deployments and in some instances, may raise questions over the overall safety of operations. It is clear that for potential customers in this segment, deep vertical expertise is a requirement to deliver on expectations of security as well as overall deployment design and configuration, and as such, CSP partnerships with relevant systems integrators should be viewed as a key priority.

What are your main concerns over a potential Private LTE/5G deployment? (Cellular IoT adopter respondents)



CASE STUDY

KORE, Kigen, and Energy Web Enable Decentralised Identity Exchange for Smart Grid with eSIM

Background

Energy Web is a nonprofit organisation focused on building open source, decentralised operating systems to help decarbonise the global economy. Energy Web offers its open-source stack to organisations to build their own applications, or Energy Web will provides assistance to organisations in building applications off the open-source stack.

THE EW-STACK is a suite of open-source tools built off of the Energy Web Chain, the world's first public, enterprise-grade blockchain tailored to the energy sector.

Energy Web wanted to provide a highly secure solution for energy assets that is just as simple as their EW-STACK when it comes to security at the device level.

The Challenge

Targeting aggregators and OEMs, Energy Web identified three methods of storing private encryption keys within a device – firmware, which is not safe and easy to tamper; or an embedded SIM, which would place the onus on OEMs to add an additional integrated circuit and that was a burden Energy Web didn't want to pass down.

Far and away the best option was to leverage IoT SAFE, which is a GSMA initiative that utilises the SIM as a secure hardware element for chip-to-cloud security. Energy Web could utilise the SIM as a hardware wallet anchored to an open-source, publicly accessible blockchain powered by Energy Web.

> Securely communicating data at the packet level is a significant step toward creating end-to-end security.

The Solution

Energy Web has partnered with KORE and Kigen, pioneers in IoT security through eSIM and iSIM hardware, to implement an open IoT SAFE solution, which essentially is an open-source method for third parties to use Energy Web cryptocurrency features to store their private encryption keys and sensitive credentials in the crypto-safe enabled through IoT SAFE infrastructure.

Not only does this provide the device the same kind of authentication credentials found at the network level, but it also secures data communications at the packet level. And because Energy Web operates in a blockchain environment, it's a decentralised approach to device-level security.

The Result

This opportunity created through the partnership of Kigen and KORE and leveraged by Energy Web is a historical approach to an enterprise essentially "owning" the SIM card.

Prior to eSIM and iSIM, SIM cards were removable and treated primarily as property of the Mobile Network Operator (MNO) distributing the SIM that connected to its network.

Now it's an open platform that allows the organisation delivering the use case to own the SIM for its own purposes. And specifically in the case of Energy Web, IoT SAFE allows an enterprise – a third party – to store its own credentials and own encryption key, which truly makes this a multi-tenant solution.

Organisations using Energy Web's technology can build their own applications via the world's first open-source technology stack focused explicitly on the energy transition towards efficiency and renewables. This enables the ability to provide information to third-party IoT providers via a SIM card which in-builds device-level security and can authenticate data for a user's cloud service. Securely communicating data at the packet level is a significant step toward creating end-to-end security.

"Energy Web's focus is to use digital identities and open-source operating systems to make it easier for grid operators around the world to interact with an increasingly decarbonised, decentralised energy market," said Jesse Morris, CEO of Energy Web. "Of course, as more and more IoT devices come live and decentralised energy assets become increasingly common, protecting the infrastructural security of these systems is of the utmost importance. The work we are doing in partnership with KORE and Kigen is a perfect example of what smart, sensible, and safe IoT security solutions look like in the real world."

About KORE

KORE is a pioneer, leader, and trusted advisor delivering mission critical IoT solutions and services. We empower organisations of all sizes to improve operational and business results by simplifying the complexity of IoT. Our deep IoT knowledge and experience, global reach, purpose-built solutions, and deployment agility accelerate and materially impact our customers' business outcomes. For more information, visit **eu.korewireless.com**

About Kigen

At Kigen, we are making the future of securing connectivity simple. As simple as can be. Together with our partners and customers, we are at the forefront of unlocking a new era of secure IoT as Integrated SIM (iSIM) and eSIM becomes the mainstream choice for connected devices. Our industry-leading SIM OS products enable over 2 billion SIMs. Our GSMA certified remote SIM provisioning and eSIM services drive this momentum further placing us amongst top 5 SIM vendors globally. As an Arm founded company, we bring an ecosystem approach to driving innovation and collaboration. For more information, go to **kigen.com** or speak to us on **@Kigen_Ltd** on Twitter and LinkedIn about #futureofSIM.

About Energy Web

Energy Web is a global, member-driven nonprofit accelerating the low-carbon, customer-centric energy transition by unleashing the potential of open-source, digital technologies. We enable any energy asset, owned by any customer, to participate in any energy market. The Energy Web Chain — the world's first enterprise-grade, public blockchain tailored to the energy sector — anchors our tech stack. For more information, **visit www.energyweb.org**

KORE

IoT Connectivity Challenges & Opportunities: Industrial / Manufacturing

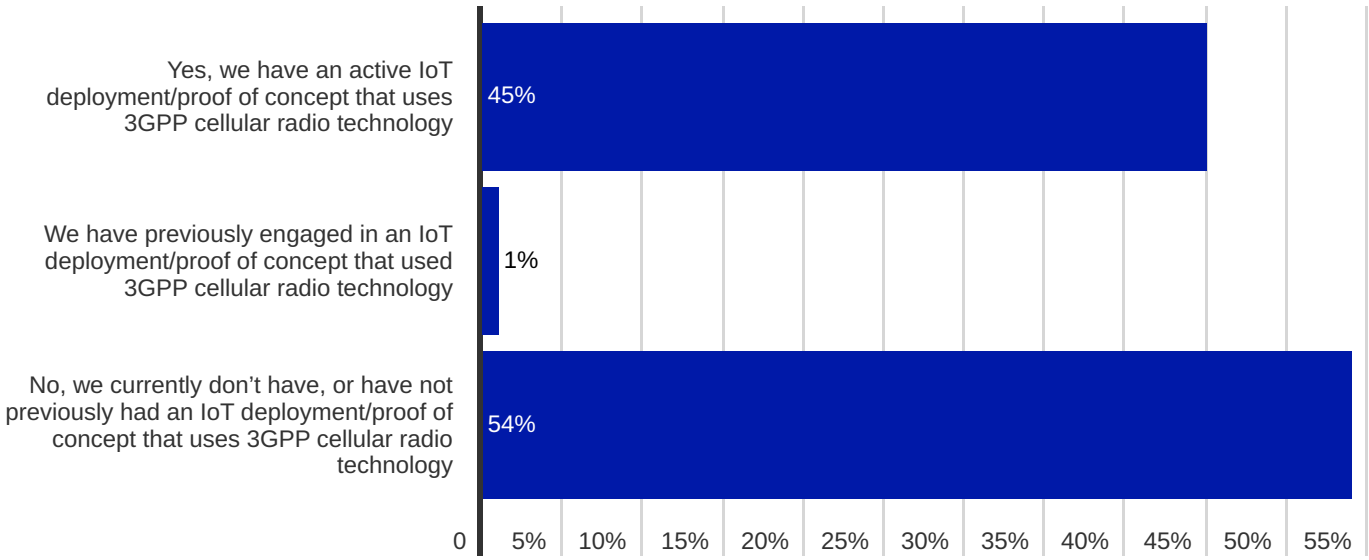
eseye iBASIS KORE TRUPHONE flo. LIVE

State of IoT - Industrial/Manufacturing

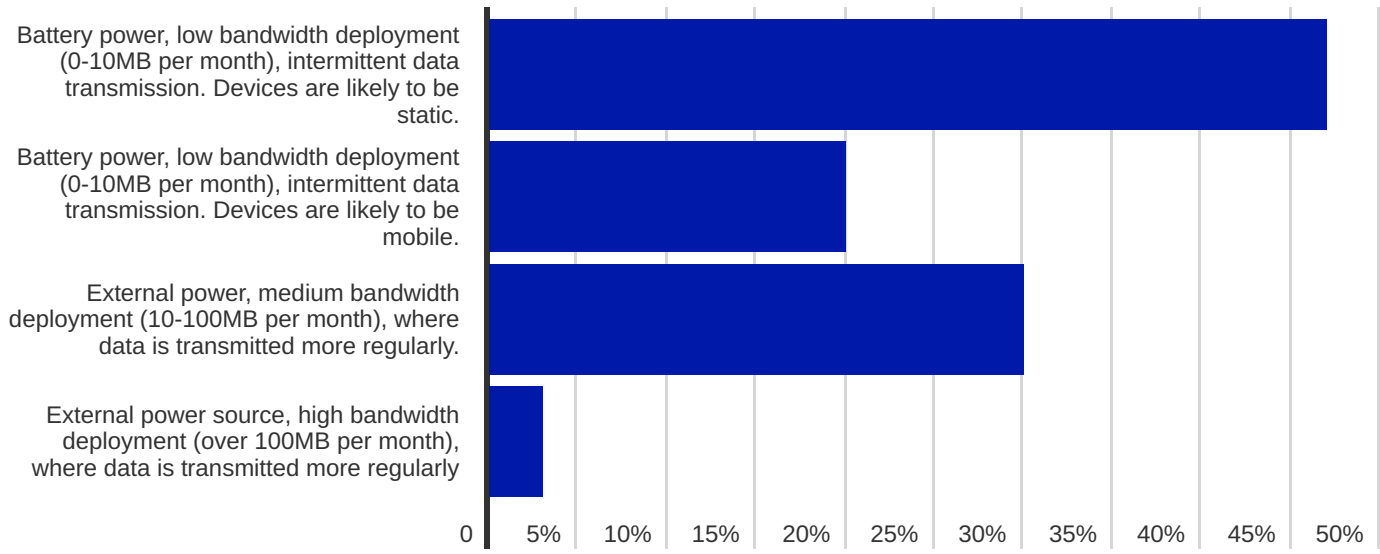
Kaleido Intelligence

The industrial and manufacturing segment has, through the advent of 'industry 4.0' initiatives, seen relatively high deployment of cellular IoT, with **46% of respondents stating that they had an active or previously active deployment. Nevertheless, a relatively high proportion of the respondent base (67%) stated that they did not intend to deploy cellular IoT over the next 12-24 months, highlighting that there is an opportunity to drive engagement with cellular technology use to support future digital transformation strategies.**

Does your business unit currently have an IoT deployment or proof-of-concept underway that uses 3GPP cellular radio technology (2G/3G/LTE/5G)? (All responses)



What type of cellular IoT deployment is this likely to be? (Cellular IoT non-adopter responses)



eseye iBASIS KORE TRUPHONE flo. LIVE

Of those intending to deploy IoT solutions using cellular radio standards, **67% of survey respondents reported that low data, sensor-based applications would be a priority over more complex high-bandwidth applications, while 30% of the respondent base expects to launch devices with medium bandwidth requirements that transmit data more regularly.** Thus, we can infer that many near-term deployments will involve connectivity to support predictive maintenance on the factory floor, in addition to more advanced devices that may be deployed to customers in other verticals. Asset monitoring is a particularly important use case within the manufacturing and industrial segment, with connectivity used to monitor equipment for reliability, compliance, and safety.

Nevertheless, it is notable that **only 3% of respondents stated that they would use cellular connectivity to support very high bandwidth applications.** In this context, video streaming, remote vehicle and robotics monitoring and guidance, in addition to advanced real-time monitoring of critical assets, provide examples of key use cases in this segment. The low proportion of respondents intending to use cellular connectivity for these applications may highlight that the majority of manufacturing and industrial enterprises are not yet in a position to implement such projects. On the other hand, it may be the case that these enterprises view alternative connectivity technologies as more suitable: indeed, **some 81% of cellular IoT adopters view either Wi-Fi or Ethernet as a viable alternative to cellular radio technology.** It is certainly the case that these technologies are in common use across factory floors today; notably, **37% of cellular IoT non-adopters ranked the belief that cellular technology is not always capable of meeting high-performance requirements as the number 3 challenge in the context of cellular IoT connectivity.** This strongly suggests that some enterprises in this segment are unaware of the flexibility of cellular technology to support a range of use cases at scale.

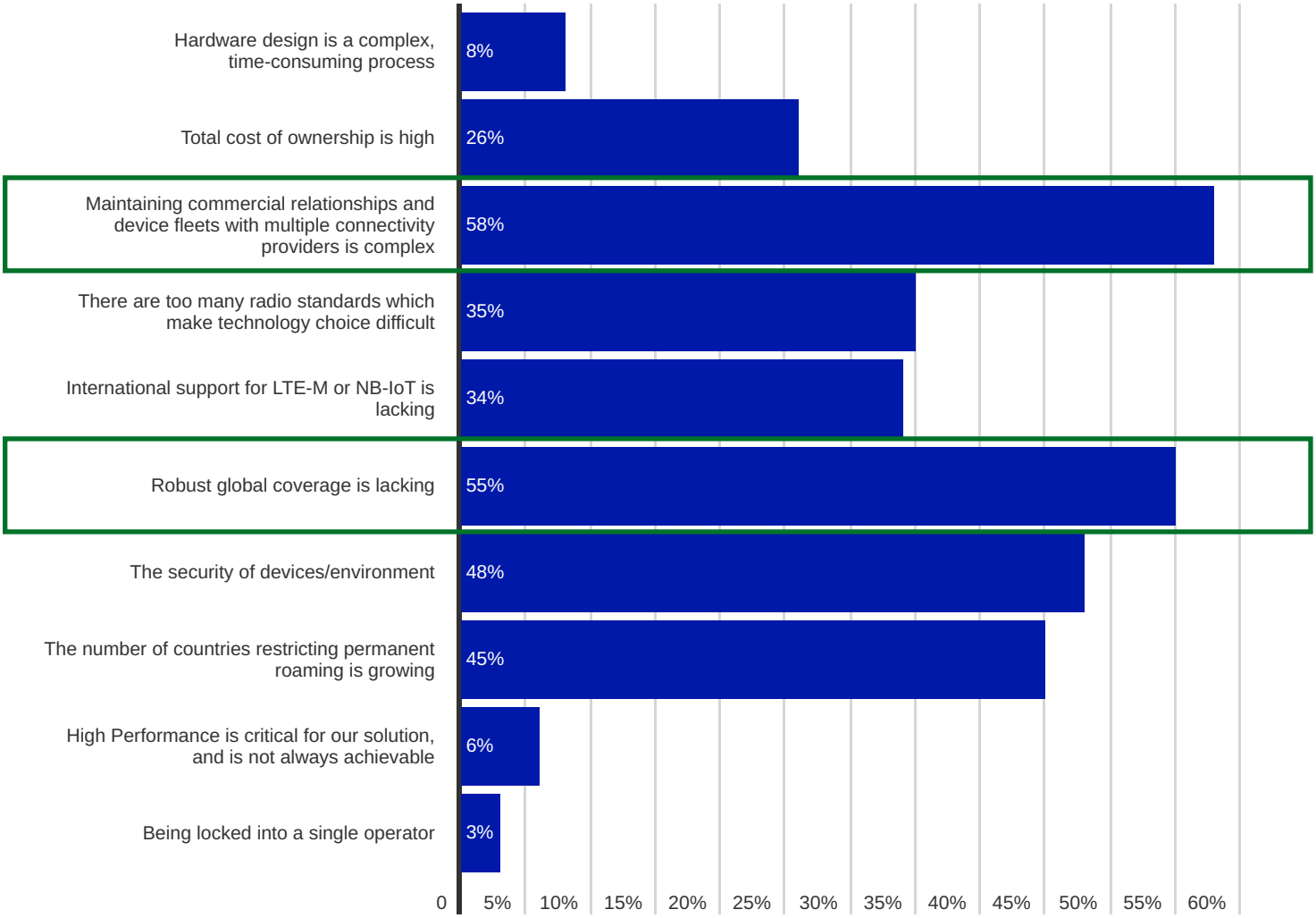
The belief that cellular IoT cannot always meet high performance requirements is a #3 concern among cellular 37% IoT non-adopters

Complexity - Industrial/Manufacturing

Kaleido Intelligence

The manufacturing and industrial sector is notable in that above-average responses were received in relation to perceived challenges with international connectivity. For example, **58% of cellular IoT adopters stated that maintaining commercial relationships and device fleets with multiple connectivity providers is complex compared with the survey average of 56%. Meanwhile, 55% of survey respondents cited robust global coverage as a key challenge, compared with a survey average of 48%.**

What do you perceive to be the main challenges where cellular IoT connectivity is concerned? (Cellular IoT adopter responses)



These results likely relate to, on the one hand, the diverse verticals that finished products are delivered to: global supply chains in this segment are likely to be more distributed than the majority of other verticals analysed in this study, with a greater mix of technical and performance requirements.

These factors by themselves introduce inherent complexity and underline the need for CSPs to streamline the connectivity solution insofar as is possible to help potential customers cost-efficiently manage connectivity solutions across a range of different products and target countries.

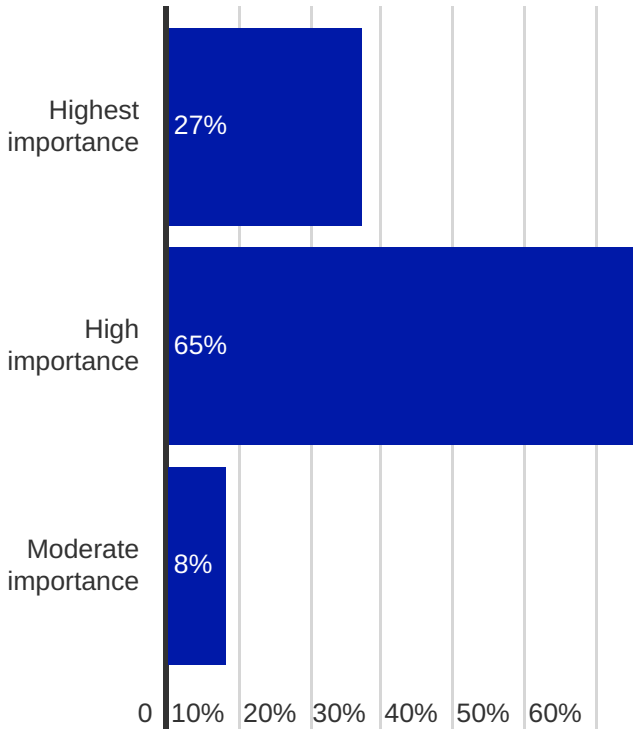
On the other hand, the issue of coverage may be somewhat more of a difficult challenge to address, particularly as many industrial sites are in remote locations with limited access to public mobile radio infrastructure. In this context, it is important for CSPs to ensure that as many incumbent operators as possible are partnered with in key locations as part of an effort to maximise the potential public mobile radio footprint. Additionally, partnerships with private mobile radio spectrum holders are likely to become increasingly important into the medium-term: this will be investigated later in this section. Importantly, the desire to maintain connectivity continuity from the factory floor to the country or region that products are eventually shipped to is likely to mean that connectivity services to support both private cellular network and public mobile network connectivity will become an important factor moving forwards.

As noted earlier, several different connectivity technologies have commonly been deployed in manufacturing and industrial environments. In today's market, **relatively few cellular IoT CSPs have developed their connectivity management platforms to incorporate support for cellular in addition to other connectivity technologies; this lack of multi-technology support is evidently viewed as a challenge by manufacturing and industrial cellular IoT adopters, with 51% of the respondent base citing issues in this respect, compared with a survey average of 46%.** From these results, we can infer that customers in this segment desire a holistic view of connected assets, and thus multi-technology asset visibility and management capability should be viewed as a key priority for CSPs aiming to deliver best-in-class solutions.

