

Magic Quadrant for Managed IoT Connectivity Services, Worldwide

4 May 2026 - ID G00834640 - 71 min read

By Pablo Arriandiaga, Kameron Chao, [and 1 more](#)

Driven by AI automation and advanced eSIM orchestration, managed IoT connectivity services simplify complex global deployments and regulatory compliance. CIOs can use this research to evaluate providers that deliver resilient, unified connectivity across cellular, satellite and edge platforms.

Strategic Planning Assumptions

By 2030, over five Internet of Things (IoT) connectivity management platforms will manage private 4G/5G networks, up from zero today, reflecting the shift to end-user-focused management.

By 2030, two companies are projected to lead global IoT orchestration with agentic AI-driven platforms, up from zero in 2026.

Market Definition/Description

Gartner defines managed IoT connectivity services as a market that enables secured connectivity, data collection, analysis and additional decision services. Managed IoT connectivity services are delivered fully managed, including dedicated help desk and project and service management capabilities, although hybrid managed and self-managed could also apply as delivery models. Self-managed is delivered through a self-

service IoT connectivity management portal, including Level 2 and Level 3 back-office support.

Internet of Things (IoT) devices can use various connectivity technologies. Connections can be cellular (2G, 3G, 4G/LTE and 5G); satellite, low-power wide-area (LPWA) networks (3GPP and non-3GPP); and managed field-area networks (FANs). Managed IoT connectivity services also enable organizations to securely collect, analyze and interact with data streams, therefore providing businesses with the ability to monitor, manage and control (manually and through automation) assets associated with business processes. This includes connected consumer, commercial or industrial products.

Additionally, managed IoT connectivity services may encompass integrated and managed IT infrastructure and systems, operational technology (OT) infrastructure and systems, software, network services (connectivity), and IT services. Managed IoT connectivity services are a solution element within the broader solution sets of digital businesses and OT systems in enterprise environments.

Mandatory Features

The mandatory features for this market include:

- Logistics management — Oversees contract-to-provision procurement and automated servicing of connectivity, hardware and IoT devices, plus reverse logistics and endpoint resale.
- IoT connectivity management portal — Centralized interface for provisioning, change/incident/problem workflows, inventory, performance monitoring, rule-based SIM actions, automation, reporting and security settings.
- Service management and support — Tracks and manages network contracts, assets, and usage; audits performance and SLAs; optimizes expenses; governs service delivery; and provides multilevel technical and on-site support.
- SIM and subscription management — Enables over-the-air (OTA) SIM control (eSIM, iSIM, multi-IMSI), zero-touch provisioning, LPWA-optimized battery profiles, interoperability, multirouting, hybrid deployments and usage analytics.
- Security management — Enforces identity, policy-based access, encryption and secure service consumption; includes change management, APN/VPN, private LTE/5G, security operations center (SOC) analytics and seamless handover.

Common Features

The common features for this market include:

- Device management — Monitors and diagnoses IoT edge devices; manages connectivity switching, OS/app releases, edge event filtering, business-automation and performance analytics.
- Application management — Supports development/distribution of IoT apps across platforms; includes release, incident management and performance analytics.
- Multisourcing service integration — Acts as an agent for customers by managing third-party providers, overseeing service contracts, financial audits, device ownership transfers and solution financing for IoT connectivity.
- Data and analytics — Provides advanced monitoring, reporting and visualization on provisioning, performance, SLAs and predictive/prescriptive analytics.
- Private mobile networks interoperability — Enables deployment of private LTE/5G networks and seamless, secure transition to public cellular services with unified policy and analytics.

Magic Quadrant

Figure 1: Magic Quadrant for Managed IoT Connectivity Services, Worldwide





Gartner

Vendor Strengths and Cautions

1NCE

1NCE is a Visionary in this Magic Quadrant. Headquartered in Cologne, Germany, this IoT mobile virtual network operator (MVNO) focuses on low and middata cellular connectivity bandwidth. Key use cases include smart metering and fleet telematics. 1NCE has expanded its support and professional services to better address complex and large-scale enterprise projects.

1NCE managed 36.5 million IoT connections in the first half of 2025, reflecting a 22.5% year-over-year increase. Its customers tend to be small and midsize multinational corporations (MNCs) across Europe, the U.S., Asia/Pacific (APAC) and Latin America

(LATAM). It is now expanding into 25 new countries to localize logistics, billing and network traffic.

Strengths

- **LPWAN focus:** 1NCE is a recognized player for midsize enterprises in narrowband (NB)-IoT and Long Term Evolution (LTE-M) (3GPP LPWAN), and has recently expanded this practice into Long Range Wide-Area Network (LoRaWAN) networks. It is currently integrating both technologies under a single pane of glass.
- **Network expansion:** Backed by Bell Canada, Deutsche Telekom and SoftBank as investors and network partners, 1NCE continues to expand its network ecosystem. This includes Tier 1 mobile network operators (MNOs) such as AT&T, China Telecom, Claro, EE, Melita and T-Mobile to enhance local access.
- **Industry-vertical assessments:** 1NCE uses AI to process over 4 billion daily data records across 17 industries, enabling cross-customer benchmarking on technical key performance indicators (KPIs). Through the 1NCE Insights platform, enterprises can access data-driven benchmarks for hardware selection and device configuration. Aggregated data also informs ongoing product development and planned AI features, including usage forecasting and personalized pricing.

Cautions

- **IoT orchestration strategy:** Although 1NCE has partnered for IoT connectivity management platform (CMP) aggregation, this integration is not offered as a standard self-service feature, but rather as a custom-made, consultant-led project. Additionally, 1NCE's deployment plans for SGP.31/32 remain unclear despite initial trials with Kigen.
- **Business model:** Although 1NCE's Lifetime Flat model is innovative and attractive, the company remains unprofitable as of June 2025 and is now shifting toward recurring charges through additional services. 1NCE also maintains a significant 2G installed base, which may be discontinued in the future, particularly in Europe. The vendor's business model has yet to prove sustainable.
- **High-bandwidth and 5G:** 1NCE currently has no active 5G connections or plans to support private 4G/5G networks, with 5G activities limited to a single research project. 1NCE's installed base remains overwhelmingly anchored to low- and mid-bandwidth use cases. As a result, 1NCE lacks commercial offerings and a roadmap in scalable 5G or private network solutions.

AT&T

AT&T is a Leader in this Magic Quadrant. Headquartered in Dallas, Texas, U.S., it offers end-to-end IoT solutions, mainly in the U.S. and Mexico. AT&T added a new small and midsize business (SMB) marketplace, 5G SA and 5G RedCap in the U.S., and IoT analytics through IoT Network Intelligence and the Global SIM Advanced service. This strengthens its presence in automotive, transportation, manufacturing, healthcare and utilities.

According to Gartner estimates, AT&T managed over 145 million IoT connections in the first half of 2025, reflecting a 7.5% year-over-year increase. Its customers tend to be organizations of all sizes in the U.S. and multinational corporations with large deployments in North America and smaller ones in other regions.

Strengths

- **Growth:** AT&T achieved notable year-over-year connection growth, exceeding 10 million connections. It leads LTE-M adoption with nearly 25 million connections. U.S. enterprise 5G uptake is strong, supported by extensive 5G NSA roaming coverage, alongside plans to launch 5G NSA roaming in Canada.
- **Connected cars and managed services:** AT&T maintains a dominant position, supporting numerous wholesale brand relationships and adding millions of vehicles to its network across more than 60 global automotive brands, mainly in North America. It also demonstrates managed services leadership for large enterprises by providing premium support for more than 30 million IoT devices globally.
- **Security services:** As part of its highly curated, multilayered security portfolio, AT&T expanded its analytics ecosystem to provide near-real-time device and network KPI visibility for advanced troubleshooting. It also integrated a zero-touch, network-based solution using AI and machine learning to proactively identify SIM swaps, botnets and behavioral anomalies, securing endpoints without impacting device performance or battery life.

Cautions

- **Local sales and deployments:** Although AT&T has a global presence across multiple regions, it is not prioritizing managed IoT connectivity services for companies headquartered outside the U.S. This continues to create challenges for customers needing local deployments in their own geographies.

- **IoT orchestration portfolio:** Despite AT&T's substantial investments in a comprehensive suite of IoT orchestration tools and emerging SGP.31/32 integrations, the extensive portfolio can be confusing for clients to navigate. The overlapping platforms require clearer value propositions and business outcomes to help prospective buyers identify the right solution for their needs.
- **NB-IoT and 5G RedCap devices:** AT&T has exited the NB-IoT market in the U.S., consolidating LPWA demand onto its LTE-M network and expanding nationwide 5G RedCap coverage. However, NB-IoT roaming is only maintained internationally, with limited global connections. While the 5G RedCap device ecosystem is in its early stages, AT&T plans to actively expand availability in 2026.

Cubic³

Cubic³ is a Challenger in this Magic Quadrant. Headquartered in Dublin, Ireland, it is a subsidiary of SoftBank Corp. This shift, with a company rebranding, continues to bolster Cubic³'s presence with global automakers. It is expanding in this segment with automated fleet migrations, autonomous AI agents for network resilience, the launch of FleetWallet³, its secure fleet payment platform, and integrated satellite nonterrestrial network (NTN) connectivity.

Cubic³ managed 25.7 million IoT connections in the first half of 2025, reflecting a 34.7% year-over-year increase. Its customers tend to be large fleets in Europe and North America focused on connected vehicles for the automotive, agriculture, heavy machinery and transportation sectors.

Strengths

- **5G NSA:** Cubic³ tailors its network expansion for high-value, data-heavy mobile assets and has added around 700,000 5G connections globally year over year. It offers broad 5G NSA coverage via global roaming partners and is upgrading to a 5G SA core, developing SA-ready policies for future scalability.
- **Connected intelligence:** Cubic³ specializes in the automotive sector, enabling OEM monetization services beyond connectivity. It introduced AI-driven operational intelligence — such as application-aware network selection and the Explore³ analytics suite — to optimize coverage, latency and insights for OEMs on network performance and data usage. It expanded DriverConnect³ for in-car digital services in North America, the Middle East and LATAM.

