KALEIDO PERSPECTIVES

NETWORKS FOR FUTURE IOT: CUSTOMER DEMANDS & SERVICE PROVIDER READINESS

INTRODUCTION

THIS PERSPECTIVES DOCUMENT PROVIDES AN ANALYSIS OF HOW SERVICE PROVIDERS IN THE INDUSTRY MUST REEVALUATE HOW THEY POSITION NETWORK INFRASTRUCTURE ON ACCOUNT OF REGULATORY IMPACTS AND ENTERPRISE AI WORKLOAD REQUIREMENTS.

IT EXAMINES HOW REGULATIONS ARE EVOLVING TO DISRUPT TRADITIONAL ROAMING ARCHITECTURES, AND HOW NETWORKS OF THE FUTURE MUST BE ARCHITECTED TO ME HIGHLY RESPONSIVE.

AN EVALUATION OF SEVERAL STAKEHOLDERS' POSITIONING RELATIVE TO EMERGING REQUIREMENTS IS PROVIDED.

Kaleido Intelligence Limited

About Kaleido Intelligence Limited

Kaleido Intelligence is a specialist consulting and market research firm with a proven track record delivering telecom research at the highest level.

Our Mobile Roaming and Connectivity research service covers the following industry leading publications:

- Manufacturing Connectivity Opportunities & Forecasts
- Cellular Satellite Communications Opportunities & Forecasts
- Smart Cities Connectivity Opportunities & Forecasts
- Healthcare Connectivity Opportunities & Forecasts
- IoT Roaming Strategies & Forecasts
- 5G Roaming Future & Forecasts
- Wholesale Roaming Strategies & Competitive Analysis
- Retail Roaming Trends & Forecasts
- Mobile Roaming Data Hub 2016-2028
- IPX Data Roaming Outlook & Forecasts
- International Travel & Tourism Trends
- International Travel & Tourism Forecasts
- Blockchain in Roaming & BCE
- eSIM Market Outlook
- Mobile Network Security & Fraud

For more information on this market study or if you have further requirements, please contact our analyst team at:

info@kaleidointelligence.com

+44 (0) 2039839843

Authors:

Steffen Sorrell, Research Lead

Nitin Bhas, Strategy & Insights Lead

Publication Date: 01-04-2026

Kaleido Intelligence aims to provide accurate information. The information provided here is designed to enable helpful data and analysis on the subjects discussed. References to companies are provided for informational purposes only. Kaleido Intelligence does not endorse any operators, vendors, services, or products mentioned in this research and market study.

Kaleido Intelligence prides itself on its reputation for maintaining the highest standards of integrity in conducting fair and impartial research. While the information and content of this publication are believed to be accurate and from sources believed to be reliable 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 study consists of the opinions of Kaleido Intelligence and should not be construed as statements of fact. It contains forward-looking statements, analyses 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.

Kaleido Intelligence's competitive analysis section is based on information provided to us by the vendors/companies as well as using product brochures, press releases, case studies and other marketing materials available in the public domain. In no event will Kaleido Intelligence be liable for loss or damages of any kind (including consequential loss) arising as a result of the use of or inability to use its research, market analysis, forecasts, vendor assessment and scores included in this document.

Table of Contents

Chapter 1: IoT Regulations Disrupt the Status Quo

1.1 Introduction

There can be no doubt that complexity in cellular IoT connectivity is increasing. Regulations in addition to shifting enterprise priorities in terms of AI deployment mean that, in many instances, traditional approaches towards connectivity enablement will either no longer be compliant, or unsuited to customer business requirements. In line with what Kaleido has been emphasising over the past 5 years is the fact that mobile network infrastructure deployed to support cellular IoT connectivity will increasingly form a differentiator for service providers aiming to win business opportunities within mission-critical segments of IoT. Moving forward, it is highly likely that the majority of IoT projects will be impacted in some manner or another by national or regional regulations that impact how enterprises must deal with approaches towards data handling and security.

