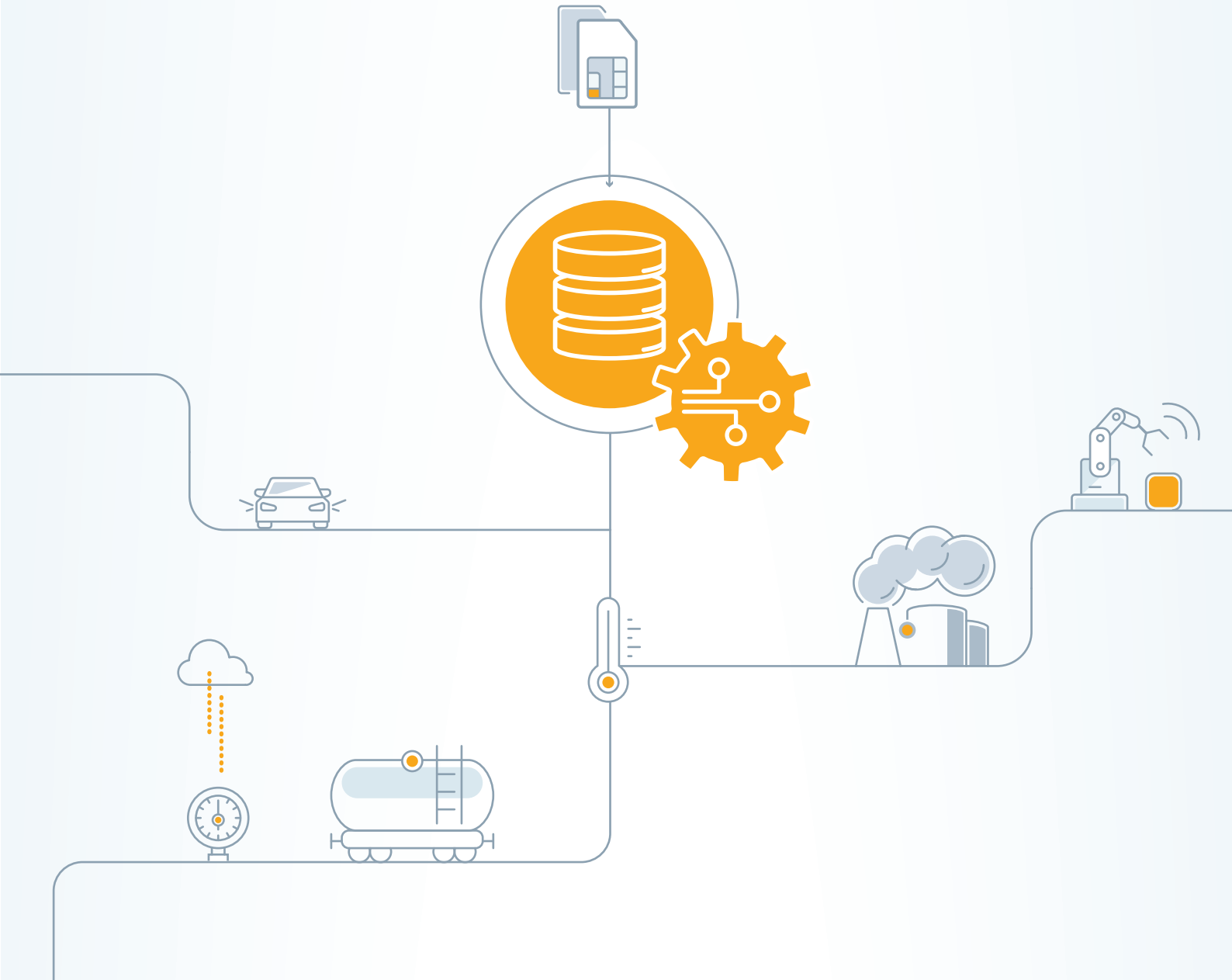
flo. LIVE

The Evolution of Core Networks in the Age of IoT



Mobile Network Operators are at a critical juncture. By 2025, there will be:

Moving into IoT services is a foregone conclusion for most Mobile Operators, but the route to get there is far from clear, starting with the infrastructure itself.