- **IoT orchestration strategy:** Prioritizing a platform-first approach, the vendor-agnostic Cubic³ Cloud empowers OEMs with bring your own carrier (BYOC) flexibility. It enables complex regulatory compliance and multicustomer profile transitions with its Fleet Migration Manager. It natively supports eSIM standards SGP.02 and SGP.22, while its next-generation SGP.31/32 architecture is in pilot for a 2026 commercial launch.

Cautions

- **Regional concentration:** Although Cubic³ is enhancing its geographical capabilities, including expanding sales across regions, its actual connections growth outside of Europe and North America remains very limited. Due to the automotive market's long purchasing cycles, broader geographic expansion will take time, even with SoftBank Corp's investment targeting the APAC region.
- **Use case focus:** Cubic³'s strategy centers on high-value, data-intensive mobile assets and fleets, not traditional low-bandwidth IoT applications. It reported no 3GPP LPWAN connections under management. Enterprises requiring low-throughput connectivity — such as stationary sensors or utility meters — may find Cubic³'s market focus less aligned with their needs.
- **Field support:** Cubic³ offers a robust cloud-based orchestration platform but does not provide global physical field services, hardware or on-site support such as installation, repair or logistics. Enterprises needing end-to-end managed hardware deployment must rely on their own resources or third-party integrators.

Deutsche Telekom Group

Deutsche Telekom Group is a Leader in this Magic Quadrant. Headquartered in Bonn, Germany, it serves as a communications service provider (CSP) and IT services company. Apart from its European subsidiaries and T-Mobile for Business in the U.S., T IoT, a global IoT business, is one of the entities operating under the T Digital division. In 2025, T IoT continued to expand in APAC, building on its Bridge Alliance membership.

Deutsche Telekom Group managed 59.3 million IoT connections in the first half of 2025, reflecting an 11.9% year-over-year increase. Its customers tend to be multinational corporations and enterprises in Europe and the U.S., primarily within the automotive, manufacturing, transportation and utilities sectors.

Strengths

- **Multinational execution:** T IoT delivers unified solutions by integrating native European and North American networks with its Bridge Alliance partnership in APAC. This approach has secured cross-regional enterprise wins in automotive, logistics and utilities, including revenue-generating automotive deals. Deutsche Telekom Group recently signed a two-year extension of the partnership.
- **5G innovation:** Leveraging native 5G SA networks, T-Mobile US and Deutsche Telekom Germany deliver advanced market capabilities, including 5G RedCap with a focus on wearables, live commercial 5G network slicing (e.g., T-Priority for first responders in the U.S.), and private 5G integration. Its proven execution in 5G Advanced innovation enables support for a variety of device capabilities, which may vary by region or deployment.
- **Satellite IoT strategy:** Deutsche Telekom Group integrates multiorbit satellite IoT with partners like Skylo, Sateliot, OQ Technology, Intelsat and Viasat. Commercially, its LPWAN satellite ecosystem is proving successful, securing 20+ new customer wins in the last 18 months. Deployments span European industrial monitoring, and North American rural agritech asset and livestock tracking.

Cautions

- **IoT orchestration strategy:** Deutsche Telekom Group's extensive suite of IoT orchestration tools and portals can be confusing for clients due to regional nuances and overlapping platforms. It is working to unify these systems, but clearer value propositions are needed to help multinational buyers select the right solution for global deployments.
- **Regional concentration:** Deutsche Telekom Group's year-over-year growth and revenue contribution in LATAM and the Middle East and Africa remain highly insignificant compared to its European and North American operations, yielding only single-digit new enterprise client wins. To serve these regions, the company relies entirely on local roaming partners.
- **Regional solutions:** Deutsche Telekom Group's value-added IoT solutions and beyond-connectivity portfolio are regionally fragmented. For example, T Digital offerings combining security and digital applications are mainly Europe-focused, while T-Mobile US uses specific regional horizontal partnerships for fleet and asset tracking in North America.

emnify

emnify is a Visionary in this Magic Quadrant. Headquartered in Berlin, Germany, it is a global IoT MVNO and mobile virtual network enabler (MVNE), offering cloud-native managed IoT connectivity services through its SuperNetwork platform. Recent rollouts include high-speed Bulk APIs, a modernized business intelligence (BI) layer and an AI-driven connectivity support copilot.

emnify managed 23 million IoT connections in the first half of 2025, reflecting an 11% year-over-year increase. Its customers tend to range from scaling startups to large multinational enterprises in Europe and the Americas. Primary use cases include fleet management, EV charging, asset tracking and consumer devices.

Strengths

- **Cloud-native platform:** emnify's SuperNetwork features 27 local and regional hyperscaler cloud breakouts across nine mobile core locations in all regions except the Middle East and Africa, ensuring low-latency access to 545 networks. Full core ownership eliminates MNO dependencies, enabling scalable connectivity, faster Bulk API provisioning and real-time data streaming to Amazon Web Services (AWS), Google and Azure. emnify also operates as a licensed MVNO in Brazil.
- **Hybrid networks:** emnify delivers a single-SIM converged approach across 3GPP and nonterrestrial networks, natively aggregating cellular, LTE-M, NB-IoT and 1.26 million 5G NSA connections across 200 networks. It recently added a commercially successful cellular-satellite offering via Skylo, and an ongoing secure access service edge (SASE) Proxy proof of concept (PoC) for secure private-to-public handovers.
- **Innovation:** With 45% of its workforce dedicated to R&D, emnify demonstrates rapid time-to-market. It has a no-code automation engine, and fine-tuned large language models (LLMs) that analyze device events and customer context to troubleshoot and resolve queries. Backed by patented GPRS Tunneling Protocol (GTP) processing, it is investing in SGP.32 orchestration and AI-driven anomaly detection.

Cautions

- **Direct connection volume:** Approximately two-thirds of emnify's connections are generated through platform partners and MVNOs rather than direct end-user contracts. In the 3GPP LPWAN segment, this reliance on indirect channels is nearly

absolute, which may limit ability and focus to deliver and manage 3GPP LPWAN services directly for end customers.

- **Geographic sales presence:** emnify's direct sales headcount is concentrated almost entirely in Europe and the Americas, resulting in a lack of direct sales presence across APAC and the Middle East and Africa. This may hinder its responsiveness to local market requirements and enterprise needs in those regions.
- **Growth:** emnify's year-over-year growth is low compared to other vendors in this Magic Quadrant, likely due to a strategic focus on higher-bandwidth use cases rather than simply increasing the total number of connections. End users should expect emnify's commercial and support model to prioritize high-consumption, vertical-specific use cases over low-cost LPWAN tracking.

Itron

Itron is a Niche Player in this Magic Quadrant. Headquartered in Liberty Lake, Washington, U.S., it is a network and IoT solution provider focused on implementing infrastructure and systems for utilities and smart cities. Itron's multicarrier eSIM solution provides automated network failover and is rapidly transitioning toward the eSIM SGP.32 standard. Managed IoT connectivity services account for 24% of Itron's total revenue.

Itron managed 113.7 million IoT connections in the first half of 2025, reflecting an 8.4% year-over-year increase. Its customers tend to be utilities and municipalities with smart lighting, electricity, gas and water solutions in North America, LATAM, Europe and APAC.

Strengths

- **Utilities focus:** Itron is a prominent global expert in helping utilities and cities manage electricity, gas, water and streetlights. Serving over 1,200 customers, it recently launched the Gen6 Network Platform, which adds cellular connectivity to traditional mesh networking under the UtilityIQ headend, CityEdge smart-city connectivity and AI-driven edge computing for real-time grid diagnostics.
- **Connectivity management:** Itron evolved its CMP into a single pane of glass to integrate aggregation and eSIM management across more than 250 global carriers. It also launched its Gen6 Network Platform and SGP.32 multicarrier eSIMs, which support public and private networks, and feature automated carrier fallback for both native and third-party devices.

- **Security emphasis:** Itron's defense-in-depth zero-trust architecture embeds security into hardware, firmware and software, supported by ISO 27001 and SOC 2 certifications. It enhanced this security by acquiring Urbint for predictive risk intelligence, integrating with the FirstNet program for mission-critical coverage and deploying edge AI to automatically detect operational anomalies like meter bypass.

Cautions

- **Regional concentration:** Despite managing over 113 million endpoints globally, Itron's deployments are heavily based in Western markets. For example, in its Grid Edge electricity sector, it supports over 44 million endpoints in North America, significantly fewer in the APAC region and none in the Middle East and Africa.
- **Legacy networks:** Itron has no satellite connections and is starting its 5G business, while its 4G connections are declining. Year-over-year growth in 3GPP LPWAN is average versus non-3GPP LPWAN specialists in this Magic Quadrant, while LoRaWAN growth is much higher. This aligns with Itron's utility and smart lighting focus, but also shows its large-scale operations remain heavily reliant on legacy non-3GPP LPWAN (radio frequency [RF] mesh) over modern wireless technologies.
- **Sector breadth:** Itron's portfolio has limited alignment with use cases outside utilities and smart cities, such as retail, healthcare or general manufacturing. Enterprises in these sectors may find its hardware and UtilityIQ headend software less applicable to their requirements.

KORE

KORE is a Visionary in this Magic Quadrant. Headquartered in Atlanta, Georgia, U.S., it offers differentiated managed service capabilities by integrating AI tools such as KOREY, a customer support virtual assistant. KORE is expanding its U.S. SMB channel reach via an alliance with TD SYNEX, promoting the eSIM SGP.32 standard and recently launched KORE Shop for digital self-service.

KORE managed 20.1 million IoT connections in the first half of 2025, reflecting a 6% year-over-year increase. Its customers tend to be enterprises in North America and Europe of all sizes in connected health, fleet management, asset monitoring and utilities, and it is expanding into retail and EV charging.

Searchlight Capital Partners and Abry Partners announced their intention to acquire KORE on 27 February 2026. At the date of publication, KORE met the inclusion criteria for this Magic Quadrant and continued to operate as a going concern. Gartner will provide additional insight and research to clients as more detail becomes available.

