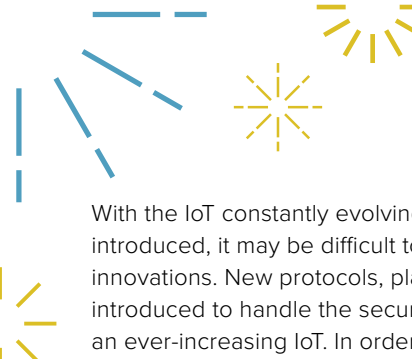


WHITEPAPER

How technology is enabling the **IoT**

Together we can do **more...**





With the IoT constantly evolving and new technology being introduced, it may be difficult to keep up with the stream of innovations. New protocols, platforms and hardware are being introduced to handle the security and scalability demands of an ever-increasing IoT. In order to keep ahead of the game, it is key for industry players to stay informed about new developments in a range of topic areas.

Over the years, we have seen many IoT deployments failing in their infancy due to lack of futureproofing, where businesses were simply not agile enough to adopt new technology and couldn't move past their PoC phases.

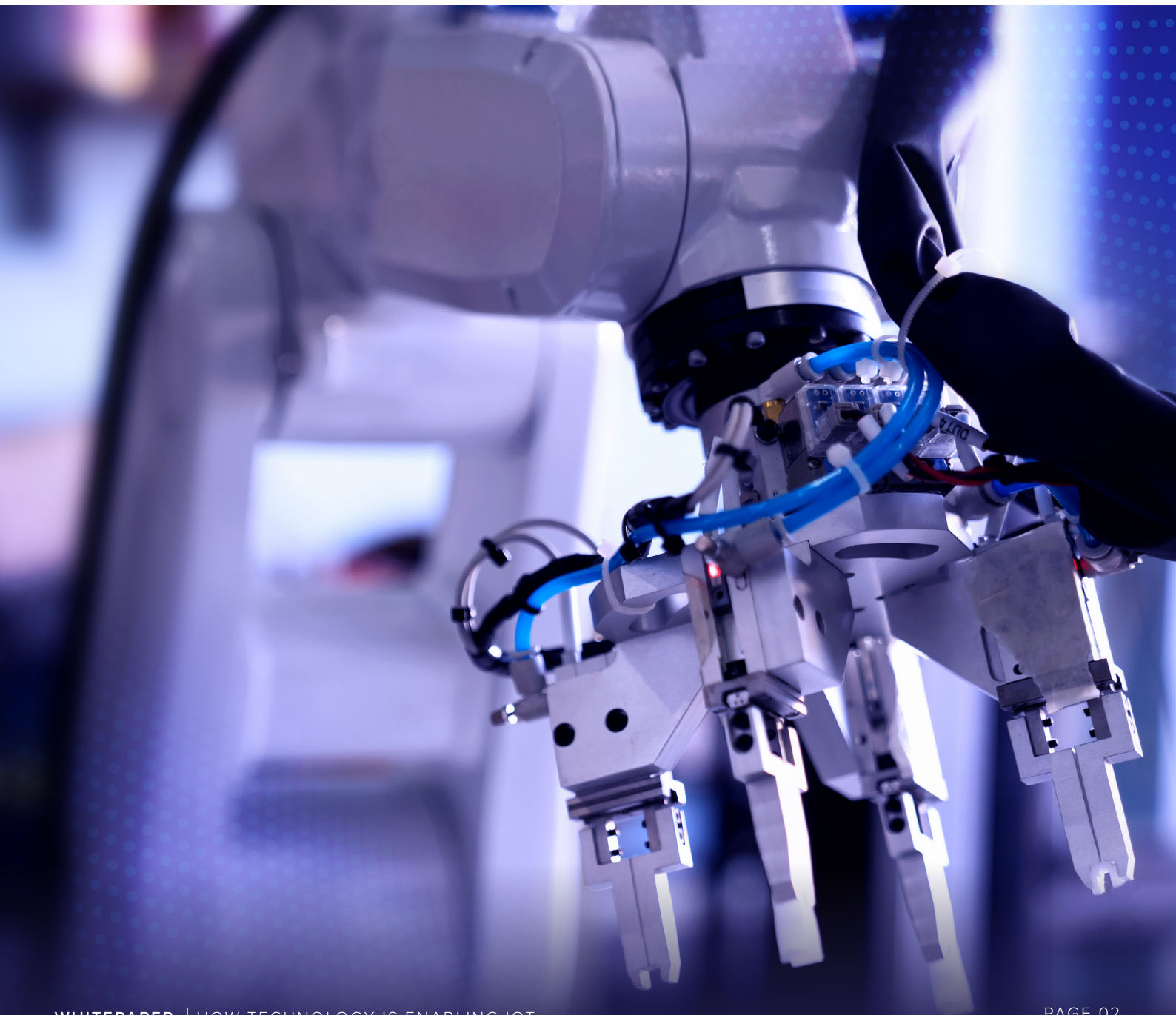
Every IoT deployment is unique, with its own set of challenges and opportunities. The decisions you make on the technology deployed in your IoT project will have implications on the end

