IoT CONNECTIVITY BUYER'S GUIDE

aeris®

INTRODUCTION

Getting your first few connected devices to market can feel like a monumental accomplishment. Then scaling your deployment to thousands, tens of thousands, and hundreds of thousands of devices introduces a whole new set of challenges: from growing your service delivery and support teams, to introducing new and more advanced products and features, to managing costs as you expand internationally. It's important to take those future challenges into account as you assemble your requirements and shop for an IoT connectivity provider.

This guide is designed to help you evaluate cellular IoT connectivity providers against the critical dimensions of coverage, support, cost control, and security with a focus on the specific capabilities that make or break success at scale.

> "Aeris and Trimble are great partners because we both focus on the same thing—quality of service. Aeris is not just a carrier, but a true partner that enhances our offering."
>
> —John Binder,
> Director of Wireless Operations,
> Trimble

COVERAGE

Coverage is the first, and perhaps most obvious, thing to consider when shopping for a cellular IoT connectivity provider.

AS YOU SCALE, LOOK FOR:

Multiple cellular connectivity technologies in multiple geographies — managed on a single platform. Newer technologies like LTE-M and NB-IoT can offer unique benefits, but they are still being rolled out by carriers, and are therefore only available in certain countries. You'll save lots of time, effort and money down the road by making sure that your provider can:

- Help you figure out which devices should be on each technology for a specific geography
- Enable you to manage all of your connected devices across all technologies and geographies on a single platform

Multi-carrier coverage with performance-optimized steering where necessary. Standard roaming protocols move devices to roaming partners only when the primary carrier is not available. This practice works well in countries like the US, where only a few large carriers have near total coverage, but can cause issues in regions where coverage is more patchwork and complex. To ensure your devices have the best connection, make sure that your connectivity provider:

- Offers access to more than one carrier network in each of your core geographies
- Can tailor network steering to optimize for performance or cost in regions outside North America, where a proliferation of overlapping carrier networks creates a complex coverage challenge

> **Real world benefits:** Aeris customers operating in rural parts of Africa reduced support costs by as much as 50% per customer per device by taking advantage of multi-carrier coverage with performance optimized steering. That translates into massive savings when you are operating hundreds of thousands of devices.

Not sure which technology is right for you? To figure out whether 2G, 3G, 4G, LTE-M, NB-IoT, or a combination will work best for you, make sure you know:

- The geographies where you plan to deploy — both today, and in the future
- Your anticipated monthly data usage
- The length of time (in years) that your devices will be deployed. In some parts of the world, this will help determine whether 2G, LTE, or LTE-M will be the best fit
- Your performance requirements (How often will you send data? How fast do you need to send it?)
- Your solution's characteristics (Will your devices need to connect indoors? Will they move around or stay in one location? Do they require voice and SMS, or just data?)

THE TEST:

Questions to ask your provider to make sure they have you covered:

□ How many carriers do you have in each country where I expect to deploy devices?

□ If my devices are mobile and routinely operate in remote areas, can you help me select carriers on the fly to ensure coverage everywhere?

SUPPORT

Once devices are connected, service delivery teams require tools and information to monitor those connections and to detect, diagnose, and resolve the wide variety of issues that can impact reliability and security.

TO PROVIDE THE HIGHEST QUALITY OF SERVICE, LOOK FOR:

End-to-End monitoring and support. Many providers only monitor and measure the reliability of their own cellular networks. However, as anyone with experience operating IoT solutions knows, reliable communication between a device and application requires multiple network components — such as the underlying cellular networks, the devices, device firmware, radio modules, VPNs, cloud infrastructure, and more — all working correctly together.