Historically, MNOs' mobile core network infrastructure has been built to support domestic operations. Tier 1 MNOs benefit from the support of OpCos in terms of available footprint and often, infrastructure, although the ability to terminate traffic based on OpCo infrastructure availability varies. Indeed, for the majority of M2M/IoT's history, international connectivity requirements have been enabled through home-routed roaming architecture. By definition, this forces payload traffic from the visited network to the home network and back, and realises compromises in terms of cross-border traffic flows in addition to higher connectivity latency. Many MNOs, and some full MVNOs have secured non-geographic '901' IMSIs to support this approach. Direct roaming agreements are commonly favoured among MNOs, while sponsored roaming or one-to-many access agreements via roaming hubs are most often leveraged by MVNOs. This has achieved scale in terms of a global footprint, and has simplified end-customers' operations due to the fact that the need to establish contracts with domestic operators in each market to be serviced is considerably reduced.

The COVID-19 pandemic represented something of an inflection point where operator and regulator stances in regard to IoT roaming is concerned. The levels of continued roaming traffic in the absence of consumer roaming due to lockdowns came as a wake-up call to many, with inbound IoT roaming not representing a metric that was closely monitored by a majority of operators. The result of this is twofold: on the one hand, dedicated IoT roaming agreements are now much more common. On the other, operators and regulators, depending on the country in question, have adopted protectionist stances towards permanent roaming (where IoT devices remain active in the visited network for 60-120 days or more). Permanent roaming has formed much of the discussion over connectivity over the past half a decade, and has driven specific permanent roaming commercial agreements as well as the use of eSIM or multi-IMSI alongside various technical setups in terms of profile/IMSI hosting as a means of compliance. That said, for MNOs, eSIM during the M2M specification era has been deployed by necessity as a means of providing an insurance model for large-scale automotive customers and utilities companies. Meanwhile, multi-IMSI has almost entirely been eschewed. This is in contrast to MVNOs that have made multi-IMSI part of a dynamic offer to support various roaming and localisation capabilities, albeit with some commercial and technical overhead impact.

1.2 Regulatory Shifts

The issue of permanent roaming restrictions has become relatively widespread. Markets such as Brazil, India, China, Turkey, USA, Canada Australia, as well as parts of the GCC, Africa and Asia have restricted permanent roaming either at the operator level, or at a regulatory level. Nevertheless, markets with clear-cut restrictions do not tell the complete story. For example, while permanent roaming in across Europe is generally permitted, that has not stopped operators applying certain contractual restrictions in terms of their commercial agreements, while countries may apply restrictions in terms of allowing M2M communications only, thus disallowing voice-enabled IoT deployments on a permanent basis.

Regulations that impact traditional IoT architectural approaches go beyond permanent roaming. Rules surrounding PII (Personally Identifiable Information) in terms of processing and storage are now well-established with nearly every country in Kaleido's database including some level of restriction in regard to how data can be processed. Regulations surrounding licencing requirements for CSPs (Connectivity Service Providers) are much more fragmented and can range from no requirement at all to a strictly enforced mandate that operating companies must have a local presence within the country which in turn entails proper application of tax liabilities and potential commercial disruption.

More importantly, data sovereignty regulations extend beyond PII enforcement, and in several jurisdictions now apply restrictions with regards to enterprise or industrial IoT data. Much of this regulation is related to 'critical infrastructure,' where country-by-country definitions vary, but typically include financial services, energy and water, healthcare and transportation applications. However, some jurisdictions are moving to create comprehensive IoT data localisation mandates. In either case, distributed network infrastructure forms a key part of being able to demonstrate compliance with local or regional regulations.