result for your business, so your main focus should be on the reliability and flexibility of your choices.

It would be beyond the scope of this whitepaper to cover every supporting piece of the IoT in detail, so we have chosen a small selection of technology terms to address, specifically aimed to help you in your path to deployment.

It may feel daunting to tackle all the complexities of the technology enabling the IoT, but it is key to be aware of what options are available to your business and how best to leverage them to your advantage.

Our hope is that this whitepaper helps advise you about your options and provides enough information to kickstart your journey to IoT success.



Connecting your device

What is it?

Naturally, you can't have IoT without the "Internet" as a key component. There's a wealth of IoT connectivity options available to enterprises and consumers, but first we'll focus on cellular.

For innovators with big goals and plans to scale out globally, cellular IoT connectivity is most likely the best way of connecting physical "things" to the internet.

Rather than creating a new, private network infrastructure for your IoT devices, they can be connected via the existing global mobile network using a SIM card. Cellular IoT provides a more reliable, higher power alternative to the LPWAN networks that we'll discuss below.

The two main types of cellular IoT connectivity are narrowband IoT (NB-IoT) or Cat-M2, and category M1 (Cat-M1) IoT. Both are derived from cellular standards, with a key distinction being NB-IoT has a much smaller bandwidth (10x less) and therefore a lower transmission power than Cat-M1.

Cellular IoT is ideal for businesses looking to benefit from the reliability and ubiquity of traditional mobile networks. However, it's important to keep in mind which cellular options will be best suited for your IoT application. With networks like 4G requiring a lot of power, it might not be preferred for small form-factor devices where small amounts of data are only transmitted very occasionally, such as environmental sensors for agriculture or smart water, gas and electricity meters (see "Other LPWAN" below).

How does it work?

While considering your options, keep in mind factors such as your device's power needs, range, data transmission requirements as well as its expected lifetime.

LPWAN and cellular IoT connectivity.

High data rate cellular

Connectivity options like 3G, 4G, and 5G cellular connections provide wide coverage multi MBps data connections that are ideal for real-time video streaming or other data-intensive applications, or highly mobile devices. This option is a great fit both for applications like public transport Wi-Fi provision using in-vehicle access points with a cellular backhaul link; or for mobile devices where high connection availability is required on a very broad basis like those implementing vehicle or package GPS tracking systems.

LPWAN cellular

Extending the traditional high data rate cellular services are newer low data rate methods with corresponding low power requirements. NB-IoT and Cat-M are increasingly popular LPWAN technologies and can be ideal as a balance for the large-scale connection requirements of a widely distributed IoT system combined with the low bandwidth requirements traditionally associated with IoT devices, and low power requirements. These connectivity options are in a state of mass deployment at this time compared to the regular cellular options that connect our mobile phones but are rolling out internationally at an increased rate. Management of IoT focused cellular connections lines up well with traditional cellular options which opens the door to systems migrating future devices over as hardware is updated.

Why should you care?