These issues grow in frequency and impact as you scale, and you'll no doubt need to build out your own monitoring and support functions over time. To cover yourself before these teams exist, and to ensure their success after they are in place, make sure your provider offers:

- **Tools**, both API and portal based, that allow your teams to see the entire connection history for each device, and take action to diagnose and resolve issues (through SMS, clear registration, etc).
- **Configurable alerts** that automatically detect when devices are behaving abnormally (i.e. are sending more data than normal or aren't connecting when they should) and take action in response to those alerts.
- **Technical support** teams with direct access to AI-based reporting, dashboards, and drill-down tools that detect anomalies automatically, characterize traffic patterns (in terms of directions, interactions with intermediate network elements such as routers and firewalls, and ultimate destinations), and enable isolation of suspect components across the entire end to end system.

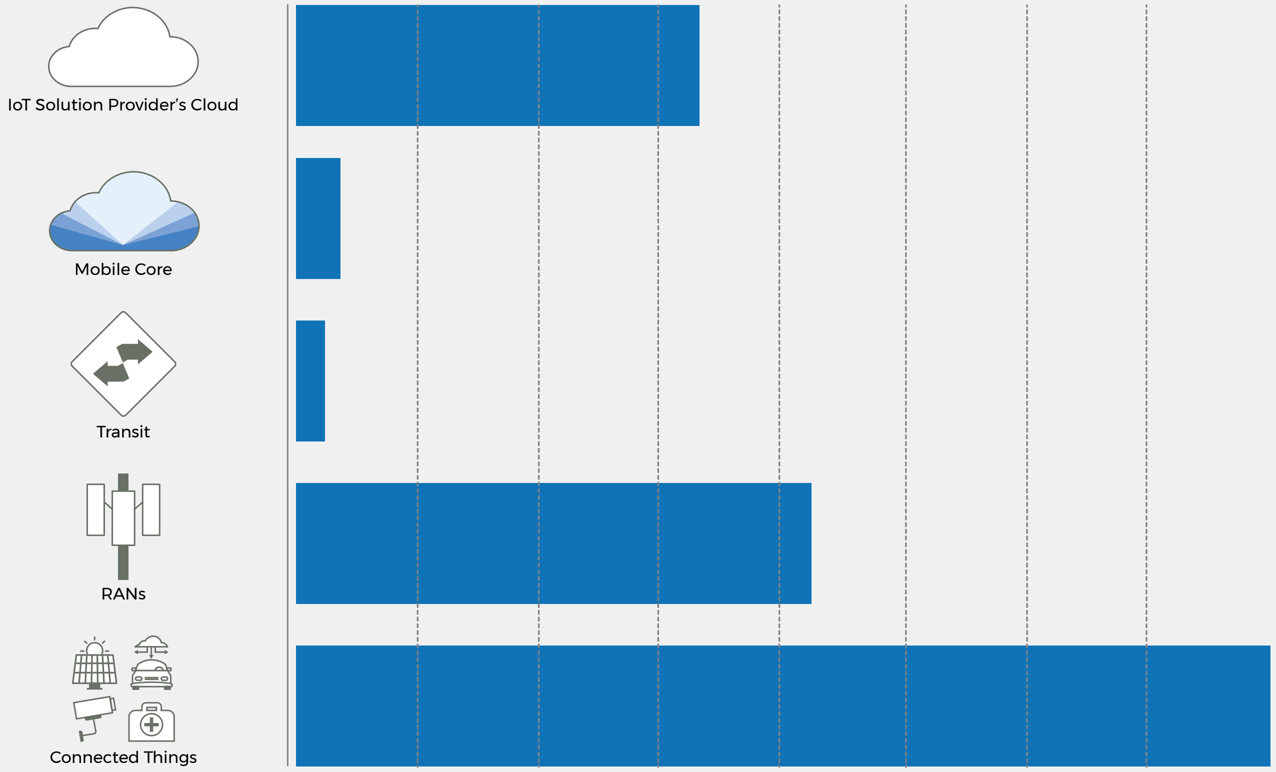
THE TEST:

Questions to ask your connectivity provider to ensure end-to-end troubleshooting & support:

- □ Do you provide complete visibility into my deployment from device through the cloud? How quickly can I see if a problem exists with my device, the network, or my application?
- □ Can you help me determine the cause of an SMS delivery failure?
- □ Will you notify me of local / regional carrier outages?
- □ How quickly can you troubleshoot device and network problems? What is your average response time? Resolution time?