Strengths

- **IoT Orchestration strategy:** KORE uses eSIM, multi-IMSI and CMP aggregation. A priority for 2026 is deploying a unified, fully certified GSMA SGP.32 eSIM standard stack with native, rule-based automated profile switching for Constrained Application Protocol (COAP) to minimize data overhead.
- **Regional integration capabilities:** KORE integrates several localized eSIM networks and nine third-party CMPs across North America, Europe, Brazil and APAC. KORE also supports 45 direct carrier integrations for its managed IoT connectivity services.
- **Cross-segment strategy:** KORE's IoT connectivity portfolio serves a wide range of industries, with notable expertise in healthcare solutions for decentralized clinical trials and large-scale deployments in the utilities and micromobility sectors. It meets global regulatory and compliance requirements via FDA-registered and ISO-certified U.S. and EU facilities, and supports SMBs and developers with its unified KORE Console, KORE Shop and rebuilt KORE Developer Portal.

Cautions

- **Growth:** KORE's growth is concentrated in North America and Europe. KORE's year-over-year growth is low compared to other vendors in this Magic Quadrant.
- **Global sales resources:** While KORE maintains a broad global sales footprint, the company has reduced its commercial resources across all regions with the exception of the Middle East and Africa. This may impact account management and local commercial sales support, particularly outside North America and Europe.
- **5G adoption:** Though KORE supports 5G across several geographies, adoption of 5G for IoT remains minimal, with little evidence of progress. All active 5G connections are in North America, with no current deployments in Europe, LATAM, APAC and the Middle East and Africa. This may constrain support for advanced, data-intensive IoT solutions in these regions.

NTT

NTT is a Visionary in this Magic Quadrant. Headquartered in Tokyo, Japan, it provides information and communication technology solutions and international communications services with IoT connectivity services through NTT DOCOMO in Japan and NTT DATA in the rest of the world. NTT offers a comprehensive end-to-end stack of IoT solutions and is expanding local breakouts from APAC and its multivendor satellite strategy for IoT.

According to Gartner estimates, NTT had 27.6 million managed IoT connections in the first half of 2025, reflecting a 30% year-over-year increase, coming from Europe. Its customers tend to be in the automotive and manufacturing sectors across APAC and Europe.

Strengths

- **Automotive focus:** NTT is rapidly expanding its global automotive presence by leveraging NTT DATA's integration services, the Ubigi consumer brand for connected cars, and Transatel's MVNO expertise in Brazil. It has added presence to support OEMs in LATAM, 5G NSA coverage in more than 80 countries with proven deployments, and 65 new Voice over Long Term Evolution (VoLTE) agreements with focus on APAC, Europe and LATAM.
- **Vertical capabilities:** NTT DATA provides comprehensive capabilities with private 4G/5G services, managed network and security services, edge computing and edge AI portfolios, enterprise IoT services, application development and system integration. It has a catalog of preintegrated industry-vertical solutions, such as connected workforce, machine vision and digital twins.
- **Global sales support:** NTT DATA delivers robust global sales and technical support through a distributed infrastructure and dedicated regional offices, enabling enterprises to access unified support and a single point of contact for fleets deployed worldwide. Its Glocal strategy combines global capabilities with local expertise, leveraging experts across more than 50 countries.

Cautions

- **Brand alignment:** NTT maintains multiple IoT brands, including Transatel, which covers connectivity businesses outside of core IoT services, as well as NTT DATA and NTT DOCOMO in Japan. This brand structure may create challenges for buyers seeking to identify the appropriate NTT entity for managed IoT connectivity services.

- **Regional concentration:** NTT's primary installed base of managed IoT connectivity connections is in the APAC region, representing a significant portion of its overall IoT connectivity business, with Europe as the second main region with contracts signed but not deployed in LATAM. This regional concentration means organizations may find limited proven scale or deployment experience for managed IoT connectivity outside of APAC and Europe.
- **LPWA and satellite emphasis:** While NTT supports LoRaWAN, its 3GPP LPWA strategy focuses solely on LTE-M, and it continues to report no connections related to NB-IoT. Furthermore, with no reported satellite connections, enterprises requiring active NB-IoT or satellite scale may find its current installed base limiting.

Orange Business

Orange Business is a Leader in this Magic Quadrant. Headquartered in Paris, France, it is the enterprise service unit of Orange Group, a global CSP focused on implementation, engineering, consulting, integration, security and analytics.

Orange reported 44.7 million IoT connections in the first half of 2025, reflecting an 11% year-over-year increase, excluding Spain. Its customers tend to have large fleets in Europe and smaller fleets in other regions for the automotive, transportation, industrial, manufacturing and smart city sectors.

Parent company Orange announced its intention to acquire the remaining 50% in MasOrange in Spain on 12 December 2025. At the date of publication, Orange Business met the inclusion criteria for this Magic Quadrant and continued to operate as a going concern. Gartner will provide additional insight and research to clients as more detail becomes available.

Strengths

- **Platform innovation:** Orange Business integrated its Malima connectivity and Live Objects device portals for unified management, adding native Amazon Web Services (AWS), Google Cloud Platform (GCP) and Azure connectors. It also added Model Context Protocol (MCP) servers for AI agents to perform cross-platform diagnostics via natural language and a premium AI anomaly detection feature based on call detail record (CDR) analysis.

- **Industry verticals:** Orange Business is expanding its European automotive focus, attracting U.S. and APAC OEMs and growing its compliant B2B2C portal to 23 countries. With its large-scale eSIM expertise, it is diversifying across Europe with new smart health (connected sleep apnea devices) and smart agri (satellite-bundled agribots), building on its strong industrial practice and private 5G in the region.
- **Growth:** Orange Business achieved year-over-year IoT connection growth progress in APAC and the Middle East and Africa, aside from Europe. In the Middle East and Africa, it is a leader for connections under management, bundling IoT with “Orange Money” for prepaid solar and smart metering.

Cautions

- **IoT orchestration strategy:** While Orange Business has global roaming, it lacks a unified, native eSIM orchestration engine to bypass permanent roaming bans in regulated markets like Brazil, China and Türkiye. Until the SGP.31/32 platform launches in mid-2026, enterprises seeking local connectivity must rely on custom-made, partner-driven SGP.21/22 workarounds.
- **IoT IT stack transformation:** Orange Business is transforming its IoT connectivity platform stack. Though it integrated its Malima and Live Objects portals, new buyers should review Orange’s platform strategy and migration roadmap to ensure long-term alignment.
- **5G and satellite execution:** Despite 5G NSA availability, a roaming ecosystem and 5G SA rollouts in Europe, Orange Business trails other market leaders in 5G connections under management. Despite various satellite initiatives, its installed base remains insignificant.

Soracom-KDDI

Soracom-KDDI is a Leader in this Magic Quadrant. Headquartered in Tokyo, Japan, it offers cloud-native connectivity, multi-IMSI orchestration and AI-enabled data services. Its operations are geographically diversified, with a strong presence in APAC. Soracom-KDDI continues to invest heavily in SGP.32 eSIM orchestration, GenAI integration such as Soracom Query and Soracom Flux, and expanded satellite network support.

According to Gartner estimates, Soracom-KDDI managed 60.7 million IoT connections in the first half of 2025, reflecting a 20% year-over-year increase. Its customers tend to be

large enterprises in automotive and utilities, as well as global innovators in payments and consumer electronics.

Strengths

- **Innovation and AI strategy:** Soracom-KDDI embeds advanced GenAI and low-code tools, such as Soracom Flux and Soracom Query Intelligence, directly into its connectivity platform. This enables organizations to quickly build AI-driven IoT applications and perform natural-language analytics without specialized data science resources.
- **Scale in key verticals:** Leveraging KDDI Group's Global Communication Platform, the company manages over 35 million connections in the automotive sector for major Japanese OEMs. This industrial scale provides Soracom-KDDI with deep expertise in high-volume, demanding deployments while supporting multiregional expansion.
- **Cloud-native platform:** By terminating device connections directly within cloud infrastructure such as Amazon Web Services (AWS), bypassing traditional telco hardware, Soracom's software-defined core unifies cellular, satellite and non-3GPP LPWAN under a single pane of glass. This architecture enables highly flexible pay-as-you-go pricing and advanced multi-IMSI orchestration, supported by a strong strategic focus on the 3GPP eSIM standard for dynamic, remote profile management.

Cautions

- **Brand and platform structure:** The vendor operates dual go-to-market motions, with KDDI handling large-scale and long-term automotive contracts, while Soracom targets cloud-native innovators. This lack of a unified brand may create challenges for enterprise buyers in identifying the appropriate commercial and technical organization from which to purchase services.
- **Regional concentration:** Although the vendor is actively expanding its footprint and channel ecosystem in North America and Europe, the vast majority of its managed connections remain heavily concentrated in the APAC region, particularly in Japan. Soracom-KDDI's concentration of managed connections in Japan may constrain local support and operational readiness for large-scale deployments outside its primary market.

- **Logistics and field support:** Soracom-KDDI relies primarily on a partner-delivered model for physical hardware sourcing, depot repair and on-site break-fix support. Enterprises seeking a single provider to manage both connectivity and direct on-site field maintenance may find this lack of native hardware support limiting.

Tata Communications

Tata Communications is a Niche Player in this Magic Quadrant. Headquartered in Mumbai, India, its Tata Communications MOVE platform is an orchestration-led, multibearer IoT solution that abstracts network complexity for global deployments. Tata operates globally, with a strong presence in Europe, APAC and North America. It continues to invest in AI-driven analytics, advanced eSIM orchestration, including SGP.32, and hybrid multiaccess connectivity with cellular, private 5G, LoRaWAN and satellite technologies.

Tata managed 9.7 million IoT connections in the first half of 2025, reflecting a 35.8% year-over-year increase. Its clients tend to be large multinational enterprises in the automotive, industrial and transportation sectors.

