Kaleido Intelligence

CELLULAR IOT

ADDRESSING THE CHALLENGE OF IOT SECURITY

END-TO-END REQUIREMENTS FOR SECURE IOT DEPLOYMENTS

2024 SURVEY REPORT SPONSORED BY

Kigen

TABLE OF CONTENTS

Introduction

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

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

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

Transportation & logistics

Healthcare

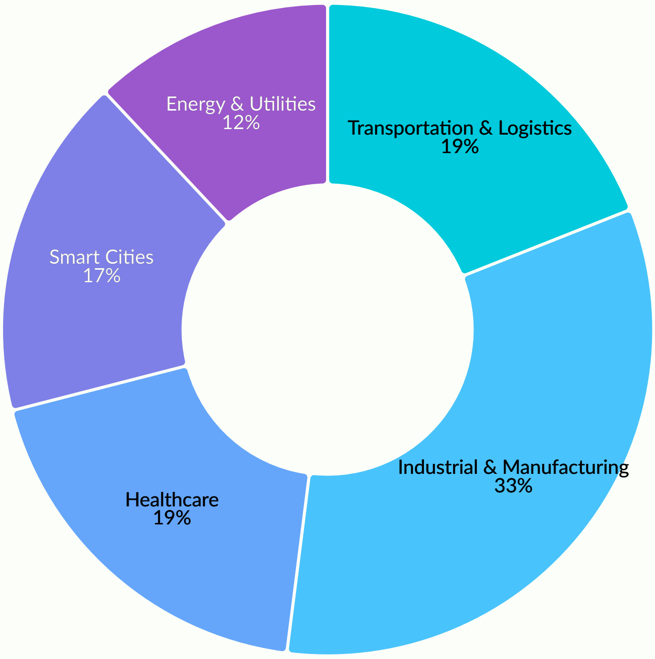
Industrial & manufacturing

Enrergy & utilities

Smart Cities

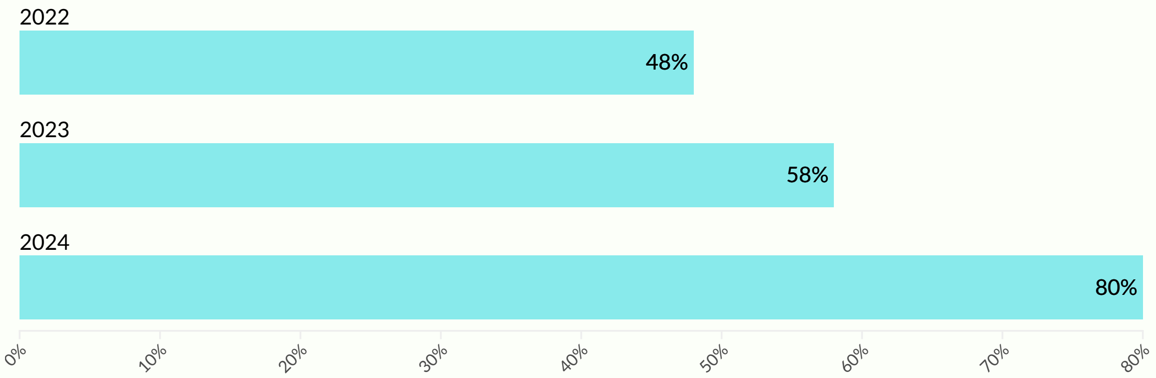
All respondents were decision-makers at managerial level or higher within their organisation, in addition to having a good knowledge of the cellular IoT ecosystem.

In what market segment does your business unit primarily operate?



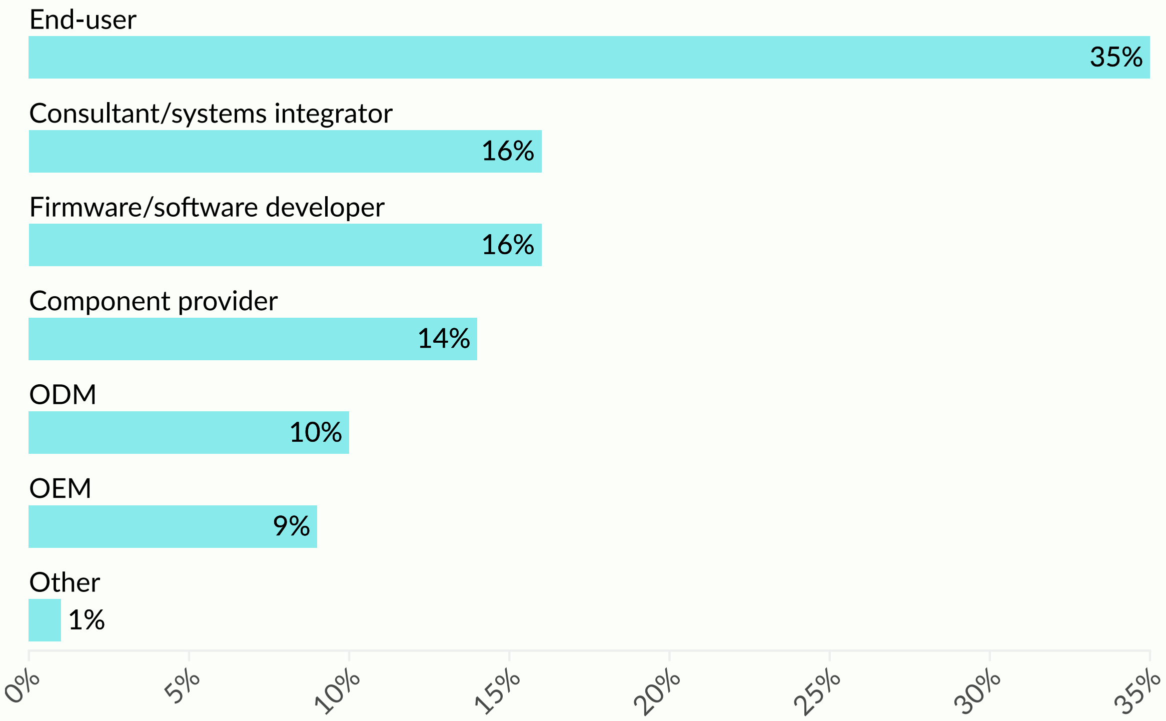
A significant proportion of respondents, at around 80% of survey participants, reported that they have an active cellular IoT programme in the field. While this proportion may not reflect the absolute state of adoption of cellular IoT among enterprises globally, it does serve to highlight that growth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

