Particle

SHOULD YOU BUILD OR BUY AN IOT PLATFORM?

November 2021

IoT is challenging even for the most well-resourced enterprises. A successful IoT deployment requires seamless orchestration of different components and four layers of the technology stack, including hardware, operating systems, cellular connectivity, and software.

Solving business and customer problems is hard enough, but taking on the task of building and managing an IoT deployment that drives business value is enormously tricky and resource-intensive.

The "build in-house" approach, which can sound appealing if you have a strong engineering and IT team, is full of risks, such as delayed time to market, interoperability between microservices, and uncontrollable costs.

In short, IoT is complex, and building it in-house makes it even harder.

BUILDING IOT - THE DRAWBACKS OF DIY

SPEED

18-24

Months to complete an average IoT project.

IoT Analytics, Guide to IoT Solutions, September 2019

QUALITY

23+

Vendors on average needed.

PTC, Source:LiveWorx June 2019

COST

4X

Total cost of ownership to build from scratch.

MachNation, June 2018

That's why if you're thinking about how IoT can augment your business, it's worth considering buying the hardware, connectivity, and software from a third party, so you can focus on solving your customers' problems and driving value. Rather than reinventing what's already been done well, you can devote your resources to what makes you different.

Startups and enterprises alike can't afford to waste resources on failed or delayed projects. You may be able to build a solution, but buying an integrated IoT solution can get you to market faster and with less risk.

IN THIS WHITEPAPER, WE'LL COVER:

- What it means to build vs. buy an IoT solution.
- How to evaluate your core competencies vs. outsourced solutions.
- What are the most critical build vs. buy decision factors, and how Particle helps make the decision easier.

BUILD VS. BUY - WHAT DO THEY MEAN?

Before we get deeper into the "build vs. buy" debate, it's essential to define what we mean by building an IoT product from scratch vs. buying the technology stack to help with the product.

Building an IoT product from scratch generally refers to the practice of devoting in-house teams to building some or all of the components of an IoT technology stack, including the hardware, operating system, connectivity, and cloud. It can also include buying point solutions and microservices to supplement homegrown systems.

"Buying" an IoT platform generally refers to buying a platform that comes out of the box with easy-to-deploy components, whether it's hardware, an operating system, connectivity, or software. You buy the platform, configure it to your needs to the extent the solution allows, and deploy quickly.

> You buy the platform, configure it to your needs to the extent the solution allows, and deploy quickly.

EVALUATING YOUR CORE COMPETENCIES VS. AN IOT PLATFORM

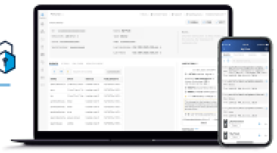
Suppose you've validated the business case for your IoT project. In that case, the next step is to determine what your internal team is capable of building and decide if it's worth devoting them to the project or buying an IoT solution on which they can build.

Any IoT ecosystem is really a collection of smaller systems and microservices that have to work together seamlessly for the end product to function as promised to the end-user, whether it's a consumer, a technician, or an analyst who needs to use IoT data to make decisions.

The core components of IoT are:

- Hardware - sensors, gauges, trackers, location tracking, etc.
- Operating system
- Cellular Connectivity
- Cloud
- Software/Business Intelligence tools

Hardware	Operating System	Connectivity	Cloud
Sensors	OTA software updates	Wireless Network	Device service
Microcontroller	User application	Certifications	Device broker
Device software	Cloud communication	Comms protocol	Microservices
GPIOs Peripherals	Hardware abstractions layer	Provisioning	Data storage
Power management	Firmware library	Data plans	Application server
Radios	RTOS	SIM management	REST API



Behind these core components, one needs to account for the associated microservices. This process becomes more complex when you try to build the core components of the IoT technology stack on your own or when you try to mix and match a solution from different vendors.

This complexity is why so many IoT initiatives fail at the PoC stage, usually after years and hundreds of thousands of dollars have been wasted. Research from Microsoft revealed some common issues:

Business Factors	Other Internal Factors	Security	Scaling Issues
Pilots demonstrate unclear business value/ROI (29%)	Not enough training/guidance on how to deploy (26%)	Concerned about consumer privacy (26%)	High costs of scaling (33%)
Hard to justify business case (28%)	Lack of technical knowledge and skills (26%)	Lack of technical knowledge and skills (26%)	Lack of resources to scale (25%)
Lack of leadership buy in (22%)	No budget (23%)	Unwilling to store data in public cloud (20%)	It takes a long time to scale (21%)

Source: IoT Signals 2020 Report, Microsoft.

If you're trying to determine what you should build or buy, you should start with your core competencies. What systems do you already have in place, and what in-house or consulting talent? Do you have access to, and how can those resources be best deployed?