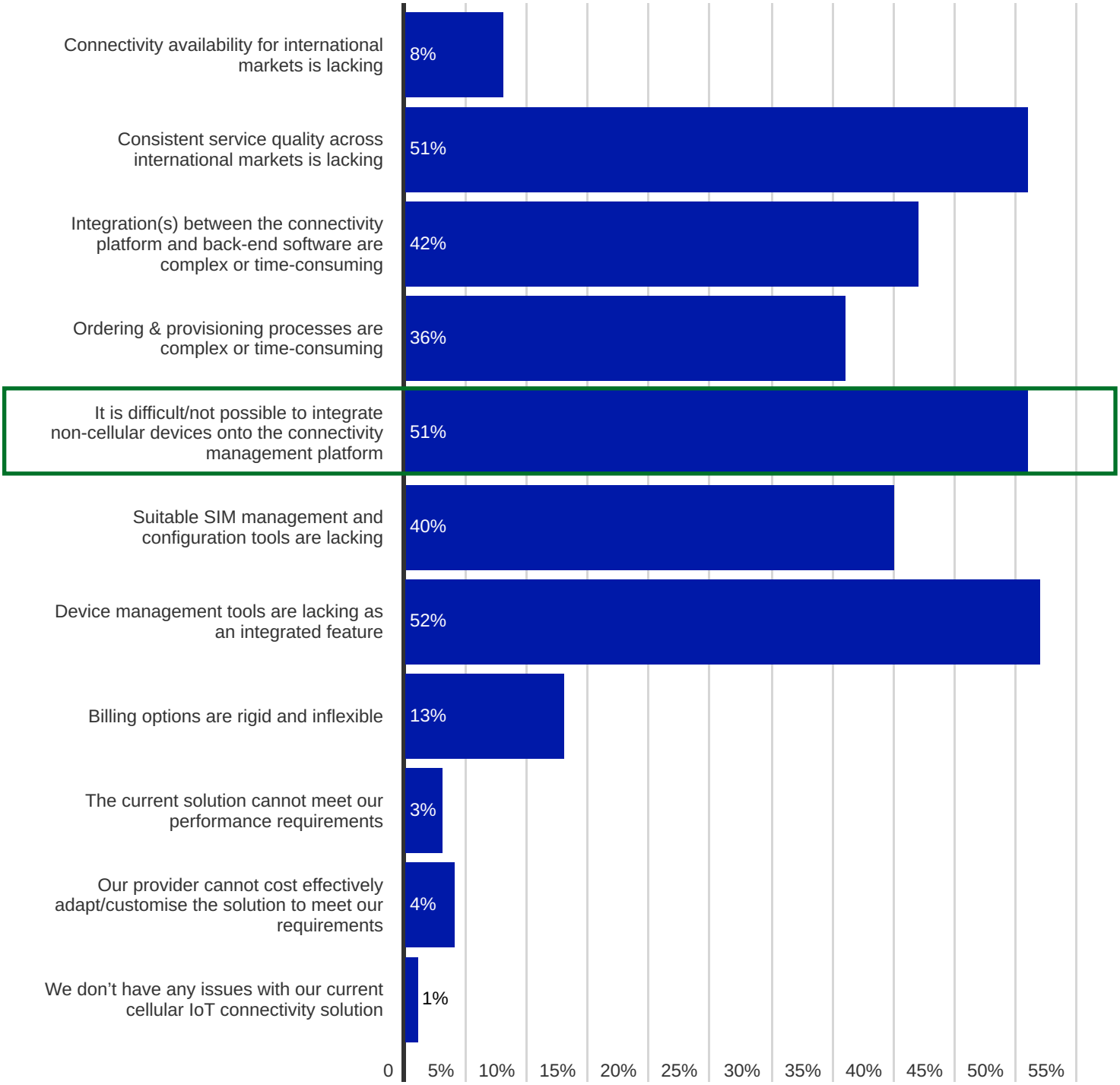
On a similar note, some **52% of cellular IoT adopters reported that a lack of device management capabilities integrated into the connectivity solution caused issues for them, compared to a survey average of 48%.** This again highlights a desire to engage with the connected fleet via a single platform solution as far as is possible.

In line with the above comments, **customers in the manufacturing and industrial segment place a high emphasis on their connectivity partner providing vertical-specific analytics tools, with 92% of the respondent base stating that this capability is of high or highest importance to them.**

How important is it that your cellular connectivity solution provider can offer vertical-specific analytics tools and services to supplement the connectivity offering? (Cellular IoT adopter responses)



What are your biggest issues with your current cellular IoT connectivity solution? (Cellular IoT adopter responses)



The results show that where manufacturing and industrial clients are concerned, an end-to-end solution is preferred in terms of connectivity provision and management, device management and analytics capabilities. There are relatively few players on the market today that have not only have such diverse offerings but are also able to cater to requirements that minimise the number of connectivity relationships required. Traditionally, this type of market niche has been occupied by large MNOs, although these providers do not typically offer the same type of flexibility in terms of customisation and adaptability that IoT connectivity specialists offer. As such, there is a significant opportunity for innovative or capital-rich CSPs to develop or acquire the necessary expertise to deliver against customer preferences in this segment.

Roaming - Industrial/Manufacturing

Kaleido Intelligence

It is interesting to note that the **issue of permanent roaming among manufacturing and industrial enterprises reaches a higher level of concern when compared with other verticals: 39% of cellular IoT adopters ranked this as their number 2 concern with IoT connectivity, compared with a survey average of 29%**. Connectivity for devices is frequently provisioned at the production stage which means that when devices are shipped to their country of operation, roaming is inevitable. However, maintaining connectivity uptime to support operations is a fundamental requirement and has thus led to understandable concern among device OEMs. Undoubtedly, CSPs must be transparent in the context of countries that they have agreements or capabilities to permanently roam in, in order to aid potential customers in choosing the most appropriate provider for connectivity services.

39% cellular IoT adopters ranked permanent roaming as a #2 challenge

The issue of permanent roaming is less of a concern for enterprises in this segment who have not yet adopted cellular IoT: this issue was ranked fourth in terms of IoT connectivity challenges by 27% of the respondent base, but is ranked as the second-highest priority for cellular IoT connectivity by 33% of respondents. It is thus evident that cellular IoT non-adopters believe that the issue of permanent roaming has largely been solved (when this is not necessarily the case among all CSPs), and leads to the hypothesis that cellular IoT non-adopters are understandably not fully familiar with the nuances of the cellular connectivity ecosystem.

It is therefore important that potential clients are alerted to challenges associated with cellular connectivity from the outset in order to bring expectations to a realistic level: customer acquisition potential will be raised if connectivity partners are able to both raise these issues as well as provide practical solutions that offer pathways around them.

58% cellular IoT non-adopters see extensive reporting capabilities in the CMP as a top priority

Transparency is an additional key factor for consideration where manufacturing and industrial enterprise clients are concerned. For example, cellular IoT non-adopters stated that extensive reporting capabilities were their top priority when considering a connectivity partner's capabilities, while **single pane of glass management and extensive reporting capabilities was ranked as the fourth-highest priority for IoT connectivity by 25% of cellular IoT adopters.** Not only do these results highlight how roaming and operator partnerships are fundamental for CSPs to help streamline operations and fleet visibility, but also that significant insight into fleet activities is desirable no matter where connections are operating. This means that efforts to extend coverage footprints and ensure that appropriate core network integrations are established to maximise transparency should be viewed as a priority by CSPs.

25% cellular IoT adopters ranked single pane of glass management & extensive reporting capabilities as a top 4 requirement

Security - Industrial/Manufacturing

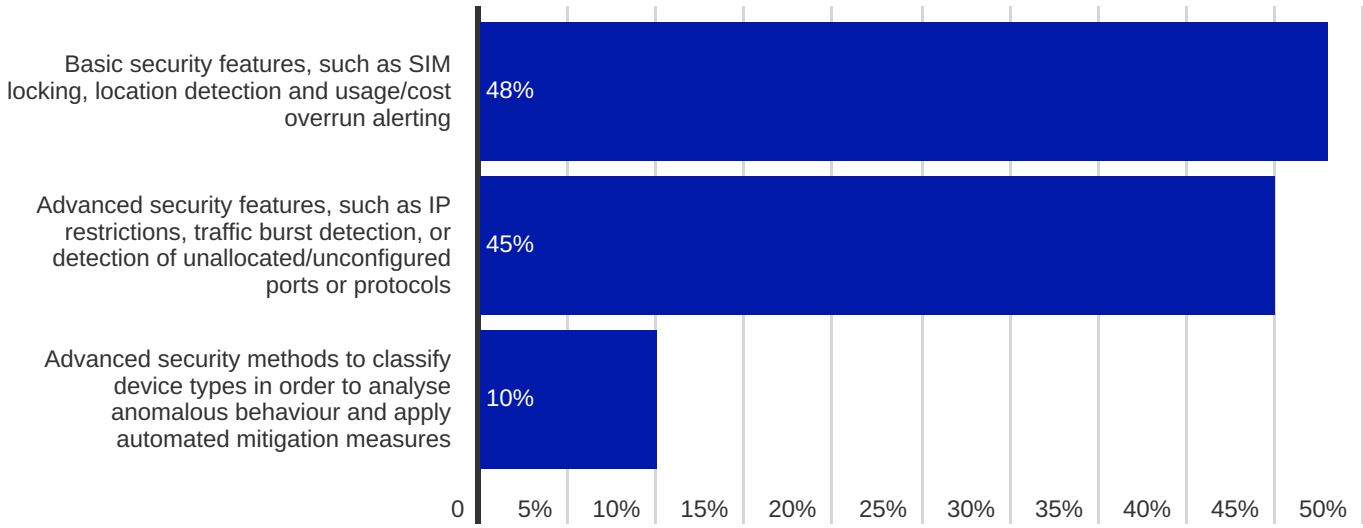
Kaleido Intelligence

In common with several other verticals, **end-to-end security is of considerable importance to cellular IoT adopters as well as cellular IoT non-adopters, with 70% of the former group ranking it as their top priority where IoT connectivity is concerned, compared with 57% of the latter group**. Among cellular IoT adopters, this proportion of respondents should be noted as the second-highest among all verticals analysed in this report, only behind enterprises concerned with healthcare applications and services.

70% cellular IoT adopters ranked end-to-end security as their #1 priority

In this segment, it becomes clear that the connectivity partner role in security is more highly emphasised than in other verticals. **44% of the cellular IoT adopter respondent base reported that more advanced security features**, such as IP restrictions, traffic burst detection, or detection of unallocated or unconfigured ports or protocols should be offered by the connectivity partner, while **25% of cellular IoT non-adopters believe that the connectivity provider's product should incorporate extensive security features as a top 5 priority**, compared with a survey average of 22%. In total, **55% of cellular IoT adopters stated that their connectivity partner should offer advanced or highly advanced security features as part of the overall solution, compared with a survey average of 53%, while a lower-than-average (48%) number of respondents preferred that their connectivity partner only provided basic security capabilities.**

What security features do you expect your cellular IoT connectivity partner to provide? (Cellular IoT adopter responses)



Connectivity security becomes apparent when considering that many manufacturing and industrial enterprises are now migrating from closed-loop SCADA systems to cellular technology. This migration does not diminish the importance of industrial control systems security, and it is clear that CSPs have the potential to play a significant role in ensuring data confidentiality and integrity in order to aid customers avoid the high costs associated with security breaches in industrial environments. The capability to support more advanced security services thus undoubtedly raises the potential for VAS monetisation over and above simple connectivity provisioning.

eSIM - Industrial/Manufacturing

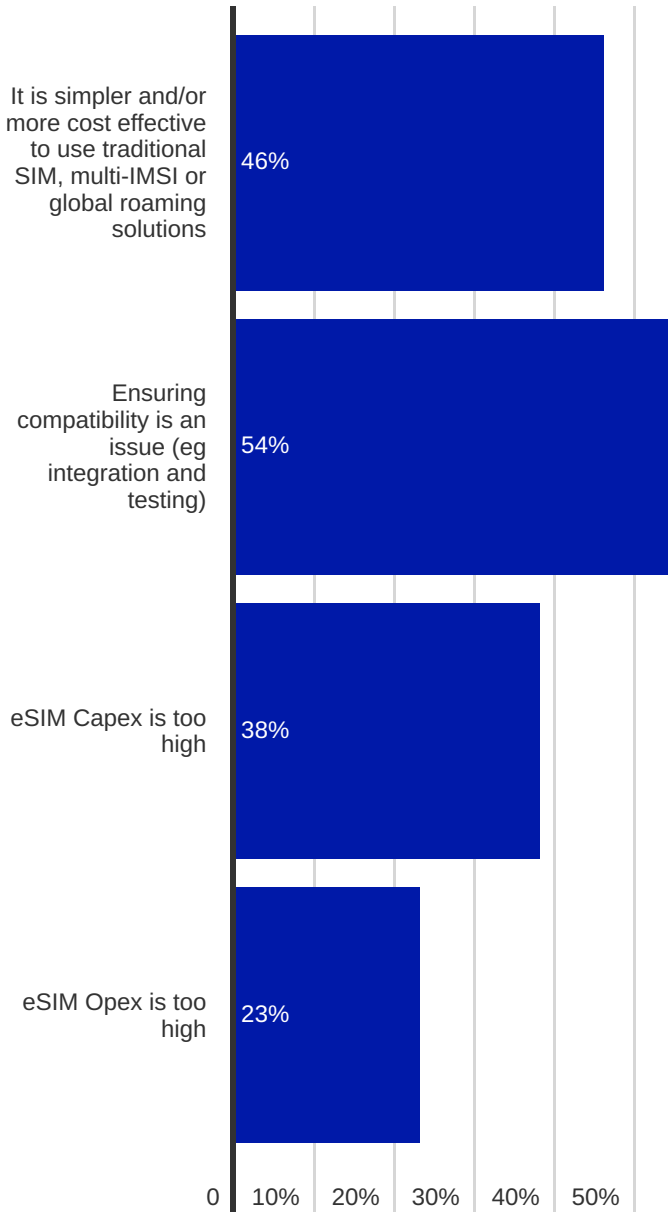
Kaleido Intelligence

eSIM adoption among manufacturing and industrial cellular IoT adopters was reported as slightly lower than the survey average, with **83% of respondents stating that eSIM formed part of their IoT deployment, compared with a survey average of 85%.**

Notably, **eSIM Capex was cited as a significant reason behind not adopting eSIM, with 38% of cellular IoT adopter respondents stating this as a key reason, compared with 27% across all survey respondents.** Capex for eSIM solutions is typically raised for 2 reasons: hardware costs can be elevated due to the increased memory capacity of SIM cards to support the storage of multiple network operator profiles, while setup fees to support the RSP side of the solution are often applicable. Each of these aspects can raise costs by several tens of thousands of dollars over a traditional SIM solution, and has served to dampen eSIM traction among smaller businesses that do not have a significant amount of capital. While it is true that the entry cost for eSIM is normally higher than legacy SIM solutions, it is important for CSPs to note that the total cost of ownership where eSIM is concerned is typically lower than other SIM solutions. In large part, this is due to the guaranteed longevity afforded by eSIM, given that OTA management capabilities allow migration to a new network operator without physically swapping SIM cards. As device fleet sizes increase in volume, these cost savings become even more apparent: however, enterprises are not necessarily aware or willing to consider this long-term benefit. It is thus important to raise this point at the outset of any negotiations where connectivity is expected to be required for a number of years.

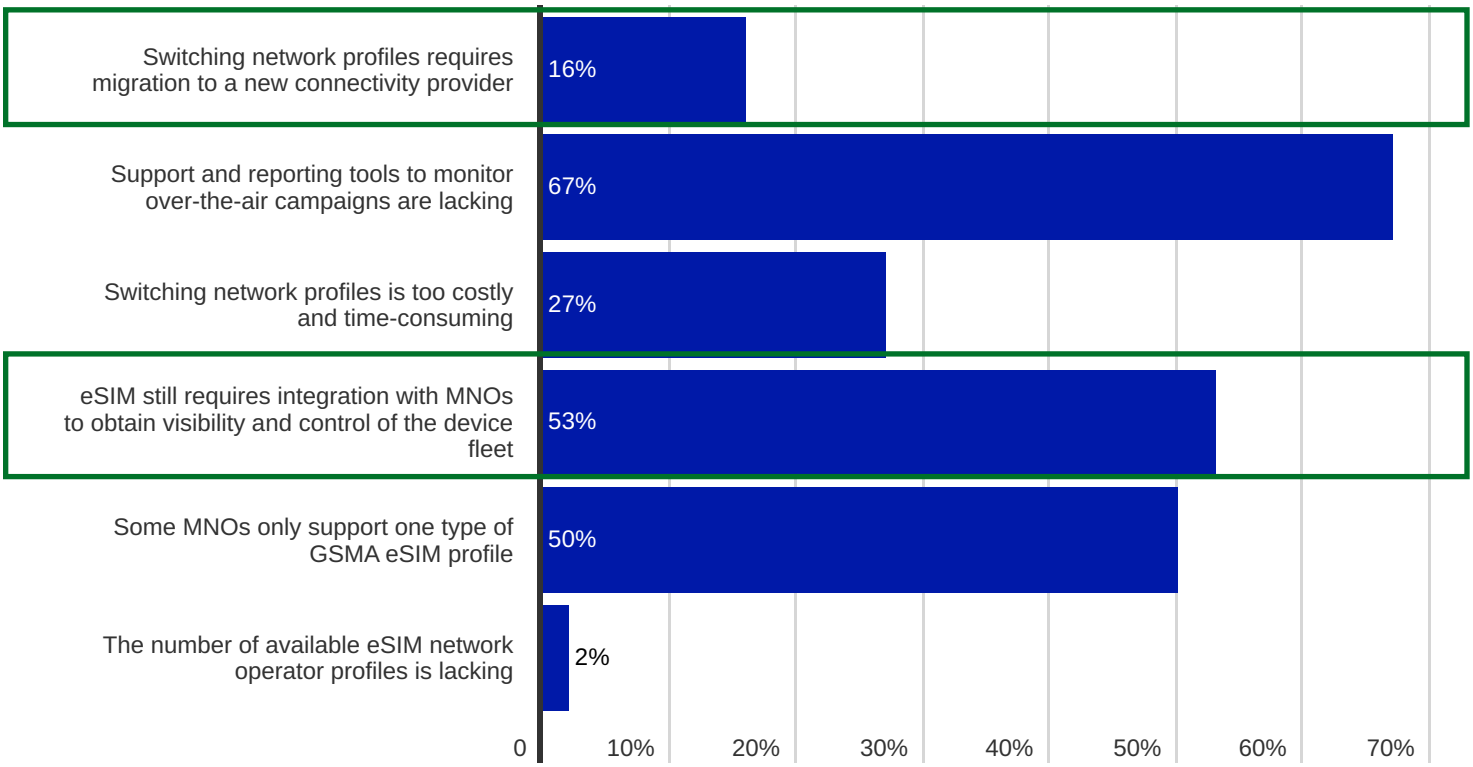
It should also be highlighted that eSIM does not necessarily have to be deployed as a standalone technology: it has been, and is, commonly combined with other technical solutions that allow cost or performance optimisation of the fleet without incurring many of the costs associated with physical SIM swaps or Opex-based charges associated with eSIM OTA campaign transactions.

Why have you chosen not to use eSIM (eUICC)? (Cellular IoT adopter responses)



Meanwhile, **16% of eSIM adopters stated that they had concerns over the fact that swapping eSIM network operator profiles requires migration to a new connectivity provider, compared with a survey average of 13%.** While this may be the case for many MNOs and some IoT MVNOs, there are several players on the market in the latter group that incorporate a library of eSIM profiles that devices on their platform can switch to without the customer having to migrate that portion of the fleet to a new provider. This capability highlights an exceptional level of flexibility on the market, particularly when multi-IMSI technology is combined with the overall solution: these eSIM profile libraries typically incorporate profiles for use in markets where roaming is challenging in some form or another, allowing customers to localise connectivity and bypass roaming altogether. Multi-IMSI is used alongside eSIM to deliver optimisations in terms of costs, or even performance, depending on customer requirements, and the fact that many MNOs are now willing to participate in the wholesale market through the sale of IMSI ranges or eSIM profiles means that the flexibility afforded by this type of combined solution is rapidly increasing in scope.

What are your main issues with your current eSIM (eUICC) solution? (Cellular IoT adopter responses)



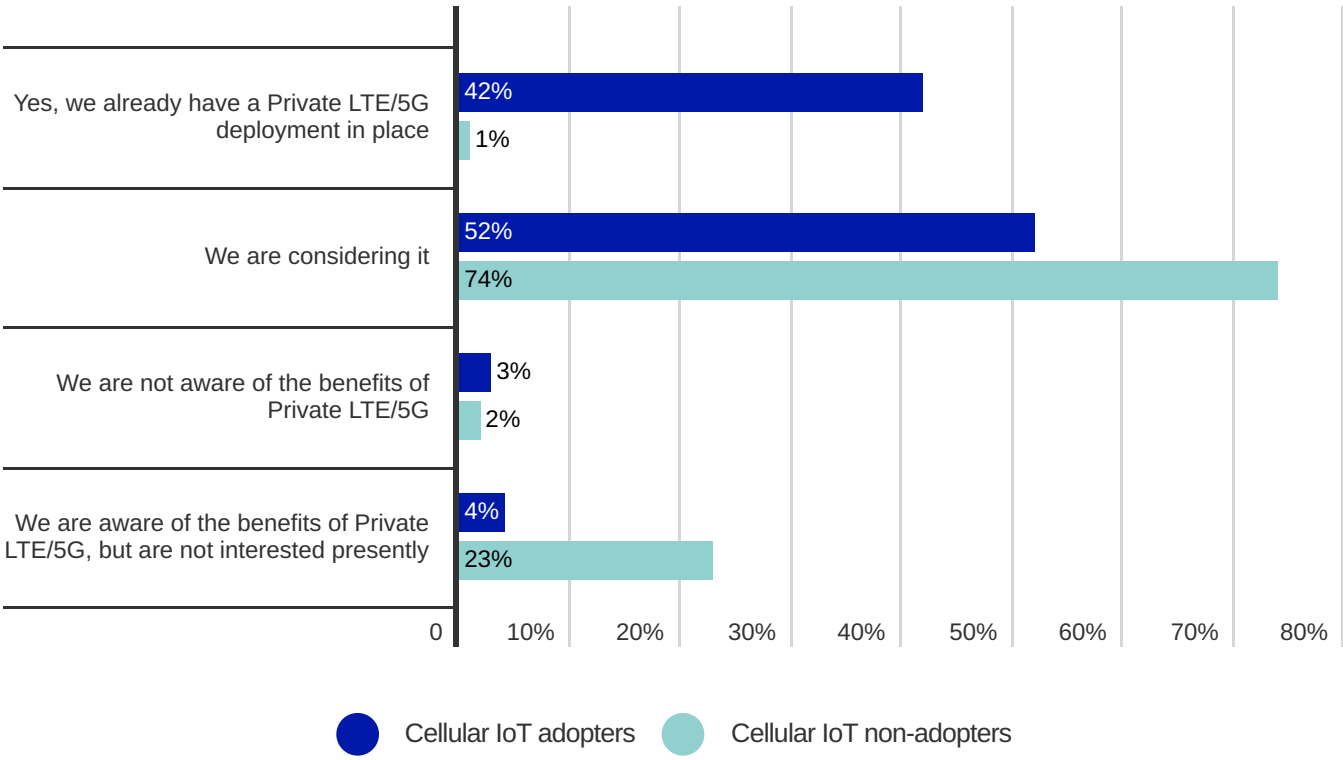
Notably, **53% of respondents reported that eSIM still requires integration with Mobile Network Operators to obtain visibility and control of the device fleet.** When considering the fact that when eSIM is used to download and operate a local operator profile, this inevitably becomes a point of concern if the CSP wishes to support ongoing management of devices that have migrated away from the original network profile. However, in similar fashion to the issue of robust support for global IoT deployments, many CSPs have secured integrations with operator networks to facilitate this kind of functionality. It is thus once again important that potential connectivity partners are transparent with prospective clients in terms of the level of support that they are able to offer via their eSIM solution, and to establish what level of local profile use will be required by clients and if these expectations can be met.