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



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

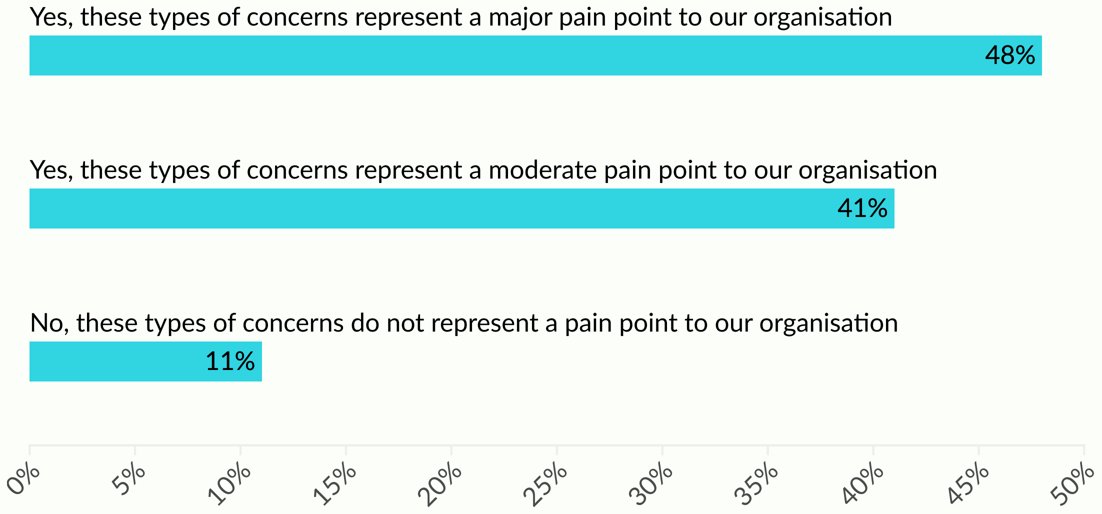
How would you describe your organisation’s position within the IoT value chain?



Addressing the Challenge of IoT Security

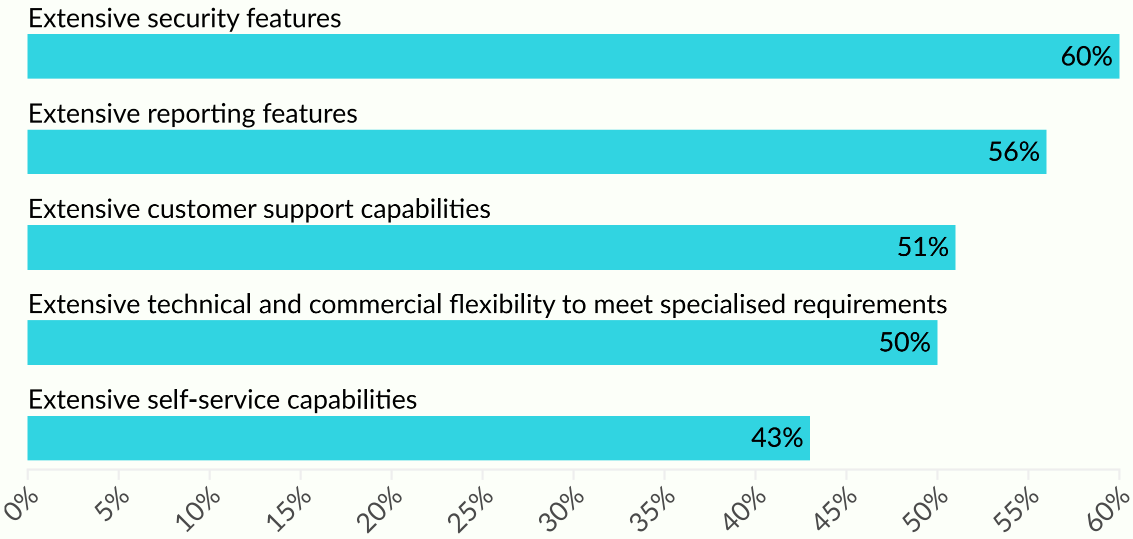
The importance of security for IoT has never been more apparent than in this year's survey. Likely this is driven not only by the fact that the industry is starting to mature, with more sophisticated enterprise customers aware of the risks with larger device estates, but also by the fact that the regulatory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