Some mobile operators are planning to hold onto their existing core infrastructure used for their mobile phone subscribers, and tack on IoT functionality. At a glance, this could appear to make sense. After all, they have already invested heavily into a core network, they have employees highly skilled in operating and maintaining it, and in theory at least – the more that this investment can provide, the better. After all, isn't connectivity just connectivity, whether it's for mobile devices or IoT?

This path could be a huge mistake for today's mobile operators, and cause more problems further down the line. This white paper will look at the evolution of the IoT market and how mobile operators can get ahead of the challenges.

Get the Best Quality of Service out of 5G

ABI research has collaborated on a new white paper[1] that discusses a "horizontal play among CSPs, solution providers, and end verticals to create new value based on use cases that leverage high-capacity and scalable networks." One example is the gaming sector, where the industry requires guaranteed low latency and high performance, with an inherent ability to quickly scale up and down.

There are limitless opportunities in the market for mobile operators, but guaranteeing the quality of service necessary to commit to these use cases needs a high amount of flexibility and control. Without this adaptability, MNO's may struggle to gain the full advantages offered by new 5G deployments.

5G networks will be built for IoT, offering better bandwidth and performance, (we're talking 100x better here) and the unique ability to link not just people, but devices, networks and systems. With the right foundation, 5G is a key to exponential growth for Mobile Operators, but not if your systems are outdated or built for a different purpose.

1. https://www.abiresearch.com/blogs/2020/04/06/cloud-native-networking-5g-era/

The Unique Nature of IoT Connectivity

Understanding what's necessary for a core network that meets the future roadmap of IoT means understanding how disparate IoT solutions can really be. Think about the diversity of requirements between use cases such as a connected car and a smart meter for example. The connected vehicle has high signalling and data plane throughput, the necessity for frequent mobility, and a moderate tolerance for latency. In contrast, the smart meter has extremely low data and signalling requirements, zero mobility, and a very high tolerance for latency. While connected vehicles may number many millions in a short amount of time, smart meters need an even higher ability to scale.

Massive IoT

- Low-cost devices, battery operated
- Small data volumes
- Massive numbers (many millions)

Broadband IoT

- High throughput
- Low latency
- Large data volume

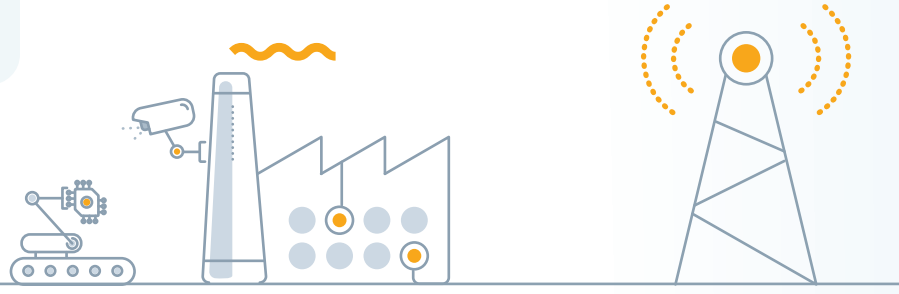
Critical IoT

- High reliability
- Very low latency
- Very high availability

Both of these are technically IoT use cases, but they have very little in common. For your business to support them both, it needs flexibility, adaptability and control.

This is where cellular connectivity is head and shoulders above any other technology. It offers stronger coverage and better reliability that is under continual improvement when compared to solutions such as WiFi, it guarantees lower latency resulting in better speeds, higher throughput, and adaptive power consumption to meet specific business requirements.

Cellular connectivity allows any enterprise to cater to many different IoT use cases, all from the same network, utilizing different technologies such as NB-IoT and CAT-M. On the other side of the coin, unlicensed LPWA technologies for example are only built for very specific use cases, namely low-end Machine Type Communication (MTC) without particular security constraints.



What Capabilities Do I Need on the Core Network Side to Manage IoT?

Utilizing a mobile subscriber oriented core network infrastructure for IoT use cases is a little like putting a round peg into a square hole. It might fit if you force it, but you're going to end up with gaps. It's not only that IoT behaves differently to mobile, there is no one size fits all IoT - as we've shown with the examples above. There are many types of IoT devices, services and use cases that behave differently, and therefore require different network capabilities.