Private LTE/5G - Industrial/Manufacturing

Kaleido Intelligence

Among cellular IoT adopting enterprises, private LTE and 5G adoption was reported as highest across all verticals analysed in this research report, with **42% of survey respondents stating that they had a private cellular network deployment. Additionally, 52% of the respondent base reported that they were considering private LTE or 5G for future operations enhancement. Among cellular IoT non-adopters, those that are considering deploying private LTE or 5G is significantly higher (74%) than the survey average (69%).**

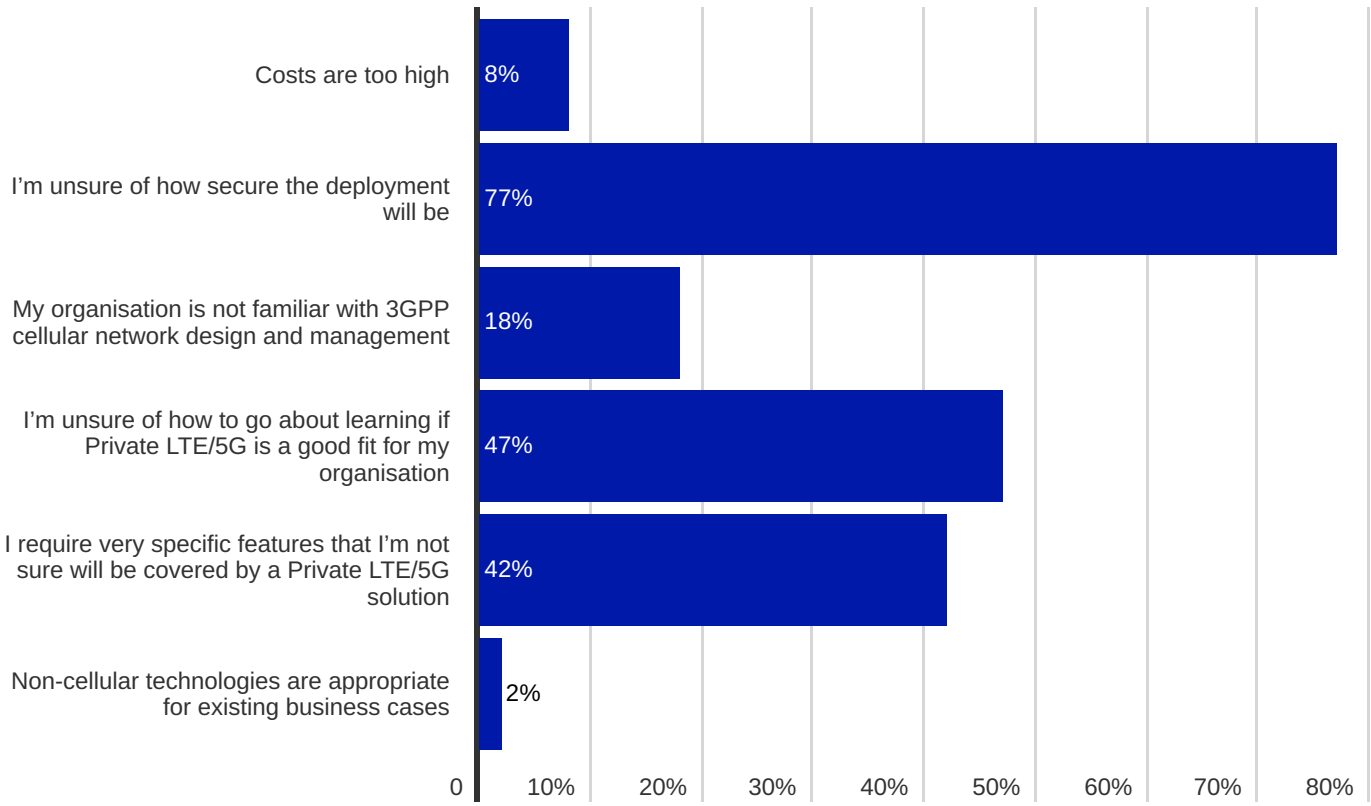
Does your business unit have an interest in Private LTE/5G to enhance business operations? (All respondents)



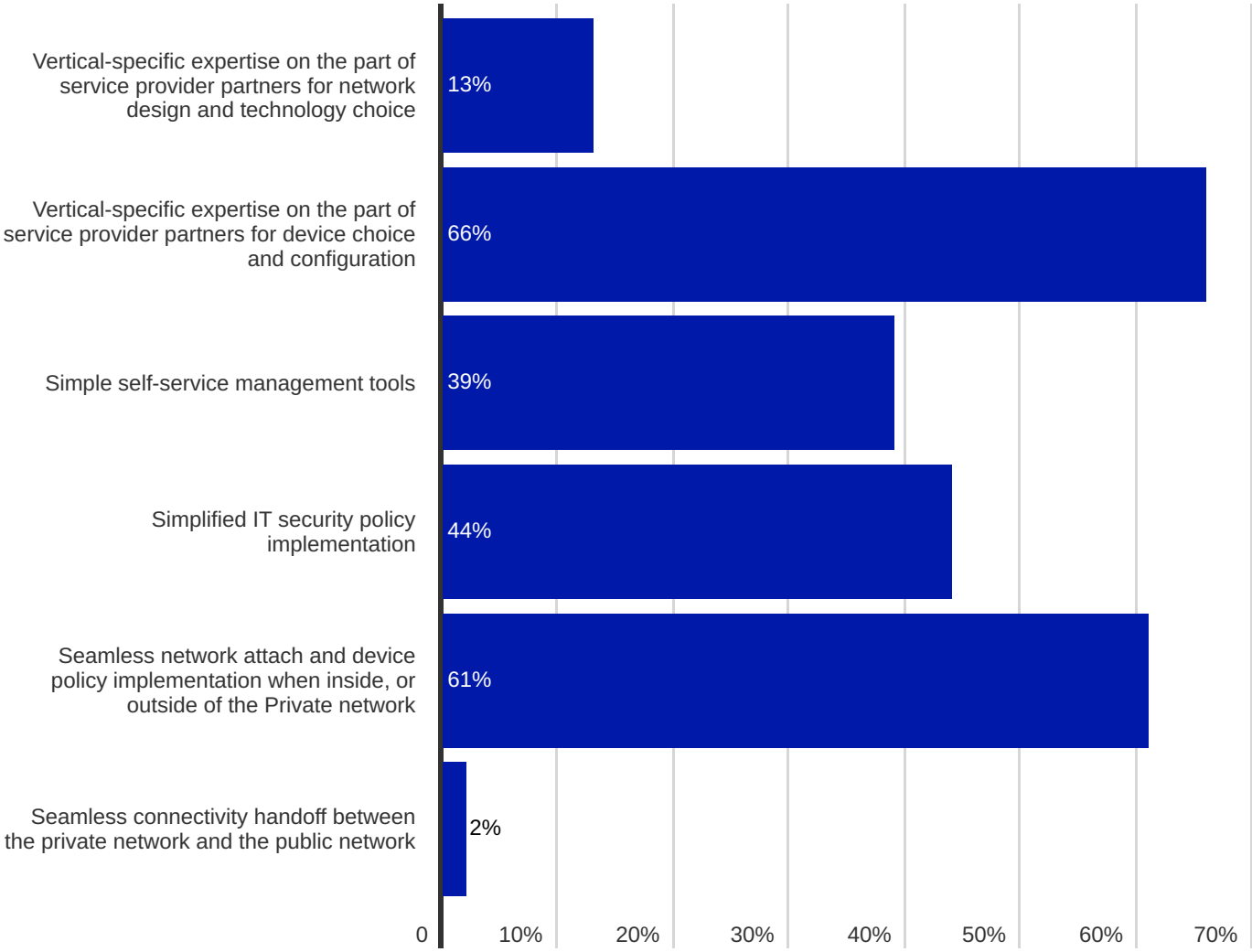
The release of dedicated enterprise spectrum and access processes across several countries worldwide has catalysed the market for private cellular network adoption in this segment. Germany, the US, the UK and Japan in particular have seen considerable interest from industrial clients due to the relatively simple processes involved in accessing spectrum. Meanwhile, the fact that 5G network slicing has failed to emerge commercially in a timely fashion has driven many impatient industrial companies to seek alternative solutions, with those companies inevitably landing on potential private LTE or 5G solutions. In addition to this, we have seen earlier how Wi-Fi and Ethernet remain in common use on factory floors, with each of those connectivity technologies carrying significant compromises in terms of flexibility or reliability. In particular, 5G is viewed as a core technology to replace both Wi-Fi and Ethernet, owing to its wireless capability, capacity to support millions of devices within a small coverage zone, and support for features such as ultra-low latency and centimetre-level asset positioning accuracy.

The nature of industrial and manufacturing use cases means that connectivity, particularly in the case of device OEMs, will be required both at the production site in addition to the eventual country the device is shipped to. This means that CSP capabilities must extend to provisioning and management of connectivity both for private network sites as well as public networks. Typically, this will be achieved through hybrid private network architecture, with dedicated private radio (or potentially public radio infrastructure) deployed in conjunction with globally distributed core network infrastructure. In some cases, enterprises are likely to deploy more than one private network site, and require that the sites are interconnected to facilitate information sharing. With some **77% of enterprises in this segment citing concerns over the overall security of private LTE or 5G (compared with a survey average of 67%)**, it is clear that enterprises are unsure as to how effectively traffic security can be maintained in 'roam in, roam out' or multi-site interconnect scenarios. Indeed, **61% of respondents stated that seamless network attach and device policy implementation when inside or moving outside of the private network zone was one of the most important factors for private LTE or 5G consideration.**

What are your main concerns over a potential Private LTE/5G deployment? (Cellular IoT non-adopter responses)



What are the most important factors for consideration where Private LTE/5G is concerned? (Cellular IoT adopter responses)



Enterprises must be assured of the security of private LTE or 5G networks. It is thus important to underline the security of hybrid architectures by educating enterprises on how user plane data can be kept securely within the private network zone, while solutions such as secure IPX routes can ensure that any data that is routed between the public and private network is kept away from the public Internet, thus ensuring a high level of data confidentiality. For CSPs, the selection of best-in-class providers to deliver this aspect of the solution will be a critical factor in convincing enterprises of the overall security of the solution. Meanwhile, CSPs must work closely with potential clients to help them understand how security policies can be managed and implemented across different coverage footprints.

Internet of Cranes® Provides Intelligent Control Through Real-Time Data

A leading manufacturer of articulated and hydraulic cranes, Fassi Gru has customers all over the globe and the ability to produce 12,000 cranes on average per year. As a pioneer in its sector, it has always sought to create innovative services to support operators. In 2015 Fassi began developing a unique system that would take advantage of IoT technology to provide intelligent control for the remote management of cranes, by making all information related to operation, performance, and status available in real-time.
The goal of the system – christened the Internet of Cranes® (IoC) – was to enable operators to create manufacturing and operational efficiencies and improve crane performance. Remote access to vital data would enable rapid response diagnosis and assistance, from either the operator or the Fassi support team, and swift resolution of malfunctions.

Fassi Gru needed hardware and connectivity expertise to bring this dedicated IoT system to life, so turned to cellular connectivity specialist, Eseye, and IoT solutions provider, Micro Systems, for design, development, and deployment support.

Open dialogue between operator and crane

Fassi's vision for its IoC system was that operators should have up-to-the-minute data at their fingertips, and the ability to rely on a permanently active assistance service. This required constant, dependable internet connectivity.

This was a challenge: Fassi has customers in all corners of the world, and its cranes are operating in myriad demanding operational environments. When the IoC project was initiated, cellular coverage was fragmented across the globe – with a mix of 2G and 3G networks, and carriers using a range of communication frequencies. The network management task involved would be monumental.
Fassi needed to find a reliable, ubiquitous connectivity solution with a single IoT data gateway and a single eSIM card that would streamline operational processes and enable its cranes to communicate wherever they were deployed in the world. In addition to simplifying device management, this would allow it to standardize on one IoT board instead of having to manufacture several regional versions.

Seamless global cellular connectivity

A long-term systems integrator partner of Eseye, Micro Systems partnered with Eseye to take advantage of its **AnyNet+ eSIM cards with multi-IMSI and advanced eUICC technology** to deliver the universal connectivity required to operate Fassi's IoC system to its full potential, through a single device. **Combining localization and roaming partners, Eseye has access to over 700+ networks, and holds roaming contracts with all of the world's major mobile phone operators covering 190 countries.**

Eseye's AnyNet Federation global mobile network alliance allows it to offer the widest range of interconnects and provide the most comprehensive eSIM localization strategy in the IoT market today. This grants the AnyNet eSIM the unique ability to connect directly and automatically to the best available network and avoid permanent roaming, data sovereignty and regulatory issues.

The bespoke electronic board designed by Micro Systems is fitted with a Thales Cinterion UMTS 2G/3G cellular module with GPS, which is connected to the web by Eseye's AnyNet eSIM. The SIM is installed directly on the board during the production phase resulting in a single SKU that can be easily activated by the end customer when required.

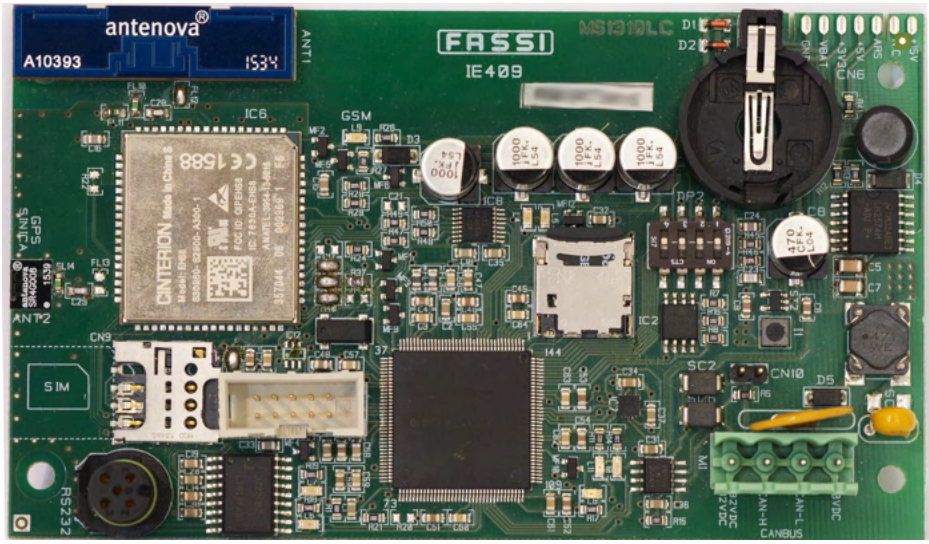
The board also has an integrated shock detection sensor via accelerometer, as well as an SD card for storage of firmware updates and software update of the crane control unit. The board control software collects data from the crane's control unit, interfacing via CAN (control area network) communication, then transmits it to the AWS data cloud server. The cloud server collects and securely stores data from the entire Fassi machine fleet around the world.

"With the Internet of Cranes project, we wanted to propose a product innovation that moves towards a service logic that actively involves crane operators during the support phase of their machines. Fassi Gru was the first company in the world to develop a remote diagnostics solution, by connecting the articulated cranes to our technical assistance via the internet."- Roberto Signori, R&D SPE Manager, Fassi Gru

A dedicated web portal allows operators and the Fassi support centre to view and manage the data from each crane. The integration of Eseye's Infinity IoT Platform™ allows the operator and Fassi to monitor eSIMs in a single virtual space – including details on the activation/suspension date, phone number, monthly traffic and location. Eseye provided device onboarding services and rigorous connectivity testing to ensure Fassi's IoC system could be deployed, managed, and supported successfully.

Optimized operation across the entire fleet

Through the development of its Internet of Cranes, Fassi Gru has been able to offer operators around the world an exceptional value-add service that enables them to monitor their machines remotely, in real-time.



Benefits include:

Improved performance and uptime

Immediate access to usage statistics brings operators a more accurate knowledge of their machines, with a full understanding of how they're being used, how they're performing, and their condition.

The availability of detailed usage data supports predictive maintenance and estimate of residual life, as well as the planning of scheduled maintenance. Fassi's support team can monitor cranes during operation on request, to provide rapid remote diagnosis and assistance to resolve breakdowns and malfunctions.

Greater efficiency

Operators have been able to move from a scenario where maintenance was carried out in person by technicians to one where information is verified and managed remotely by a single operator.

More precise control

Operators can remotely set and modify crane parameters, such as the electronic moment limiter, and monitor safety. Real-time tracking of a crane's position means they can pinpoint its location in case of theft.

Low technical burden and simplified operations

For the end customer, no configuration of the AnyNet SIM is required – they simply activate connectivity when they start using the IoC service. The fully GSMA compliant AnyNet SIM has a single SKU code, making it easier for Fassi to track inventory and deploy its IoC in all territories.