According to Mariano Goluboff, Senior Solutions Architect at Particle, there's a reasonably simple way to figure out what to build and what to buy according to your core competencies.

Buy what doesn't differentiate you and build what does.

Connectivity and the hardware and operating systems that enable it tends to be the same across industries and IoT deployments. It's unlikely that you would be able to differentiate yourself in those respects.

"Everybody that does an IoT project has to figure out an embedded operating system, connectivity, security certifications, data management, etc.," Mariano said.

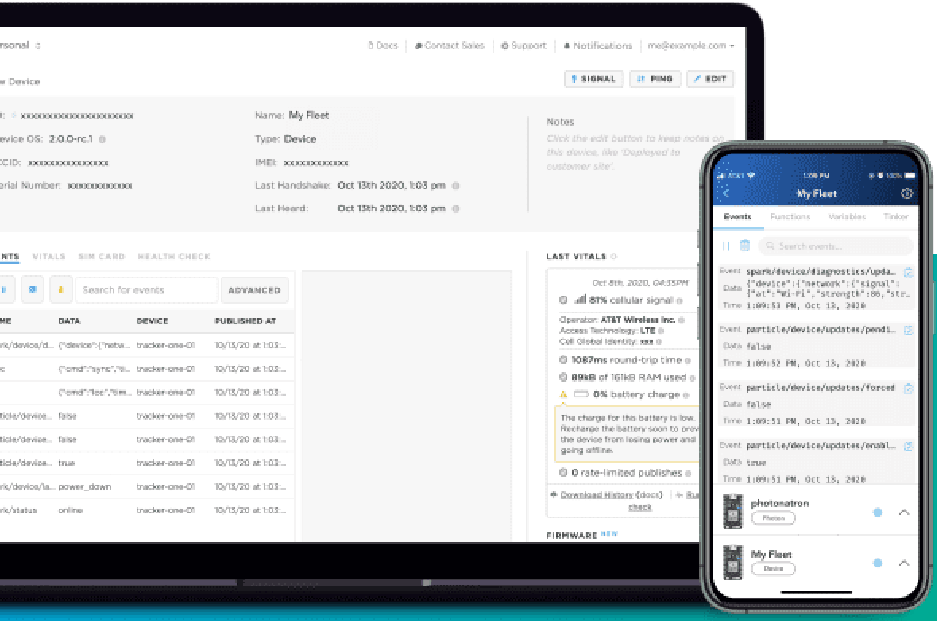
"But all of those things are the same for everyone regardless of the use case or vertical. They don't differentiate you," he added. "At Particle, we've built an integrated platform that works and is secure from edge to cloud right out of the factory. Why would you spend the time to build what we've already done? If we've done 80 percent of the work of building an integrated IoT platform, you can focus on the 20 percent of the IoT project that you're uniquely suited to build yourself."

Even if you're producing thousands or hundreds of thousands of devices, it's unlikely that you'll make the money back you put into hiring engineering teams that are essentially replicating what's already been built.

That's why you should focus your hiring and internal resources on what makes your business model unique in solving customer problems and what sets you apart from your competitors. The opportunity cost of reinventing what already exists won't give you a competitive advantage.

The size of your company also plays a role in how you evaluate your core competencies for building IoT products. IoT involves significant human resources in manufacturing, sourcing, IT, and engineering. As your company grows, you need to decide if it's worth adding headcount in those areas or if you're better off investing in roles that can grow the business.

"Particle maintains a team of dozens of engineers to constantly work on our cloud, cellular connectivity, hardware, and other areas," Kate said. "That's what it takes to deploy IoT at scale."



w Device

D: xxxxxxxxxxxxxxxxxxxxxx
evice OS: 2.0.0-rc.1
CID: xxxxxxxxxxxxxxx
erial Number: xxxxxxxxxxxx

Name: My Fleet
Type: Device
IMEI: xxxxxxxxxxxx
Last Handshake: Oct 13th 2020, 1:03 pm
Last Heard: Oct 13th 2020, 1:03 pm

Notes
Click the edit button to keep notes on this device, like 'Deployed to customer site'.

Search for events

ME	DATA	DEVICE	PUBLISHED AT
rk/device/d...	{"device":{"netw...	tracker-one-01	10/13/20 at 1:03:...
c	{"cmd":"sync","ti...	tracker-one-01	10/13/20 at 1:03:...
	{"cmd":"loc","tim...	tracker-one-01	10/13/20 at 1:03:...
ticle/device...	false	tracker-one-01	10/13/20 at 1:03:...
ticle/device...	false	tracker-one-01	10/13/20 at 1:03:...
ticle/device...	true	tracker-one-01	10/13/20 at 1:03:...
rk/device/la...	power_down	tracker-one-01	10/13/20 at 1:03:...
rk/status	online	tracker-one-01	10/13/20 at 1:03:...