Strengths

- **IoT orchestration strategy:** Tata simplifies global connectivity and regulatory compliance with its MOVE platform. It has advanced eSIM life cycle management, multi-IMSI orchestration and native SGP.02, SGP.22 and SGP.32 capabilities. It has direct local eSIM profile integrations in key markets including India, China, Brazil, Germany, Canada and the United Arab Emirates.
- **Industry vertical capabilities:** Tata demonstrates expertise in automotive, aligned with its 5G performance, aviation and industrial sectors, by bundling connectivity with end-to-end capabilities. To scale and secure complex deployments, it uses its broader corporate ecosystem, partnering with TCS, Tata Technologies and Tata Elxsi. This integrated approach enables specialized solutions such as predictive software over-the-air (SOTA) updates for connected vehicles and AI-powered connected worker safety applications.
- **Security services:** Tata embeds robust security and data privacy protocols directly into its connectivity fabric rather than treating them as add-ons. It integrates zero-trust architectures, IoT SAFE and agentless threat detection via its Ijura solution.

Cautions

- **SMB alignment:** Tata's solution design and direct sales approach are heavily optimized for large, complex multinational programs. SMBs seeking simple, self-service connectivity may find the platform's advanced orchestration capabilities and pricing models less aligned with their needs.
- **Sales cycle structure:** Buyer engagement can be challenging because Tata positions its managed IoT connectivity within broader, highly integrated digital transformation programs and aims to build long-term strategic partnerships, which could affect sales execution. Organizations may experience prolonged implementation cycles due to the extensive architectural alignment required across multiple stakeholders.
- **Scale:** Tata has a notably smaller number of connections compared to other vendors in this Magic Quadrant. While it targets complex multinational programs, its reduced connection base may limit its ability to simultaneously support large-scale IoT global deployments, creating uncertainty regarding rapid rollouts, shorter implementation cycles and future performance.

Tele2 IoT

Tele2 IoT is a Niche Player in this Magic Quadrant. Headquartered in Stockholm, Sweden, it offers global IoT connectivity, agnostic connectivity services and horizontal managed IoT connectivity. It uses Cisco IoT Control Center as its IoT CMP. Tele2 IoT continues to expand investments in eSIM SGP31/32, and has enhanced its local breakout nodes in Miami and São Paulo to reduce latency.

Tele2 IoT managed 21.5 million IoT connections in the first half of 2025, reflecting a 26.5% year-over-year revenue increase. Its clients tend to be multinational corporations across Europe and organizations with fleets in other regions, with suitability for manufacturing, healthcare, automotive, transportation, retail and energy.

Strengths

- **5G strategy:** Tele2 IoT maintains a significant 5G installed base, supported by extensive global 5G NSA/SA roaming. Its strategy future-proofs high-bandwidth enterprise deployments. Additionally, Tele2 IoT bridges private 5G islands with macro public networks, enabling seamless profile reuse for continuous connectivity from in-factory operations to the global supply chain.

- **Growth:** Experiencing double-digit year-over-year growth, Tele2 IoT has evolved into a global provider, driven by successes in the automotive, energy and tracking sectors. With North America as its second-largest region through indirect channels, it is targeting LATAM for direct expansion using Iliad, NJJ and Millicom affiliations spanning more than 20 countries.
- **IoT orchestration strategy:** Tele2 IoT's strategy has evolved beyond a stand-alone Cisco approach to a federated, multivendor model for eSIM. Its "IoT Passport" over-the-top (OTT) layer abstracts fragmented global networks into a single API/CMP interface. Alongside remote SIM provisioning (RSP) integrations via 2SWITCH, Tele2 is testing prestandard SGP.42 In-factory profile provisioning (IFPP) to embed connectivity directly at the manufacturing line.

Cautions

- **Connectivity focus:** As a horizontal provider, Tele2 IoT strictly focuses on connectivity and does not natively offer device management, application management, hardware bundles, vertical point solutions or OT capabilities. Enterprises seeking end-to-end turnkey solutions must rely on Tele2 IoT's third-party partner ecosystem to fulfill capabilities beyond the SIM.
- **Direct presence:** Despite North America being its second-largest region by volume, Tele2 IoT currently lacks a dedicated direct sales force there, relying entirely on indirect channels and global partners. Customers requiring robust, localized direct sales engagement in North America may find this limiting until roadmap plans are executed.
- **2G/3G sunsets:** Tele2 IoT maintains a substantial 2G and 3G installed base. While it provides a Devices at Risk portal report and account support for migration planning, it does not offer a centralized migration program. Customers using legacy 2G/3G devices may face risks as networks sunset globally and must manage hardware transitions independently, though commercial incentives can be negotiated.

Telefónica

Telefónica is a Leader in this Magic Quadrant. Headquartered in Madrid, Spain, it is a global CSP. It leverages Telefónica's strong direct presence in Europe and LATAM to build

its managed IoT service business, which is organized within the Telefónica Tech company.

According to Gartner estimates, Telefónica managed 73.1 million IoT connections in the first half of 2025, reflecting a 14.6% year-over-year increase. Its clients tend to be multinational corporations in the energy and utilities, automotive, retail, manufacturing, agriculture and transportation sectors, as well as organizations involved in smart city initiatives across Europe and LATAM.

Strengths

- **Growth:** Telefónica has added 9.3 million new connections since June 2024, with nearly 60% of these additions coming from Europe, followed by LATAM and North America. The company saw significant increases in both 5G and NB-IoT connections while also continuing to expand its installed base of satellite connections.
- **Platform innovation:** Telefónica's Kite platform features AI-driven tools, including a natural language inventory assistant, behavioral clustering and automated resolution for 70% of operational tickets. It also integrates a proprietary eIM as an SGP.32 eSIM IoT remote manager (eSIM) orchestrator, centralizing management of Telefónica and third-party profiles in a single pane of glass, along with integrated CMP API aggregation for comprehensive IoT orchestration.
- **Industrial capabilities:** Telefónica delivers managed IoT, private 5G and edge computing across Europe and LATAM, strengthened by its acquisition of Geprom's OT engineering, with Geprom's CEO now leading IoT within Telefónica Tech. With ongoing rollouts of 5G SA, 5G Slicing and RedCap across its operations, and 17 new edge computing nodes in Spain, it supports mission-critical industrial solutions with advanced OT capabilities.

Cautions

- **LATAM divestments:** Telefónica is divesting from most LATAM operations except Brazil, reducing its direct capabilities in the affected countries. While maintaining a direct presence in major regional markets, buyers should note that it now has reduced ability to implement full-fledged IoT services in divested countries.
- **Regional concentration:** Telefónica's direct presence remains limited in the APAC region and the Middle East and Africa, where it relies on local partners to deliver

managed connectivity services. This reliance may constrain support and service consistency for organizations with operations in these regions.

- **Global delivery:** Telefónica distributes its end-to-end IoT capabilities between a central unit (Telefónica Tech) and local operating companies (OpCos). While Kite provides unified global management, buyers should note that local infrastructure — such as 5G SA, NB-IoT coverage, and edge nodes — as well as specialized IoT sales, integration and industry expertise, varies internally. This results in uneven service availability across countries.

Telenor Group

Telenor Group is a Leader in this Magic Quadrant. Headquartered in Fornebu, Norway, it is a CSP providing managed IoT services globally through its dedicated unit, Telenor IoT (Telenor Connexion). After recent consolidation, Telenor IoT directly manages core IoT customers, while regional OpCos act as resellers for broader telecom agreements.

According to Gartner estimates, Telenor managed approximately 30 million IoT connections in the first half of 2025, reflecting a 15.4% year-over-year increase. Telenor's customers tend to be in large-scale utility solutions, connected vehicles/products, smart cities and fleet management solutions for multinational corporations with IoT connections deployed across Europe and the APAC region.

Strengths

- **AI innovation:** Telenor's AI Engine delivers predictive network health, AI security and global latency optimization, while Telenor Maritime's Unified Data Service (UDS) platform provides real-time edge AI insights at sea. Parallel to these IoT capabilities, Telenor's NVIDIA-backed AI Factory provides a sovereign, secure cloud service, enabling local GenAI processing in the Nordics, with the potential to support industrial IoT edge-AI capabilities.
- **IoT orchestration strategy:** Telenor's proprietary cloud-native layer runs atop platforms like Aeris, Cisco, Comarch, Arquia and ThingSpace to deliver a unified CMP. This accelerates its eSIM roadmap, with over 15 customers already staged for the 2026 SGP.32 launch. It further enhances orchestration with AI-driven global latency optimization and a dedicated SGP.32 test lab.

- **Automotive focus:** Telenor demonstrates deep penetration in the Asian automotive market, securing business with eight of the top 10 Chinese OEMs. Building on this, it launched IoT Drive, a tailored offering that provides advanced SLAs, global compliance and in-car connectivity monetization, supported by industry expertise.

Cautions

- **Regional concentration:** Telenor's sales execution and direct presence remain limited in the Middle East, Africa and LATAM, and it has not yet demonstrated the ability to deploy 3GPP LPWA network projects at scale outside its home countries. This may constrain support for organizations seeking managed IoT connectivity and large-scale LPWA deployments in these regions.
- **Proprietary platform maturity:** While Telenor is actively developing its proprietary cloud-native IoT connectivity platform, targeting enterprises with smaller fleets, it is still gradually approaching feature parity with mature third-party systems like Cisco IoT Control Center and Aeris. Organizations with highly complex needs in this segment may find some advanced or legacy features currently lacking on Telenor's native platform.
- **Industrial solution scope:** Telenor's value-added services for industrial use cases, such as private 5G and end-to-end applications, are mainly available in the Nordics and Telenor Maritime. Industrial enterprises in other regions may encounter limited access to advanced industrial IoT capabilities.

Telit Cinterion

Telit Cinterion is a Visionary in the Magic Quadrant. Headquartered in Boca Raton, Florida, U.S., it manufactures wireless connectivity modules and operates as an IoT service provider and full IoT MVNO in the U.S., Europe and Brazil. Telit Cinterion is expanding with NExT eSIM Flex, eSIM Protect and SGP.32 eSIM with IoT Profile Assistant embedded (IPAE) for dual-core failover, seamless in-factory or OTA provisioning and AI-driven anomaly detection.

According to Gartner estimates, Telit Cinterion managed over 12.9 million IoT connections in the first half of 2025, reflecting a 16.9% year-over-year increase. Its clients tend to be in manufacturing, communications, transportation and utilities in Europe and North America.