IoT Connectivity Challenges & Opportunities: Smart Cities

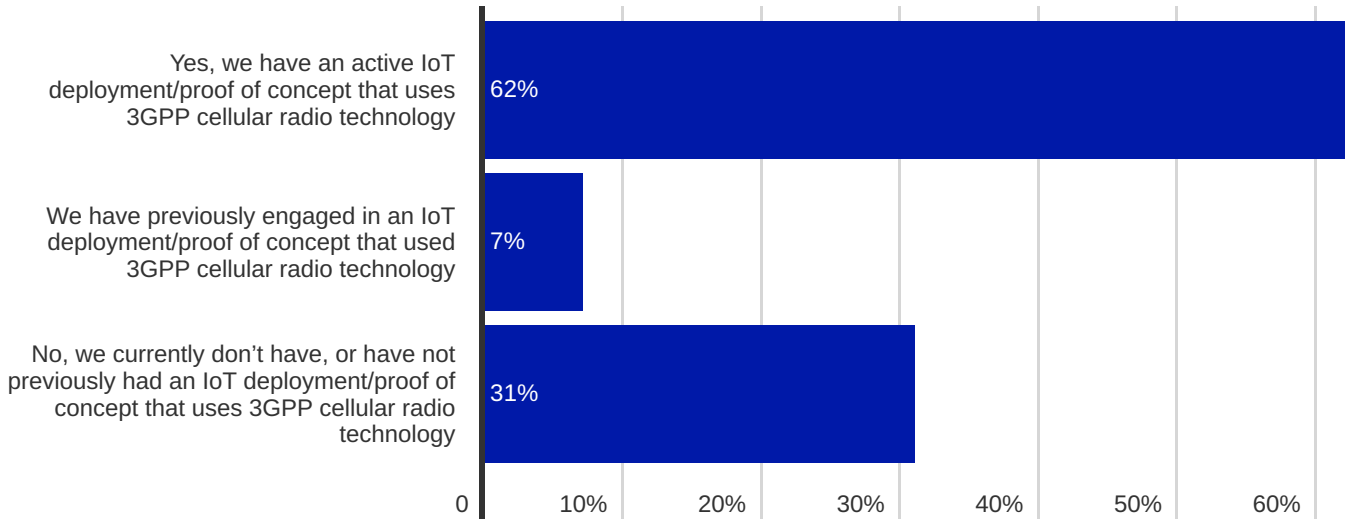
eseye iBASIS KORE TRUPHONE flo. LIVE

State of IoT - Smart Cities

Kaleido Intelligence

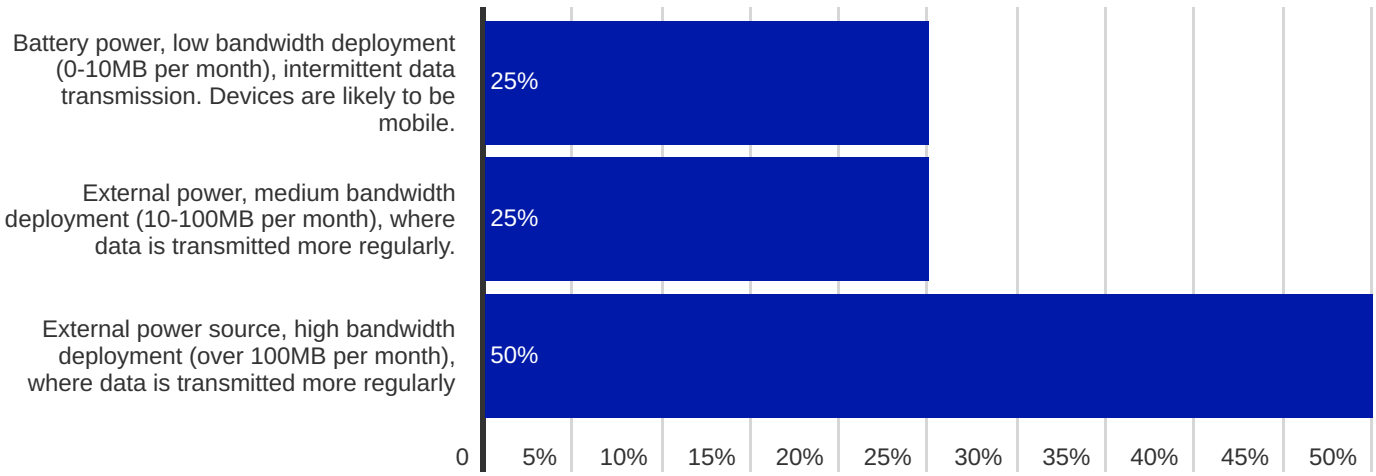
Enterprises in the smart cities segment reported the highest levels of cellular IoT adoption overall within the survey respondent base, with some **69% of respondents stating they had an active or previous cellular IoT deployment.** Nevertheless, **only 12% of those who had not adopted cellular IoT stated their intention to deploy IoT using cellular technology over the next 12-24 months.** Indeed, **when respondents were queried over which alternative technologies they viewed as viable for IoT deployments, SIGFOX and LoRaWAN saw 42% and 36% of the vote, respectively, with Wi-Fi counted as viable by 64% of respondents.**

Does your business unit currently have an IoT deployment or proof-of-concept underway that uses 3GPP cellular radio technology (2G/3G/LTE/5G)? (All responses)



12% intend to deploy cellular IoT in the next 12-24 months

What type of cellular IoT deployment is this likely to be? (Cellular IoT non-adopter responses)



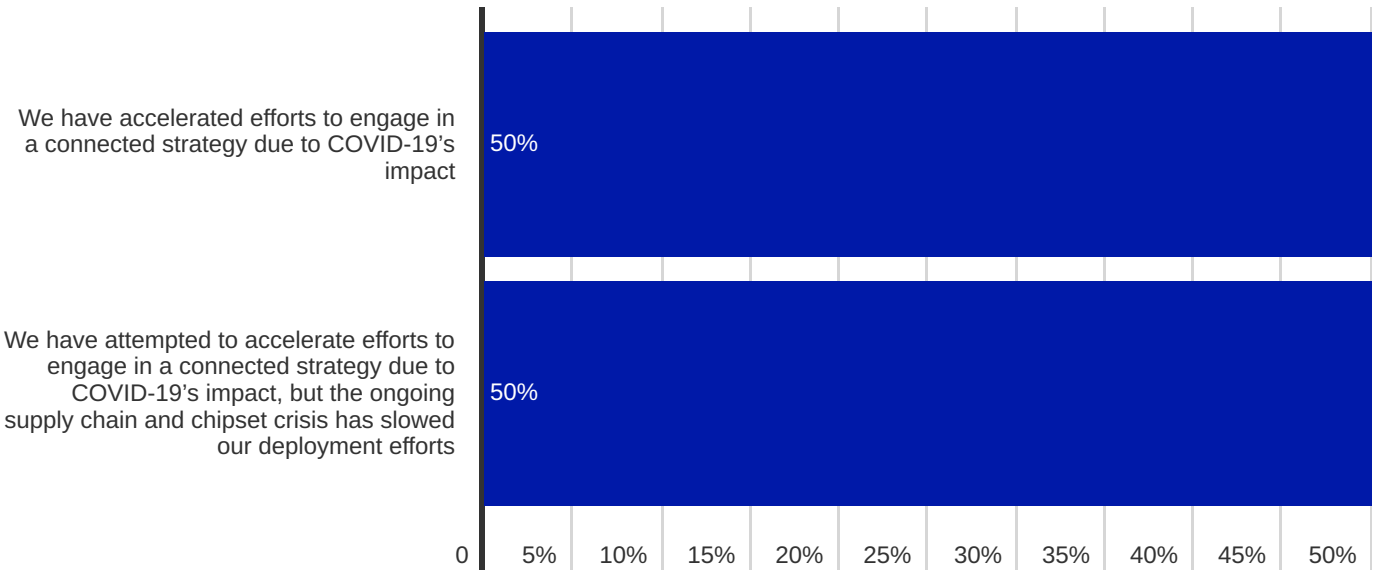
eseye iBASIS KORE TRUPHONE flo. LIVE

Despite several technical compromises, the technologies cited above are typically associated with lower deployment and operational costs, which may be a factor in reduced demand for cellular connectivity. Nevertheless, it is notable that SIGFOX has recently experienced considerable financial difficulties, and does not have the broad support of over a thousand network operators, as is the case with cellular technology. Meanwhile, LoRaWAN and Wi-Fi have particular issues with scaling and coverage, respectively, although this may be less of an issue when considering the overall connectivity requirements for a smart city deployment. Most notably, **among respondents that do intend to deploy cellular IoT in the near term, a significant majority (50%) stated that they would be aiming to leverage devices that consume considerable bandwidth; this is a significant divergence from the survey average of 7%.**

This result undoubtedly points to applications related to public safety and monitoring, where video content is often used in public spaces and at traffic intersections. Emergency services across the globe are increasingly using high-bandwidth devices, such as body-worn cameras for transparency purposes; meanwhile, issues with congestion have led to demand for video-monitored traffic routes and parking zones to facilitate smart traffic applications.

Within the smart cities space, COVID-19 was cited as a significant reason behind accelerated IoT connectivity rollouts, with **50% of the respondent base reporting the pandemic had accelerated efforts to engage in a connected strategy. This proportion is considerably higher than the survey average of 32%** and is likely related to worldwide efforts to improve transport infrastructure and municipal services to aid in COVID-19 compliance requirements. **An additional 50% of the respondent base reported that they had attempted to accelerate efforts to engage in a connected strategy due to COVID-19's impact, but the ongoing supply chain and chipset crisis has slowed deployment efforts.**

What type of cellular IoT deployment is this likely to be? (Cellular IoT non-adopter responses)



Complexity - Smart Cities

Kaleido Intelligence

Overwhelmingly, **100% of cellular IoT non-adopters stated that hardware design complexity was the top barrier to cellular IoT connectivity**. The various radio standards available to support device communications, certification and testing requirements have evidently led to significant perceived challenges that industry actors must help address: as stated earlier, connectivity choice now often forms part of the early device design consideration process, and it is clear that CSPs have an opportunity to engage with potential customers at this early stage to help with technical decisions for rollouts. This may be facilitated by providers that are able to directly supply hardware in addition to connectivity solutions: 75% of cellular IoT non-adopter respondents reported that this is the second most important factor for consideration where cellular IoT connectivity is concerned. Indeed, the ability to combine hardware and connectivity expertise should be viewed as a differentiating factor across most IoT verticals, and not only smart cities. Being able to draw on this type of expertise not only aids in the device development process, but also allows providers to expedite support capabilities in instances where issues are encountered either with the device or SIM connectivity. Many device OEMs on the market are now looking to resell CSP connectivity solutions as part of their offering, and as such, there is an opportunity for close partnerships to be developed between connectivity providers and OEMs, where a strong relationship is likely to deliver obvious benefits for the customer.

Further emphasis on this hypothesis is brought about by the fact that t**he need for domain expertise to aid in management and optimisation, in addition to consulting services to aid in device design and project deployment, were ranked third and fourth in terms of importance for an IoT connectivity partner's capabilities among those which have not yet adopted cellular IoT, respectively**. Undoubtedly, the ecosystem presents a confusing landscape for enterprises that can only be solved through early-stage, expert guidance.

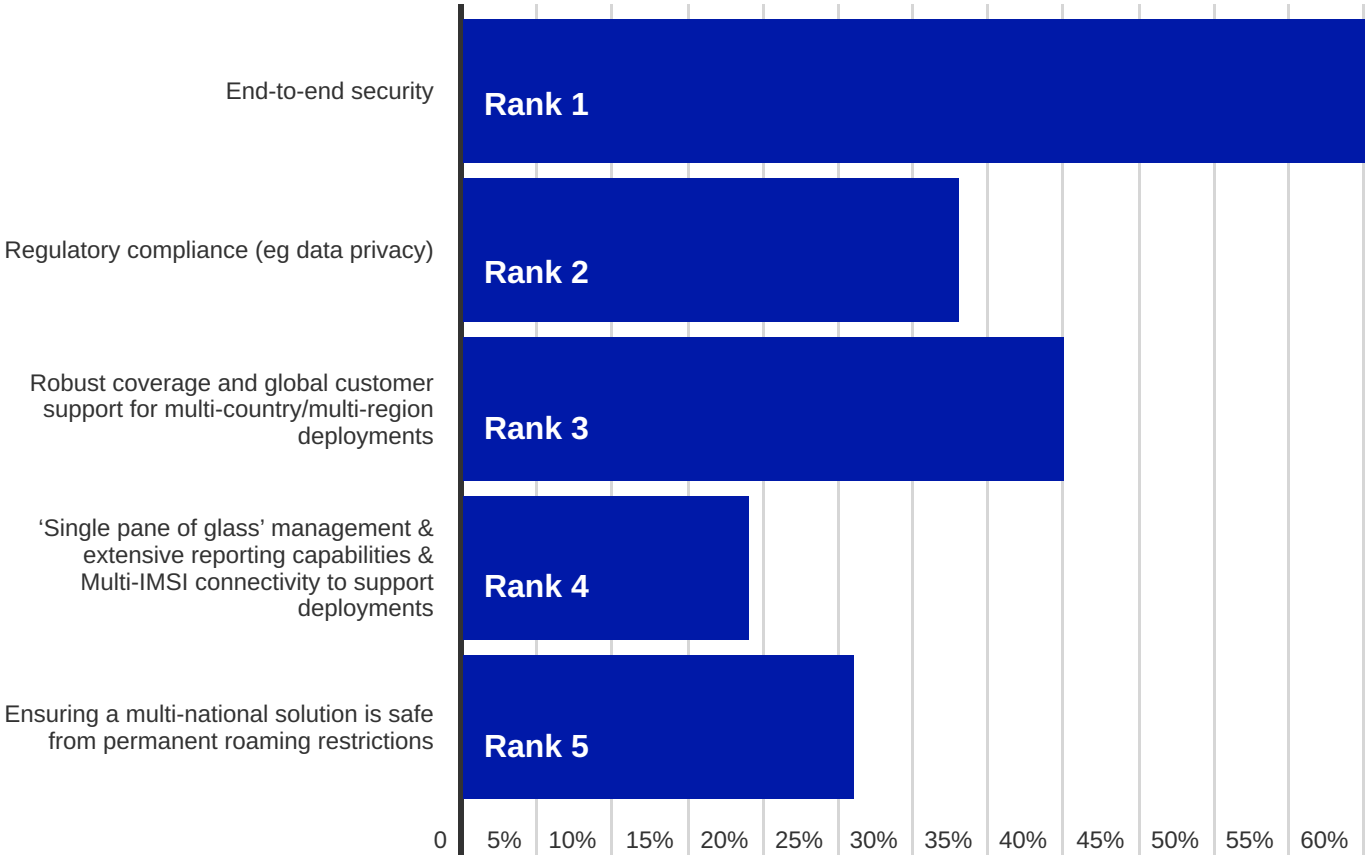
In common with several other verticals, **the need to engage with several disparate connectivity partners for deployments is viewed as a major challenge, with 63% of cellular IoT adopters** believing this to be the case. The need to avoid this type of complexity is reflected in the fact that **75% of cellular IoT non-adopters believe that connectivity partners must have an extensive set of mobile network operator partnerships as a number one priority.**

75% cellular IoT non-adopters ranked an extensive set of MNO partners as a top CSP requirement

63% cellular IoT adopters view multi-operator connectivity contracts as highly disruptive to scale

eseye iBASIS KORE TRUPHONE flo. LIVE

What are your top 5 factors that are most important where cellular IoT connectivity is concerned? (Cellular IoT adopter responses)



Meanwhile, **global coverage and support for international deployments featured strongly as challenges towards cellular IoT, with 40% of cellular IoT adopters citing this as the third most important factor for cellular IoT consideration, compared with a survey average of 34%. Among cellular IoT non-adopters, this issue was listed as the second-highest priority, with 25% of respondents in agreement.**

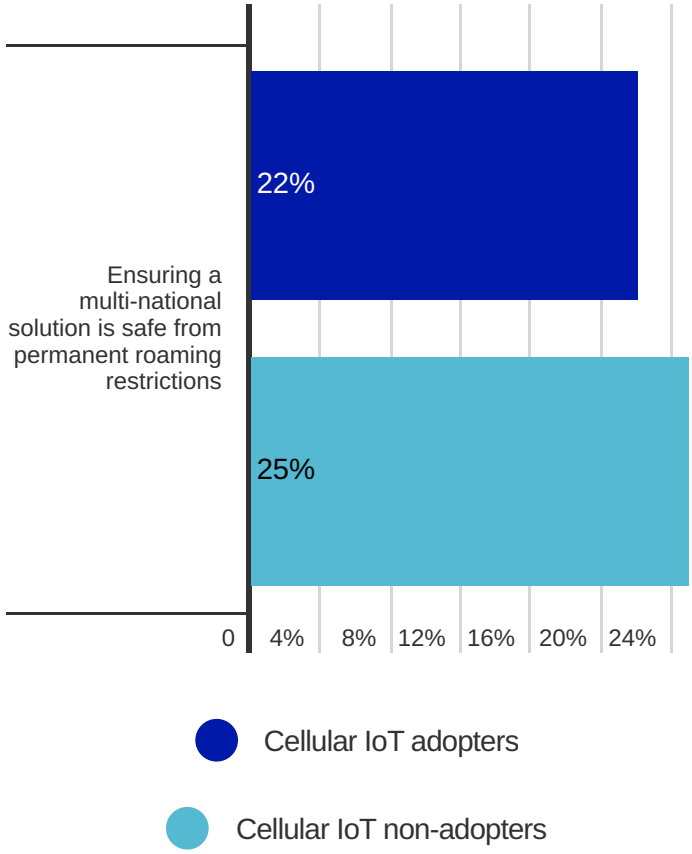
Roaming - Smart Cities

Kaleido Intelligence

The survey results highlight that concerns over permanent roaming are diminished compared to other verticals. When the most important factor for IoT connectivity is examined, **only 25% of cellular IoT non-adopters ranked permanent roaming as the most important, with this falling to 22% of respondents where cellular IoT adopters are concerned.**

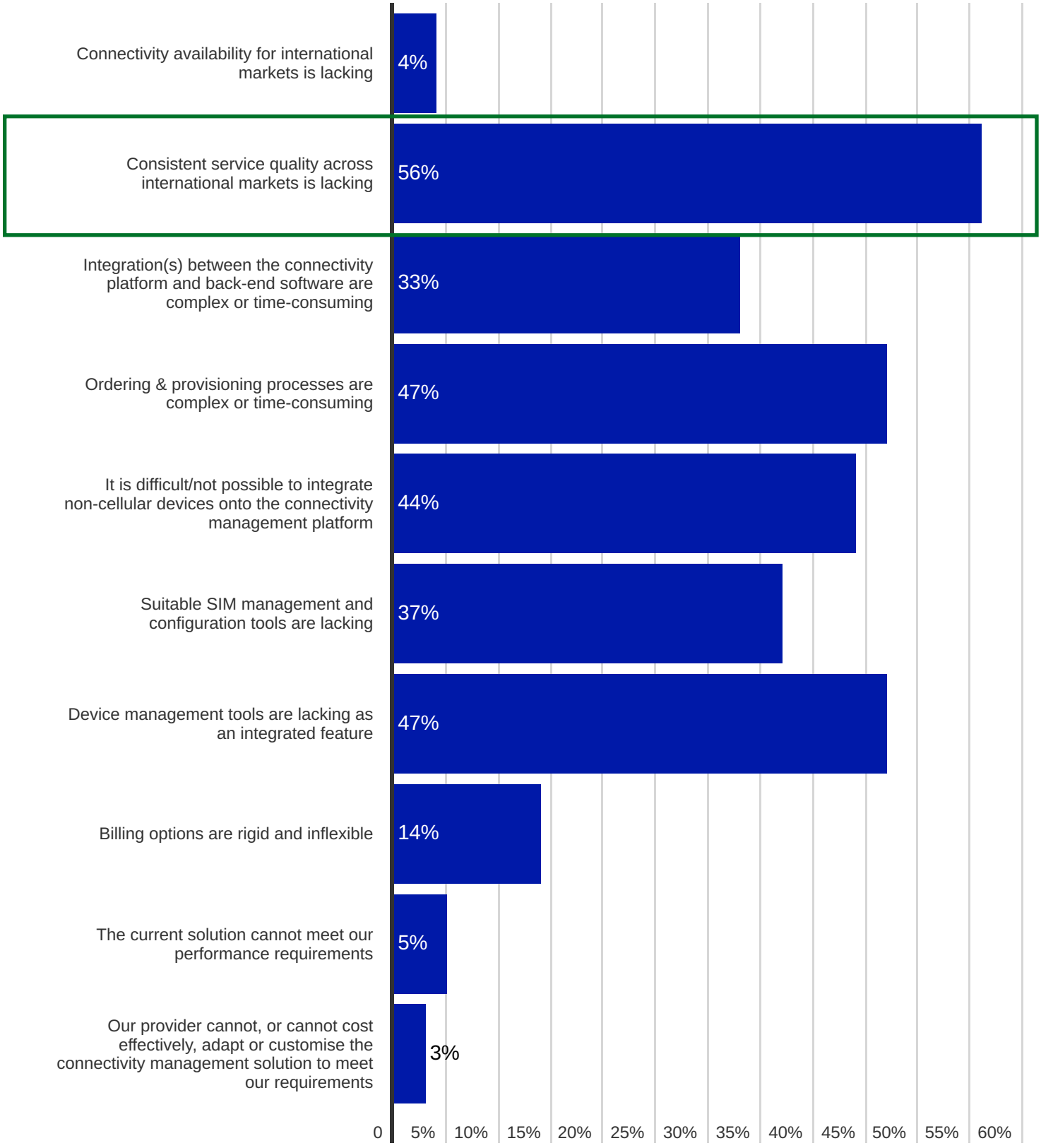
In part, this may relate to the fact that smart city projects often arise as a result of local tenders, with clarity provided in terms of the connectivity and coverage requirements for devices. In turn, this means that a local connectivity partner is selected for coverage, despite creating challenges in terms of contractual relationships, as highlighted earlier. In addition to this, some smart city deployments rely on technologies such as NB-IoT and LTE-M which have poor international support in terms of roaming and power-saving feature compatibility. Globally, only around 25% of international roaming agreements for these technologies incorporate features that allow very low power modes, aimed at considerably increasing the lifespan of battery-operated devices. These 2 factors combined mean that up **until now, the majority of NB-IoT and LTE-M deployments have been in partnership with local connectivity providers rather than operating in roaming scenarios. Indeed, this lack of international support was cited as the third most important challenge for IoT connectivity among those that had not adopted cellular IoT, with 50% of the respondent base in agreement. This is considerably higher than the survey average of 14% that assigned this challenge to this rank.**

What are your top 5 factors that are most important where IoT connectivity is concerned? (Rank 1 response strength)



The lack of roaming support for certain radio technologies in addition to the perceived general state of international IoT roaming, means that **56% of cellular IoT adopters reported that a consistent level of service quality was lacking across international markets.**

What are your biggest issues with your current cellular IoT connectivity solution? (Cellular IoT adopter responses)



It is clear from these results that CSPs aiming to deliver against enterprise customer expectations within this sector must place heavy emphasis on expanding roaming coverage for NB-IoT and LTE-M (incorporating power-save modes as part of IR.21 agreements), while additionally promoting capabilities to offer flexible and consistent support and service via their solutions.

