emnify

Navigating IoT Connectivity Services

The comprehensive buyer's guide for procurement and product managers.

Navigating IoT Connectivity Services

The IoT landscape is changing quickly. Selecting the best providers for your IoT solutions and services can determine how quickly you're able to get your product to market, overall performance and customer adoption and satisfaction of your offering, and most importantly, how well your offering is future-proofed to meet new market challenges and opportunities.

This guide provides a comprehensive set of considerations to help you assess and select an IoT connectivity service provider.

The fact is, that while telecommunications is a highly regulated and standardized industry, IoT is a relatively nascent part of a traditional network operator's business. Leading Mobile Network Operators built their systems for voice so coverage, adaptability, scalability, compatibility, and security for IoT all vary widely from one provider to another. And these are six key areas where your connectivity solution significantly affects your IoT business.

New approaches to IoT connectivity are tackling these challenges and closing the gap between traditional telecom and IoT business. Choosing the best IoT provider for your connectivity needs will impact your IoT business in critical areas such as time to market, reliability and availability, connectivity and device management, cost optimizations, and most importantly, your ability to adapt and innovate. This guide will provide you with deeper insights into these areas, and how to assess potential connectivity providers.

Need a summary?

Need a summary to share with colleagues? At the end of this resource, you'll find an evaluation checklist of the capabilities covered in the guide.

CONTENTS

COVERAGE

IoT Connectivity Coverage and Network Access

Coverage is one of the first things that comes to mind when IoT businesses compare connectivity options. The most basic question to ask is does a provider deliver coverage in the regions you plan to deploy, but there's a deeper set of considerations to assess potential providers that goes beyond geographic footprint. You'll want to understand how the provider has access to the networks and technologies you need for your use case.

Today, it's typical that IoT businesses need to rely on multiple providers, platforms, portals, features, and processes to get the coverage they need. Working with multiple providers does introduce inconsistent capabilities for connectivity management and device deployments. IoT businesses relying on traditional telecom providers find that making updates to coverage, configurations or policies, typical requirements for managing IoT solutions, involves slow, manual processes, with changes and deployments often taking several weeks.

As you assess whether a cellular connectivity provider has the coverage your business needs, you'll want to consider the following questions:

1. **Does the provider offer multi-network access, and if so how?**
2. **What happens if your device crosses into another country?**
3. **How can you add or change coverage in the future?**
4. **Will you have access to the network types and types of technology you require such as 5G, satellite, NB-IOT?**
5. **Does the provider use network steering?**

Did you know?

The emnify SuperNetwork's growing collection of networks includes 2–3 network providers in most countries, giving you redundant coverage wherever you need to deploy. ***Explore our coverage here.***

1. **Does the provider offer multi-network access, and if so, how?**

   For most businesses one network provider on their own will not have the coverage needed to deploy devices in multiple markets. Even large, traditional MNOs rely on roaming agreements to provide coverage outside of their home networks. You'll want to ask how they have set up their access to partner networks.

   - Do they have direct network access partnerships? This will make a difference in the consistency and control your provider (and you) has across all of your networks, for example ensuring permanent roaming agreements and technology commitments that you can rely on.
   - When there is a coverage issue, is your supplier a reseller, operator, or carrier who can troubleshoot directly with other network providers? Direct access partnerships allows a provider visibility into all partner networks which enables troubleshooting and faster resolution of connectivity issues.

   You'll also want ***network redundancy*** in every country to ensure your devices can switch to a backup network if your primary network goes down, increasing your overall uptime.

2. **What happens if your device crosses into another country?**

   If you have devices that cross borders, you'll want to make sure you don't lose connectivity or end up with a higher-than-expected invoice for roaming outside of your primary network. Does your connectivity provider provide coverage on demand and flexible coverage plans or is it only a fixed term contract? For example, can you activate a device in one region, deactivate it remotely, and then activate it in another region?

3. **How can you add or change coverage in the future?**

   Over time, your business needs and/or your provider's coverage map may change. Ideally, your devices should be able to automatically access additional coverage, networks and technologies with over the air (OTA) updates via an ***eUICC*** standard ***eSIM***.