Strengths

- **Deployment support:** Telit Cinterion maintains a strong focus on North America and Europe, while expanding in LATAM and APAC, utilizing local IMSI sponsors like NLT in Brazil. It supports global deployments through a dedicated workforce of over 180 sales professionals across 50 offices.
- **Integration and enablement:** Positioning itself as a full-stack IoT enabler, Telit Cinterion integrates industrial-grade hardware, secure embedded software and cloud-native connectivity. Its new NExT Connected module-as-a-service provides a turnkey solution that bundles IoT modules, connectivity and management tools into a single subscription to accelerate deployments.
- **Security emphasis:** Telit Cinterion has evolved its secure-by-design approach to prioritize critical network resilience. It launched NExT eSIM Protect, featuring a dual-core architecture for instant failover, and it enhanced threat protection with a new Security Extended Detection and Response (XDR) dashboard and ISO 27001-certified operations.

Cautions

- **Growth:** Telit Cinterion's year-over-year growth is low compared to other vendors in this Magic Quadrant, likely because its connectivity expansion is heavily tied to its hardware business, which serves as its main indirect channel. Globally, its managed IoT connectivity revenue represents a small portion of its overall IoT revenue.
- **Regional concentration:** While actively expanding in LATAM and APAC through strategic partnerships, Telit Cinterion's presence remains heavily concentrated in North America and Europe. Service delivery outside these regions is managed chiefly through Telit Cinterion's partner ecosystem.
- **Target priorities:** Telit Cinterion's premium strategy deliberately targets critical and regulated IoT segments, explicitly avoiding the IoT long-tail market. Furthermore, while 5G NSA and LPWAN coverage has significantly expanded, advanced network technologies like 5G stand-alone (SA) are not short-term priorities, planned instead for a 24- to 36-month horizon.

Verizon

Verizon is a Leader in this Magic Quadrant. Headquartered in New York, New York, U.S., this CSP offers value-added IoT applications, including fleet management, utility solutions and asset monitoring. Verizon's launch of 5G SA, including slicing capabilities, enhances its private 4G/5G and edge computing (Verizon AI Connect) offerings, combined with improved security features for IoT use cases.

According to Gartner estimates, Verizon managed over 68.5 million IoT connections in the first half of 2025, reflecting an 8.9% year-over-year increase. Its customers tend to be in sectors like manufacturing, automotive, logistics, transportation management, smart grid and smart meter solutions, and smart cities, spanning national and multinational U.S. companies of all sizes.

Strengths

- **IoT platform:** Verizon's proprietary ThingSpace IoT CMP integrates with private 5G and eSIM SGP.32, enabling unified IoT orchestration, seamless device handovers, zero-touch eSIM provisioning, single-SKU global deployments, and an embedded AI assistant for context-aware troubleshooting and code generation.
- **AI-driven integrated solutions:** Verizon acts as a digital transformation partner by integrating private 5G and edge computing with specialized AI SaaS solutions. This includes Sensor Insights, a protocol-agnostic platform for asset and environmental monitoring; 5G Video Insights, which leverages edge AI to transform passive IP cameras into smart sensors for real-time analytics; and Edge Transportation Exchange, an integrated mobile-network vehicle-to-everything communication platform allowing vehicles to communicate with other connected vehicles, road users and infrastructure around them.
- **Security services:** Anchored by a zero-trust architecture, Verizon delivers native network-layer protection. Key features include SIM Secure for hardware binding and an upcoming agentless IoT Network Firewall to protect constrained edge devices.

Cautions

- **Regional concentration:** Verizon's managed IoT connections remain predominantly U.S.-based, with limited expansion in other regions. International device growth remains marginal, as its international business is based on serving U.S. multinationals' expansion. It has notably limited regional diversity in its installed base.

- **International execution:** Although Verizon has invested in eSIM, multi-IMSI orchestration and IoT CMP aggregation in Europe, there are few documented examples of organizations actively implementing these capabilities. Without this evidence, organizations may find it difficult to assess the maturity of these capabilities outside the U.S.
- **U.S. 5G RedCap support:** Verizon has conducted RedCap hardware testing, has certified 5G RedCap devices on its network and will soon launch 5G RedCap for IoT use cases. However, it is the only major U.S. MNO that has not already launched 5G RedCap availability in the country. As a result, enterprises may miss out on early access to cost-effective, low-complexity 5G IoT solutions that RedCap enables.

Vodafone

Vodafone is a Leader in this Magic Quadrant. Headquartered in Newbury, U.K., Vodafone IoT, now a separate entity, operates the GDSP platform for global managed IoT connectivity, including outside its footprint via partners. Recent launches include AI-driven bundles, the OneCharge prepaid model and advanced SGP.32 eSIM orchestration.

Vodafone managed 219 million IoT connections in the first half of 2025, reflecting a 7.3% year-over-year increase. Its clients tend to be across all B2B segments in multiple vertical markets globally, including automotive, energy and utilities, health, insurance, agriculture, industry, public sector, transportation, natural resources and retail.

Strengths

- **Growth:** Vodafone is the leading vendor in absolute growth in this Magic Quadrant, adding 14.8 million connections year over year. With an increased sales focus in North America, where it has launched a new stand-alone sales unit, it also demonstrates the most balanced growth across regions, with only LATAM lagging behind the double-digit growth seen elsewhere.
- **5G and satellite:** Managing millions of 5G connections in 78 countries, Vodafone supports 5G SA slicing, multi-IMSI for seamless public-private transitions, and cross-border SA trials for automotive OEMs and next-gen eCall. With active 5G SA ecosystems (AT&T, A1 and Vodafone Germany), Vodafone also expands through satellite partnerships with Iridium, AST SpaceMobile and Inmarsat.

- **Postquantum security:** As part of its security-by-design strategy, Vodafone differentiates itself as one of the few providers in this Magic Quadrant actively deploying postquantum security. It integrates Quantum-Ready VPN technology via Pairpoint into its hardware, establishing quantum-secure communication channels to protect critical infrastructure in the post-RSA (Rivest-Shamir-Adleman) era.

Cautions

- **Connectivity-centric focus:** As a newly separated entity, Vodafone IoT focuses on horizontal managed connectivity, not full end-to-end IoT solutions. Clients seeking integrated projects — especially outside Vodafone's core footprint — may face complexity, as advanced apps, private networks and edge depend on other Vodafone units or third-party partners.
- **Orchestration roadmap:** Vodafone recently partnered with Simetric to address historical limitations in third-party CMP aggregation. However, the long-term roadmap for natively integrating these external orchestration capabilities into the core GDSP platform remains uncertain, potentially introducing complexity for clients managing diverse global estates.
- **Off-footprint localization constraints:** While positioning itself as a global IoT connectivity provider, Vodafone IoT lacks independent MVNO capabilities outside its core network footprint. Beyond existing roaming agreements and single-partner integrations, it does not offer clients multiple options for localizing connectivity, limiting flexibility in highly regulated markets.

Wireless Logic

Wireless Logic is a Leader in this Magic Quadrant. Headquartered in Reading, U.K., it is a privately held global IoT MVNO with managed IoT connectivity services. Recently, the company acquired Arqia, Brazil's largest MVNO, and U.S.-based Zipit Wireless to expand globally and help OEMs create subscription-based IoT revenue streams. Wireless Logic continues to deliver composable solutions, bundling connectivity with its Kheiron IoT Suite.

Wireless Logic reported more than 18.3 million connections in the first half of 2025, reflecting a 27.3% year-over-year increase. Wireless Logic's customers tend to be

enterprises of all sizes operating globally in transportation, energy, security, logistics, retail and healthcare.

Strengths

- **IoT orchestration strategy:** Wireless Logic is evolving its platform into an intelligent control plane, aggregating IoT CMP APIs to integrate more than 50 MNOs into a single interface. It supports all eSIM standards — SGP.01/02, consumer SGP.22 for OEM needs like permanent roaming and data sovereignty, and the new SGP.32 standard. Its eSIM Orchestrator (eSO) pools, sources and automates policy-based deployments, combining third-party and in-house capabilities.
- **Growth:** Over one-third of Wireless Logic's revenue is now driven by customers in APAC, China and the U.S., fueled by major wins with Chinese EV manufacturers expanding globally. The Arqia acquisition provides access to all major Brazilian carriers, solving roaming challenges and securing a significant competitive advantage in South America.
- **Value-added services:** A new dedicated Solutions unit, led by the CEO of IoThink, delivers end-to-end IoT offerings, including advanced data visualization and digital twins. Private 5G is built on the private 4G/5G and Starlink backhaul capabilities gained through the Arqia acquisition in Brazil, and security leverages an AI-powered anomaly and threat detection (ATD) tool, protecting almost half a million devices and supporting cybersecurity compliance.

Cautions

- **Regional concentration:** Despite adding over 200 employees in South America via the Arqia acquisition, Wireless Logic's footprint remains unbalanced, with a majority of its workforce still concentrated in Europe. Organizations operating in the Middle East and Africa must carefully verify if there are sufficient local commercial and support resources to meet their regional needs.
- **Pricing structure:** Wireless Logic uses a custom-made pricing model that fluctuates based on individual use cases and bundled value-added services, making standard line-item comparisons difficult. Enterprises seeking simple, itemized price comparisons may experience friction or elongated procurement cycles.
- **LPWAN strategy:** Wireless Logic is steering customers away from LPWAN toward LTE Cat 1 for multinetwork global deployments, anticipating NB-IoT marginalization. The

strategic focus on 5G SA cores and higher-bandwidth applications may make these offerings less suitable for enterprises reliant on large 3GPP LPWAN deployments.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

- emnify
- Soracom-KDDI
- Tata Communications

Dropped

No vendors were dropped from this Magic Quadrant.

Inclusion and Exclusion Criteria

The inclusion criteria represent the specific attributes that analysts believe are necessary for inclusion in this research.