One of the most disruptive shifts in the regulatory environment is with regards to AI. Over the past 2 years, performance of both 'frontier' closed-weight LLMs (Large Language Models) as well as open-weight models has substantially improved, while the ability to apply generative AI for more advanced business applications has been facilitated by ever-improving agentic frameworks to support multi-step process automation. Trillion-parameter frontier and hundreds of billions of parameters open-weight models require large-scale infrastructure for both training and inference, even as Mixture-of-Experts (MoE) models have emerged to substantially reduce the number of evaluated parameters per pass. This is well beyond the computing power of nearly all IoT devices, and is largely unsuited to edge processing facilities due to the hardware and power investment required. On the other hand, the increased quality of large-scale models has opened the door for quantised or distilled SLMs (Small Language Models, typically under 8 billion parameters) to be deployed on devices, or within edge processing facilities.

The result of this is that, at national and regional level, regulations are being developed that are likely to expand in scope moving forward. This directly impacts the connectivity landscape, owing to the fact that, for training and inference workloads, there is now incentive to ensure that data sovereignty requirements are met. **Kaleido's full Networks for IoT report** provides clear summaries of data sovereignty regulations across 24 selected markets worldwide.

1.3 AI Regulation

The drivers behind AI sovereignty are broadly driven by the prevailing geopolitical environment in addition to operational and technical factors.

Whilst the full impact of current advances in AI are both not yet fully understood nor evaluated, the level of investment that is being injected into the industry means that at a political level, it is viewed as a technology of critical national or regional importance. With tensions between global superpowers at their highest level for decades, entities such as Anthropic are pushing for greater AI regulation, while it is certainly the case that the US has adopted a protectionist stance where supply of critical technology and intellectual property is concerned. The net result of these factors is that in general, the regulatory environment and how the landscape will evolve remains uncertain.

Today, several nations in addition to the EU have developed, or begun developing frameworks that have an impact in terms of how AI-related data must be handled. Our full **Networks for IoT** report cites examples of this in countries across global regions.

1.3.1 Enterprise Strategy

The forthcoming uncertain and potentially fragmented regulatory environment provides part of the necessary amplification needed to drive demand for sovereign AI capabilities. However, there are also technical and operational factors to consider:

- Data used to train AI systems is considered valuable IP which must remain under the control of the entity that produced it.
- Compliance overhead will be encountered where international organisations deploy AI workloads where the regulatory environment differs substantially so as to require differing approaches towards training and inference.
- AI will frequently demand low connectivity latency to support responsiveness.

Evidence points to the fact that many enterprises have already made the decision to emphasise a localised strategy with regards to AI. Findings from Deloitte's 'State of AI in the Enterprise' survey, published in January 2026, highlights that 8 out of 10 enterprises view sovereign AI at least moderately important to strategic planning. Meanwhile, 58% of the audience reported that their AI stacks are primarily built with local vendors, with a high emphasis being placed on full in-country infrastructure.

With the same survey reporting that 74% of enterprises plan to deploy agentic AI within their organisations within 2 years, the combination of regulation and enterprise requirements regarding AI inference location as well as performance requirements offer powerful drivers towards the re-examination of traditional mobile network architecture.

1.4 Network Topology & Security

Developing regulations associated with data security as well as AI workloads serve to drive new demands where both the topology of the network as well as the security implementation of the network are concerned.

Security

As part of Kaleido's annual **Connectivity Vendor Hub analysis**, respondents were asked to provide feedback covering both how clients across verticals were using CMPs (Connectivity Management Platforms) in addition to features that were being demanded by clients.