Security - Smart Cities

Kaleido Intelligence

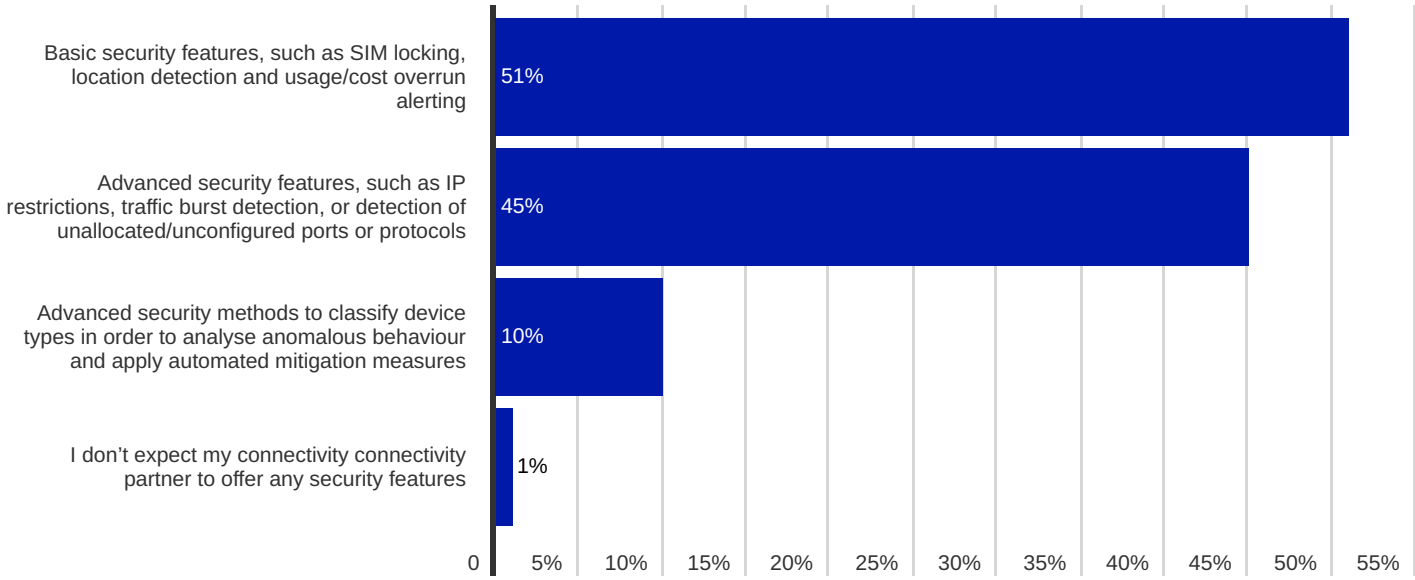
While end-to-end security is viewed as a top priority for cellular IoT adopters in this segment, **only 60% of the respondent base reported this as the main factor for consideration where connectivity is concerned**, which is markedly lower than all other verticals save for energy and utilities. Additionally, **only 50% of cellular IoT non-adopters ranked end-to-end security as the leading factor for consideration in the context of IoT connectivity, compared to a survey average of 55%**. These results are considered as somewhat unexpected, given the fact that connectivity for smart city applications often involves municipal infrastructure and thus, in some instances, may have some potential impact on the safety of citizens in the city.

60% cellular IoT adopters ranked end-to-end security as a #1 priority

33% cellular IoT adopters ranked data compliance as a #2 priority

However, when examining the results more deeply, it should be noted that **cellular IoT adopters in this segment are additionally heavily concerned with data compliance concerns, with 33% of the respondent base naming this as the second most important factor for cellular IoT connectivity.** In part, ensuring that data compliance requirements are met forms a part of the overall security consideration of the solution, given the fact that cybersecurity data breaches could compromise sensitive personal information. These results indicate that CSPs would benefit from being able to offer enhanced security solutions, such as IoT SAFE, or some similar solution to guarantee end-to-end data integrity between devices and supporting software back-end platforms.

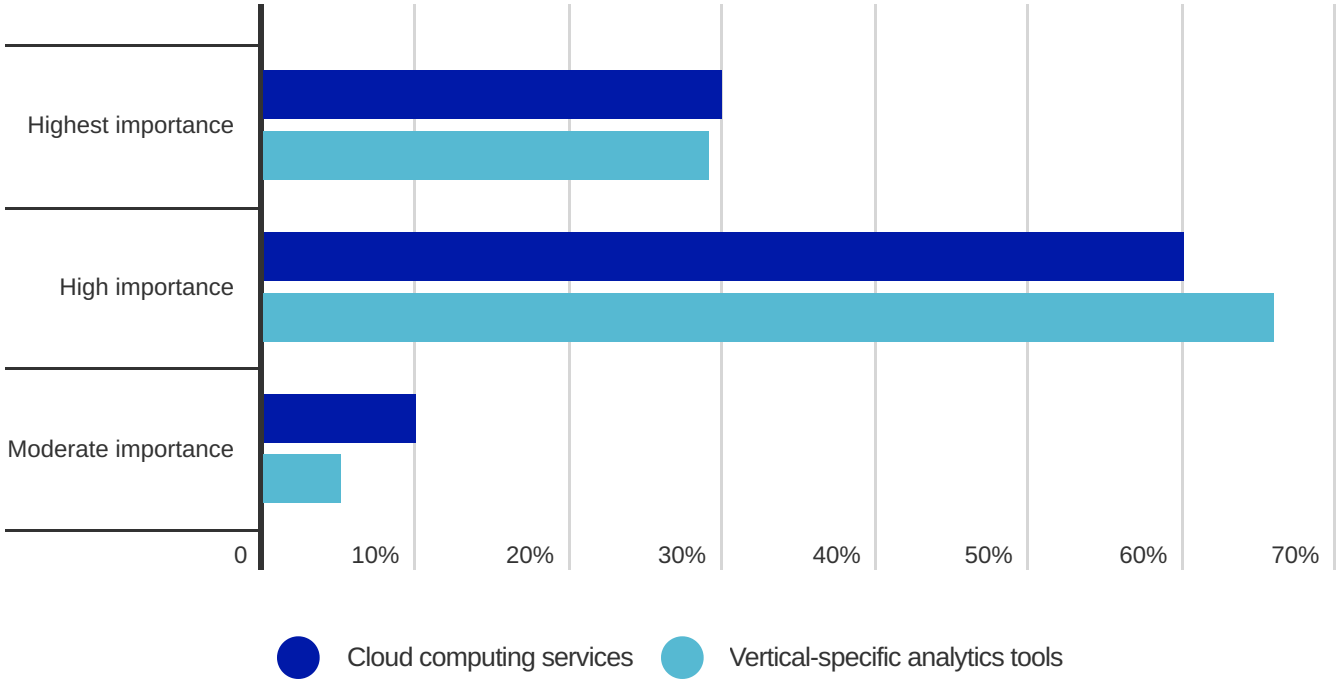
What security features do you expect your cellular IoT connectivity partner to provide?(Cellular IoT adopter responses)



eseye iBASIS KORE TRUPHONE flo. LIVE

In addition to solutions such as IoT SAFE, it is apparent that enterprises in the smart city segment value-enhanced security services from their connectivity provider. In this context, **45% of cellular IoT adopters stated that they valued their connectivity partner offering more advanced security services, such as traffic burst detection and attempts to access unusual ports or IP addresses.** This proportion represents the highest of all verticals analysed in this study, and underlines that smart city customers are likely to place a high value on security VAS to a greater extent than the majority of other verticals. Given the fact that **smart cities cellular IoT adopters reported high levels of amenability towards pre-integrated cloud services (60% believing this to be of high importance) as well as vertical-specific analytics tools to supplement the connectivity offering (66% stating this is of high importance)**, one can infer that there are opportunities to develop solution-based offerings that incorporate hardware and connectivity bundling as discussed earlier, in addition to a comprehensive set of cloud, security and analytics tools. Although this type of end-to-end offering is out of scope for many connectivity service providers, a focus on at least one of these VAS elements undoubtedly provides upsell opportunities beyond simple connectivity provision.

How important is it that your cellular connectivity solution provider offers integration with the following tools/services out-of-the-box? (Cellular IoT adopter responses)

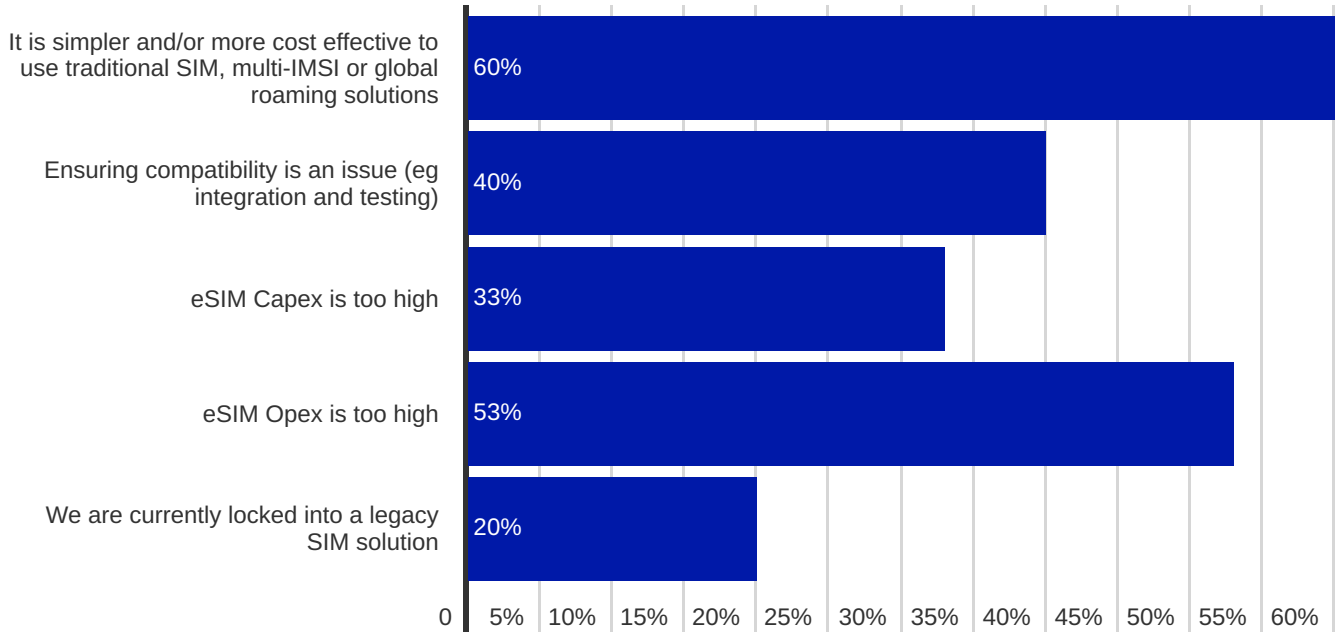


eSIM – Smart Cities

Kaleido Intelligence

eSIM adoption as part of cellular IoT deployments in this vertical was the lowest recorded among the verticals surveyed, with some **79% of cellular IoT adopters stating that eSIM forms part of the device fleet; this proportion is markedly lower than the survey average of 85%.** The results show that there is an ongoing perception among enterprises in the smart cities segment that t**raditional SIM solutions are either simpler or more cost-effective to deploy: this was reported by 60% of respondents, and is considerably higher than all other verticals.**

Why have you chosen not to use eSIM (eUICC)? (Cellular IoT adopter responses)

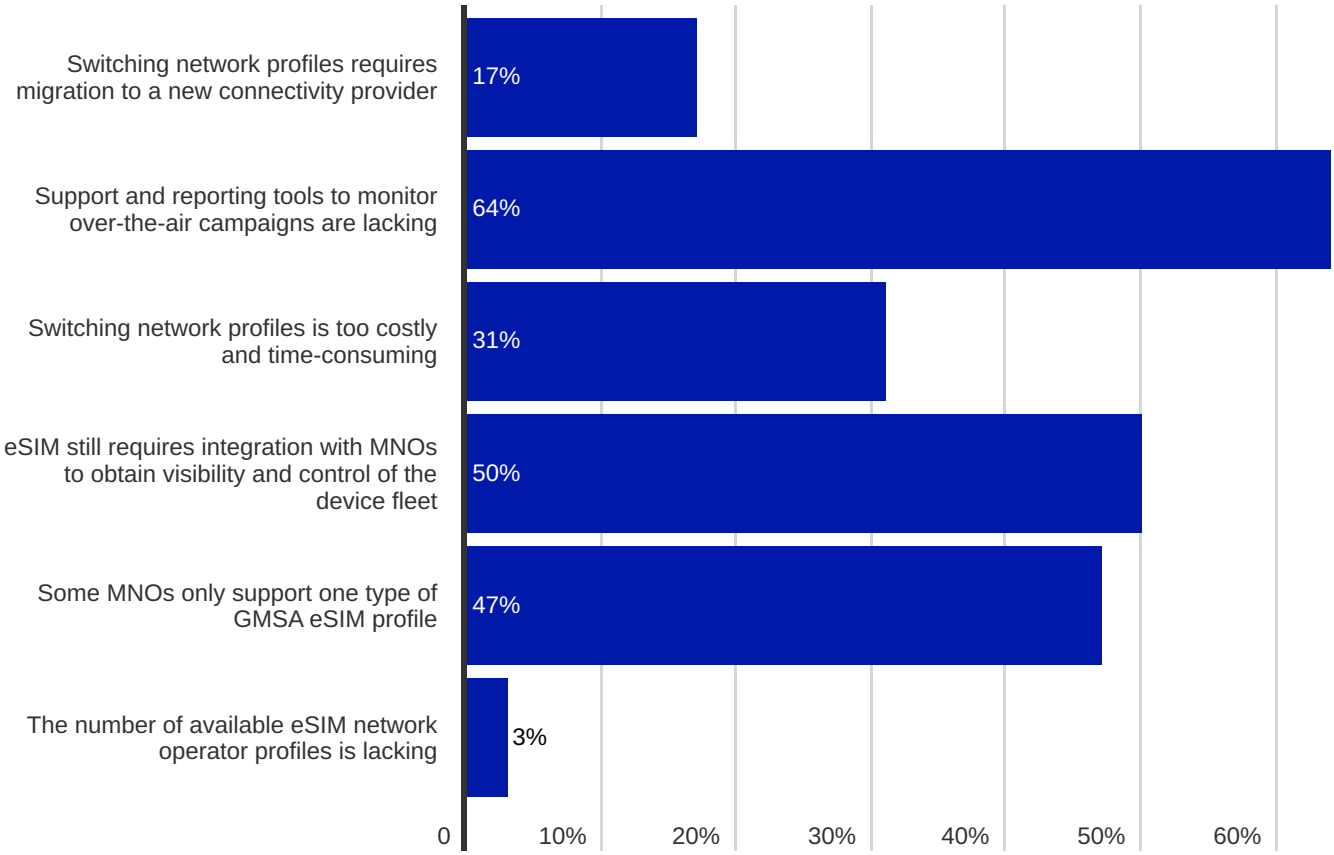


While it can be true that traditional SIM solution routes can simplify the rollout of IoT devices; this is especially true where NB-IoT or LTE-M or local tenders are concerned; these solutions offer only limited flexibility to the overall solution, which may, in turn, lead to a requirement for costly physical SIM swaps. For example, it is important to consider that eSIM is not simply useful for optimisations on the international stage: the technology can be leveraged to additionally allow customers to optimise connectivity within a domestic deployment. eSIM can thus offer total cost of ownership savings for all types of IoT deployments, assuming that in-field device rollouts reach a moderate level.

At the very least, multi-IMSI technology should be considered as a tool to optimise coverage in domestic and international scenarios, but due to the fact that multi-IMSI is invariably a provider-proprietary implementation, similar lock-in challenges associated with standard SIM card deployments can arise. This is highlighted in the survey, with **20% of respondents stating that they had not adopted eSIM due to the fact that they were locked into a legacy SIM solution. This challenge has impacted smart city enterprises to a greater extent than other verticals, with only 13% of all survey respondents reporting lock-in issues preventing them from deploying eSIM.**

Enterprises in this segment reported issues with eSIM roughly in line with other verticals, with support, integration and testing in addition to a lack of MNO support for both M2M and consumer eSIM profiles.

What are your main issues with your current eSIM (eUICC) solution? (Cellular IoT adopter responses)



Notably, **17% of the respondent base reported that switching network profiles requires migration to a new connectivity provider, which is higher than the survey average of 13%.**

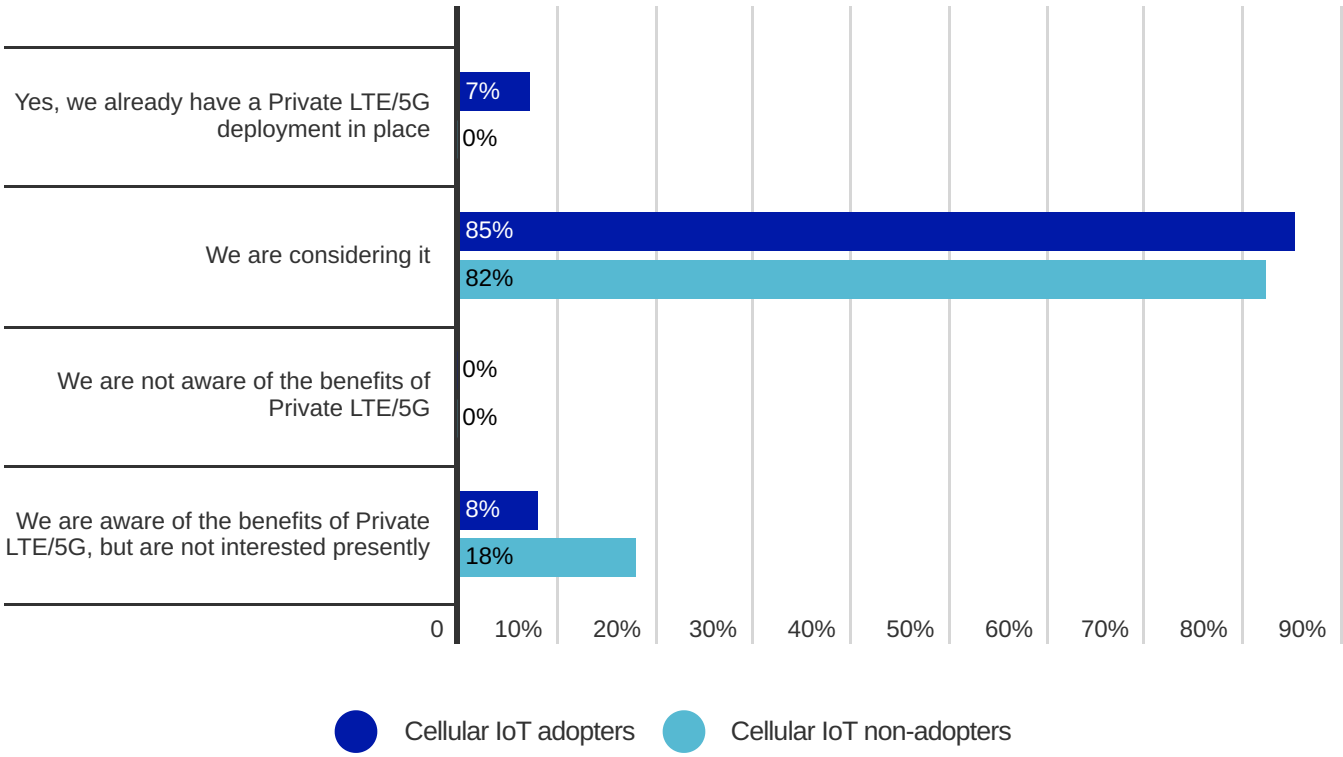
This suggests that enterprises in this segment have an increased desire to optimise the device fleet by leveraging eSIM OTA capabilities but have encountered technical or commercial challenges in doing so. In part, this may relate to the fact that the connectivity partner only supports a single eSIM profile on its platform, and means that there is an opportunity for IoT MVNO players able to support the management of devices using various eSIM profiles to offer an improved customer experience. On the other hand, it may also indicate that smart city enterprise customers would particularly benefit from a connectivity provider with support for the emerging IoT eSIM specification. This specification brings several benefits in terms of reduced technical integration requirements to execute operator profile swaps, in addition to the removal of SMS dependency for OTA campaign execution commands, which is an important step towards a standardised method of using eSIM for NB-IoT devices. Additionally, the new IoT specification offers the opportunity to streamline eSIM subscription management given the broad range of devices involved in the smart city, of which some may operate with a user interface and some without, and thus may benefit from the IoT specification's converged features.