To qualify for inclusion:

- Providers must have at least 9.5 million connected IoT devices under management by the cutoff date of this Magic Quadrant and Critical Capabilities (30 June 2025). These connections should be uploaded into the managed IoT connectivity platform (not just contracted or committed). Connections can be cellular (2G, 3G, 4G, 5G), LPWAN (3GPP and non-3GPP), satellite and managed FANs. However, public hot spots are not acceptable. Laptops, tablets or smartphones that could have the purpose of mobile broadband connections and belong in mobile voice and data subscriptions together

with Mi-Fi devices are not acceptable either. This applies unless their exclusive use is to function as a gateway for an IoT solution or act as an HMI (human-machine-interface) terminal to access asset data and visualizations.

- Providers must solicit and deliver panregional or global services. Panregional services require delivery of services to at least three of the following five geographies, including direct local commercial presence in those regions by the cutoff date of this MQ/CC:
 - Asia/Pacific and Japan (APAC)
 - Europe
 - Latin America (LATAM)
 - Middle East and Africa
 - North America
- Providers must have at least 20% of their managed IoT devices under direct end-user contract (versus under partner/channel contract independently of the support you are providing to this partner) by 30 June 2025. For CSPs, this number should not reflect IoT connections under management by partner MVNOs. Additionally, for all providers, connections hosted in their platform but not directly managed by them for the end user *do not* count as *direct*. For example, if a provider offers its IoT connectivity platform to a telco or an IoT MVNO that uses it to sign contracts to end users, those connections are not considered direct..
- Providers must have at least \$42 million in managed IoT connectivity-related revenue by the cutoff date of this Magic Quadrant and Critical Capabilities. Revenue may include bundled connectivity, IT (hardware and software) and IT services for IoT connectivity and IoT solutions.
- Providers need to have won at least four new clients in at least three different regions since 30 June 2024 and support at least five unique customers that have presence in at least three geographies simultaneously.
- Providers need to have at least 100,000 managed IoT connections in at least two industries (100,000 managed IoT connections minimum in each industry).

- Providers must offer life cycle management services, including professional and support services (inclusive of reverse logistics), as a component of their managed IoT connectivity solution (e.g., device engineering, consulting and advisory services, service contract management, device warranty management, management software/middleware integration, device disposal and recycling, depot repair, kitting, on-site support, help desk and service desk). These services may be delivered via partners but the rated vendor must act as the prime contractor.
- Providers must extend to enterprises a portal for accessing data related to monitored assets/processes. Providers must also offer the ability to administer and control network services related to the monitored assets, as well as the ability to provide change and release management relating to connectivity, connectivity modules, gateways and other support systems.
- Providers must maintain infrastructure and network systems that add value to the resale of network services and SIMs (often referred to as “heavy or full MVNOs”). Providers that resell network services will be considered for this Magic Quadrant; however, resellers of connectivity services must provide life cycle management of the relevant contracts. Gartner prefers resellers that bundle IoT connectivity and IoT solutions and own the service contracts (service novation). Such reseller providers are often referred to as “light MVNOs.”
- Providers may sell bundled solutions; however, providers must also make IoT hardware and IoT connectivity management available as separate saleable offerings.

Honorable Mentions

A1 Digital is a European digital solutions provider headquartered in Austria and part of the A1 Telekom Austria Group. The company offers IoT, cloud, network and cybersecurity solutions for enterprise customers. Its portfolio includes managed IoT connectivity, hardware and device integration, data platforms and industry-specific services. A1 Digital also provides cloud infrastructure through Exoscale, its European public cloud platform. The vendor did not meet the Magic Quadrant criterion of having a direct local commercial presence in at least three regions.

KPN is a telecommunications service provider headquartered in the Netherlands. The company delivers managed IoT connectivity and related services primarily across Europe, and supports multinational deployments through a combination of direct

operations and international partner networks. KPN supports IoT use cases across sectors such as automotive, manufacturing, healthcare, utilities, agriculture and public services, with a focus on mission-critical and regulated environments. Its IoT offering includes managed connectivity, device management, secure network services and customer self-service access via the KPN Things Portal, with solutions delivered directly and through partners to support cross-border deployments. The vendor did not meet the Magic Quadrant criterion of having a direct local commercial presence in at least three regions.

Pelion is a U.K.-based MVNO specializing in managed IoT connectivity. The company provides global cellular IoT services through the Pelion IoT Platform, which enables connectivity management, eSIM functionality, secure networking and operational visibility. Pelion supports multinet connectivity across numerous countries and focuses on scalable IoT deployments for enterprise customers. The vendor did not meet the criterion of having at least 9.5 million connected IoT devices under management.

Proximus Global is a global communications and connectivity provider. Through its subsidiary BICS, headquartered in Belgium, the company delivers international connectivity, interoperability and IoT services for mobile operators, MVNOs and enterprises. BICS offers global IoT connectivity via a single SIM and platform, supporting deployments across Europe, Asia/Pacific, North America and other regions. Its IoT portfolio includes cellular IoT, roaming and satellite-enabled connectivity. The vendor did not meet the criterion of having at least 20% of its managed IoT devices under direct end-user contract.

UnaBiz is a global IoT service provider and system integrator headquartered in Singapore. The company owns and operates the Sigfox OG technology and delivers massive IoT solutions optimized for low-power, low-data use cases. UnaBiz supports a hybrid connectivity approach that includes Sigfox, LoRaWAN, LTE-M and NB-IoT, along with additional cellular and satellite technologies. Its services span solution design, device manufacturing, connectivity and data platforms, serving customers across multiple regions. The vendor did not meet the Magic Quadrant criterion of having a direct local commercial presence in at least three regions.

Evaluation Criteria

Ability to Execute

Gartner evaluates a provider's Ability to Execute in the managed IoT connectivity services market by assessing how effectively its processes, systems and service delivery meet the complex, global demands of modern connected enterprises. For this Magic Quadrant, all standard Ability to Execute criteria were utilized to provide a comprehensive assessment, meaning no criteria were excluded from the evaluation table.

Product or Service is a primary driver. This criterion evaluates a provider's comprehensive portfolio of cellular, LPWAN, satellite and private network solutions alongside advanced eSIM orchestration. It also assesses value-added IT services, robust partner ecosystems and proven innovation in AI/ML and security.

Sales Execution/Pricing is a primary driver. This assesses presales capabilities, deal management and flexible pricing models. Evaluators specifically look for balanced global execution across diverse verticals and the ability to monetize value-added services beyond baseline connectivity.

Customer Experience is a primary driver. This measures how effectively products and support programs help clients achieve their desired business outcomes. Success is quantified by evaluating technical support quality, SLA adherence, Net Promoter Scores and formal customer feedback.

Operations is a primary driver. This evaluates an organization's ability to govern service delivery, meet SLA commitments and maintain robust global help desk structures. It heavily emphasizes continuous service improvements, specifically the integration of AI/ML to optimize daily processes.

Market Responsiveness and Track Record is of secondary importance. This evaluates a provider's agility in adapting to macroeconomic turbulence and evolving enterprise demands, such as the need for hybrid management and localized connectivity.

Marketing Execution is of secondary importance. This assesses the effectiveness of promotional campaigns and quantified marketing activities designed to increase global market awareness across geographically balanced channels.

Overall Viability is considered to a lesser extent. This assesses the organization's broader financial health, the practical success of its specific IoT business unit and the likelihood

of continued product investment.

Ability to Execute Evaluation Criteria

<i>Evaluation Criteria</i>	<i>Weighting</i>
Product or Service	High
Overall Viability	Low
Sales Execution/Pricing	High
Market Responsiveness/Record	Medium
Marketing Execution	Medium
Customer Experience	High
Operations	High

Source: Gartner (May 2026)

Completeness of Vision

Gartner evaluates a provider’s Completeness of Vision in the managed IoT connectivity services market by assessing its ability to anticipate evolving enterprise requirements, shape market changes and drive innovation beyond baseline connectivity. For this evaluation, all standard Completeness of Vision criteria were utilized, meaning no criteria were excluded from the assessment.

Market Understanding is a primary driver. This evaluates a provider’s global reach, ecosystem partnerships and strategic integration of emerging technologies like 5G, satellite, AI and edge computing. Evaluators also look for a demonstrated ability to deliver value and robust security beyond baseline connectivity.

Sales Strategy is a primary driver. This assesses a provider's Ability to Execute a homogeneous global selling strategy across both direct and indirect channels. It specifically looks for a shift toward solution-oriented sales where IoT is bundled with security, cloud and private networks.

Offering (Product) Strategy is a primary driver. This focuses on a provider's approach to product development, specifically assessing IoT orchestration maturity and the simplicity of its centralized management portal. It also evaluates strategic integrations with hyperscalers, AI enhancements and comprehensive IoT security standards.

Vertical/Industry Strategy is a primary driver. This evaluates a vendor's ability to direct resources and tailor customized value propositions to meet specific industry needs. Evaluators specifically look for balanced expansion beyond traditional core verticals like automotive, transportation and utilities.

Innovation is a primary driver. This assesses how effectively a provider aligns its investments with portfolio evolution, network capabilities and geographic expansion. It also looks for active co-innovation with clients and ecosystem partners alongside a robust developer API ecosystem.

Geographic Strategy is a primary driver. This measures a provider's ability to seamlessly support regions outside its native footprint either directly or through strategic partnerships. Success requires demonstrating homogeneous global capabilities across sales, operational execution and overall service coverage.

Marketing Strategy is of secondary importance. This assesses a provider's ability to clearly communicate differentiated messaging and manage a homogeneous worldwide marketing organization. Evaluators specifically look for quantified marketing activities and campaigns designed to increase global market awareness.

Business Model is of secondary importance. This evaluates the flexibility of a provider's CAPEX and OPEX models and its agility in combining horizontal and vertical strategies. It also assesses its specific approach to monetizing new network technologies like 3GPP LPWAN, 5G and satellite.

Completeness of Vision Evaluation Criteria

<i>Evaluation Criteria</i>	<i>Weighting</i>
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	High
Offering (Product) Strategy	High
Business Model	Medium
Vertical/Industry Strategy	High
Innovation	High
Geographic Strategy	High

Source: Gartner (May 2026)

Quadrant Descriptions

Leaders

Leaders invest in the future of IoT that includes a continuum of value from IoT edge devices to IoT platforms and related analytics and AI capabilities. Leaders perform skillfully and often exceed expectations. They have a clear vision of the market's direction and develop competencies to maintain their leadership.