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



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

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

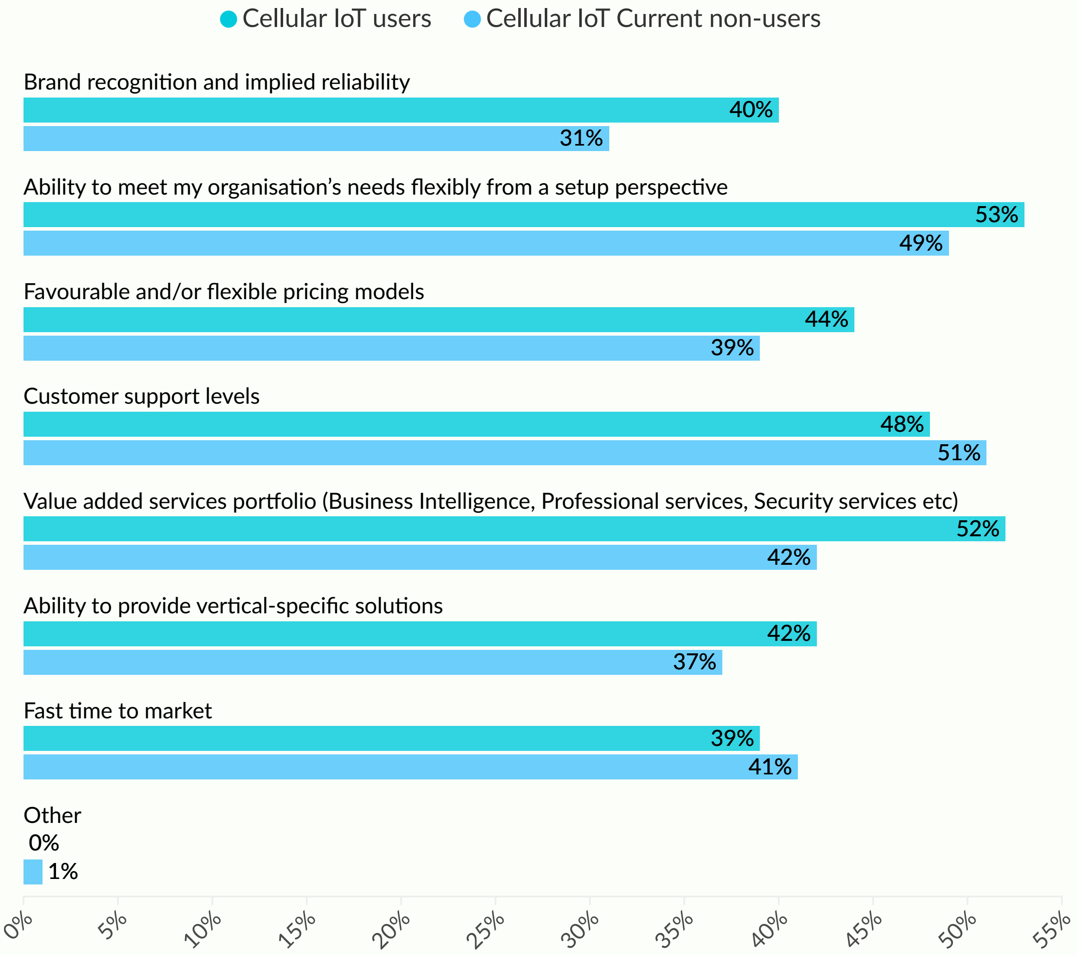


However, the requirement for security features is distinct from the perception of actual threat; security is still a highly popular feature even among those who consider data breaches less of a pain point for their business. This also holds true for a desire for network threat mitigation capabilities. As such, the main driver here is likely a requirement for regulatory compliance, or an increasing general awareness of the need for cybersecurity, rather than an increased perception of threat to organisations as such. Organisations can leverage cellular technology with eSIM as the root of trust to deliver end-to-end security and help mitigate cybersecurity risks.

The high desire for security holds for all forms of CSP, with respondents showing very little difference in attitude to security features whether they engage an MNO or MVNO as their IoT CSP, which means that all need to be able to offer security products, either through partnerships or their own in-house products. Partnerships are probably the best model for smaller MVNOs, who may not have the requisite in-house expertise but still need to offer security VAS as an option.