Private LTE/5G - Smart Cities

Kaleido Intelligence

Enterprises in the smart cities segment reported the lowest level of private LTE and 5G adoption out of all the verticals surveyed. **Only 7% of cellular IoT adopters reported having a private LTE or 5G deployment, compared with a survey average of 29%. However, a significant proportion of IoT adopters (85%) reported that they were considering private LTE or 5G for their organisations, with this proportion reaching 82% among those who had not adopted cellular IoT.**

Does your business unit have an interest in Private LTE/5G to enhance business operations? (All respondents)



Notably, when the results of cellular IoT adopters and non-adopters are combined, r**espondents that stated that they had no interest in private LTE or 5G at this stage were the lowest out of all verticals, with 26% of the combined response base reporting that they would not consider a private cellular network deployment. This is markedly in contrast to healthcare (36%) and the energy and utilities sector (35%).**

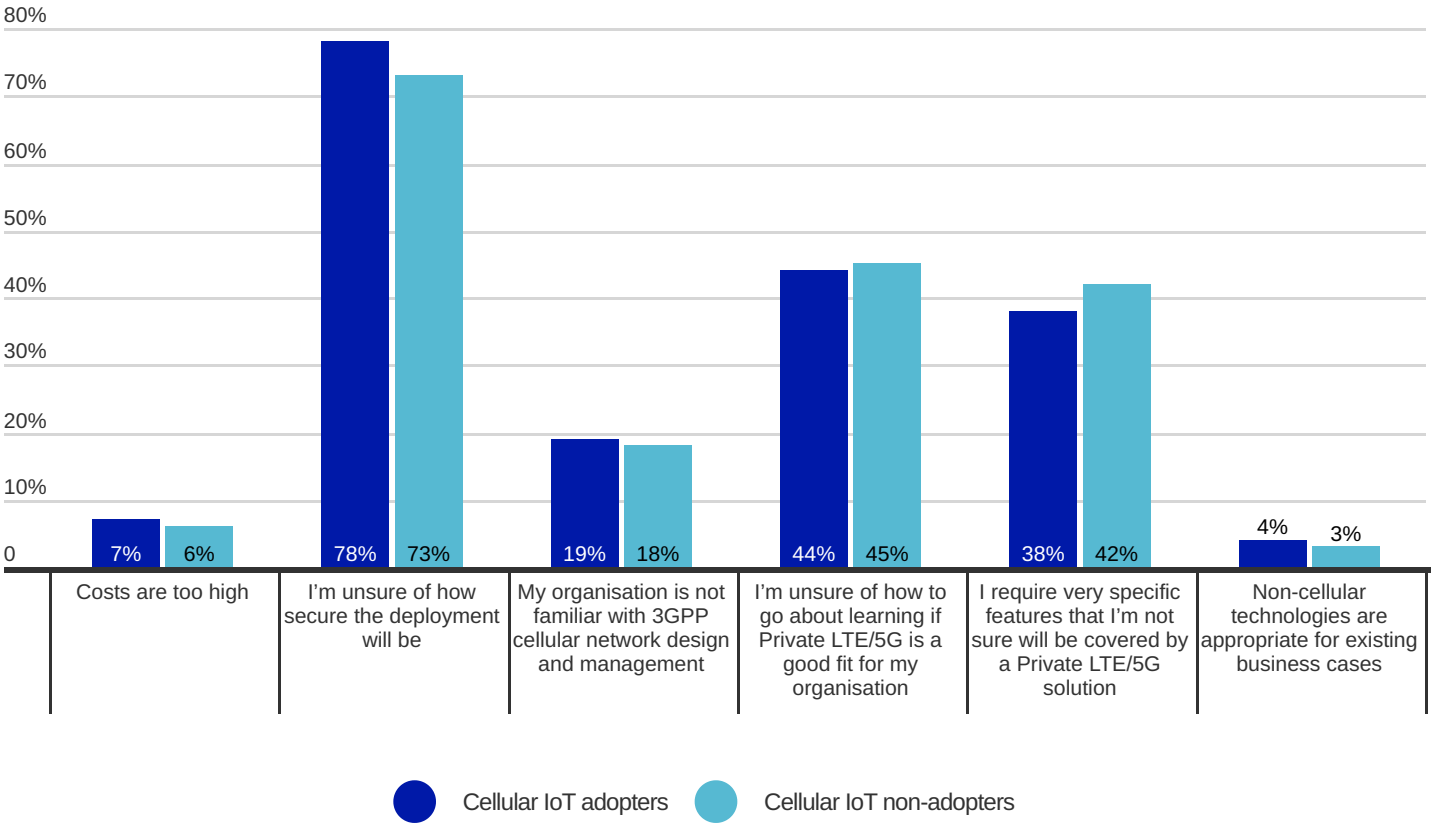
Evidently, the prospect of private LTE or 5G is of considerable interest to enterprises engaged in the smart cities segment. This is not surprising, owing to the fact that connected municipal services would invariably benefit from either the increased security or the reliability that private cellular networks are capable of delivering.

Given this high interest in private LTE and 5G solutions, it is worth considering why this particular vertical lags behind others in terms of adoption.

When asked to indicate their concerns over private cellular network deployments, enterprise **cellular IoT adopters notably reported above-average concerns over security (78% vs. a survey average of 69%), as well as a high level of uncertainty over the capabilities of private LTE or 5G to meet their requirements (38% vs. a survey average of 30%).**

This sentiment was mirrored a**mong cellular IoT non-adopters, with 73% reporting security concerns and 42% unsure of private LTE or 5G suitability for the enterprise strategy.**

What are your main concerns over a potential Private LTE/5G deployment? (All respondents)



From the results above, it would appear that many enterprises in this segment are unsure as to the particular use cases that can be supported through private LTE or 5G, and if the technology is able to deliver value for money. This is not always clear from the outset, given that enterprises have limited knowledge of performance, coverage and security capabilities of private cellular networks. Above all, it is apparent that privacy concerns are of paramount importance for cellular IoT adopters, given that **53% of respondents perceive that improved privacy is a key benefit of private LTE or 5G, while 58% of the same respondent base saw the need for a simplified IT security implementation as a key factor consideration.**

IoT Connectivity Challenges & Opportunities: Healthcare

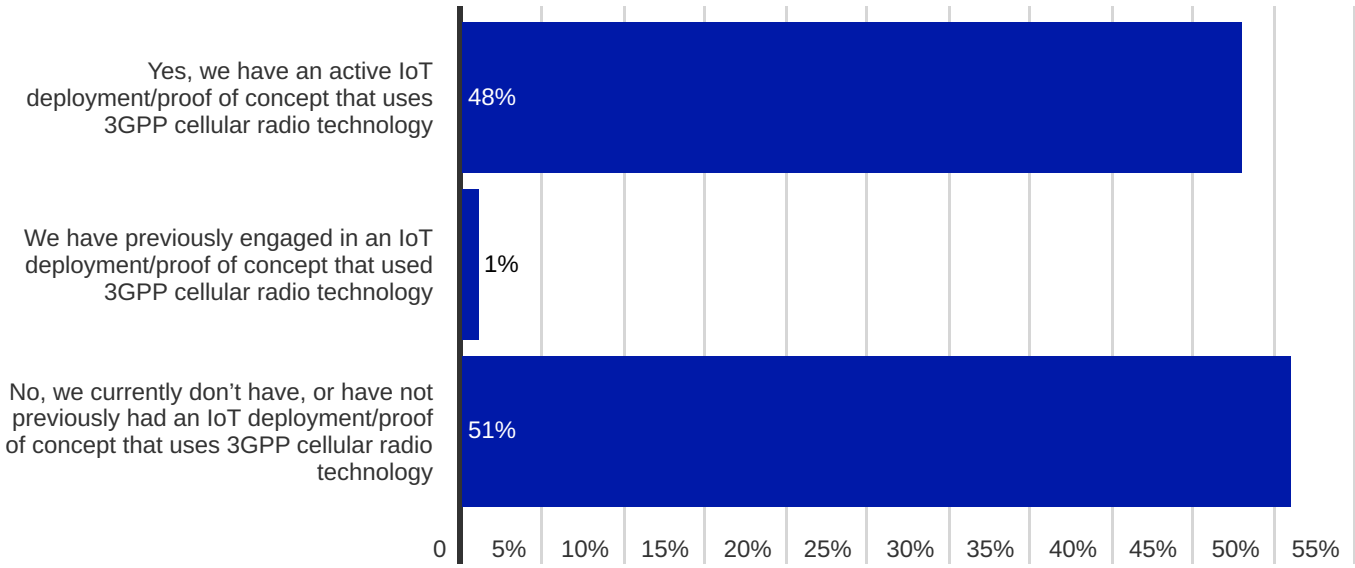
eseye iBASIS KORE TRUPHONE flo. LIVE

State of IoT - Healthcare

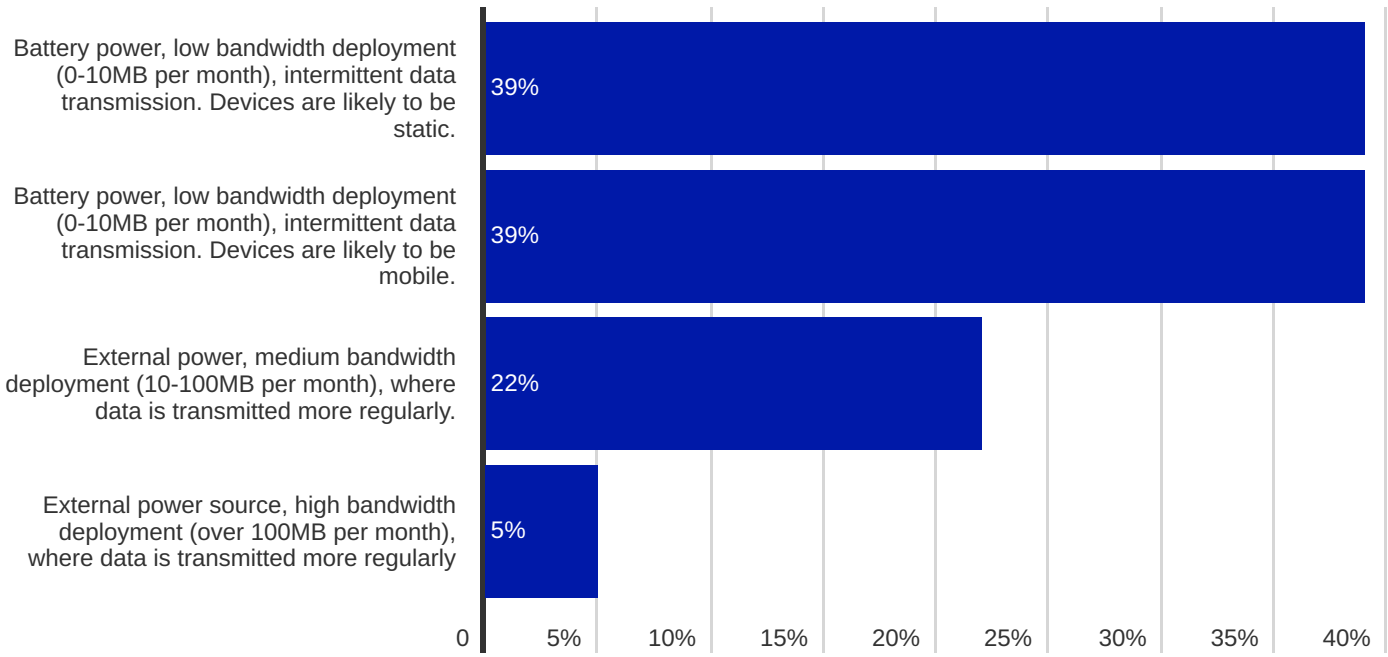
Kaleido Intelligence

Enterprises in the healthcare segment reported an average level of cellular IoT adoption, with **49% of respondents having an active or previous cellular IoT deployment.** This segment is notable in that survey respondents reported the highest rate of intention to adopt cellular IoT out of all verticals surveyed. **49% of respondents that had not yet adopted cellular IoT reported that they intended to over the next 12-24 months, which is markedly higher than the average 35% reported across combined verticals surveyed.**

Does your business unit currently have an IoT deployment or proof-of-concept underway that uses 3GPP cellular radio technology (2G/3G/LTE/5G)? (All responses)



What type of cellular IoT deployment is this likely to be? (Cellular IoT non-adopter responses)



In line with other verticals, a majority of future cellular IoT healthcare deployments are likely to involve devices that periodically report small volumes of data and, as such, exclude video-based telehealth applications in the majority of cases. Meanwhile, **only 22% and 5% of respondents stated that they intend to deploy devices with medium or high bandwidth applications, which is below the overall survey average of 31% and 7%**, respectively.

The pandemic has meant that many caregivers across the globe have been restricted in terms of their capability to assess patient condition in a face-to-face environment. In turn, this has led to an increased need to monitor patient metrics, such as blood pressure, sugar levels, temperature, etc. remotely.

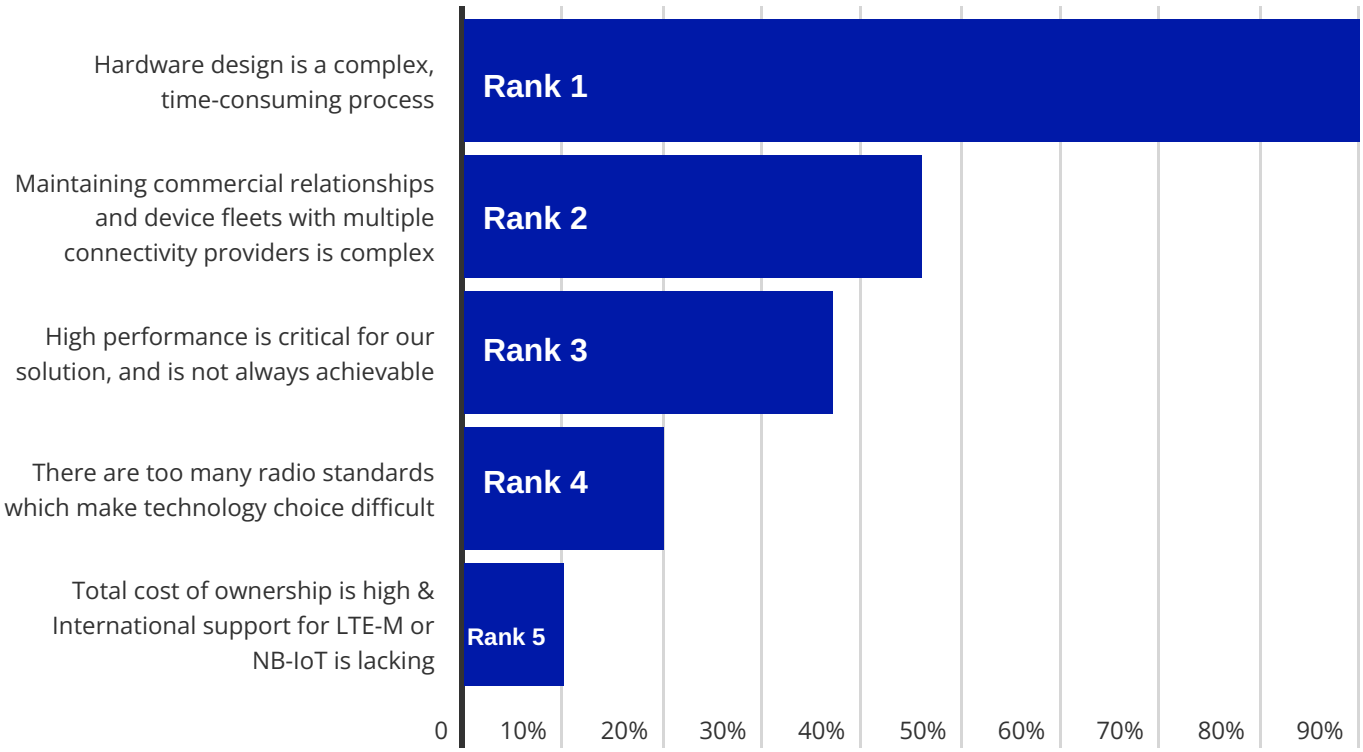
Meanwhile, connected wearable devices have been used to provide indicators for COVID-19 prevalence and legislative compliance in certain countries. Although restrictions related to the virus are now easing in many instances, telehealth monitoring offers efficiencies that allow caregivers as well as patients to save valuable time in cases where regular doctor or nurse appointments may have been used previously.

Complexity - Healthcare

Kaleido Intelligence

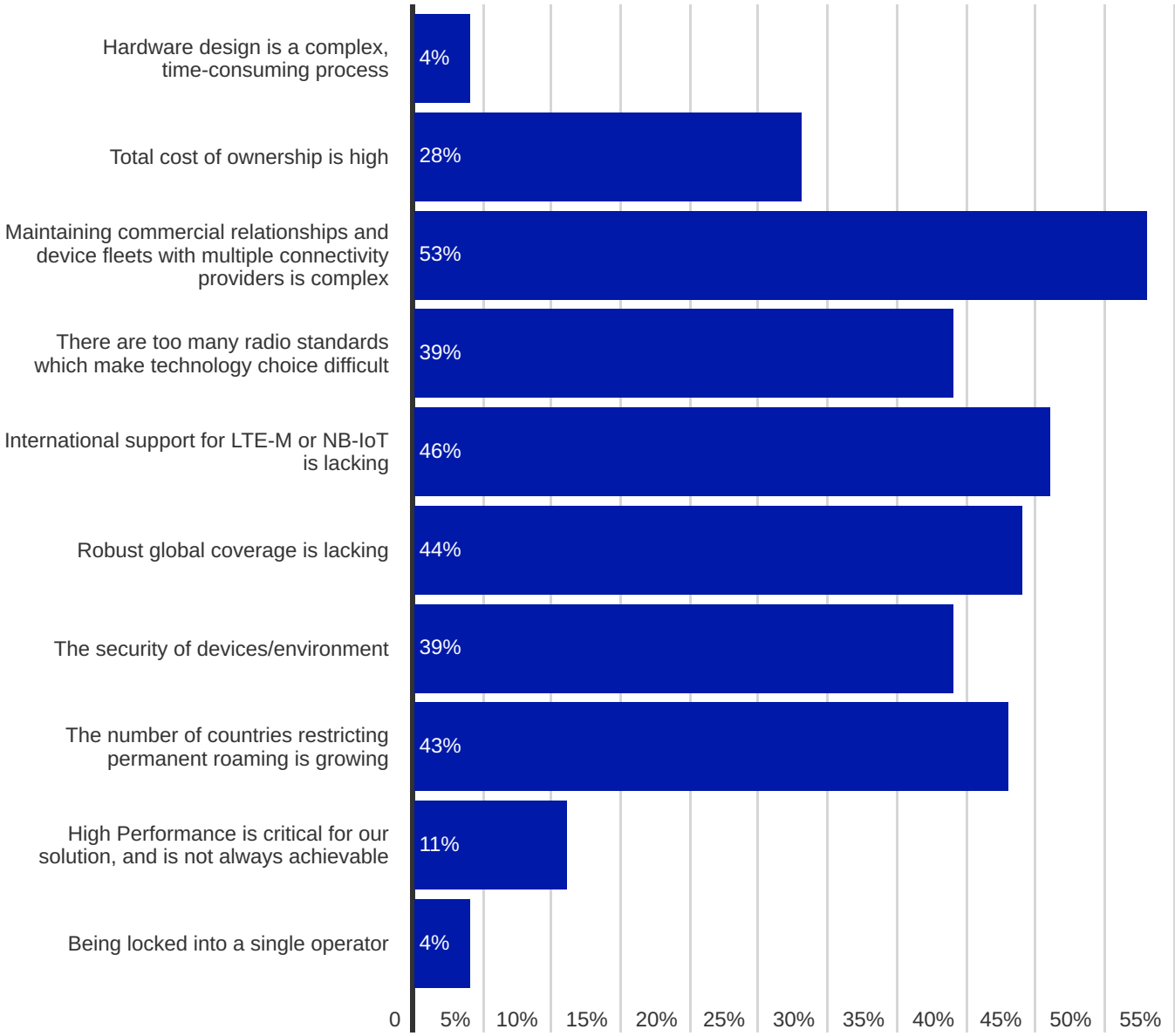
Concerns related to cellular IoT complexity voiced by enterprise survey respondents were relatively similar in nature to other verticals, with **hardware design complexity ranked as the top barrier by 90% of cellular IoT non-adopters.** Meanwhile, **46% of the same respondent base reported that maintaining commercial relationships and device fleets with multiple connectivity providers is challenging, with an additional 37% of respondents believing that the ability to achieve high performance through cellular IoT is not always possible.**

What do you perceive to be the top 5 challenges where cellular IoT connectivity is concerned? (Cellular IoT non-adopters responses)



Hardware design complexity is of much lower importance among cellular IoT adopters, with only 4% of survey respondents reporting that this is a key barrier to cellular IoT deployments. Rather, the main challenge appears to be related to the availability of LTE-M and NB-IoT support, with 46% of surveyed enterprises perceiving a lack of international support for these technologies.