Cellular IoT offers a wide range of benefits. We consider it to be one of the most flexible and scalable options, as cellular technologies offer ubiquity, reliability, security, and manageability.

Since cellular networks are built on already existing infrastructure, they generally offer excellent (and secure) network coverage, which is typically easy to activate right out of the box. Leveraging a pre-existing network significantly reduces the development time you'll be putting into your IoT solution. With so many cellular IoT options available, it's pretty straightforward to find a network type that will work for your application, whether it's high or low bandwidth, or if it's located indoors, outdoors or on the move, globally.

Cellular technologies also enjoy the support of a global and mature industry focused on standards for wireless connectivity and its ever-growing ecosystem of providers. Cellular connections have proven their ability to support data connections effectively around the world as well as new developments that will dramatically improve cellular data connectivity thanks to the addition of physical layer signals and channels designed for extended coverage in rural locations and applications that are deep indoors.

To learn more about Pelion's cellular IoT connectivity offering, visit <https://pelion.com/product/iot-connectivity/>.

Other LPWAN

What is it?

Low-power WAN (LPWAN) refers to wireless wide area networks that connect low-bandwidth, energy-efficient devices over long ranges. With the rise of use cases connecting a huge number of small devices spread across large areas, LPWAN technologies have been key to the evolution of the IoT.

They are specialist, usually private networks, that are better suited to extremely low-bandwidth applications with small amounts of data being transmitted, such as air quality information gathered by sensors, the monitoring of occupancy levels in a building, as well as tracking assets as they move around a designated area.

How does it work?

LPWAN doesn't refer to one single technology or network, but instead a plethora of various network technologies, using licensed or unlicensed frequencies and including proprietary or open standard options. Among the features shared by LPWAN technologies are:

Confined or remote coverage: LPWANs are frequently used to provide coverage for devices in hard-to-access locations. Some technologies are focused more on distance and others on underground facilities.

Power efficiency: Most LPWAN technologies were designed to extend the battery lifetime of a device—sometimes for as long as ten years.

While some features are shared, others are available only with specific solutions. It's therefore important to evaluate all of them to identify which best meets your requirements.



Here are a few of the common non-cellular LPWAN options:

LPWAN	Range/ Bandwidth	Use cases	Pros and Cons
LoRaWan (Long Range Wide Area Network)	5-20 km Up to 50 Kbps	Smart agriculture, supply chain and logistics, asset tracking.	Designed for ultra-low bandwidth and infrequent communication. Proprietary technology with potential for vendor lock-in.
Wi-SUN (Wireless Smart Ubiquitous Network)	4km Up to 300 Kbps	Smart city, smart utilities (metering, distribution automation and more)	Suitable for applications that require high data throughput, and high node counts. Mesh capabilities provide greater flexibility and reliability.
SigFox	10-40 km Up to 100 Kbps	Smart building, environmental monitoring.	Complicated by operator limitations, varying from country to country. Not available everywhere, so scale out will be an issue. Data transfer can prone to interference, not suited to critical applications.

Why should you care?

There are a few advantages to utilizing LPWAN technology. The most obvious benefit is in the name, low-power and wide area. Businesses will see the most benefit from LPWAN when they have large numbers of tiny devices deployed over a long range. When you're optimizing for power consumption, devices deployed over LPWAN can run on small, inexpensive batteries for 10-15 years. Not only does this extend the life of your devices, it also reduces the time and resources required to maintain or replace devices.

Another consideration is cost. In the right use case, LPWAN can reduce complexity in hardware design, reduce the price of devices, and lower bandwidth cost with the use of license-free or already owned licensed bands.

[Watch our webinar "Is LPWA the future of IoT connectivity?"](#) to gain more insight.

Not only does this extend the life of your devices, it also reduces the time and resources required to maintain or replace devices.

eSIM/eUICC

What is it?

Often used interchangeably, eSIM and eUICC are two different (yet complementary) technologies enabling cellular IoT connectivity. The term eSIM specifically refers to the physical hardware component of the SIM and eUICC refers to the software that allows multiple profiles (the unique identity that enables access to a cellular network) to be configured, otherwise known as remote SIM provisioning. eSIM brings greater flexibility to the IoT connectivity landscape, future-proofing network choice and massively streamlining the supply chain.