Did you know?

*The **emnify IoT eSIM** is based on **eUICC architecture**, our state-of-the art IoT **eSIM platform** allows us to continuously update SIM profiles, providing you with the best coverage with a single eSIM.*

4. Will you have access to the radio access network types you need?

IoT businesses increasingly want more control over their technology, including connectivity coverage. There are many different cellular technologies available: ***4G LTE***, ***LTE-M***, ***NB-IoT***, and more. You can't assume that having access to a carrier's network means you'll have access to every radio access network of that carrier. For example, let's say a provider does have LTE-M, 4G, and 5G coverage in Germany, will you have access to each of those networks? Can you isolate the network types that are compatible with your device, or will your devices still attempt to connect to 4G and 5G service by default, when they're only compatible with LTE-M?

This is why it's important to work with an IoT experienced provider that's investing in new IoT-specific network partnerships to provide access to IoT network technology like NB-IoT over satellite and LTE-M. So if your IoT solution relies on LTE-M coverage and you have customers in Germany, you can get LTE-M coverage in Germany—a provider that only offers 4G or 5G coverage in Germany won't do you any good, no matter how good that coverage is.

5. Does the provider use network steering?

Many connectivity providers give you little control over which carriers your devices connect to. For example, due to your provider's agreements with operators, your devices may always connect to Carrier A when it's available, even if Carrier B or Carrier C has a stronger signal. This is called ***network steering***. Look for providers that offer agnostic, multi-carrier coverage so you can prioritize connectivity for your business versus theirs.

Breadth and depth of connectivity management capabilities

The IoT landscape is constantly changing. Your connectivity provider should provide a single, core mobile network to ensure a consistent set of connectivity capabilities, and single-pane of glass visibility and management tools across all access networks to manage SIMs, devices, network optimization, analytics, and accounts.

Here are some helpful questions to assess a provider's connectivity management capabilities:

1. How will the provider help you manage SIM lifecycles?
2. What kind of device management capabilities does the provider give you?
3. How will you manage separate accounts and users?
4. What reporting and analytics capabilities will you have access to?
5. How is the provider demonstrating their investment in innovation?

1. How will the provider help you manage SIM lifecycles?

In cellular IoT, SIMs remain in the field for years. Here's what you should consider about your provider's SIM lifecycle management capabilities:.

- How does your provider help you adapt as MNOs repurpose network infrastructure, sunset older technologies, or discontinue their service?
- Can they ensure interoperability with future IoT devices and applications?
- Can you use a single management portal for automated global provisioning, activation, configuration, and deactivation of SIMs, or will you have to log into and manage SIMs from multiple providers via multiple management portals?
- Can you configure, provision, and activate devices automatically in near-real time or does this process require manual interactions that take days or even weeks? Are you able to buy SIMs and only pay for them once you activate them? Are you able to suspend and reactivate them as your business requires?
- Does the management platform scale for multiple geographies, use cases, and volumes, with a consistent set of services and features?
- Can you customize ***network selection*** for your specific use case and hyperlocal region, ensuring devices have the best possible connectivity?
- Will crossing borders require new SIMs or can connectivity be switched to a new provider via over the air updates?

2. **What device management capabilities are available?**

   How your provider enables you to configure and control your devices will directly affect your operations. Here's what to consider:

   - Does the provider enable VPN services for remote access for device management? How long does it take to provision and is there an additional fee?
   - Is real-time device location tracking available?
   - Do they have batch management capabilities to automatically configure every device that will use the same settings, whether there are hundreds or hundreds of thousands of them?
   - Can you control if your device can access certain radio access networks like 2G or 5G?

3. **How will you manage separate accounts, users, and deployments?**

   As your business grows, more individuals will need access to your connectivity data. Here's what you'll want to consider:

   - Does the provider offer hierarchical accounts with distinct entities, sub accounts, users, access, billing, currencies?
   - Is modern authentication and SSO offered?