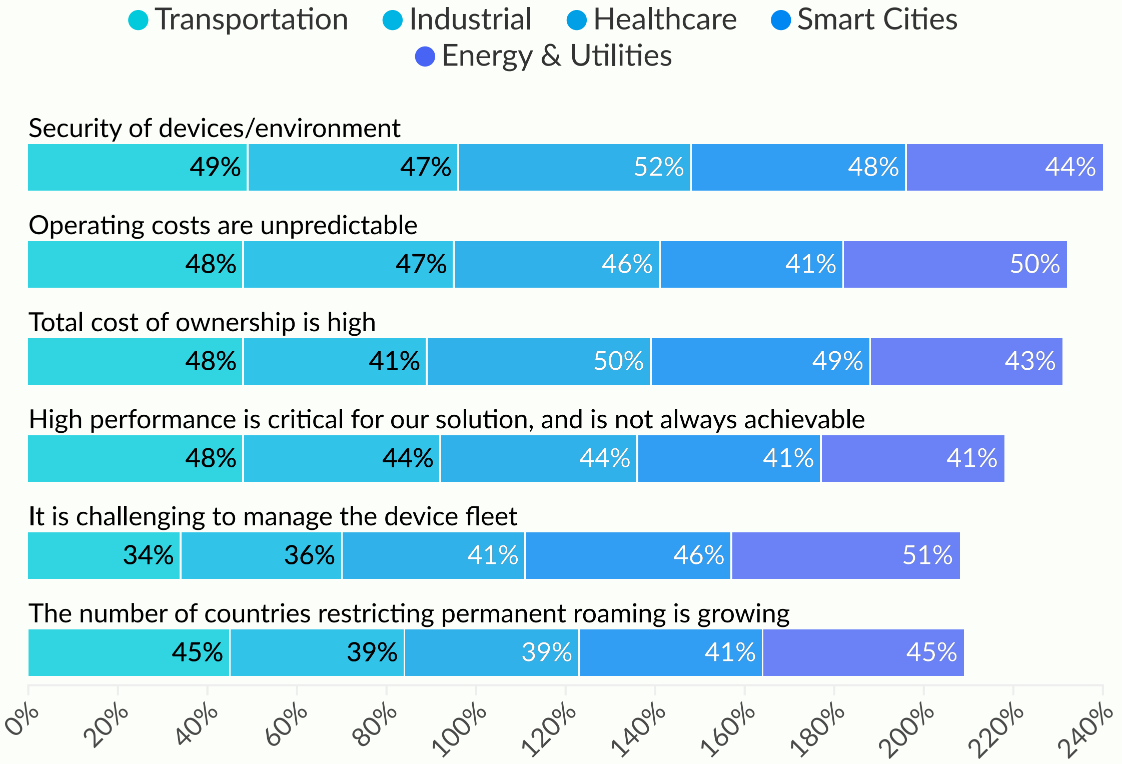
Security is an important VAS to offer, with respondents reporting network threat detection and mitigation as the second-most popular VAS among current cellular IoT users. With a strong VAS portfolio given as the second most common non-technical influence on purchase decisions for these users, and being chosen by over 40% of current non-users, presenting a strong set of security features will be key to attracting customers to a CSP's product overall.

What are/would be the main non-technical/commercial influences impacting your choice of potential IoT connectivity service provider? (Cellular IoT users and non-users)



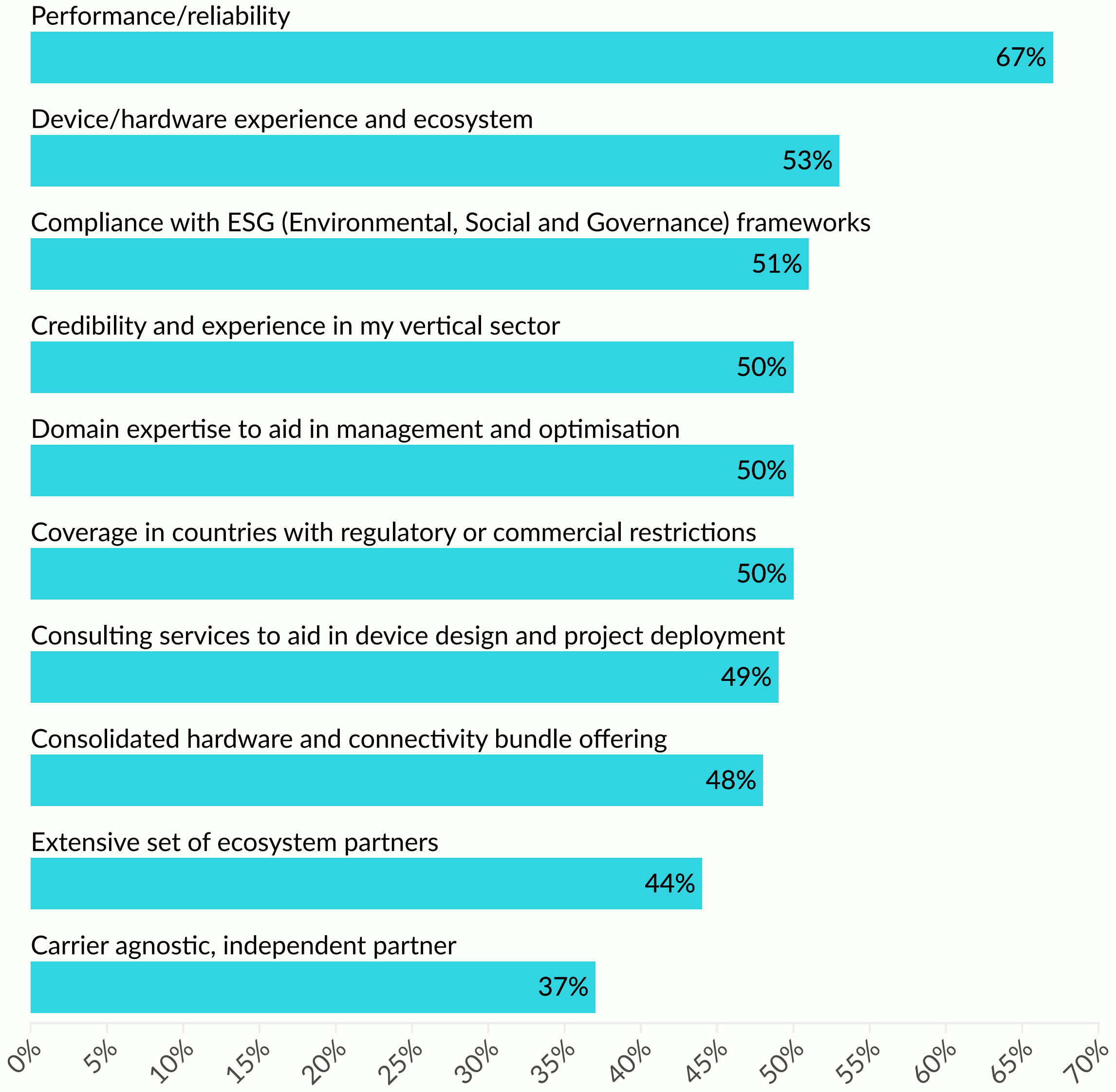
This security also needs to be end-to-end, desired by more than half of respondents as noted above. To fully achieve this, security needs to be a concern from early in the IoT connectivity journey, with hardware security a potential concern alongside network security. Indeed, device security is considered the biggest challenge for scaling up IoT deployments, with 48% of respondents putting it in their top 5. The IoT SAFE solution should be considered early in deployments to enhance integration within enterprise systems, allowing for better scalability and improved trust among users.