Leaders engage customers and typically provide value across multiple geographies. They shape the market rather than follow it, and they often set the benchmark for market growth.

Leaders generally have the size and scale (for example, operations, sales and marketing, formal bid, and product management) to pursue large panregional and multinational

opportunities for IoT connectivity. They have established a robust and diverse ecosystem of technology alliances and service delivery partnerships spanning IT, OT and IoT to meet broad market requirements.

Challengers

Challengers execute well today and maintain a sizable, geographically diverse installed base. However, they have a view of the market's direction that is not aligned with the largest and most demanding customers. This can be in terms of the breadth of value and targeted industries, service delivery operations or the continuum of investment for resources and value that a broader IoT platform and portfolio offer.

Challengers in the market for managed IoT connectivity services need to be more aggressive in outlining and communicating their strategy for the future outside of their core focus on connectivity services and associated customer support. They must also be more aggressive in how they invest in innovative offerings or industry expansion. Such offerings include areas like end-to-end IoT solutions predicated on the capabilities to offer a complete service-based IoT platform or the market partnerships to resell and manage on the customer's behalf.

Challengers must also work to extend into adjacent market capabilities, leveraging the experience gained to offer more value and reduce the friction of adoption for their customers and prospects.

Visionaries

Visionaries have a clear view of the market's requirements and direction. They focus on providing a broader continuum of value to meet future market needs and effectively upsell and cross-sell within their installed base through trust and the extension of recognizable, iterative value. Visionaries expand their capabilities through acquisitions, internal development and, increasingly, robust partnering.

Visionaries need to improve their ability to meet customer expectations through process improvement and service center investment. Visionaries also should onboard executives and personnel with valuable market experience. Where investment resources do not exist, Visionaries must work to expand through service delivery partnerships and technology alliances (for example, resell and OEM agreements).

Additionally, Visionaries must work to expand their market focus through catalog expansion, sales force growth in key geographies and/or industry-specific expansion to penetrate the market for global managed IoT connectivity services.

Niche Players

Niche Players focus successfully on a constricted channel to market, a particular service, a particular set of industry markets, a limited number of regional markets or a combination of all of these strategies. The narrower focus of Niche Players may affect their ability to outperform or innovate. Often, their revenue and installed base growth rates lag behind the market average, or they may be unprofitable or exhibit extremely low operating profits in a market that is enjoying relatively high margins.

A provider can be successful in a single capability focused on a single market industry or segment, or a single geography, or selling through partners only. However, Niche Players may have difficulty expanding into alternative geographies, industries or upselling broader value to their installed base.

Niche Players are still very much viable providers of managed connectivity services for managed IoT connectivity and IoT use cases. However, users must be aware that broader IoT expansion may not be possible with these providers.

Context

Multinational enterprises requiring managed IoT connectivity services across different countries and regions are still facing a number of challenges (see Note 1 for the difference between managed IoT connectivity and broader IoT):

- There is a lack of homogeneous service across countries for certain IoT connectivity technologies, such as NB-IoT or LTE-M, and for certain capabilities, such as multisourcing service integration (MSI) or sourcing and logistics.
- eSIM and BYOC have evolved from insurance policies to core IoT orchestration strategies for global deployments. MNOs and MVNOs now act as IoT orchestrators, leveraging API CMP aggregation and eSIM orchestration to enable enterprises to switch profiles and manage local carriers within unified portals. However, IoT orchestration complexity is rising, compounded by delays in the eSIM SGP.32 launch

by vendors. Enterprises must also navigate a fragmented landscape of proprietary or interim solutions. Vendor differentiation becomes harder as many providers rely on the same third-party partners (e.g., Simetric) for API aggregation and BYOC visibility, making it challenging for CIOs to evaluate true platform value.

- Connectivity is a commodity. Elements such as IoT connectivity platform simplification, integration, APIs, a vendor's partner ecosystem, AI-driven operations and predictive analytics, or managed service depth are critical factors that enterprises need to assess. Evaluating these elements helps identify providers capable of supporting regional or global deals and delivering significant performance improvements.
- Enterprises have moved beyond a mere lack of understanding of IoT security and are now actively responding to escalating cyberthreats and stringent new regulatory mandates, such as the EU's NIS2 Directive and Cyber Resilience Act. Consequently, the market is shifting toward embedded "security-by-design" architectures. Organizations must now evaluate providers based on their ability to deliver comprehensive, end-to-end protection — including advanced network-layer controls (such as Secure Access Service Edge [SASE], Zero Trust Network Access [ZTNA], and AI-driven anomaly detection) — alongside device-level cryptography that leverages the SIM card as a secure hardware root of trust (e.g., IoT SAFE).

At the same time, businesses are becoming more mature in the way they interoperate IoT and OT. However, many connected solutions are planned, deployed and maintained within invisible silos in business units such as product marketing, or in regional business units or operations and engineering.

CIOs must actively guide vendor selection by evaluating providers that offer turnkey, industry-vertical bundles. Instead of generic data pipes, leading vendors now package connectivity, certified edge hardware, and hyperscaler data routing into single, outcome-based subscriptions tailored to specific industries.

This Magic Quadrant assesses the Ability to Execute and Completeness of Vision of 18 managed IoT connectivity service providers (see Note 2 for the different types of providers). CIOs building IoT-enabled businesses can use this information and analysis to help them select provider contracts that support critical functions and business objectives. They can also use this information to assess the provider for future capabilities as the enterprises work toward broader IoT solutions.

For further guidance, a more detailed analysis of the service providers' capabilities, with scoring based on different use cases, is available in Critical Capabilities for Managed IoT Connectivity Services.

Market Overview

The managed IoT connectivity market is experiencing rapid growth, now driven by autonomous operations, network-centric security and agentic AI. As device fleets scale globally, vendors are seeing double-digit increases in both connections and revenue, with generative AI (GenAI) chatbots and self-healing networks emerging as key differentiators. The average year-over-year growth of connections among all participants in the Magic Quadrant is over 16%. However, the convergence of IT and OT, as well as new technologies such as eSIM, are amplifying cyber risks, increasing demand for proactive security solutions like agentless firewalls and immutable identity binding.

IoT connectivity price erosion continues, with both global and North American rates dropping by over 10% on average, while highly competitive deals are seeing even steeper declines. To offset this, platform pricing has become mixed: vendors heavily discount basic access but increase fees for advanced orchestration capabilities. Meanwhile, hardware prices have risen marginally due to lingering supply chain costs. Conversely, IoT security pricing has remained completely flat industrywide, underscoring its resilience as a highly stable, premium-margin service.

As IoT connectivity becomes commoditized year over year and revolutionizes various sectors, prospective buyers should consider these five influencing trends in the managed IoT connectivity services market:

Enhancing Capabilities With D&A and AI Integrations

Managed IoT connectivity vendors have moved well beyond basic analytics, embedding GenAI and autonomous agentic AI directly into connectivity management portals (CMPs). These integrations now deliver operational efficiency, proactive innovation and advanced security. Key benefits include:

- Transition from predictive maintenance to autonomous operations, with AI proactively detecting issues and triggering automated remediation to minimize downtime.

- AI-driven security and self-healing networks that continuously monitor for threats and automatically resolve network issues.
- Real-time agentic AI optimization of network performance, bandwidth and energy use, especially for large-scale deployments.
- GenAI chatbot management of up to 70% of support tickets, reducing mean time to repair and freeing engineering resources.
- AI-powered natural language interfaces that democratize data access, enabling faster, data-driven decisions across the organization.

GenAI has quickly evolved into an essential differentiator for leading managed IoT connectivity platforms, while autonomous agentic AI is rapidly transitioning from advanced pilots to commercial production, driving the next generation of self-healing networks.

Safeguarding Against the Challenges of IoT Security

- Device vulnerability and supply chain risks: Many IoT endpoints operate with limited computational resources, making them susceptible to firmware exploits, insecure default configurations and supply chain attacks.
- Data privacy, sovereignty and regulatory compliance: The growing importance of data privacy is underscored by evolving regulations such as GDPR, the EU Cyber Resilience Act (CRA), and NIS2 Directive. Managed IoT connectivity providers must ensure compliance with regional and sector-specific mandates.
- Fragmented ecosystems and lack of unified security standards: The heterogeneity of IoT devices, protocols and connectivity options (e.g., cellular, LPWAN, Wi-Fi) complicates the deployment of standardized, end-to-end security solutions. Industry initiatives such as the GSMA IoT Security Guidelines and ETSI EN 303 645 are gaining traction, but widespread adoption remains a challenge.
- Emerging threats: Increasing threats from ransomware, AI-powered attacks and emerging risks like quantum computing are being targeted against IoT infrastructure.
- Network-level risks and SIM/identity attacks: Managed IoT connectivity services are increasingly targeted by attacks on SIM cards, eSIM profiles, and network identities (IMSI catchers, SIM swapping).

To address these risks, vendors are implementing comprehensive safeguards:

- Zero-trust security models, microsegmentation and continuous monitoring.
- Secure boot mechanisms (e.g., GSMA IoT SAFE), regular firmware updates, and hardware-based security leveraging the SIM/eUICC as a secure hardware root of trust — rather than relying on external Trusted Platform Modules — are essential.
- Strong encryption, data minimization and secure communication protocols (TLS/SSL, VPN).
- Proactive threat intelligence, regular security audits and penetration testing.
- Postquantum cryptographic algorithms are being prepared for the eventual impact of quantum computing on IoT security.
- Integration of managed security services, including 24/7 SOC monitoring, anomaly detection and automated threat response, is becoming a differentiator for IoT connectivity providers.
- Robust device identity management (X.509 certificates, PKI), secure onboarding and automated decommissioning processes are critical for maintaining trust and compliance throughout the device life cycle.

These measures are critical for building trust and differentiating in a competitive IoT market.