Notably, several vendors noted that demand for anomaly-based detection is increasing, particularly in verticals such as:

- Automotive
- Logistics and Fleet Management
- Security/surveillance cameras
- Retail and Point-of-Sale
- Industrial and Utilities

Many use cases under these verticals fall under areas where regulation is having an increasing impact. On the one hand, this increases the need for real-time asset visibility to better manage security threats, and also encourages network operators to adopt more security-conscious approaches to connectivity service provision, such as through zero-trust security models and exposing capabilities to allow enterprises to continuously monitor assets via their own SIEM, or via tooling embedded into the CMP. While not ubiquitous, the last 3 years have undoubtedly seen an increasing number of players adopt these models in the form of agentless security monitoring capabilities either in partnership or through in-house development activities. As regulations impacting the handling of AI-related data become more prevalent, features such as FQDN (fully qualified domain name) filtering, anomalous behaviour detection and packet capture solutions are likely to become table stakes for customers within 'high risk' verticals, while the network posture itself must pivot towards the ability to support long-term device auditing, dynamic policy enforcement on a granular basis, rather than at APN- or service-plan level.

Network Topology

Traditional mobile network architecture supporting IoT deployments on an international basis frequently relies on a centralised core, with limited availability of distributed packet gateway infrastructure to support data sovereignty or application performance requirements. Meanwhile, the availability of 5G Standalone (SA) on a consistent basis even among tier 1 operators is almost entirely absent today, with rollouts impacted by the deployment model of 5G when moving from 4G, in addition to a highly complex and much-disputed implementation of the security model for 5G SA under roaming scenarios.

The ecosystem has now matured to a point where infrastructure as well as 5G SA are very real considerations. Given the context provided in this report, both infrastructure as well as 5G SA capabilities should be viewed as complementary, particularly in IoT verticals where AI workloads are deployed and rely on shared pools of data. A byproduct of this is that, due to the slow progression of 5G SA roaming, the need for 5G technology to support advanced workloads may actually increase the demand for localised connectivity even in enterprise use cases that are not heavily impacted by regulation.

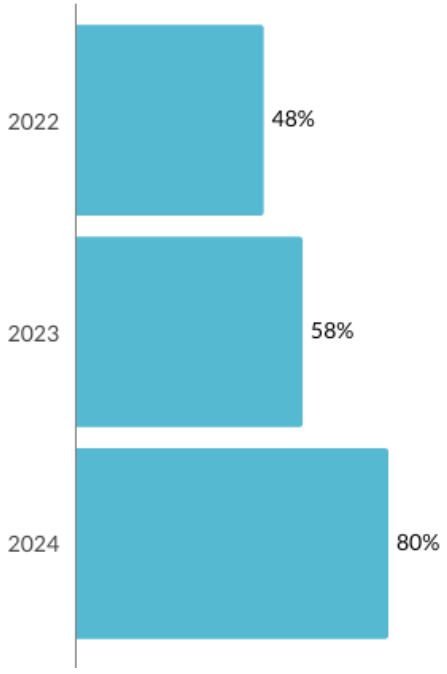
Proximity of infrastructure to devices is likely to become more important over time, as more enterprises deploy AI inference on devices, edge gateways and routers, or MEC infrastructure.

Chapter 2: Enterprise Requirements

2.1 IoT Maturity Signals Change

It is undeniable that IoT as a concept is maturing and, for many businesses, has become a core part of operations. In Kaleido's own enterprise surveys, reported adoption of cellular IoT rose from 48% of surveyed enterprises and OEMs in 2022 to 80% in 2024. Naturally, this is not an absolute reflection of the market in terms of adoption, but highlights rapid growth in take-up of cellular IoT solutions.

Figure 2: Cellular IoT Adoption Evolution 2022-2024. Survey Qu 'What is Your Organisation's Stance Towards IoT?'



Source: Kaleido Intelligence Enterprise Surveys 2022-2024

There are further patterns that highlight a growing maturity among IoT customers. Adoption of specialised single-pane-of-glass CMPs such as Simetric and IoTM is driven by enterprise requirements where organisational IoT deployments are multi-country and fragmented across a number of service providers. As part of this maturation, the need to support end-to-end device contexts, policy enforcement and automation across the cellular network in addition to adjacent technologies has driven Simetric to undertake a 2-year ServiceNow mapping project in order to extend orchestration capabilities according to large automotive and utilities clients. Meanwhile, solutions such as Aeris's Watchtower product, initially delivered as a pure network layer security solution, is now viewed as both an observability as well as a security product. Regulation forms a part of this, as enterprises must ensure that they remain compliant, but a significant additional driver is the need to ensure that device estates are behaving as expected, as deviance from this state may have significant cost implications.