What do you perceive to be the main challenges where cellular IoT connectivity is concerned? (Cellular IoT adopter responses)



These results represent a relatively mixed bag of concerns, although it is clear that challenges concerned with multiple connectivity contractual relationships and a lack of support for LTE-M and NB-IoT on the international market are likely to be related. CSPs must therefore focus on accelerating roaming support for these types of connections, either through the establishment of direct roaming agreements with operator partners or through indirect roaming hub partnerships that enable a one-to-many model of securing multi-network access. In the case of IoT MVNOs, the latter approach is likely to be favourable.

Whichever route is taken, it is important that CSPs promote the ability to minimise the number of commercial relationships and integration points required to roll devices out in multiple international markets, in addition to how this can reduce time-to-market and costs involved with deploying IoT at scale.

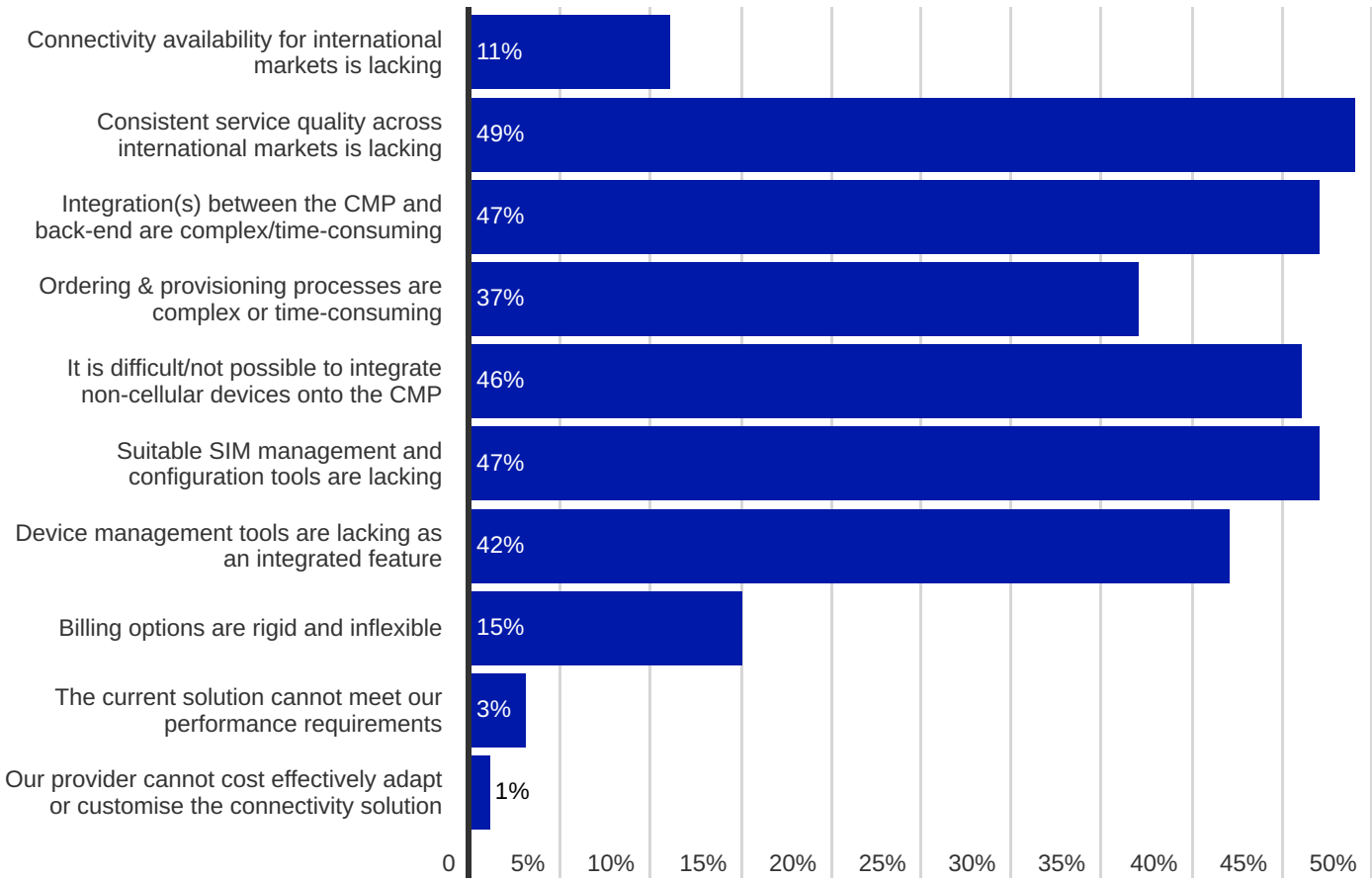
CSPs will likely also benefit from accelerating efforts to establish partnerships with hardware module providers in order to enable a smoother path to cellular IoT adoption for those that have not yet chosen a cellular IoT deployment.

With **20% of cellular IoT non-adopters reporting that the various cellular radio standards available make technology choice difficult,** it will be important to establish communications with potential enterprise healthcare customers at an early stage in order to help with module selection and guidance related to performance, global network availability and fallback requirements. The ability to consolidate a hardware and connectivity offering is evidently important to healthcare enterprises, with **54% of cellular IoT non-adopters stating that this is the second-highest priority for them where a connectivity partner's capabilities are concerned.**

54% cellular IoT non-adopters rate a consolidated hardware & connectivity offering as their #2 priority

Importantly, **46% of the cellular IoT adopter base stated that the ability to integrate non-cellular technologies into the connectivity solution is lacking, while 47% additionally noted that SIM management and configuration tools were lacking from the offering**. Many healthcare devices are often equipped with Wi-Fi technology in addition to cellular radios, with these results highlighting that enterprises prefer to have a holistic view of deployments for connectivity management. The stated lack of SIM management and configuration tools likely relates to data security and compliance requirements, with stringent regulations often imposed on enterprises operating in this segment. Tools must therefore be made available to aid in delivering against these requirements.

What are your biggest issues with your current cellular IoT connectivity solution? (Cellular IoT adopter responses)



Roaming - Healthcare

Kaleido Intelligence

63% of cellular IoT non-adopters stated that their connectivity partner must have an extensive set of mobile operator partnerships in place as the top priority towards optimising fleet performance and costs across domestic and roaming footprints. Given that performance concerns have been raised by this group of respondents, simply being able to offer coverage within a given country is unlikely to match enterprise expectations, and means that CSPs must be capable of delivering connectivity through partnerships with at least 2 providers. Above all, healthcare applications will rely on the high reliability of the connectivity solution to ensure that data can be transmitted in a timely fashion without the service interruptions associated with other connectivity solutions, such as Wi-Fi.

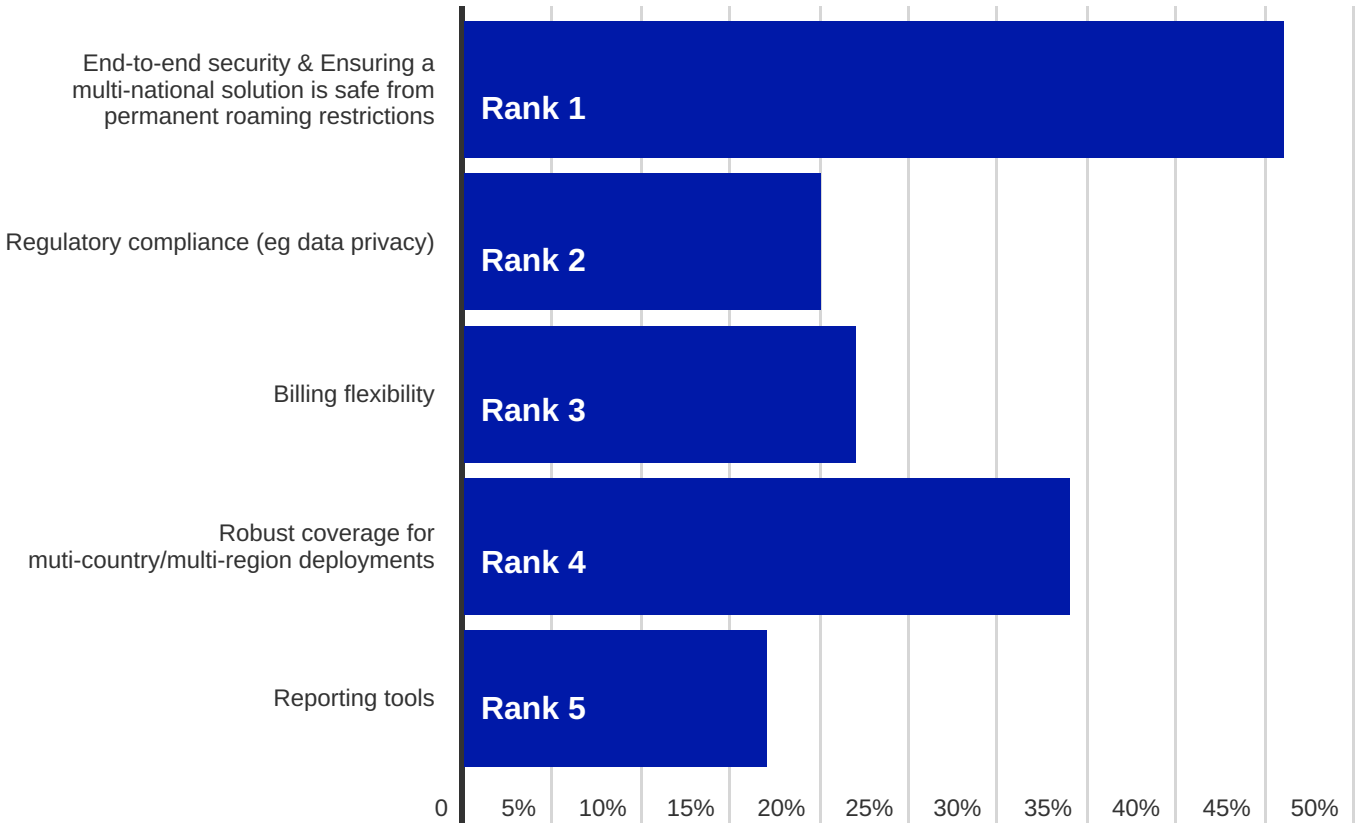
This type of issue continues to be experienced by enterprises that have selected cellular technology for their deployments: some 44% of the cellular IoT adopter respondent base reported this to be a key issue, although this proportion is below the survey average of 48%.

44% cellular IoT adopters stated robust global coverage is lacking

Notably, **49% of the cellular IoT adopter respondent base reported that consistent service quality across international markets is lacking** and relates to non-adopter concerns noted earlier over the ability to support performance expectations. Capabilities that enable the selection of regional or local Packet Data Network Gateway (PGW), in addition to the ability to optimise performance through intelligent steering and IMSI selection, offer differentiation points here that CSPs can help convince healthcare customers that performance expectations can be met.

Permanent roaming is the joint top point of consideration where IoT connectivity is concerned for non-cellular IoT adopters, with 46% of survey respondents assigning the ability to guard against permanent roaming risks as their highest priority.

What are your top 5 factors that are most important where IoT connectivity is concerned?(Cellular IoT non-adopter responses)



The importance of permanent roaming is not diminished when enterprises choose cellular connectivity for their IoT deployments, with 38% of respondents requiring assurances against permanent roaming risk as their second-highest priority for cellular IoT connectivity. The need for guaranteed service uptime in the healthcare domain is perhaps more important than in any other vertical, and as such, enterprises in this segment cannot afford to take any risks that might disrupt the connectivity side of the solution. With some 40% of cellular IoT non-adopters stating a lack of ability for enterprises to customise commercials with preferential network operator contracts such as through Bring Your Own Connectivity (BYOC), flexibility to guard against permanent roaming restrictions through a mix of in-house commercial agreements, technical solutions to avoid roaming, as well as an open approach to onboard customer operator connectivity partner relationships into the overall solution, will enable the highest level of choice for customers.

Security - Healthcare

Kaleido Intelligence

The sensitive nature of data associated with healthcare IoT solutions means that the security of the deployment is of the utmost importance. Indeed, this is highlighted in the survey results, with **46% of cellular IoT non-adopters ranking end-to-end security as their top priority for IoT connectivity, with regulatory compliance voted as the second most important factor for IoT connectivity.** Meanwhile, the ability of a connectivity partner to offer extensive security features was ranked as the fifth most important facet of a CSP's product by the same respondent base.

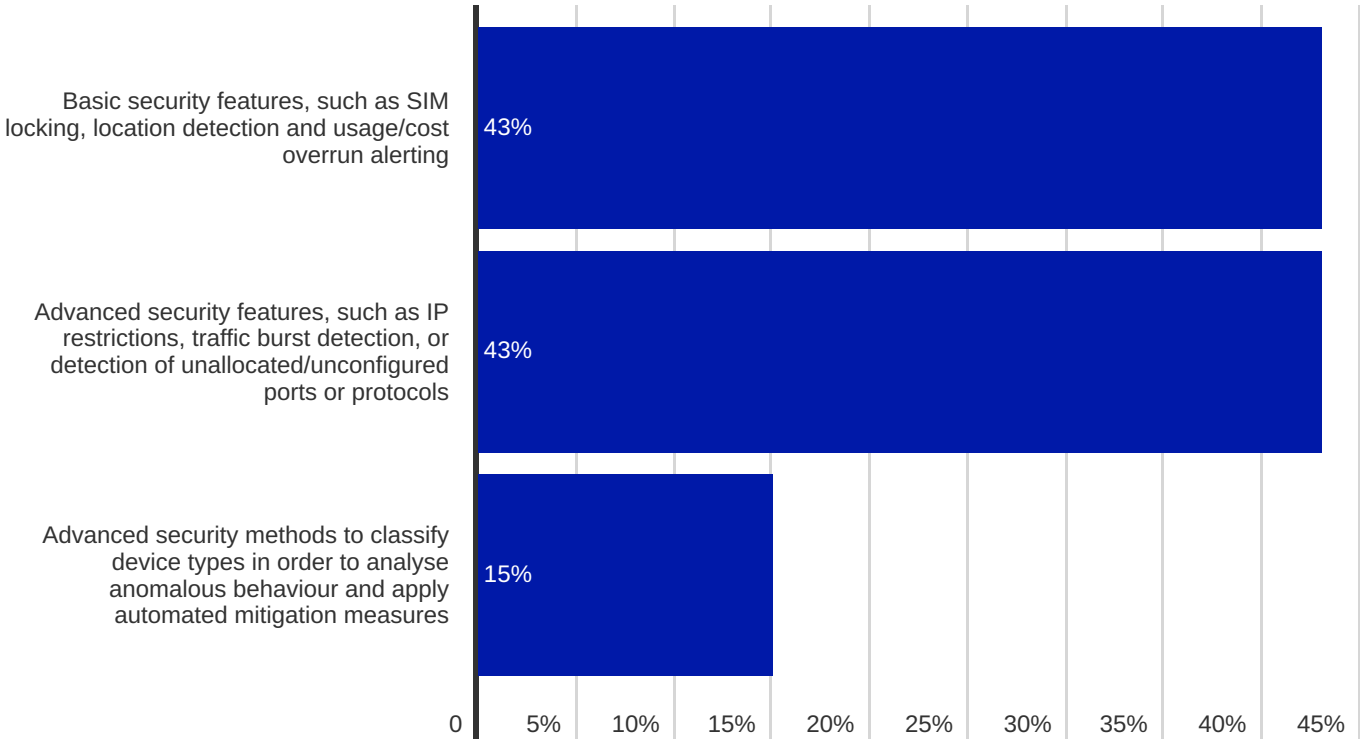
Security & regulatory compliance are the top 2 priorities for cellular IoT non-adopters

This need for security becomes further evident when considering the cellular IoT adopter portion of the respondent base: **73% of surveyed enterprises named this as their top priority for cellular IoT connectivity, with this proportion significantly higher than the survey average of 59%.**

In the same respondent base, **39% of survey respondents reported that the security of devices and the environment was a major challenge for cellular IoT connectivity**, with this metric being viewed as less challenging only against issues related to the streamlined rollout of international connectivity and support.

Expectations in terms of the CSP's role in data security are higher in this vertical than all others, with notably elevated demands for more advanced security services. While 4**3% of the respondent base require the CSP to incorporate mid-level security features** such as IP restrictions, traffic burst detection, or detection of unallocated/unconfigured ports or protocols, **15% of the surveyed enterprises stated that high-end security capabilities, such as automated device classification and advanced behavioural monitoring should be an important feature of a CSP's VAS offering**. This proportion is markedly higher than the survey average of 11% of respondents, with enterprises in all other verticals only reaching a maximum of 10% of those stating that this type of advanced capability is required.

What security features do you expect your cellular IoT connectivity partner to provide? (Cellular IoT adopter responses)



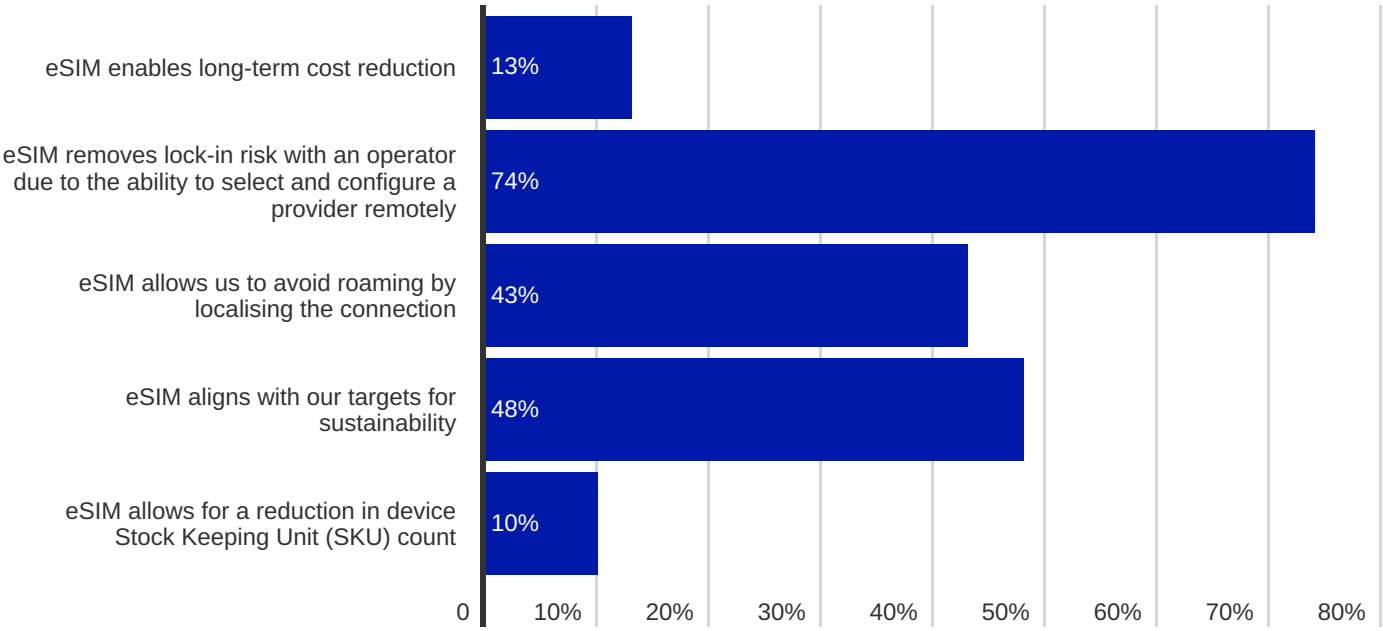
Evidently, the ability for CSPs to demonstrate a very high level of security expertise as a core part of their offering will generate a notable point of differentiation for players aiming to compete in this space of the market and underlines the need to develop a merger and acquisition (M&A) or partnership strategy to deliver against enterprise expectations.

eSIM - Healthcare

Kaleido Intelligence

eSIM adoption among healthcare cellular IoT adopters was among the highest of the verticals analysed in this study, with **87% of respondents stating that eSIM formed part of their device fleet. Key reasons behind the decision to use eSIM were cited as the ability to avoid operator lock-in, with 74% of respondents stating as such, while 43% of surveyed enterprises named the ability for eSIM to avoid roaming as a key reason behind choosing eSIM. The strength of both of these opinions was above the overall reported survey average for lock-in avoidance (71%) and roaming avoidance (40%).**