What do you perceive to be the top 5 challenges where scaling up cellular IoT connectivity deployments is concerned? (All respondents; proportion selecting items within their top 5)



As a concern at both hardware and software levels, it is clear that security is not just a nice-to-have extra, but something that needs to be introduced and addressed throughout the whole development and deployment process. CSPs need to be ready to offer thoroughgoing security services in their products. However, they will often be able to affect a large portion of the ecosystem for any given customer; almost half of respondents are looking for consulting services for device design from their CSP, giving connectivity providers the ability to step in at the hardware level. Being able to offer device security as part of that package will be an attractive proposition, particularly given the desire for security by design in many places. This means that end-to-end security provision, becoming more involved with device design or provision can bring in new service revenue for CSPs that can deliver it.

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

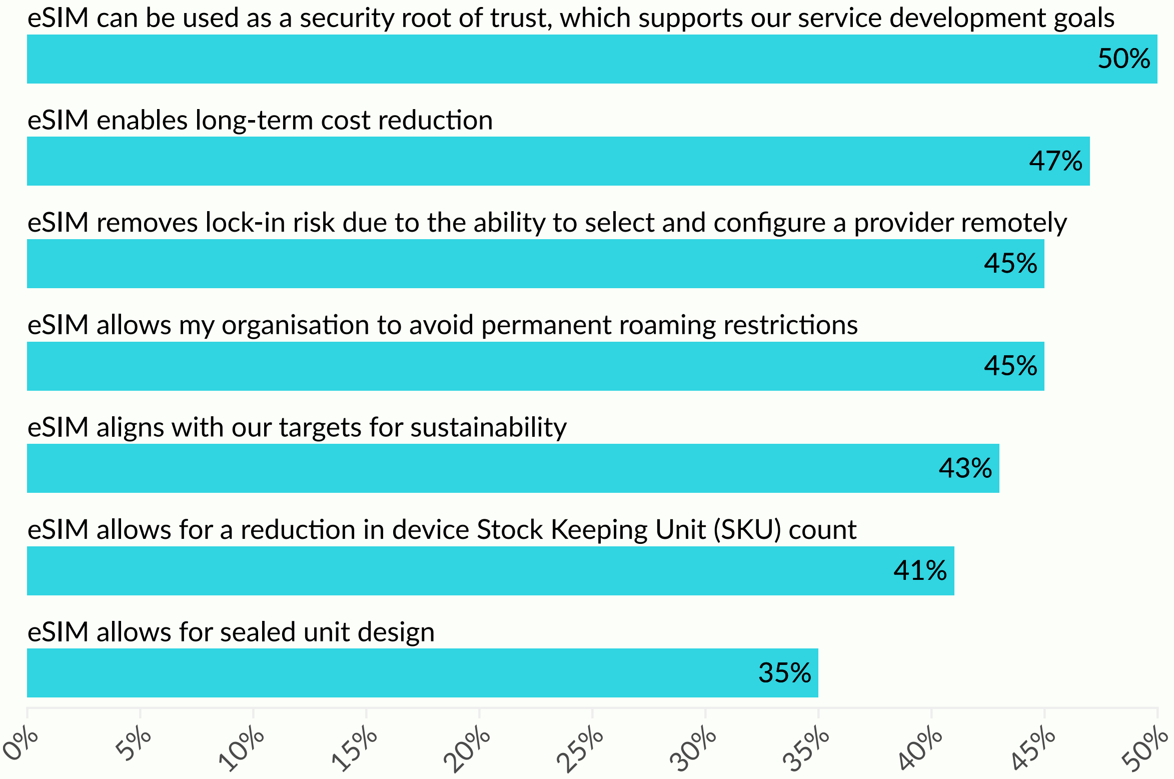


Indeed, the above chart shows that being able to offer strong consultative services in general is something that is desired, which includes security but goes beyond it. After the expectation of performance, many capabilities are linked to the ability to customise deployments and make them relevant to the context of the enterprise. Customisation and flexibility are vital at the product level too, as 60% of respondents placed extensive security features as part of their top 5 product factors, and 50% want technical and commercial flexibility. Both of these factors will require a high degree of customisation to fully meet customer expectations, which can only really be addressed through a consultative approach.