In Kaleido's 2024 enterprise IoT connectivity survey, a substantial majority of respondents reported that the ability of the CSP to support data routing in the context of low latency (68%) and data sovereignty (72%) was either of high, or highest importance to their organisation, with data sovereignty proving top-of-mind within the question's framework.

For advanced enterprise and OEM IoT clients, it is evident that new demands are creating opportunities for players able to deliver well beyond traditional IoT connectivity approaches.

2.2 Core Network Design Evolution

Until recently, connectivity was primarily considered as simply a transport layer for the real value in IoT: the data. The result of this is that, despite the fact that connectivity

forms the bedrock of IoT programmes, and that IoT would not be possible without connectivity, its revenue remains a small fraction of the total market value in applications and professional services.

Architecture & Deployment: Addressing Regulation & Mission-Critical Applications

Cloud-native principles are a fundamental part of connectivity resilience. The ability to containerise components and better ensure (versus monolithic designs) that data plane and control plane elements can scale independently from one another are key where applications may trigger spikes in data consumption but maintain steady levels of signalling. Stateless design applied to the network means that, should any network component fail, the session information is not lost while a recovery process is activated. Additionally, stateless design coupled to network nodes in active-active mode ensure that failover is almost instantaneous. This is in contract to active-backup deployment methods, where traffic is mirrored from active to backup nodes. Here, even small delays in traffic mirroring could potentially disrupt applications where, if nodes are not fully in-sync, a connection reset might be required.

Meanwhile, it is important to consider a fragmented regulatory environment. The UK's Telecom Security Act, for example, makes it very difficult for operators of a certain scale to deploy a core network on public cloud infrastructure. Designs that support both public and private deployment types is key to addressing international enterprise requirements.

The Convergence of Transport and Computing

For years, CSPs have transported and processed mountains of data from IoT SIM cards and devices, albeit with limited direct value exposed to the end customer in terms of what the connectivity and the data means to the application, and the net outcome for the customer. Connectivity has largely been considered in a vacuum. Concepts such as 'network for AI' are changing that, with companies such as Ericsson in particular advocating for AI computing resources at the RAN to enable 'AI for network' (RAN resource optimisation), with spare resources potentially devoted to AI inference capabilities at the tower. Overall, this represents an emerging opportunity to monetise connectivity as a value asset, and not merely as a transport mechanism.

Flexible architectures in core network design as outlined earlier mean that from a proximity perspective, potential support for enterprise AI inference requirements is more adaptable than simply placing AI computing resources at the RAN. That said, the deployment of GPU and DPU (Data Processing Unit) resources at edge PoPs is not common today among operators. However, this approach is likely much more efficient than placing AI capabilities at the RAN:

- Resources at the RAN are limited to devices within the proximity of the tower. This raises the risk of unused resources.
- Cooling and power challenges mean that many RAN sites will be unsuited to AI workload deployment, without significant Capex investment.
- AI resources at edge PoPs receive aggregated traffic in most instances. This means that the likelihood of resources remaining idle are much lower.

- Given global investment in data centre resources to support AI training and inference capabilities, access to relevant resources to support AI workloads is more readily available when compared to RAN sites.

It is unlikely that all workload requirements can be met purely by placing resources in the network. An enterprise's own, or cloud-based frontier model is more than likely to be required, which has additional implications. Here, the ability to flexibly deploy infrastructure becomes fundamental as part of capabilities to ensure the lowest latency and highest quality links to interconnects and on-ramps to hyperscale infrastructure.