How does it work?

In the past, the typical cellular connectivity solution required you to provision, stock, and ship various SIM cards based upon every combination of regional or network access requirements, massively complicating the manufacturing or deployment process. The outstanding flexibility offered by eSIM is revolutionizing the IoT connectivity space. A single eSIM improves efficiencies by eliminating the time, cost and complexity associated with ordering a range of SIM cards with different network operator profiles, all depending on where the devices may be deployed. By building with eUICC eSIMs, OEMs or service providers can decide (and change as needed) which network operator is most appropriate for their IoT application.

eSIM truly shines in a manufacturing use case, where device manufacturers can integrate eUICCs with predefined bootstrap profiles directly into their devices, already building in flexibility from the factory floor onward. Once the device is deployed, network configuration can be fine-tuned to choose a specific operator which will work best for the device, depending on location and coverage, at the most convenient time and place in the product's supply chain.

Why should you care?

As we mentioned earlier, one of the key criteria to consider when building a future-proof IoT deployment is flexibility. One of eSIM's main benefits is the ease of switching mobile network operators (MNOs) as needed. Empowered by over-the-air replacement of the MNO profile (without having to replace the physical SIM) itself, network lock-in becomes a thing of the past.

Saving on time and resources is also a key benefit; the actual physical swapping of SIM cards located in remote IoT devices can be a costly endeavor. Another cost saving is provided by the ability to "roam" using eSIM. Once the device is connected, it can retrieve a profile of a local MNO no matter where it's located, usually at a much lower rate.

Another common pitfall for IoT deployments is reliability. With the IoT landscape evolving constantly and some services being sunset, the ability to switch MNO and adapt to change quickly is key. For end users, disruption of service contributes to bad customer experience and can greatly reduce your ROI for deployed IoT solutions.

Find out more about [Pelion's eSIM-as-a-service](#).

eSIM truly shines in a manufacturing use case, where device manufacturers can integrate eUICCs with predefined bootstrap profiles.



Deploying and managing your device

What is it?

So, you've deployed a range of IoT devices. What comes next? Once a device is in the field, how do you keep it updated, harvest its data, or decommission it? This where is IoT device management comes in.

Device management refers to the huge range of processes that are involved in the connecting, provisioning, configuring, and updating of IoT devices, regardless of location,