eSIMs for Enhanced Security

While not conventionally thought of or often marketed as a security solution, the eSIM (embedded SIM) can significantly enhance security. With the SIM function provided as a chip rather than a removable card, many tampering risks are eliminated, and the SIM's cryptographic production and storage capabilities can provide a solid identity basis for devices. As the technology is a permanent part of device hardware with established cryptographic capabilities, eSIM and iSIM (integrated SIM) can perform this function in a way that previous generations of SIM technology never truly could. The ability to provide a hardware-based root of trust is of particular use in mixed-vendor environments, which will be common in an enterprise context. eSIMs can offer a means to bridge the gaps between different systems used across an enterprise's operations, with a consistent trusted identity for network entities that persists between systems.

What factors made you choose eSIM (eUICC)?



The potential to use eSIM as a form of security is being steadily recognised by enterprise users of the technology; 50% of eSIM users reported that they see the eSIM's ability to be used as a secure root of trust as a core benefit of the technology, scoring highest of all drivers for eSIM usage. However, it should be noted that users who want to use eSIM as a root of trust also report high levels of belief in eSIM's other benefits, meaning that the security messaging surrounding eSIM has often been communicated alongside the other benefits. As such, it may not drive strong adoption of eSIM on its own, but rather is part of an appealing package of benefits the technology offers.

The ability to include eSIM as part of a security solution makes truly end-to-end security far more possible. This potential will only increase with the forthcoming SGP.42 standard, which will enable in-factory provisioning, making the audit trail of the SIMs and the devices they are attached to much clearer than previously possible. This feature should be emphasised for the market as part of generalised eSIM marketing; with 30% of eSIM non-users reporting they are unsure of the benefits, a security-first posture for the technology can act as an appealing hook through which to begin presenting eSIM's benefits.

With a security feature part of device hardware, it makes interception and replacement of connectivity elements far harder, with baked-in encryption and identification present through the IoT SAFE standard. While there are some alternatives to these implementations, they are very often proprietary or flawed in some way. For example, the Generic Bootstrapping Architecture (GBA) provides identification linked to the SIM application, which will change if the profile is changed. As a result, this and other software-based approaches have significant flaws in comparison to using eSIM hardware-based security.

Security has remained a consistent appeal of eSIM over the years of this survey, and now has a slightly greater value to respondents than the traditional benefit of removing operator lock-in. This indicates both a maturation of the technology, and signals that from a customer perspective, understanding of the technology is improving. It also means more stable revenues for MNOs from eSIM users, who are becoming less concerned with the ability to switch providers and more aware of the other benefits of the technology.

The ability to guarantee continued secure international connectivity is vital, and eSIMs can provide both that international continuity and a secure and persistent identity for connected assets.

Across all surveyed sectors, respondents placed end-to-end security in their top five challenges overall and nearly half place device security in their top five scaling challenges. The good news is that there are provisions within the SIM itself such that it can be used as a trust anchor to be utilised as a root-of-trust for end-to-end security. Traditional approaches in end-to-end security would entail highly specialised hardware for key and credential storage, adding costs to the Bill of Materials.

To take advantage of the ubiquitous presence of SIM, eSIMs and iSIMs across sectors served by cellular IoT, in the following pages, Kigen highlights a few examples of pragmatic approaches to ensure efficient global deployments, profitable operations, and end-to-end trust that delivers new revenue streams.

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

The Challenge

There are several proprietary hardware SE (Secure Element) solutions available to to execute security services and store security credentials, as a ‘Root of Trust’ but market fragmentation introduces a key challenge.. Many IoT solutions rely on proprietary hardware SEs, creating market fragmentation and complicating the process of delivering consistent security across different devices. Enterprises now face the challenge of ensuring end-to-end security for their IoT deployments while maintaining interoperability and scalability.

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

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

The Solution

Developed by the mobile industry, the GSMA IoT SAFE (IoT SIM Applet For Secure End-2-End Communication) standard enables IoT enterprises, device manufacturers and service providers to leverage the SIM, eSIM or iSIM as an applicative KeyStore where security keys are securely stored and dynamically managed. There is also no need for an expensive and dedicated Secure Element. What's more, Kigen's IoT SAFE solution goes further to ease the development of integration into enterprise solution stacks to deliver greater scalability, simplicity, and trust.

Each SIM produced by Kigen is fully certified in both manufacture – GSMA Security Accreditation Scheme for UICC Production (SAS-UP), and management – GSMA Security Accreditation Scheme for Subscription Management (SAS-SM). Combined with the industry-leading secure SIM OS, Kigen's IoT SAFE solution addresses key design hurdles, simplifying how design middleware can easily access SIM, eSIM, or iSIM services. This radically changes the way enterprises can use SIM, eSIMs or iSIMs as a viable and available solution that works in tandem with Crypto Quantique's market-leading solution to fully secure connections for authentication, encryption and service acceleration.