The Rise of the Smart IoT Orchestrator: Navigating eSIM, SGP.32 and BYOC

As IoT projects grow in scale and complexity, vendors are evolving to deliver seamless device and connectivity experiences, addressing new use cases such as edge AI deployment and increased data transfer between cloud and edge. However, enterprises remain hesitant to switch connectivity providers due to cost and deployment challenges, prompting vendors to differentiate through advanced orchestration and integration capabilities. Overall, the estimated adoption of eSIM among vendors participating in the Magic Quadrant is approximately 22% of their installed base. This estimate is equally balanced between deployments characterized by low-to-mid bandwidth consumption and those involving high bandwidth consumption, thereby providing a representative average across both usage profiles. Key developments include:

- Adoption of the SGP.32 IoT eSIM standard, enabling “build-once, ship-globally” hardware strategies and dynamic over-the-air profile localization.
- Support for native BYOC models, reducing MNO vendor lock-in, optimizing costs and bypassing permanent roaming restrictions.
- Unified platform aggregation and hybrid network federation, allowing seamless integration of public cellular, private 5G, LPWAN and satellite (NTN) networks.
- Advanced IoT orchestration platforms that federate multiple third-party connectivity management portals via standardized APIs and eSIM.
- Streamlined integration with hyperscalers and back-end IT systems, enabling centralized policy management, cross-regional deployments and unified billing and diagnostics.

These advancements position vendors as smart managed connectivity enablers, capable of supporting increasingly complex, global IoT deployments.

Accelerating Adoption of 3GPP LPWA, LTE Cat 1/Cat 1bis, and RedCap

IoT connectivity is evolving rapidly, with strong growth in 3GPP LPWAN (close to 100 million connections reported in this Magic Quadrant, compared to 200 million LPWAN connections reported globally) and LTE Cat 1/Cat 1 bis (150 million connections reported in this Magic Quadrant). Key developments include:

- Migration from legacy 2G/3G networks to LTE-M and NB-IoT, with a preference for LTE-M in multicountry deployments and roaming scenarios.
- Utilization of LTE Category 1 (Cat 1) and LTE Category 1 bis (Cat 1 bis) as flexible alternatives for midtier global IoT connectivity.
- Commercial rollout of 5G standalone (SA) RedCap networks, beginning with hot spots and dongles and expanding to broader deployments.
- Acceleration of certification and testing for 5G RedCap modules and chipsets, supporting the transition to low-cost 5G devices.
- Expansion of proofs of concept (POCs) for RedCap, with anticipated commercial launches and enhanced RedCap (eRedCap) support within one to three years.

- Alignment of RedCap adoption with ecosystem and network readiness, including core network development for massive IoT and constrained devices.
- Divergent 5G RedCap adoption strategies are emerging for both high-end and low-cost use cases. Hardware vendors are introducing AI-powered 5G RedCap modules that are tightly integrated with edge-compute platforms to support advanced computer vision applications while, in parallel, utility vendors are leveraging existing LTE-M and NB-IoT deployments as a foundation to eventually migrate to standard, cost-optimized 5G RedCap devices for long life cycle smart grid endpoints.

These advances are driving a more flexible, scalable and cost-effective IoT connectivity environment.

Bridging Managed IoT Connectivity with 5G, Private Networks and Edge Computing

The integration of 4G/5G private mobile networks (PMNs) and edge computing within managed IoT platforms has become a commercial imperative, enabling seamless control across public cellular, private networks and OT environments. Key developments include:

- Unified SPoG control for managing previously siloed public, private and OT networks.
- Seamless public-to-private orchestration through automatic, policy-driven handovers using multi-IMSI profiles, dual-core architectures and SGP.32 eSIM orchestration.
- Continuous, secure connectivity for industrial assets, including autonomous guided vehicles and logistics fleets, across private and public networks.
- Commercialization of 5G standalone (SA) networks, enabling dynamic network slicing and multiaccess edge computing (MEC) for ultra-low-latency, bandwidth-intensive use cases.
- Isolation of critical OT traffic through dedicated network slices, meeting stringent security and compliance requirements.
- Expansion of private network management beyond Tier 1 mobile network operators (MNOs) to IoT mobile virtual network operators (MVNOs) and connectivity orchestrators offering flexible, pay-as-you-grow network-in-a-box solutions.
- Democratization of edge computing through partnerships with hyperscalers, private network infrastructure providers and edge AI vendors, enabling organizations of all sizes to deploy robust edge ecosystems without deep telecommunications expertise.

These advancements are redefining managed IoT connectivity as a strategic bridge to next-generation networks and edge computing (see [Hype Cycle for IoT, 2025](#)).

Note 1: Distinguishing Managed IoT Connectivity Services and IoT

The technology and service functions defined below fulfill critical parts of typical IoT solutions with a particular focus on the IoT edge, which encompasses IoT endpoints, gateways, edge computing and connectivity services. Many providers in this Magic Quadrant have moved away from references to machine-to-machine (M2M) in their messaging and catalog descriptions to create the perception that their solutions are more IoT-aligned, labeling them as “IoT solutions.” In fact, most have changed their business unit names to include IoT in the title.

The market for managed IoT connectivity services is mature and does not present the attention and buzz of broader IoT solutions. These rebranding efforts are meant to convey broader solution value to the market. However, relabeling their offers and business units to “IoT” or “IoT connectivity” does not make their solutions IoT solutions.

While not explicitly codified, what distinguishes typical managed IoT connectivity solutions from IoT solutions is the existence of broader platform capabilities in an IoT solution. An example is the capability for IoT endpoint and device management, where most vendors in this Magic Quadrant manage the SIM card and related data, rather than IoT edge device OSs and agents, and other management capabilities. Also, offerings and definitions for IoT solutions include an application enablement and management capability within the IoT platform (see [Magic Quadrant for Global Industrial IoT Platforms](#) for a further discussion on the components of an IoT solution).

A key offering of competitive IoT solutions and platforms in the market also focuses on integration capabilities. Examples include integration platform as a service (iPaaS), API management, various software development kits (SDKs), and software connectors and extensions to facilitate integration and interoperability with third-party software and applications.

Increasingly, we see CSPs and MVNOs choosing to ignore the build-out of broader and higher-value IoT platforms. Rather, they favor creating and acquiring IoT vertical applications (such as fleet, smart meter and energy demand management), which can be integrated into enterprise applications. Without a broader, true IoT platform, CSPs and

MVNOs are forced to sell these vertical applications as point services that require the user to explore, validate and acquire IoT platform elements, such as device management and data management. This happens when these point solutions don't cover the enterprise use case beyond the horizontal connectivity and value added, such as security or managed services that these vendors provide.

Note 2: Provider Models

Communications Service Providers

CSPs typically bundle connectivity services (such as cellular, LTE and connectivity management). However, some providers offer cloud-based IoT platforms composed of messaging, device management and storage and base-level analytics (utilization reporting and asset tracking). The enterprise service organization of some CSPs amortizes device charges across the term of an agreement as a recurring add-on charge.

Additionally, some providers offer application enablement platforms and a modest catalog of vertical applications (most commonly fleet management and asset monitoring). For noncellular use cases, most CSPs provide managed services for wireless LAN (WLAN), some LPWA networks (3GPP and non-3GPP), limited satellite and managed security services for IoT gateways. Most CSPs have created access partnerships to augment their global IoT connectivity management capabilities. Examples of this type of provider include AT&T and Vodafone.

Mobile Virtual Network Operators

The immediate value that MVNOs bring to customers is the aggregation and management of multiple CSP networks to provide regional and global connectivity coverage. Additionally, as with the CSPs, hosted and cloud-based connectivity management applications provide users with device metadata, status information and diagnostics information.

The management platform also extends to users of the self-management capabilities, such as SIM management actions for bulk operations on many devices. Some IoT MVNOs have been acquired by CSPs to address specific segments and verticals to complement their IoT capabilities. Examples of this type of provider include Aeris Communications, Cubic³, KORE and Wireless Logic.

Hardware Module Manufacturers and Hardware Intellectual Property Companies

Traditional hardware module manufacturers and hardware intellectual property companies are shifting their strategies to leverage their hardware (or hardware they power) and bundle it with connectivity, cloud access, device management and, in some cases, data management. This strategy brings to hardware-related manufacturers the ability to provide powerful device management capabilities on top of managed IoT connectivity services.

Due to their hardware capabilities, these vendors integrate some device and data management capabilities into their own connectivity platforms. These vendors try to tie customers to their own hardware-related modules, so the offer can be reduced when not using their own hardware or hardware modules they power. Examples of this type of provider include Telit Cinterion and Semtech.

IT Outsourcers and Integrators

These providers offer traditional IT outsourcing and managed IT services, but they now have practices that focus on delivering managed and professional services for IoT technology management. Many of these providers enter the IoT solution market with the advantage of legacy vertical-centric go-to-market structures that provide subject matter expertise presale and postsale. Many of these providers also own vertical-centric back-office applications (such as manufacturing execution systems and insurance industry applications) that will leverage IoT data.

The number of IT outsourcers and integrators that maintain and manage MVNO operations is still small, but is increasing slowly. As managed IoT service adoption increases in the market, and the price to build and manage MVNO capabilities decreases because of cloud and virtualized technologies, the number is expected to increase over the next three to five years. Examples of this type of provider include Accenture and Fujitsu.

Dedicated IoT Network Providers

This segment represents providers based on public and private networks in the unlicensed spectrum. These providers sometimes manufacture their own IoT edge equipment and develop their own IoT platforms and IoT vertical applications. These

providers present focused offerings, usually predicated on use cases such as automated meter infrastructure, fleet management, smart parking and smart lighting.

While there is no stand-alone vendor from this category for this Magic Quadrant iteration, an example of such a provider from previous research was Silver Spring Networks, acquired by Itron (which is included in this research). Another example is companies that only manage LoRa networks or proprietary systems.

⊕ Evaluation Criteria Definitions

Unlock more AI value

With unmatched, proprietary AI insights from Gartner

[Explore the AI Hub](#) ↗

© 2026 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by [Gartner's Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "[Guiding Principles on Independence and Objectivity](#)." Gartner research may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.