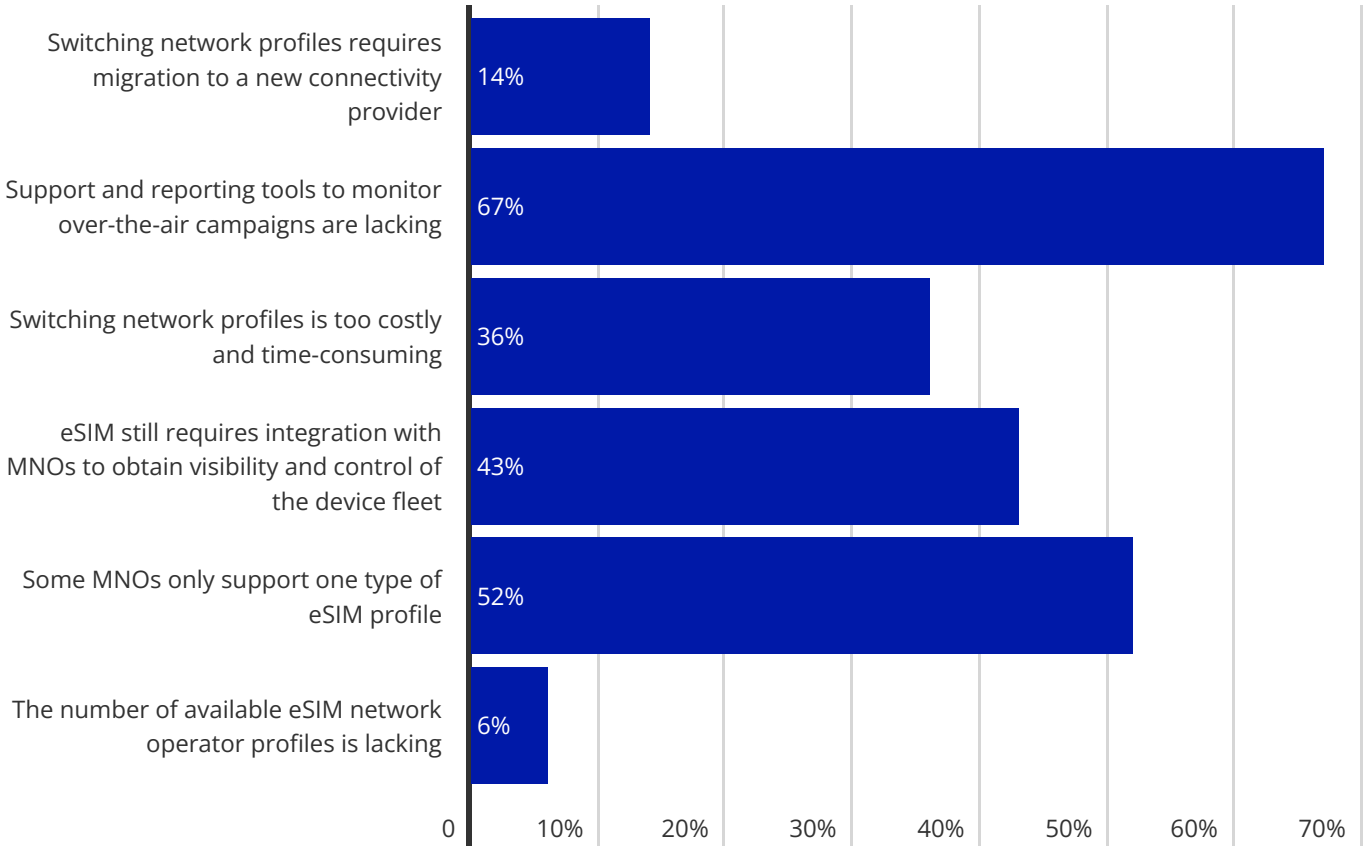
What factors made you choose eSIM (eUICC)? (Cellular IoT adopter responses)



Given the challenges uncovered earlier in relation to international rollout complexity and permanent roaming concerns, it is critical that CSPs support the capability to localise connectivity in as many countries as possible for enterprises in this segment. Although eSIM is often viewed as the primary technology choice to achieve this, core network integrations coupled with IMSI translation capabilities in addition to partnerships to secure local IMSI ranges offer alternative technical solutions to the issue of connectivity localisation and, when coupled with eSIM, offer customers a very high level of flexibility that minimises the risk of lock-in and loss of connectivity through permanent roaming commercial or regulatory challenges.

The ability to supplement eSIM with alternative localisation options becomes apparent when considering the fact that **36% of respondents stated that switching network profiles is too costly and time-consuming, while a small (6%) but higher than average (4%) proportion of respondents reported that the number of available eSIM profiles was lacking. Meanwhile, 50% of respondents that had chosen not to use eSIM stated that alternative SIM solution technologies, such as multi-IMSI, were simpler and more cost-effective to deploy.** These results indicate that a combination of eSIM and multi-IMSI technology is a necessity rather than simply an advantage for CSPs.

What are your main issues with your current eSIM (eUICC) solution? (Cellular IoT adopter responses)



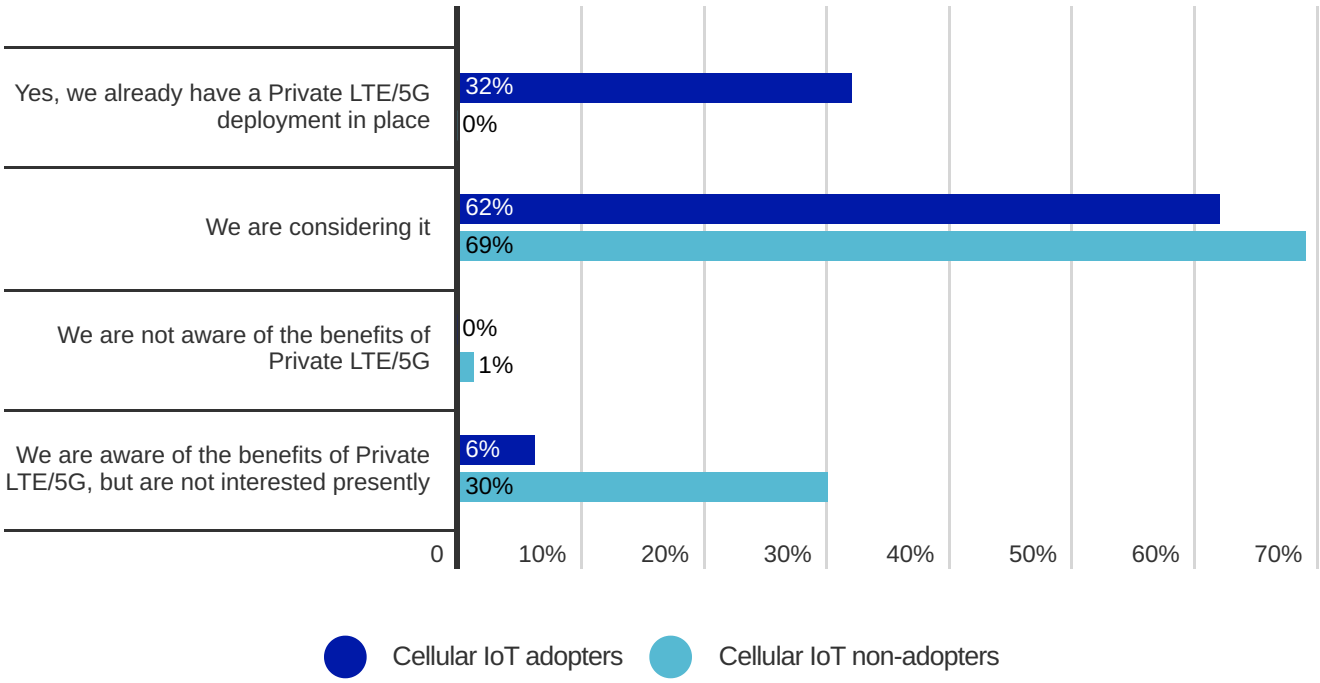
Nevertheless, the ability for eSIM to function as expected is clearly a highly important factor for consideration in this vertical. **50% of those that had not adopted eSIM stated that ensuring compatibility with devices and networks was a major reason behind the decision not to use the technology, while 67% of eSIM adopters stated that support and reporting tools for OTA campaign monitoring were lacking in their current solution.** Evidently, the need to ensure that issues are resolved as quickly as possible is highly valued in addition to solutions that maximise the potential for successful eSIM use prior to full rollout.

Private LTE/5G - Healthcare

Kaleido Intelligence

Positive enterprise sentiment towards private LTE or 5G was high, with some **32% of cellular IoT adopters stating that they had a private cellular network deployment in place, with an additional 62% of respondents stating that they are considering deployment.** Meanwhile, a further **69% of cellular IoT non-adopters reported that they were considering private LTE or 5G for operations**, in line with the overall survey average response. The potential for solutions in this vertical can thus be viewed as relatively strong, although it is likely that in most instances, private LTE or 5G will be used to facilitate enhanced connectivity in healthcare institutions, such as hospitals and pop-up care facilities; dedicated radio capabilities will be an element of the solution here. In the case of telehealth devices, the business case for private LTE or 5G is likely diminished, although some enterprises may look to deploy private network architecture on a national scale, which in turn is likely to rely on public radio network infrastructure.

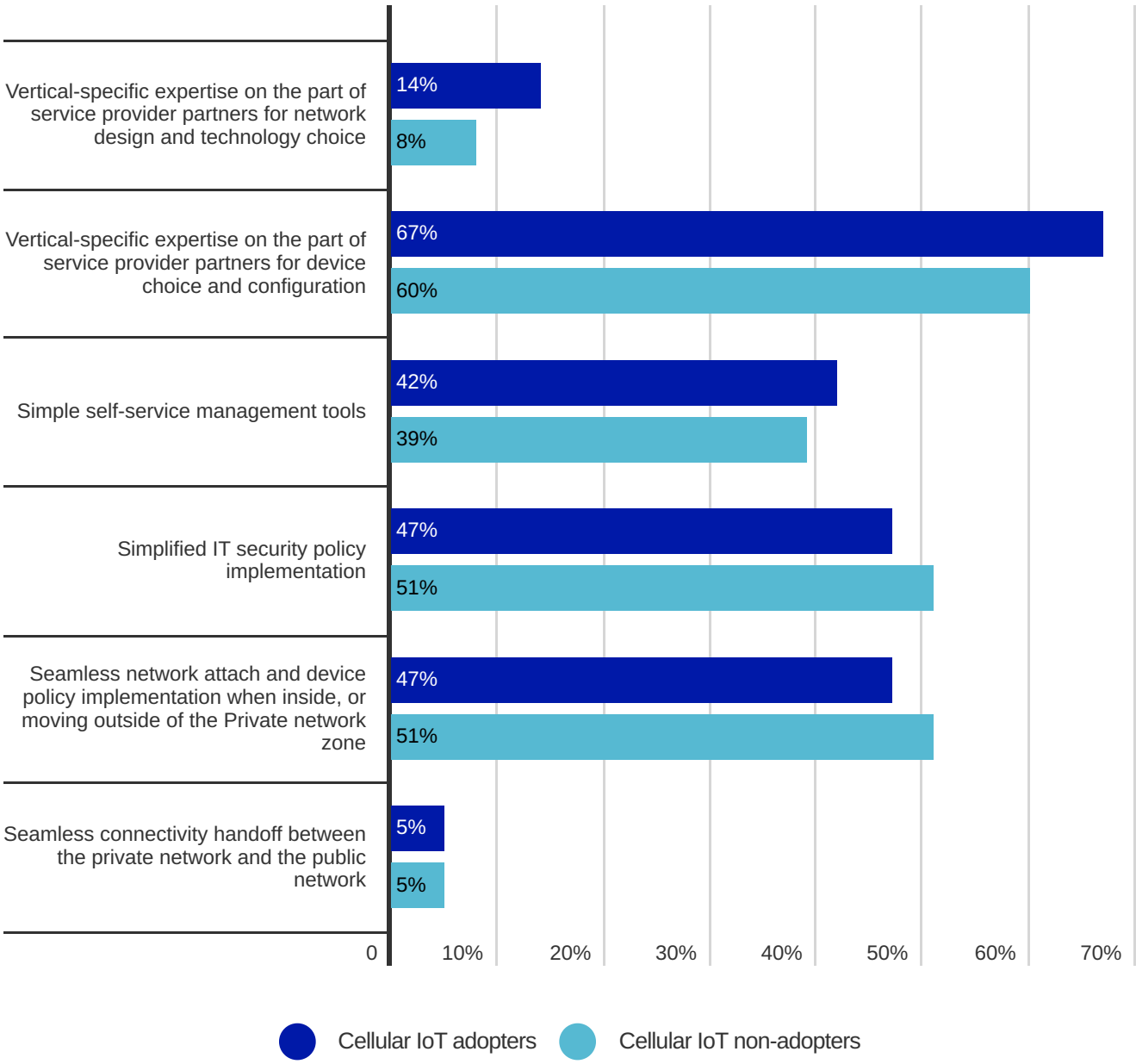
Does your business unit have an interest in Private LTE/5G to enhance business operations? (All respondents)



Expertise in guiding potential customers through the capabilities and nuances of private cellular network solutions is elevated in the healthcare vertical: 25% of cellular IoT adopters and 29% of cellular IoT non-adopters reported that a lack of 3GPP network design and management knowledge was holding them back, with these results being higher than the survey averages. Additionally, **54% of cellular IoT adopters were unsure of the solution's fit with their organisational strategy, compared with 58% of respondents who had not yet adopted cellular IoT.** Highlighting the benefits of cellular radio technology over Wi-Fi, cellular upgrade paths and the potential to introduce robust positioning features through 5G will likely be important factors to help enterprises understand how private cellular can enhance operations.

Healthcare facilities represent another area where both caregivers and connected assets are likely to move between sites and will thus lead to the need for private network site interconnectivity and 'roam in, roam out' capabilities to ensure connectivity continuity. **51% of cellular IoT adopter respondents stated that the capability to ensure seamless network attach and device policy implementation was a key factor for private LTE and 5G rollout consideration**, and should thus form a key part of strategy for CSPs aiming to deliver solutions in this vertical. Connectivity continuity and security are, as has been discussed, key priorities for IoT solutions in this segment, and will mean that forcing customers to manually attach devices to networks will be an unacceptable customer experience. Technical solutions must be found to ensure that this functionality is achieved as seamlessly as possible, while also ensuring that a high level of data confidentiality and integrity is maintained in line with industry compliance requirements.

Does your business unit have an interest in Private LTE/5G to enhance business operations? (All respondents)



iBASIS
POWERED BY TOFANE

BE THERE FIRST

RESCUESTAT + iBASIS

Over 50,000 Automated External Defibrillator (AED) units globally will be monitored and managed remotely

RescueStat

RescueStat, a leading provider of Automated External Defibrillator (AED) Management products and services, wanted to leverage their patented technology to monitor the readiness status of AEDs around the world. The iBASIS eSIM enables RescueStat's Remote Monitoring System (RMS) to access more than 700 networks worldwide, transmitting critical data from the AED to the end user. If the AED ever fails its self-test, the iBASIS eSIM alerts the user and RescueStat so that an experienced support team can troubleshoot the problem and get the AED back to working condition, ready to save a life!

RESULTS

- Dramatic increase in effectiveness of Public Access Defibrillation (PAD) programs combining RescueStat Automated External Defibrillators (AEDs), Remote Monitoring System (RMS), and iBASIS eSIM
- Over 50,000 RescueStat AED units will be globally remotely monitored via the iBASIS eSIM
- One of the fastest implementations of our IoT solution to date, completed in just five days

> "The iBASIS eSIM is the perfect solution to further enhance the effectiveness of critical public access defibrillation programs by enabling remote monitoring of AEDs.
>
> This solution ensures that devices will be fully available in critical circumstances and we are very proud to partner with a company that shares our commitment to delivering life-changing innovation and performance."
>
> **Carl Dixon**
> **CEO, RescueStat**

ABOUT iBASIS

iBASIS is the leading communications solutions provider enabling operators and digital players worldwide to perform and transform. Powered by Tofane Global, the new iBASIS is the first independent communications specialist, ranking third largest global wholesale voice operator and Top 3 LTE IPX vendor with 660+ LTE destinations. With the integration of Tofane's acquisition of the Altice Europe N.V. international voice carrier business in France, Portugal, and the Dominican Republic, iBASIS today serves 1,000+ customers across 18 offices worldwide.

iBASIS provides the end-to-end Global Access for Things™ connectivity solution, delivering single source cellular IoT access (LTE, LTE-M, and NB-IoT) worldwide provisioned through GSMA-standard eSIM/eUICC technology. The solution simplifies IoT device connection through one unified platform for seamless, remote, programmable, and secure communication. For more information, please visit www.iBASIS.com.

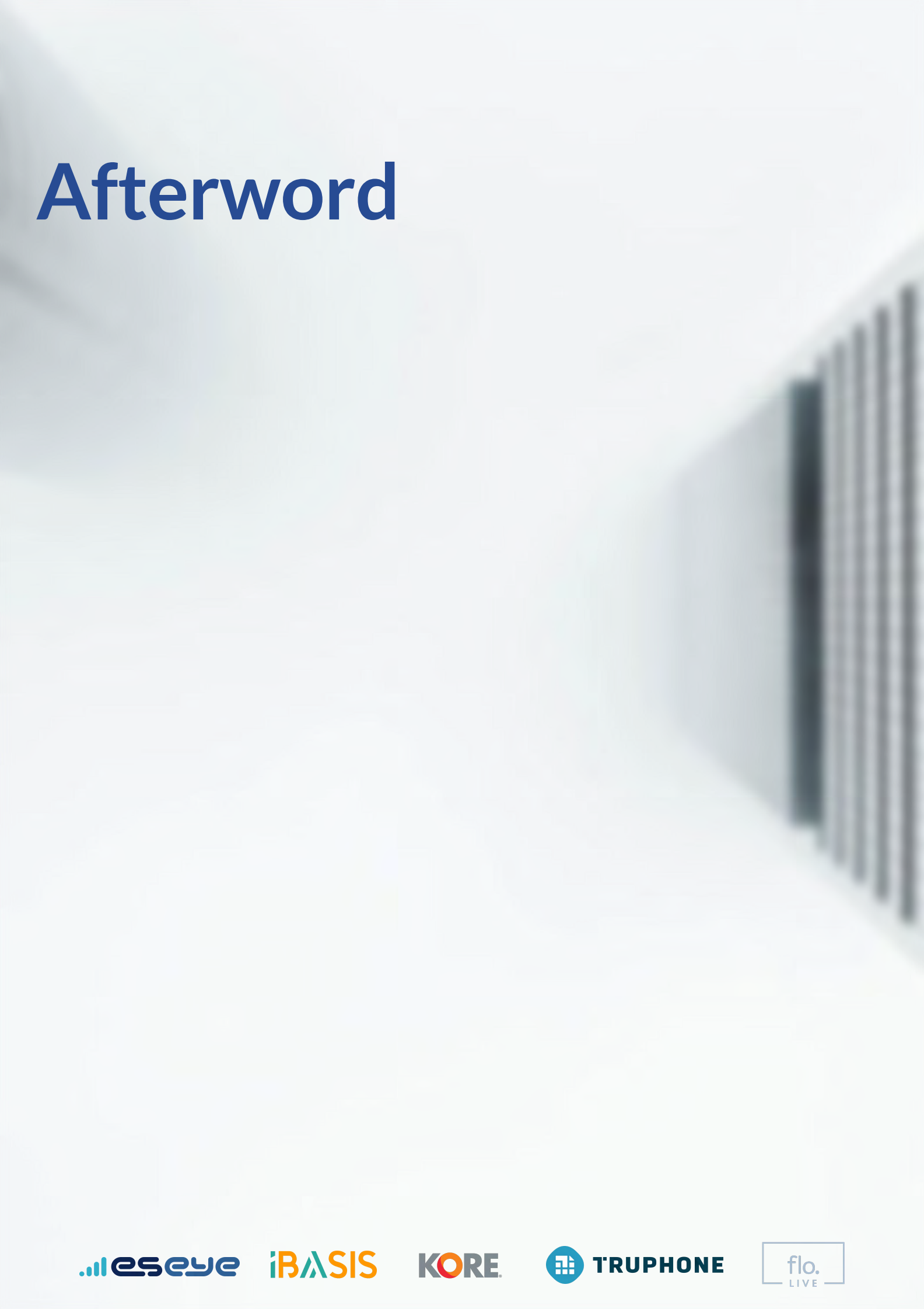
CORPORATE HEADQUARTERS

10 Maguire Road, Building 3
Lexington, MA 02421

T +1 781 430 7500
F +1 781 430 7300
E info@iBASIS.net

iBASIS.COM

Afterword



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, along with Kaleido and IoT Now, are supporting our vision of enabling business decisions across the enterprise sector through inspiring, educational and accessible insights.

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: June 2022

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

Kaleido aims to provide accurate information. The information provided here is designed to enable helpful data and insights on the subjects discussed.

References to companies are provided for informational purposes only and Kaleido does not endorse any operator, vendor or service included in this research and market study. While information and content of this publication is believed to be accurate at the date of publication, neither Kaleido Intelligence nor any person engaged or employed by Kaleido Intelligence accepts any liability for any errors, omissions or any loss or damage caused or alleged to be caused directly or indirectly by what is contained in or left out of this publication. This report consists of the opinions of Kaleido and should not be construed as statements of fact. It contains forward-looking statements and market forecasts that have been developed based on current information and assumptions. These are subject to market factors such as, but not limited to, unforeseen social, political, technological and economic factors beyond the control of Kaleido Intelligence.