Looking Ahead

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

Smart metering: simplifying connectivity anywhere, at scale

The Challenge

For manufacturers of connected products, the challenge lies in providing the SIM card with appropriate cellular connectivity for the countries where the device will be deployed. Physical SIM cards had to be manually inserted into each device based on their intended use, adding an extra step to the production process.

Global smart metering solutions provider Iskraemeco, set out to help energy companies effortlessly deliver customer insights and functionality thanks to secure and trusted 'built-for-Internet of Things (IoT)' solutions for its smart meters, that are destined for multiple markets across the world.

The Solution

Prior generations of smart meters relied on Radio Frequency (RF) communication technology which is prone to interference from other devices in high concentration areas, vulnerable to obstructions, such as walls, which cause signal instability and result in shorter effective communication distances.

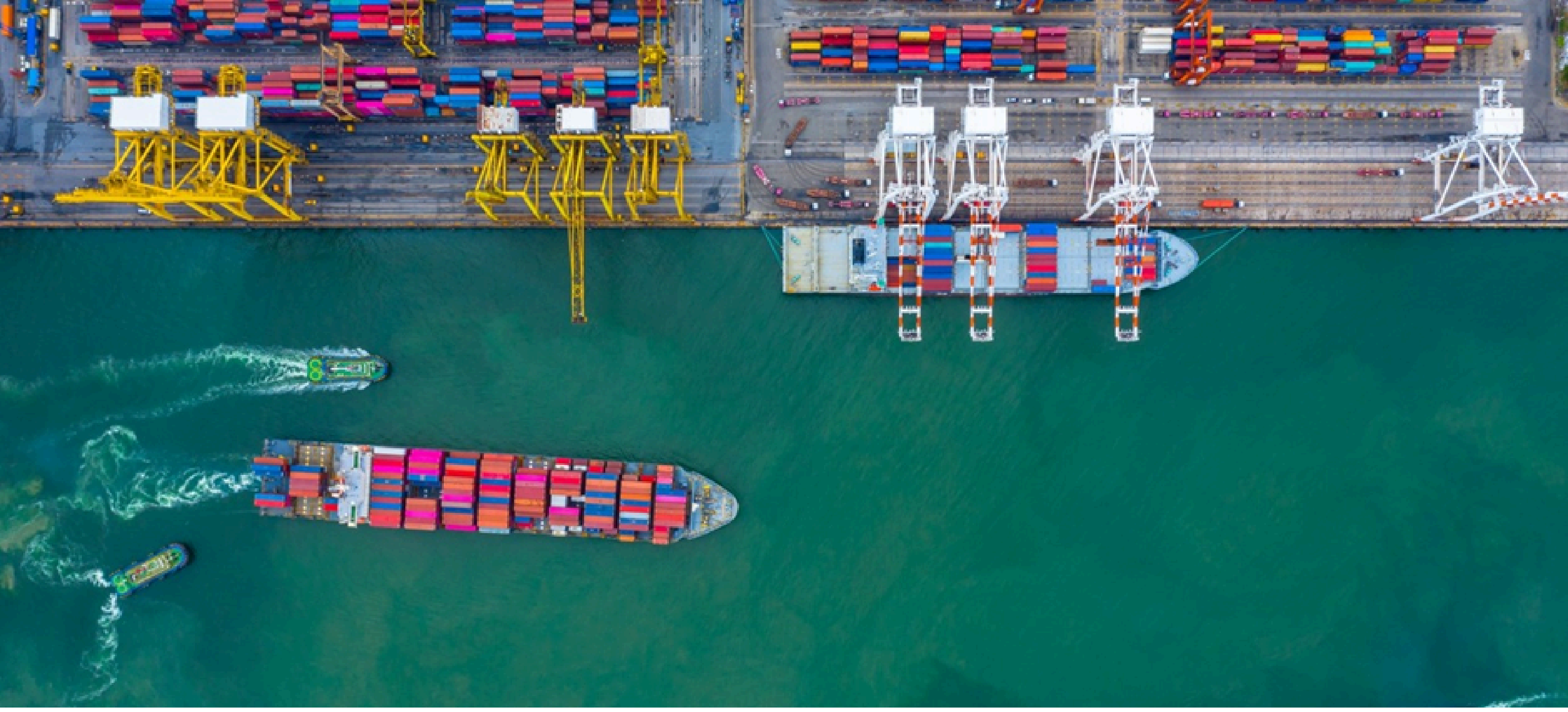
Increasingly to avail new possibilities in how data can generate revenue streams for utility providers, cellular technology proved to be the right choice.

Iskraemeco foresaw that fast-changing legislation could become a hurdle for energy companies looking to scale. Further, Kigen's eSIM solutions opened new possibilities in how data can generate revenue streams for utility providers, positioning them as broader service providers.

Flexibility is key for smart grid-ready solutions. That's why Iskraemeco transitioned to an eSIM with Kigen M2M OS software. Each eSIM comes personalized with a global bootstrap, enabling both factory over-the-air meter testing and out-of-the-box global connectivity from Kigen's ecosystem of partners. If a local network is preferred, the Kigen remote SIM provisioning (RSP) service can provide a local operator profile with no need for physical access to the device. Interoperability across MNO profiles, as well as modular subsystems, remove hurdles for utilities when integrating mobile technology for large-scale, cost-sensitive smart meter deployments.