Let's look at IoT en masse, as a business challenge in comparison to traditional mobile customers. Instead of having 10 million subscribers who might each use a few GB per month, utilizing resource-intensive apps such as Zoom, Netflix or WhatsApp, you now have a hundred million devices, but this time they consume as little as 1MB each month. This is because intelligent data exchange and power consumption methods such as NB-IoT and CAT-M allow IoT devices to simply wake up each hour to send or receive a message, perhaps consuming 5KB each time.

This low ARPU and high signalling behavior need a totally different type of network, built to make IoT profitable, and inappropriate for a core infrastructure that was intended to support humans and smartphones.

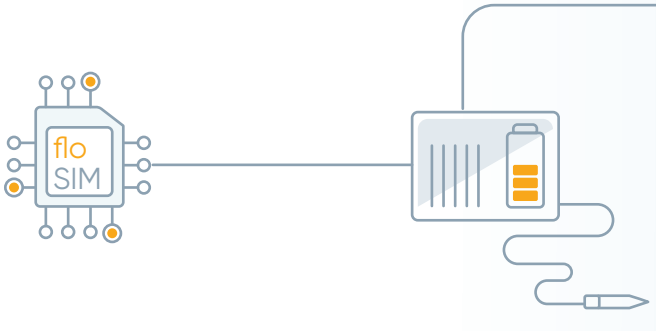
To get the most out of your IoT offering, you will need to adapt your existing core to suit, but this is easier said than done whilst your core needs to continue to support smartphone users, all without impacting their service. Think about credit control, where IoT devices use the same amount of data in a decade as a phone might use in an hour, or signalling requirements, where a phone needs constant availability while an IoT device might only need a periodic connection to send specific data. Networking requirements need to be able to be adapted to allow the resource load to be lighter, optimizing for battery life, speed and performance.

The same disconnect happens when you think about security and overarching risk across different use cases. Unlike mobile phones that can be defended with Antivirus protection, VPN and the like, IoT devices cannot protect themselves. This means that you need to have stricter security on the core network side, and more so for use cases like Healthcare and Finance, or where you have greater compliance responsibilities.

You might think, great – I'll factor that in, but in reality, this could start impacting other users if you're looking at a shared network. A MNO can't simply start blocking ports, IPs, or packet data on a country-level for all subscribers, or how will users browse freely on mobile devices, or get the same experience they expect for varied new IoT use cases?

Meanwhile, if you go too far in the other direction, and fail to adequately protect your network for shared devices, it impacts the whole business, from mobile user data that is likely to be compliance-sensitive, all the way to IoT networks that could impact agriculture, utilities, or even healthcare. By separating out core networks, you can provide the right level of security to each business unit, getting it right from the start.

The natural answer is that mobile operators will need multiple core networks, either per customer, or per different type of use case, not only one for mobile and one for IoT, but several - for various IoT business models, such as Massive IoT, Critical IoT, Broadband IoT, or Industrial IoT.



Supporting Lower TCO

Making this affordable starts with understanding the impact of low ARPU devices. Mobile operators can pay higher prices per user, but this is impossible when it comes to IoT.

This is where mobile operators are beginning to understand the necessity of turning to the cloud, and utilizing network slicing - the most efficient and cost-effective way to handle multiple use cases. This has a number of benefits:

Scalability

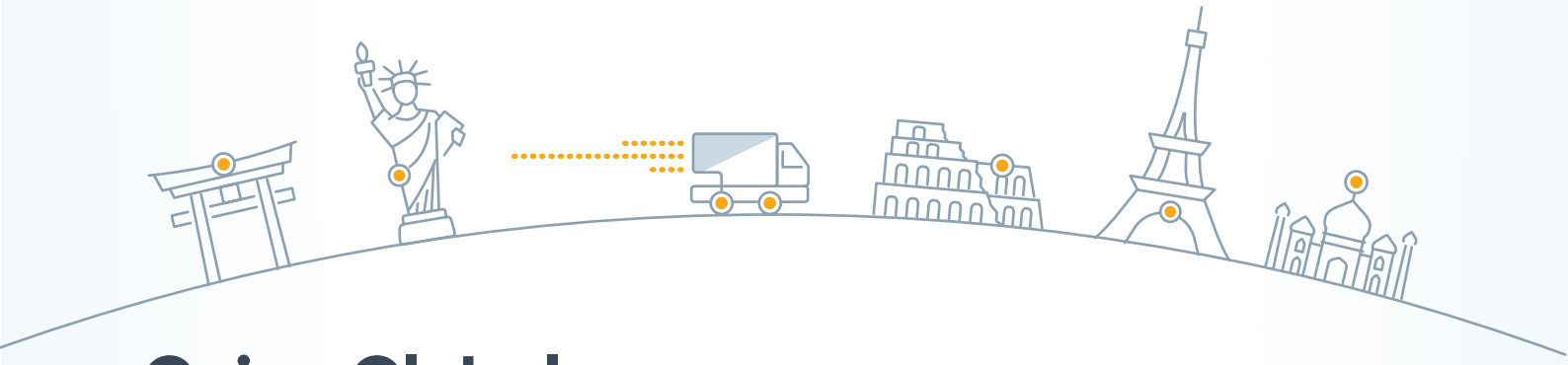
At the start, mobile operators will not be able to accurately forecast what their most profitable or in-demand IoT use case will be. A flexible cloud-based core can offer auto scaling as the business needs, ensuring that resources are available when they're needed, and you only pay for what you use.

Ease of use

One cloud provider for your core network has a ripple effect on maintenance and support. You can more easily meet SLA, fix maintenance issues, or communicate to customers with transparency, when you don't have another third-party vendor in the mix. This in turn inspires loyalty and growth, not to be underestimated on your own bottom line.

No CAPEX

The infrastructure costs of setting up multiple core networks is heavy to say the least. A cloud-native core means no initial capital investment, and your connectivity offered as-a-service, the most agile way to do business, especially when you're testing the waters with a new business model.