Network Programmability & Compliance

Programmability in terms of API use among large enterprise customers to monitor and manage SIM estates is already common. Over the past few years, some players have been positioning themselves as 'network as a service' providers, with an emphasis on programmable policy enforcement. How APIs are used by platform users is of growing importance among both CSPs as well as enterprises as API calls made not only provide a beneficial service, but also serve as an indicator of possible configuration issues, or possibly malicious activity.

With several platforms developing MCP servers to enable LLMs to programmatically access platform capabilities, the definition of what underlying APIs are capable of, and how their use is monitored becomes even more important. Naturally, this also becomes an opportunity to develop monetisation opportunities, depending on the expanse of capabilities exposed. For example, if new network resources are added through a programmatic request, this is most likely a chargeable event.

While there is a revenue opportunity here, it must be considered in balance with potential security risks, particularly where LLMs and agentic AI frameworks are utilised to access MCPs. Here, zero-trust policies become more important than ever, while API resource monitoring to the benefit of both the CSP as well as the enterprise is fundamental.

Chapter 3: Mobile Infrastructure Service Provider Positioning

3.1 Introduction & Methodology

One aim of this report is to analyse how various players are positioning on the market to deliver against the changing ecosystem. To that end, Kaleido invited several CSPs during January-February 2026 to provide technical information regarding their core network infrastructure, with questions formulated to understand key performance metrics within the solution.

Each participant was issued the same set of 18 questions, covering core network architecture, optimisation capabilities as well as monitoring and audit capabilities. From these questions, Kaleido has developed a framework to evaluate how different players' core networks are capable of addressing complex demands in terms of:

- Data sovereignty
- Connectivity resilience
- Enterprise AI workloads

Questions covered:

- Cloud Native Architecture
- Jitter Monitoring & Control
- Edge Computing Support
- Path Optimisation
- Point-of-Presence Coverage & Depth
- Traffic Termination Capabilities
- IMSI Redundancy
- High Availability Mechanisms
- Core Deployment Flexibility
- Component Stack Flexibility
- LPWAN Compatibility
- Signalling Storm Mitigation
- APN Handling
- PGW Handling
- IP Address Handling
- Audit Capabilities
- Real-Time Asset Observability
- Core Network Monitoring/Telemetry

All CSPs invited either deploy a fully in-house core network for operations, or deploy via third party partners. In all cases, management of the core network is under the CSP's control. In cases where entities deploy solutions via their own as well as through MNO partners' core networks, only the solution under the CSP's own control was evaluated.