   Do they offer flexible options for data plans and give you the ability to create multiple data plans based on business needs?

Did you know?

*The SuperNetwork creates a consistent set of **connectivity capabilities**, regardless of which network your SIMs connect to. You can view and manage all of your deployments from a single pane of glass, no matter which carrier is providing the underlying coverage.*

Did you know?

*IoT businesses that have switched from other cellular IoT connectivity providers to emnify have noted that our automation, testing, and **configuration capabilities** have shaved days, weeks, and even months off their deployment times.*

4. What reporting and analytics capabilities will you have access to?

Your connectivity data becomes far more useful when your provider gives you tools to organize it in meaningful, relevant ways. Here's what to consider when it comes to reporting and analytics:

- Do you have full visibility into network level events across all of your networks with granular data on each carrier, every connection and disconnection, network type, device data usage, warning and error events you need to optimize and control your connectivity and uptime?
- Will you have real-time data usage analytics across all of your networks?
- Do they have timesaving out-of-the-box reports available to show data usage by device, timeframe, and geography, as well as visualizations and dashboards to make insights easier to consume and share across the organization?

5. How is the provider demonstrating their investment in innovation?

The world of IoT is constantly evolving—and your connectivity provider should be, too. Here's what to consider about their investment in innovation:

- Are they making continuous improvements in ease of use?
- How frequently do they update their platform interfaces?
- Do they make changes to their applications or portal in response to customer feedback?
- Are they delivering a modern user experience?

ENSURING DATA COMPLIANCE

Data Compliance: Intelligent Data Routing, Regional Breakouts

As of 2023, the following countries currently have some form of data localization laws which ban, regulate, or restrict the storage or processing of data in other countries: Brazil, Turkey, Nigeria, China, Egypt, India, Saudi Arabia, Singapore, United Arab Emirates, Germany, United States, Canada, and Australia.

How does the provider maintain compliance with data localization laws?

Data localization laws create challenges for some connectivity providers: they can't legally process your data through their core network if it's in another country. Core networks are how providers authenticate devices, ensure you're billed appropriately for data consumption, and route your data to its destination. Normally, connectivity providers route your transmissions through their core network before sending them to the recipient. It's called Home Routing, and it can violate data residency laws if the home network is outside of the country.

What this means for your IoT business:

When you deploy in one of these countries, your SIMs have to use a profile from a local carrier. Your SIMs can only use roaming agreements to connect to local carriers for a limited time before your business will incur penalties or potentially even get banned from operating in the country.

Providers can relieve this pain point by deploying their core network through regional Internet breakouts that keep your data local. This requires that their core network is distributed and not tied to a specific data center. Cloud-based, distributed core networks solve this issue by routing data through regional breakouts, so your data doesn't have to cross borders to travel back to a home network.

Did you know?

The SuperNetwork's distributed data plane enables device data to breakout locally, keeping customer data within the same region which also helps reduce network latency. You can either select a specific breakout region or the network automatically selects the breakout region closest to the device.

INTEGRATIONS

Integrations with IoT applications and infrastructure

Integrations across the IoT stack stream connectivity data to IoT applications and workflows to provide new levels of insights, control, and automation. There's a high degree of variability among connectivity providers in their approach to enabling integration, from network architecture to API management to support. With 90% of IoT applications built on top of cloud services, your provider's ability to integrate seamlessly with cloud applications becomes increasingly important.

Here are some questions to ask as you consider how compatible an IoT connectivity provider is with your current tech stack:

And most importantly, if you plan to use multiple providers for your IoT connectivity, ***will you have a single platform for cross network integrations or will you need to drive new integrations for every provider?***

1. **Does your provider offer industry standard APIs and data formats?**
2. **How will integrations affect your time to market?**
3. **Are there no-code and low-code options to allow for faster, flexible workflows?**
4. **Which connectivity services do you plan to integrate with your IoT applications or infrastructure?**
5. **How many platform services are accessible via API? Is it simply connectivity data or are there more resources available?**

Did you know?