LAST VITALS

Oct 8th, 2020, 04:35PM
81% cellular signal
Operator: AT&T Wireless Inc.
Access Technology: LTE
Cell Global Identity: xxx
1087ms round-trip time
89kB of 161kB RAM used
0% battery charge
The charge for this battery is low. Recharge the battery soon to prev the device from losing power and going offline.
0 rate-limited publishes
Download History (docs) | Ru check

FIRMWARE NEW

Event particle/device/diagnostics/upda...
Data {"device":{"network":{"signal":{"at":"Wi-Fi","strength":86,"str...
Time 1:09:53 PM, Oct 13, 2020

Event particle/device/updates/pendi...
Data false
Time 1:09:52 PM, Oct 13, 2020

Event particle/device/updates/forced
Data false
Time 1:09:51 PM, Oct 13, 2020

Event particle/device/updates/enabl...
Data true
Time 1:09:51 PM, Oct 13, 2020

photonatron
Photon

My Fleet
Device

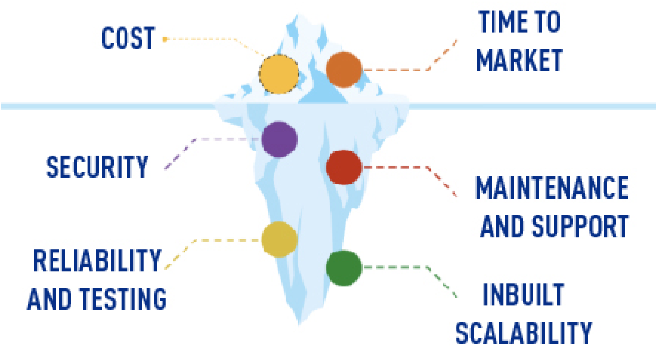
> Buy what doesn't differentiate you and build what does.

IOT - BUILD VS. BUY DECISION FACTORS

In our experience, even the most sophisticated enterprises fail to anticipate what goes into a successful IoT project. Thus, they make the decision to build or buy based on an incomplete picture of what IoT will look like for their specific use cases.

Very often, enterprises are thinking most about the cost of hardware and time to market for IoT projects. These are important, but they're the tip of the iceberg.

Security and certifications, ongoing reliability and testing, scalability, and ongoing maintenance and support are all critical parts of an IoT deployment, and yet, they're often invisible until an enterprise runs up against the difficulties they present.



In this section, we'll dive deep into the most important considerations you should make when deciding what you will try to build in-house and what you'll bring in a strategic IoT partner for.

Internal expertise and resources

IoT platforms involve dozens of different systems and technologies. In trying to build, secure, and maintain these platforms, you'll instantly become a general contractor with the responsibility of managing and juggling multiple vendors and contracts. Research from PTC showed that the average enterprise IoT project involved over 23 different vendors for a single product.

Here are some of the critical areas you'll need to evaluate your team on to see what they're capable of building:

- Embedded device hardware and firmware
- Networking and communications
- Cloud computing
- Mobile application development
- Data security and privacy
- Integrations
- Data storage architectures
- Performance tuning
- Reliability testing
- Over-the-air updates
- Interoperability
- Power optimization
- DevOps
- User experience design

A startup or small company would need to add more than a dozen full-time engineers with expertise across these areas just to have a baseline team capable of building an IoT product. Larger enterprises would likely have to add teams of experienced engineers to add these capabilities at the necessary scale.

You may have engineers on your team that can handle some of these areas, but very few companies have the level of expertise across all of them they need.

> ...even the most sophisticated enterprises fail to anticipate what goes into a successful IoT project.

Total cost of ownership

There are two major cost drivers in building an IoT product - business transition costs and technology costs.

In a report for Siemens Advanta, Dr. Peter Louis, Gerhard Geisert, and Rainer Blessing wrote that many business leaders underestimate the costs associated with transforming their business with IoT.

They're great at projecting the technical costs of buying point solutions, hardware and devoting internal resources to the project. Still, they fail to project the costs of developing new processes and tools, developing their workforces to handle those new additions, and change management across departments.

Focusing only on costs incurred within the technical stack leaves out a significant portion of the total cost of ownership.

"The budget for an IoT initiative must cover not only the direct investment for the complete technology stack including infrastructure for data processing and storage, license or subscription fees as well as resources for cybersecurity. It also has to cover the transition costs including efforts for processes and tools, skill development, and Change Management to facilitate a successful digital transformation," Louis et al. wrote.

The human costs are where projections often get muddied. Bringing in engineering talent, hiring consultants, and aligning the rest of the business to adapt to new business models are substantial costs that often don't get factored in.