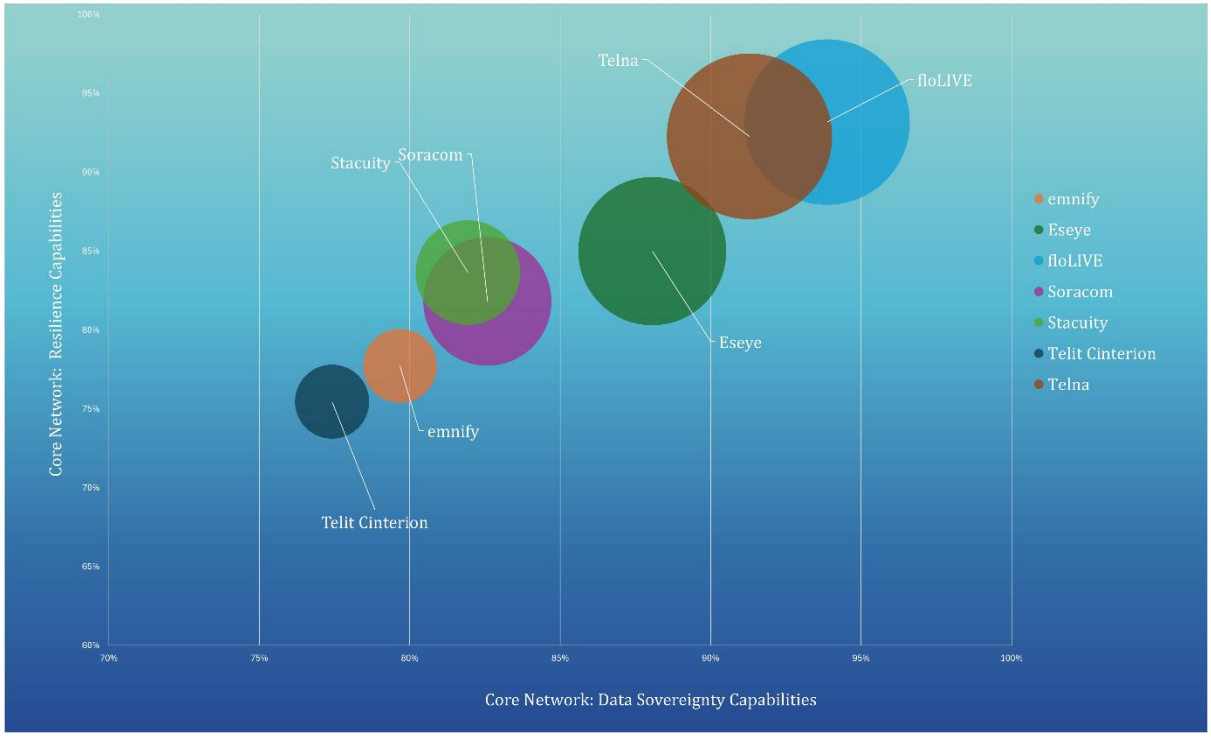
Weightings and focus areas assigned according to the category in question are contained within Kaleido's full report, and available upon request from our support team.

Readers should note the list of vendors within this analysis is not exhaustive, but presents a list of innovative solution providers with a key focus towards IoT connectivity. Vendors that did not provide complete responses to the questionnaire were excluded from the study, on account of the technical nature of the responses required and absence of publicly available data to fill any gaps.

3.2 Mobile Infrastructure Positioning for IoT

The following chart present's Kaleido's analysis of selected players from the ecosystem. The x-axis represents an evaluation of performance in the context of data sovereignty, and the y-axis an evaluation of performance in the context of connectivity resilience. Bubble sizes represent Kaleido's evaluation of how players are positioned to meet enterprise AI workload requirements, with a larger bubble size indicating that the vendor is viewed as more capable.

Figure 4: Core Network Infrastructure Capabilities Analysis



Source: Kaleido Intelligence

3.3 Player Summary

- floLIVE was found to excel in all categories. The company has placed a heavy focus on developing core and packet gateway instances across numerous locations across the globe, and has strong capabilities to enable complex routing requirements in order to meet data sovereignty requirements at a granular level. The cloud-native architecture coupled to high availability mechanisms supports a high level of resilience, which is bolstered by the company's strategy to host IMSIs at strategic locations. Tooling to monitor connectivity jitter and optimise connectivity pathways, coupled to the ability to support edge AI workloads means that the company is well-positioned to meet complex enterprise requirements.
- Telna showed strong capabilities to deliver against enterprise AI workloads, with true app-aware routing capabilities coupled to the ability to deploy edge AI workloads. Distribution of its core assets are very broad in the context of global markets, and the company showed excellent capabilities to mitigate issues such as signalling storms and

support seamless failover mechanisms. Connectivity routing capabilities are expansive, although the company prefers to support this on a managed basis, rather than fully enabling a self-service environment as a means of ensuring guardrails. Additionally, Telna showed capabilities to both meet and extend audit capabilities where required, which underlines a commitment to supporting customer compliance needs.

- Eseye reported one of the highest number of PoP locations worldwide which it couples with high availability mechanisms that are backed by customer SLAs. Multiple MNO core networks support resilience, although this type of approach was outside the scope of this analysis. The solution highlighted strong flexibility in terms of deployment options, and core capabilities to address enterprise edge AI workloads are already in place.