*The emnify SuperNetwork provides a single connectivity platform to enable **seamless integrations** for all of your connectivity data and network management. The SuperNetwork is built to accelerate integration across front and backend IoT applications **with capabilities including:***

1. *REST API integrations and GraphQL for CRM, ERP, and other business critical apps.*
2. *Native integration of data into major cloud IoT services from AWS (Kinesis, Quicksight), Microsoft Azure (Event Hubs, Power BI), and Google (Pub/Sub, BigQuery) and other data analytics platforms.*
3. *No-code and low-code options with leading providers like Zapier.*

SECURITY

How to compare security

IoT devices are notoriously vulnerable to hacking and data theft, especially since most lack the battery power and data throughput to support basic security functions. The data traffic of regular SIM cards is secured within the mobile network but traverses the public internet between the mobile network and the application. The device and application are not only susceptible to attacks but it also makes it difficult to establish remote device management.

Working with multiple connectivity providers adds complexity to your security management. The lack of cross-network visibility and data reduces the ability to detect anomalies that point to misuse or attacks on your devices and data.

It's clear that IoT connectivity plays a large role in securing your IoT devices and data.

Here are some questions ***to help you evaluate a provider's impact on your IoT security:***

1. **How will the provider help you adapt to emerging IoT security standards and technologies?**
2. **How does the provider help protect your IoT devices and data?**

1. How will the provider help you adapt to emerging IoT security standards and technologies?

Security is an area of IoT that's advancing rapidly to help organizations mitigate risks and build more trustworthy and robust IoT systems. IoT SAFE (IoT Security Assurance Framework) is a standardized framework developed by the Global System for Mobile Communications Association (GSMA) to address security challenges inherent in IoT. IoT SAFE is focused on securing communication between IoT devices and application servers, particularly in scenarios where cellular networks are involved.

Another emerging framework is Secure Access Service Edge (SASE). SASE is a network architecture that combines network security and wide-area networking (WAN) capabilities into a unified cloud-based service. SASE provides security and networking services from the cloud, closer to the user or device, rather than backhauling traffic to a centralized data center. SASE integrates multiple security functions, such as secure web gateways, firewalls, intrusion prevention systems, data loss prevention, and more, into a unified service. These security functions are delivered from the cloud and applied dynamically based on policy and context.

Some emerging security trends and standards you'll want to ask providers about include:

- Are their SIMs ready for IoT SAFE?
- Can the provider take advantage of a cloud-native, distributed SASE approach to data, security, and networking services?
- Does your provider rely on the public Internet for device management and data routing?
- Is the provider SOC 2 certified?

How does the connectivity provider help protect IoT devices and data?

In the field, IoT devices aren't just vulnerable to network-based attacks. Your devices might be in public places or other environments where people can physically access them. Someone may steal your device itself, or if you have removable SIM cards, they may just take the SIM to use it in another device.

Every device has an ***International Mobile Equipment Identification (IMEI)*** number which enables a carrier to identify specific devices that are authorized to use their network. Some connectivity providers can set IMEI locks which prevent a device with a different IMEI from using the SIM card. So if the SIM card is ever stolen, that doesn't mean your data will be, too.

Depending on your provider, you may not learn about data theft until it shows up on your bill. Even if you can manually monitor your data usage, that may not be enough. More sophisticated providers, however, can analyze data consumption patterns and recognize anomalies in real-time—whether they're caused by attackers or even just human error. Ideally, your provider should proactively notify you when their analysis detects a potential threat.