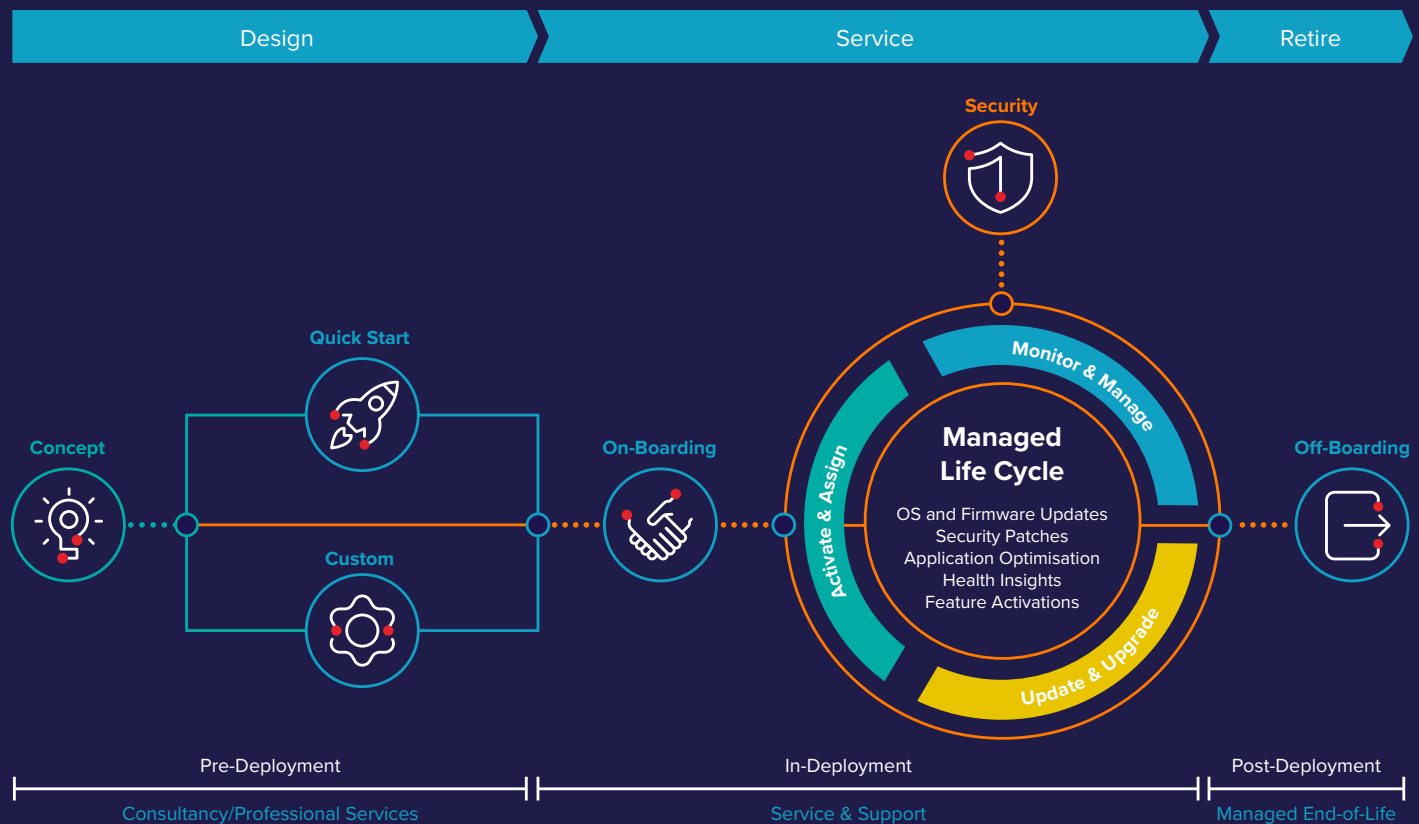
connectivity protocol or device type. One of the pitfalls of IoT innovation is the realization that you must support the whole spectrum and lifecycle of IoT devices, especially to keep your deployment secure and your data trusted. Device management is therefore an integral part of any IoT deployment, requiring a reliable and effective platform to keep your devices up-to-date, secure, and always accessible.

How does it work?

The lifecycle of an IoT device is a complex creature.

Support the Entire IoT Device Life Cycle

Pelion Device Management simplifies and secures the IoT device lifecycles - with reliable design, in-service management, and managed retirement.



From pre-deployment to on-boarding of the device, through to its active use in the field and finally to its decommissioning, it is vital to stay on top of firmware updates, data transmission, battery life, security concerns, remote management, and much more.

IoT device management first comes into play when a device receives an identity; this is the activation and provisioning process, when the device connects to the network for the first time.

Device authentication is a critical part of provisioning, establishing a secure connection between the device and an IoT service or IoT platform. During this process, the device presents its credentials to the server and receives further configuration data.

Once onboarded, the device must be configured. In many cases, the “things” of the IoT are shipped with a generic configuration provided by the OEM. You’ll have to give some thought to the configuration of the IoT devices, depending on your specific deployment, taking into consideration factors like the devices’ installation location and the role they will play within your evolving IoT ecosystem.

Afterward comes the monitoring and management phase. Your devices have been securely provisioned and configured, but what’s next? You’ll be focusing on ensuring that the device stays active and transmitting data as intended, while avoiding any unexpected operational issues.