- Soracom has operated its in-house cloud-native core network since 2015, with remarkable performance in terms of availability reported, with an architecture that supports auto-scaling of core components such as PGW on-demand. As such. the company excelled in terms of high availability infrastructure, in addition to capabilities that enable customers to configure complex data payload routing according to requirements and regulation. Despite the fact that the network is deployed entirely on AWS, the company reported flexibility in deployment capabilities, including the ability to deploy on private infrastructure if required.

- Stacuity is a relatively newcomer to the mobile infrastructure market, and delivers solutions that have been built from the ground up in-house. In particular, the company adopts a unique approach to payload routing capabilities with a flexibility that is unmatched by others. By virtue of this approach, IP addressing and asset visibility in scenarios where, for example, IMSI or serving networks are changed, does not present any issue. Stacuity has a number of additional PoPs and other features on its current roadmap which will see sovereignty as well as AI capabilities enhanced in the near-term.

- emnify operates an in-house, fully cloud-native solution with a strong set of capabilities applied to ensure that customers receive a high level of resilience across the coverage footprint. Meanwhile, an extensive number of peering points across its network serves to reduce customer latency for mission-critical applications. Notably, emnify reported an ongoing core network development strategy that will see much-enhanced flexibility in terms of deployment, and deliver benefits across data sovereignty as well as resilience focus areas.

- Telit Cinterion offers a robust solution where connectivity redundancy and high availability are key customer requirements, while supporting hybrid architectures that allow it to balance elasticity with regulatory compliance requirements. Telit Cinterion is one of the few providers to support NIDD where partner operators enable it, providing a differentiation point for satellite and LPWAN use cases. Meanwhile IP address anchoring ensures that visibility of devices is handled seamlessly even as connections move across diverse networks.

LATEST RESEARCH FROM KALEIDO INTELLIGENCE

FEBRUARY 2026: CONNECTIVITY VENDOR HUB 2025-2026

Kaleido Intelligence's Connectivity Vendor Hub presents the most detailed competitive intelligence available covering Connectivity Management Platforms, eSIM Connectivity and eSIM Subscription Management, providing new levels of product understanding for this market.

Request Access

ROAMING VENDOR HUB: FRAUD MANAGEMENT

The Roaming Vendor Hub: Fraud Management report, based on extensive primary and secondary research, enables leading roaming fraud management and security vendors to be compared equally and on their own merits.

Request Access

FEBRUARY 2026: CELLULAR IOT CONNECTIVITY SERIES - HEALTHCARE OPPORTUNITIES 2026

This latest edition to Kaleido's Vertical Connectivity reports provides an analysis of the present and future of connectivity in the healthcare industry, offering an assessment of key trends and developments for this sector, from the impact of cellular technology developments to shifts in healthcare business models enabled by digitisation.

Request Access

JANUARY 2026: CONNECTIVITY VENDOR HUB 2025-26 - PRIVATE NETWORKS

Kaleido Intelligence's Connectivity Vendor Hub presents the most detailed competitive intelligence available on cellular IoT connectivity, providing a full market understanding. The report, based on extensive primary and secondary research, enables Private Networks vendors to be compared on their own merits.

Request Access

JANUARY 2026: CONNECTIVITY DATA HUB – H2 2025

Kaleido's Connectivity Data Hub allows companies to accurately measure the current and future size of the connectivity market. This tool provides valuable insights for those interested in examining the overall cellular IoT market or specific segments such as eSIM, cellular-satellite communications, private networks or how growth will develop within key verticals within IoT.

Request Access

COMING SOON

FEBBRUARY 2026: CELLULAR IOT INSIGHTS - VEHICLE TRACKING SUBVERTICAL DIVE

This latest insights report from Kaleido Intelligence evaluates the technological trends affecting the vehicle tracking market.

Request Access