Here are some further considerations as you assess each provider's ability to keep your devices and data from being misused:

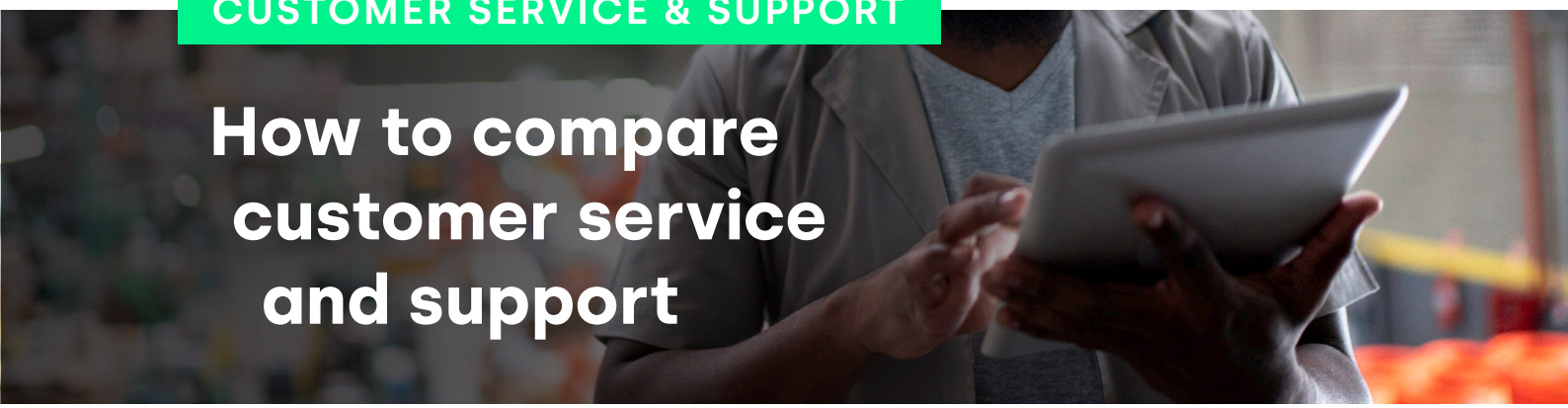
- What level of visibility and control do you have over device connectivity? How fast can you identify and react to suspicious data transfers?
- Do you have insights into network events across all networks to help detect misuse or anomalous behavior?
- Do you have secure connections for remote device management or do you have to rely on public internet connectivity? How easy is it to set up VPNs for secure communications?
- Does your provider offer advanced firewall features?
- Can you configure and utilize your own DNS to protect IoT devices from Denial of Service attacks and prevent access from devices already infected by a cyber attack?

Did you know?

*emnify's industry-first cloud-native network core protects all of your devices with **a suite of security features** including a network-level firewall, private DNS lists, custom connectivity profiles, IMEI locks, direct cloud connections, and more.*

*emnify's enterprise customers who have their infrastructure on Amazon Web Services can also use AWS Transit Gateway to provide a secure channel from the emnify AWS VPC to the enterprise's VPC. Data stays within AWS networks and does not require any public internet breakout to connect devices to the application in AWS. For customers on other clouds, the **SuperNetwork IPsec VPN solution** provides a channel between an enterprise's devices and their application infrastructure on Microsoft Azure, Google Cloud, or on-premises servers, for secure data exchange and remote access.*

CUSTOMER SERVICE & SUPPORT



How to compare customer service and support

Connectivity is such a critical component of your IoT solutions that your ability to support your customers often directly depends on your connectivity provider's ability to support you. The more fragmented your connectivity solution is, the more difficult it becomes for any one provider to have full visibility across all networks, to troubleshoot issues and work with your technicians to resolve them quickly. And while traditional telecommunications operators have support resources, IoT businesses need to ensure that their chosen provider has IoT experts available.

Here are some questions to consider as you evaluate a connectivity provider's ability to support your business:

1. **Do they provide dedicated, IoT expert guided onboarding and support resources?**
2. **Will the provider have IoT experts available to support you over the phone or online?**
3. **What do customers say about their support on third party review sites like *G2?***
4. **What kind of dedicated onboarding resources does the provider have available?**
5. **Do they have their own network operations center with operational support 24/7/365?**

Did you know?