Updating and upgrading your devices as necessary is the final part of the active management of your IoT estate. New firmware may have bugs to squash, your project scope may change, and new functionalities may be introduced which you’d like to profit from. And don’t forget the potential security vulnerabilities that may crop up. To handle all these eventualities, an IoT device management platform can facilitate firmware over-the-air and software over-the-air updates, so that every device in the field is kept secure, up-to-date and bug-free.

After a long life of serving its purpose in your IoT deployment, providing a wealth of data, functionality and services, your IoT device will eventually have to be off-boarded through a secure and cost-effective decommissioning process.

Why should you care?

The importance of IoT device management cannot be understated. It is an absolute must-have, and a critical component for your IoT deployment. Comprehensive device management capabilities will empower your business to connect, monitor and remotely manage your devices at scale, throughout the entire lifecycle of your device, as well as ensuring connectivity and security.

An IoT device management platform addresses the lifecycle process of IoT devices in an efficient manner and allows you to focus on the desired business outcomes of your IoT deployment.

Want to learn more? Attend our [virtual seminar](#) **“Demystifying IoT device management”**.

It is an absolute must-have, and a critical component for your IoT deployment.

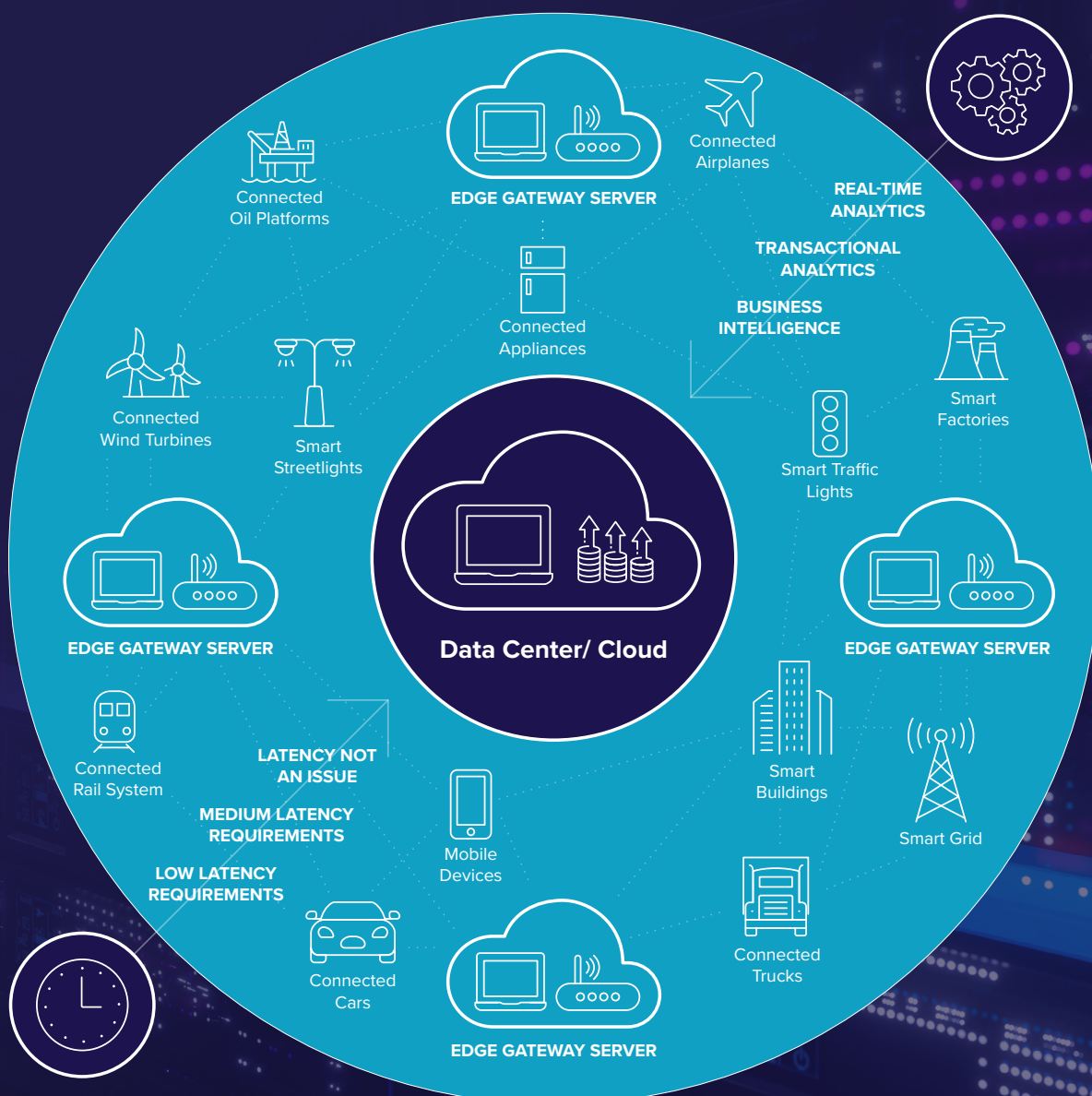


Edge IoT and gateways

What is it?

Simply put, edge computing means that data produced by a device is stored and processed directly within the device itself (the edge of the network). The Internet of Things has continued to grow exponentially, with forecasts of 1 trillion devices connected and generating an enormous flood of data by 2035. With that rate of growth, it's become ever more apparent to businesses that, by moving the processing and handling of data to the edge device, they could be saving massively on bandwidth costs, while benefiting from improved latencies and better security.

With data being stored and processed at the device level as and when it's gathered, the typical latencies of transmitting the data to a centralized cloud is avoided. Not only does edge compute improve response times and operational efficiency, it also empowers enterprises to create new and innovative real-time applications and unlock better business outcomes.



How does it work?

As explained above, edge computing happens at the “edge” of the IoT, closer to the actual smart devices themselves. As the device harvests data, the information can be stored and processed within the device, using the compute capabilities of the device to determine what needs to be done with the data.