Looking Ahead

Looking ahead to new opportunities in simplification through standards-based approaches, Kigen's eSIM OS and RSP server solutions are designed to speed up the manufacturing of large volumes of connected IoT devices by simplifying device connectivity management during deployment. It simplifies logistics by pre-configuring IoT devices with relevant cellular connectivity for specific regions, eliminating the need for OEMs to support multiple SKUs. Kigen plays a part in the industry's collaborative work on the latest eSIM standards, helping bring simplification to adopters in all sectors. Kigen's In-Factory Profile Provisioning (IFPP) involves securely digitally loading SIM profiles during manufacturing based on the device's intended deployment location – reducing the cost, risk, and total cost of lifecycle management of remote assets in critical infrastructure.



Global logistics: Reducing risk of IoT roaming restrictions for mobile assets

The Challenge

With the rise in global data privacy regulations, managing cellular connectivity for connected assets that move across borders has become increasingly complex. For instance, in Turkey, strict legislation mandates the use of local SIM profiles for devices operating within the country, complicating logistics for Original Equipment Manufacturers (OEMs). Strict legislation mandates that local profiles be downloaded onto a device with an eSIM and managed by an authorized Turkish operator.

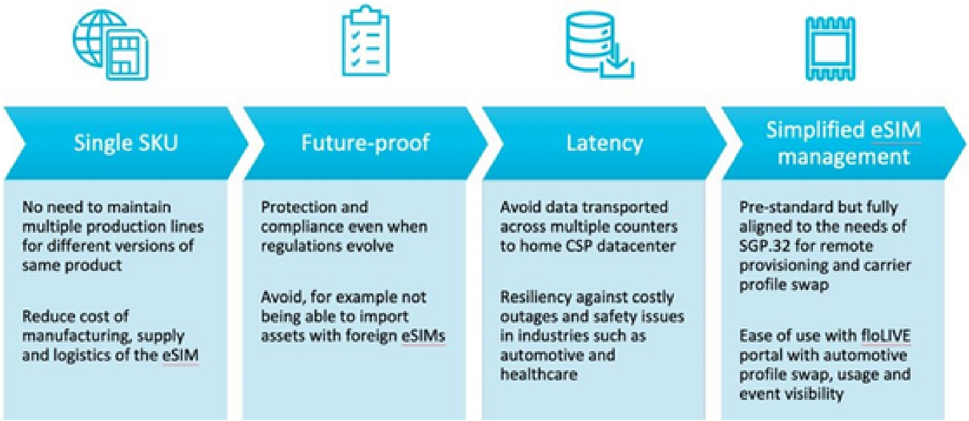
For global shipping and logistics solutions enterprises, the move to cellular eSIM eliminates additional expenses due to the need for different SIM cards for devices destined for Turkey.

The Solution

Kigen, in collaboration with global connectivity provider floLIVE and Turkish operator Protahub, developed a comprehensive solution to provide uninterrupted cellular IoT coverage across borders. By using Kigen's eSIM with remote provisioning capabilities, OEMs and logistics companies can comply with local regulations while managing connectivity remotely. This solution eliminates the need for multiple physical SIM cards, reducing production complexity and operational costs.

The eSIM technology allows a new SIM profile to be downloaded and activated remotely, ensuring devices comply with local regulations without requiring physical access to the asset. This capability streamlines supply chains, making it easier to serve global markets while adhering to roaming and data privacy laws.

As a result of rigorous testing and collaboration between the companies, the system can scale, allowing remote localization and provisioning in minutes, avoiding individual agreements, especially when multiple partners are considered. This saves time, critical 'downtime' and additional costs.



Single SKU	Future-proof	Latency	Simplified eSIM management
No need to maintain multiple production lines for different versions of same product	Protection and compliance even when regulations evolve	Avoid data transported across multiple counters to home CSP datacenter	Pre-standard but fully aligned to the needs of SGP.32 for remote provisioning and carrier profile swap
Reduce cost of manufacturing, supply and logistics of the eSIM	Avoid, for example not being able to import assets with foreign eSIMs	Resiliency against costly outages and safety issues in industries such as automotive and healthcare	Ease of use with floLIVE portal with automotive profile swap, usage and event visibility

Looking ahead

With over 162 countries that are enacting data privacy and localization laws, connected assets in motion have varied considerations. From devices that can be truly remote and require Non-Terrestrial Network (NTN) connectivity, to devices that may be operational on different architectures or interim and proprietary approaches such as multi-IMSI, multi-profile solutions, Kigen offers enterprises the ability to manage eSIMs throughout their lifecycle through a consolidated portal, in Kigen Pulse.

Kigen Pulse allows for defining business rules that govern the automatic profile swap process and provides visibility to profile usage and network events, making connectivity transparent. Kigen's eSIM solutions are designed to allow enterprises to leverage connected devices while maintaining full control of their connectivity deployments with a world class choice in connectivity providers. Kigen is committed to working with top operators around the world to provide you with eSIM-based access to their networks. With your business gaining global coverage, you can focus on expanding your IoT business and continue generating revenue without interruption.

About the Authors

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

Kigen

www.kigen.com

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: November 2024
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.