RELATIVE INCIDENT OCCURANCE FREQUENCY X IMPACT

As illustrated in the chart below, networks consisting of interconnected devices and software systems experience issues end-to-end. And the most frequent, high impact issues happen at the device level.



Source: Study of 163 Aeris connectivity-network tier 3 incident escalation and follow-up reports (20 16–2019). Impact combines breadth of issue (% of devices involved) and time to resolution. Generally, issues in device and solution cloud configuration, which can easily affect large portions or all of a customer's devices, take longer to investigate and resolve (measured in days, in the worst cases) than RAN or core issues (measured usually in minutes and at most hours).

COST CONTROL

When you only have a few devices connected to the network, connectivity costs can be nominal. But as you scale to thousands, tens of thousands, or even hundreds of thousands of devices, both the structure of your rate plan, as well as the supporting network configurations and features available to prevent overages become crucial.

TO OPTIMIZE COSTS AT SCALE, LOOK FOR:

Flexible rate plans adjusted to serve the needs of your business and your product. Depending on your business model and sales channels you may benefit from fixed bundles, single payment plans, pay-as-you-go plans, the ability to pool data across devices, and discounted, pooled rates for ultra high usage applications such as video. Look for a provider who asks questions during the sales process to really understand your business requirements in order to configure the rate plan that's right for you. Only sign long term contracts if they benefit you.

Access to near-real time usage data with options to optimize rate plans based on that data. As you scale your solution, dynamic cost control becomes even more important. With this in mind, make sure that your cellular connectivity provider offers access to near-real-time usage data and allows you to make mid-month rate plan changes based on that data.

The ability to exclude high-cost carriers. If your provider controls the preferred PLMN (as referenced in the coverage section), ask if they can exclude high cost carriers where possible to further optimize your rates.

Low cost cellular data for device activation and testing in the country of manufacturing. To ensure seamless, turnkey customer experiences, SIM activation and deactivation should be automated within your supply chain, with your cellular IoT provider ready to assist. When evaluating providers, check to make sure that they offer both:

- **Cradle-to-grave lifecycle management** to easily activate, deactivate, suspend, and reactivate devices as they move in and out of use
- **Data in the country of manufacturing** so that the devices can be tested when they come off the assembly line — without incurring data roaming or overage charges outside of the deployment country.

Real world example:

Many Aeris customers have reduced connectivity costs by as much as 30% with optimized, month-to-month pay-as-you-go rate plans applied across all global devices

THE TEST:

Questions to ask your connectivity provider to make sure they can fully optimize your costs:

□ How can you help me prevent overage charges?

□ Can you customize my rate plans on a per-application basis to meet my varying transmission needs?

□ Can you optimize rate plans on a per- device basis?

□ In what ways do you help me lower my operational costs?

SECURITY

As you gain traction in the market, the last thing you want is for a security breach to ruin your business reputation, put your company in the headlines, or even worse make your company legally liable for the damages caused by the breach.

TO HELP ENSURE BEST-IN-CLASS SECURITY, LOOK FOR:

Multi-layer best practices like authentication, authorization and access control using PCRF, a secure network edge, private dedicated IP address, and APN for enterprise traffic isolation, which can dramatically reduce the likelihood of malicious activity.

A private network to smartly leverage non-dialable numbers while retaining SMS and voice capabilities if you require them.

A secure connection to your back end to ensure that all of your data travels through your end-to-end system without touching the public internet. This can be done with traditional enterprise VPNs or through more modern and efficient approaches like direct-to-cloud data delivery, now supported by some IoT connectivity providers.

The ability to restrict devices to interact with approved endpoints only. This ensures that devices can only send data over the Internet to approved endpoints and that only authorized users can read device data on-demand.