As seen in the graphic above, edge gateways are strategically deployed to drive even more intelligence closer to the edge. An IoT gateway device bridges the communication gap between IoT devices, sensors, equipment, systems and the cloud. By offering higher processing power and storage, edge gateways act as a helpmeet for the smaller, less smart devices and sensors in a deployment. Gateways consolidate a broad range of edge devices, translate various protocols, and deliver secure, scalable, and reliable operation.

By facilitating compute at the edge, the data can be immediately processed and analyzed to determine whether the situation demands a response in real time or if the data should be sent on to the data center for further evaluation.

There are usually three different responses to the data which is gathered at the edge:

- The data can be discarded and there is no action required (ie nothing out of the ordinary has been detected by a temperature sensor)
- A recommendation that the data be stored for later analysis or recorded (ie monthly usage data for an electricity meter)
- An immediate response is needed (ie abnormal readings which could indicate downtime in a manufacturing plant)

By processing this data at the edge, enterprises are saving on huge bandwidth costs and can quickly respond to critical complications and disturbances, while saving on resources which might have been previously dedicated to monitoring all the data being produced.

Why should you care?

One of the primary drivers of edge IoT is the need for operational efficiency. You want your business to grow, scale out and evolve. With the ever-growing deluge of extremely relevant and insightful IoT data being created, enterprises see the need to automate as much of the processing as possible, while not losing out on the value of their data.

A close second to efficiency is cost savings. The cost of the bandwidth required to transmit their data from device to cloud can be staggering, and for businesses to see better ROI for their IoT deployment, it's an obvious choice to move as much of the processing of data to the edge.

It is highly recommended to implement a robust edge computing management platform for these deployments. By leveraging an open, standards-based, and interoperable mechanism to seamlessly and securely package, distribute, and manage cloud-native IoT applications to edge gateways, you'll be reaping all the benefits of edge compute without a ton of added administration burden.

Find out more about Edge IoT with our [“Simplifying IoT at the Edge” whitepaper](#).



Want to get started with connected fleet management? Tangerine's AI-powered data insights have transformed the smart mobility sector, by combining Pelion's reliable and resilient connectivity with their data analytics platform. Contact us to find out more at www.pelion.com/contact/