*According to the third-party review site, **G2.com**, emnify scores above the industry average for quality of support with a score of 9.8 out of 10. Our team of IoT experts are available 24/7/365 to help our customers troubleshoot and resolve connectivity issues.*

Conclusion:

choosing the IoT connectivity provider that's right for your IoT business

Your IoT connectivity provider and the services they offer will have a significant impact on the success of your IoT solution. Device uptime, operational efficiency, security, and the longevity of your solution in market are all dependent on choosing the right IoT connectivity service provider for your business. The best cellular IoT connectivity provider for your business will:

- Offer the redundant, IoT-specific network access your business needs today and as you grow.
- Future-proof your IoT solutions to adapt to changes in the industry and new opportunities.
- Scale connectivity management as your business grows.
- Provide the integration tools and technology to make your connectivity capabilities compatible with the rest of your IoT stack.
- Increase IoT security with a consistent, modern set of security capabilities regardless of which network you're connecting to.
- Support your business and your teams with IoT specific knowledge and expertise.

As a leader in cloud-native, cellular IoT connectivity, emnify delivers on the key considerations highlighted in this guide. The SuperNetwork reduces the complexity of IoT connectivity with a distributed, global network for reliable and redundant coverage across the globe. A modern approach to connectivity management enables our customers greater consistency and control to deploy, monitor, manage, secure, and optimize all of their devices across all networks from a single connectivity portal. Open APIs, low-code, and no-code integrations streamline access to SuperNetwork data and tools across your entire IoT stack. And importantly, the SuperNetwork embraces state-of-the art security technology to protect data and devices.

Want to see what emnify can do for your business?

Talk to one of our IoT experts today. We'll give you a tour of the features that matter most to your business and discuss the best solutions for your application. If you prefer a self-guided approach, you can also start a free trial. We'll send you everything you need to start testing.

Talk to an IoT expert

As promised, we also have a comparison checklist to help you evaluate cellular IoT connectivity providers. If you want to compare more options or add your own custom criteria, we have a *downloadable spreadsheet* as well.

IoT Connectivity Provider Checklist

COVERAGE	☐ Redundant coverage in the countries you want to deploy
	☐ Coverage in the network type your devices use
	☐ Coverage can be optimized by signal strength or cost
	☐ Intelligent data routing through regional breakouts
CONNECTIVITY MANAGEMENT	☐ One management portal for all networks and countries
	☐ Automatically change SIM profiles to comply with regulations
	☐ Automation capabilities for configuring, provisioning, and activating devices
	☐ SIM deactivation available in the connectivity portal
	☐ Batch management for mass configurations
	☐ Real-time device location tracking
	☐ Configurable access to radio access networks
	☐ Hierarchical accounts with distinct billing, users, access, etc.
	☐ Single Sign On (SSO) available
	☐ Flexible data plans
	☐ Modern UI/UX
NETWORK INSIGHTS	☐ Visibility into network events across all networks
	☐ Real-time analytics across all networks
	☐ Out-of-the-box reports available
INTEGRATION	☐ API enables integration with entire IoT tech stack
	☐ Clear, comprehensive integration guides available online
	☐ No-code integrations available to save dev time
SECURITY	☐ Set SMS and data limits
	☐ Custom DNS limits communication to trusted devices and applications
	☐ IPSec, VPN tunnels, AWS transit gateways for secure cloud connections
	☐ IMEI lock to reduce threat of SIM card theft
	☐ Anomalous data usage detection and real-time alerts
	☐ SOC 2 certified
SUPPORT	☐ Support provided by IoT experts
	☐ Dedicated onboarding support
	☐ 24/7 operational support

About emnify

Every day thousands of businesses rely on emnify's SuperNetwork to connect millions of devices worldwide, including GPS fleet trackers, smart meters, predictive maintenance sensors, medical devices, and more. The SuperNetwork encompasses more than 540 networks in over 180 countries, all accessible through a single eSIM. Our intuitive connectivity management platform empowers businesses to monitor, analyze, control, and automate their device connectivity, with multi-layered IoT security to protect devices and data.

We hope this free resource helps you confidently compare cellular IoT connectivity providers and make the selection that's right for your business.

Get In Touch

www.emnify.com/talk-to-us

www.linkedin.com/company/emnify

@emnify