Automated alerts that notify you of suspicious activity (such as a device sending data when it shouldn't or connecting to unknown networks) and automatically suspend the device until the issue is resolved.

Device blocking to isolate devices that may have been compromised due to a bug or malicious activity.

End-to-end visibility to enable your security teams — and those of your network provider — to rapidly detect and respond to security threats.

THE TEST:

Questions to ask your provider to make sure they have you covered:

□ What options do you provide for securing the connection to my data center or cloud provider?

□ How do you ensure that my devices only connect to authorized endpoints?

□ How do you prevent unauthorized senders from connecting to my devices?

□ What tools do you provide to help my operations team detect suspicious activity?

□ What can you do if one of my devices becomes compromised?

UNDERLYING TECHNOLOGY & CAPABILITIES

Many of the critical capabilities laid out above require 1) a rare and extensive technology foundation combined with 2) the in-house network operations and software development expertise required to leverage that technology for maximum customer benefit.

TO MAKE SURE YOUR PROVIDER HAS MORE THAN JUST FANCY MARKETING, LOOK FOR:

A purpose-built core network which controls device/network interactions, including authorization, policy definition and enforcement, charging, billing, and operations and support system (OSS). A network offering this level of visibility and control allows your provider to customize coverage and rate plans to match your specific needs, prevent device communication with unauthorized endpoints, and pinpoint issues anywhere in your system.

In-house network operations and software engineering teams that maintain, operate and build tools leveraging data from the core network. Many providers outsource their IoT network operations to third parties, who in turn entrust the software in their cores to multiple large system vendors. This outsourcing results in an inflexible, complex, and slow-moving availability of diagnostic information (when your devices experience connectivity issues), and makes it economically impossible for most carriers to accommodate requests for custom configurations from customers with fewer than a million devices connected. Ask your provider how their network operations and engineering teams are structured and where they are based.

Regular feature releases. Cellular for IoT is a dynamic technology that requires keeping up with the newest technology and standards changes. Regular feature releases indicate that the provider has the technical teams to not only keep up with the changes and adapt their service, but also to develop new features that deepen the value for customers. Look for a provider with monthly feature releases.

THE TEST:

Questions to ask your provider to vet their technical depth:

□ Do you directly control authorization, policy definition and enforcement, charging, billing, and operations and support system (OSS)?

□ How are your network operations and engineering teams structured? Are they all in-house?

□ How often do you release new features?

LOOKING FOR YOUR IoT CONNECTIVITY PROVIDER?

Aeris has been serving the connected device market for over two decades. We've connected millions of things over 2G, 3G, 4G and LTE-M networks around the world — and we've leveraged that experience to build an offering that meets all of the requirements laid out above.

The Aeris Fusion IoT Network is the only cellular IoT network that provides visibility and control over your entire connected operation — globally and at scale. With Fusion, you can optimize coverage from 600 carriers in 190 countries, manage risks, and deliver the highest possible quality of service for your customers — all while optimizing costs across your business.

Fusion's unique capabilities are made possible by our purpose-built core network, which gives us control over all device/network interactions including authentication, policy definition & enforcement, charging, billing, operations, and support. Our network is backed by 200 expert engineers and network operators equipped with an array of monitoring tools developed over 20+ years of experience deploying and managing custom IoT solutions for the world's biggest brands, and tapping the latest techniques in AI/ML to automate our expertise.

United States Contact:
info@aeris.net
or +1 408 557 1993

"We have always been committed to providing the best products, support and services for our customers. Aeris exceeded our stringent requirements to ensure our customers have a reliable, scalable connection to our meters."

— John Fillinger,
Director of Marketing,
Badger Meter

BadgerMeter

"Wisepill Technologies provides a truly global data solution to our clients enabled by Aeris. This partnership with Aeris means that Wisepill can provide an awesome customer experience in every corner of the globe."

— Ricci Marshal,
Owner and Director,
Wisepill Technologies

wisepill