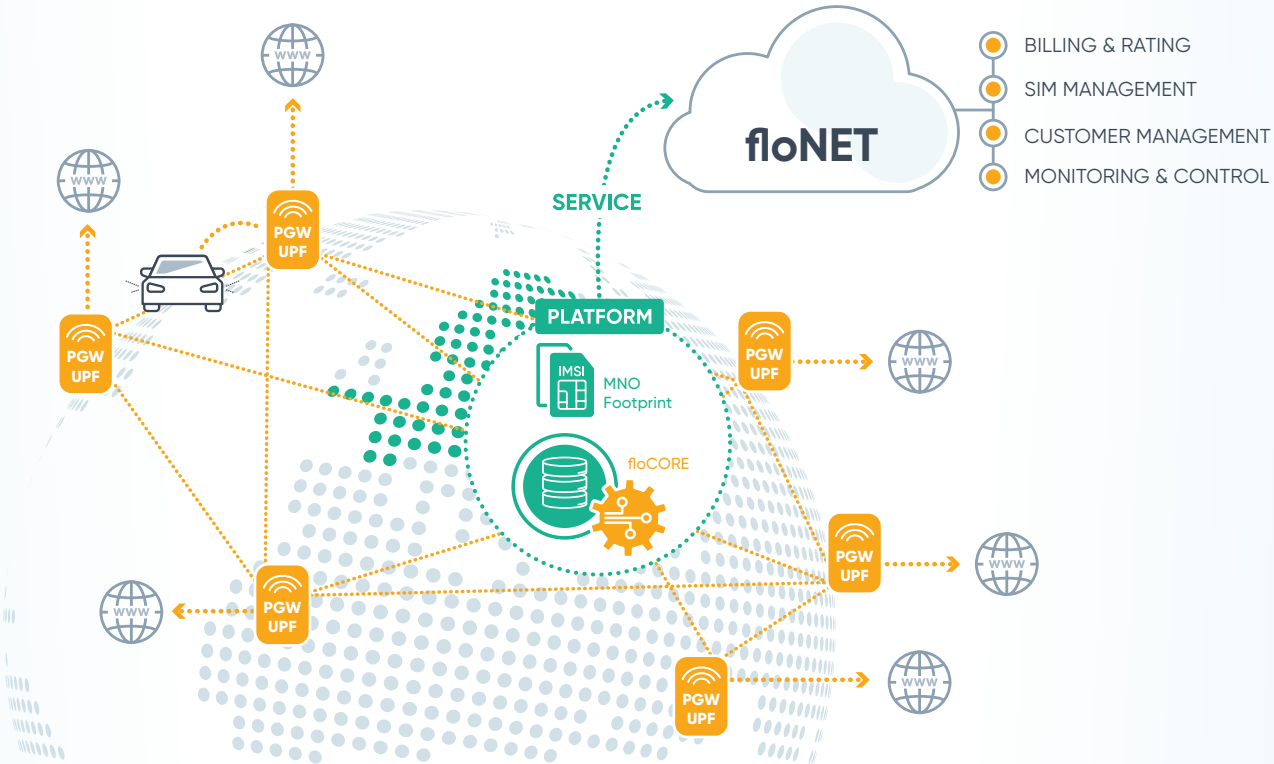
Going Global

Of course, IoT is a global business from day one, when devices are manufactured in one country, and sent to another for connection and deployment. Multiple cores with customers in need of global coverage is a new challenge for mobile operators. Most will be used to partnering with global MNOs outside of their footprint, or utilizing global roaming agreements, neither of which will suit IoT.

This is where CUPS technology is gaining traction in the market, allowing a highly flexible network extension, anywhere in the world. This separation means that you can deploy local breakouts in different locations, with centralized management and control behind the scenes from a single location. All traffic is routed to the local network, so the mobile operator ends up with localized, highly performant network solutions globally. This not only expands their reach, it also accelerates their ability to launch new IoT use cases at scale.

A call to mobile operators

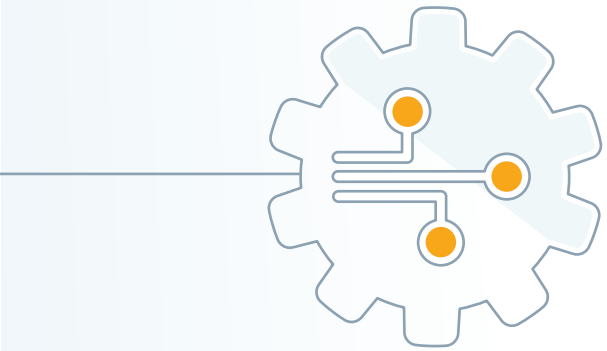
With floLIVE's global network, you can seamlessly extend your reach and offer your connected enterprises secure, compliant and high performance connectivity - we've put the infrastructure in place, and it's ready for you to use.



The Way We See it

A cloud-native mobile core network is the most efficient and cost-effective approach to launch a successful IoT business.

floCORE is offered as a service, paving the road for mobile operators to a profitable IoT business, built with the future in mind, and suited to your IoT needs - both commercial and technical:



floCORE

Want to learn more about floLIVE's Global Network-as-a-service? Download the solution sheet.

IoT-oriented

An IoT-oriented core mobile network that supports 3G and LTE as well as the latest GSMA standards - NB-IoT, CAT-M and 5G.

Low footprint

With a low footprint, it's lighter and faster to deploy, utilizing minimal IT resources

Network slicing

Supports network slicing to cater for a growing variety of IoT use cases

Dynamically scales

Dynamically scales alongside business growth, optimizing resources and contributing to your bottom line

A service-based business model

Offers the flexibility to respond to continuously evolving business requirements of connected enterprise customers

Zero CAPEX

When offered from your regional cloud provider, (e.g. AWS) therefore further reducing TCO.

floLIVE is a secure, cloud-native connectivity solution backed by strategic investors 83North, Dell Technologies Capital, Saban Ventures and Qualcomm Ventures LLC. It supports mobile operators, IoT service providers and global enterprises looking for global connectivity and networking solutions.

The platform comprises distributed core networks that provide local connectivity while being centrally managed and controlled over the cloud. This unique approach enables manufacturers to benefit from highly-performant, secure and regulatory-compliant local connectivity with the flexibility and elasticity of a cloud-native platform.

floLIVE's solutions are offered as-a-service, in a pay-as-you-grow business model.

flo. LIVE

Let's connect

Get in touch to discuss how we can meet your IoT requirements. We're sure to surprise you.

info@flolive.net

+44 20 3637 9227