It goes back to the opportunity cost of building it yourself. The resources and money you devote to producing something that's already been done well could instead be spent on aligning other business areas to the new value creation mechanism that IoT is intended to be.

> ...They're great at projecting the technical cost of buying point solutions, hardware and devoting internal resources...

Desired Time to Market

IoT is not a new concept by any means, and yet, even the most forward-looking enterprises lack a clear roadmap for developing IoT-connected products quickly and efficiently. This makes building a solution yourself difficult.

According to Mariano, the biggest question you have to answer is: What is the opportunity cost of getting to market in 1-2 years rather than a few months?

"How much revenue would you miss if you took an extra year to get to market? What would happen if a competitor beats you to market?" Mariano said.

"Building a connected product and getting certifications takes at least 18-24 months. If you could bring a product to market in four to six months by buying already-certified hardware and connectivity so you could focus on building your differentiating factor, how would that increase the lifetime value of your product?" he added.

Another factor to consider is being able to announce product launches that are timed with key industry events.

"If you have a big R&D department and you feel comfortable spending a few years developing your IoT product, you might be more comfortable with building something yourself," Kate said. "The companies we generally work with usually have a hard launch date set by a board of directors or based around an industry conference. They need to get something to market within a year or so and can't afford to spend time developing something they could buy from Particle."

By using a platform like Particle to build connectivity into your proprietary product, you can get a working POC in a shorter period of time. This can get you to a point where you can announce the new product and begin marketing it.

"The first-mover can win substantial market share. Connected products can be very sticky for end users, and once they're entrenched in the customers' life, it's hard to get them to switch," Kate said.

Integration with Other Systems

Most IoT platforms built in-house are essentially a collection of microservices that provide "point solutions" for different parts of the IoT product.

This includes device provisioning, application enablement, access control, monitoring, device management, event processing, data management, etc.

Assembling the right point solutions and integrating them into a single IoT architecture is costly and can significantly slow down your product development cycle. You would also have to build a team of engineers that have expertise in each of these areas.

By contrast, buying an integrated IoT platform makes integration simple.

"We can send our customers devices with IDs, so all they have to do is click a button to activate the SIMs. Once they're connected, they can use them immediately," Kate said. "Once your firmware is loaded onto the console, it will automatically update. You don't have to do anything else. Once your devices are connected, Particle allows you to push automatic updates to fix bugs or add features. As your devices collect data, you can easily retrieve the data from the Particle cloud.

"You can have the data ported right into a spreadsheet or an Amazon Web Services server," Kate explained. "You set up a key, set up a webhook, copy and paste the key into it, and the data is flowing. All of these parts have been masked, so you own the process."

Particle also has built-in error cases, so you can monitor the integration between your devices and the cloud and easily track performance.

"You want to hire smart people to solve problems for your customers and drive value for the business," Kate said. "You don't want to hire smart people in-house and make them put out fires and figure out how to connect things."

Cellular Connectivity

Managing cellular connectivity in an IoT ecosystem is difficult even if you have some of the expertise in-house. Cellular connectivity is essential for IoT to function properly. Interruptions in connectivity can mean the loss of vital asset data, costing revenue and additional maintenance costs.

Managing connectivity means managing a full stack of technologies, even before you get to your own hardware and software that need to be connected. Here is a list of everything you need to consider when managing cellular connectivity at scale:

- SIM manufacturers (Thales/Gemalto)
  - *SIM firmware (SIM applet, eSIM, iSIM) and OTA updates*
- Modem components
  - *Hardware*
  - *Modem firmware & updates*
- Modem Modules
  - *Hardware*
  - *Module firmware & updates*
- Microcontroller network stack
- Signal strength/quality
  - *Antennas*
  - *Dead spots*
- SIM provider MNO (such as AT&T, Telefonica, T-Mobile)
  - *SIM management (Activate/Deactivate)*
  - *APIs*
  - *Hardware certification*
  - *SIM roaming profiles and updates*
  - *Network roaming profiles and updates*
  - *Billing, negotiating plans, forecasting*
  - *Customer and technical support/account management*
- Roaming partner MNOs - usually other MNOs that have roaming agreements (e.g., AT&T SIMs roam on Rogers in Canada)
- Radio Access Technology (2G, 3G, LTE and various categories like Cat 1, M1, NB-IoT)
- Telephony network equipment providers (Cisco, Juniper, etc.)
  - *Firmware updates*
- Certification groups
  - *FCC, SIM provider, GSM, PTCRB, etc.*
- GRX interconnect provider (Syniverse)
- Internet providers
- Network protocols (ICMP, UDP, TCP, TLS/DTLS, CoAP, MQTT, HTTP)

Managing the complexity of a cellular stack can be a major source of issues that affect the functionality of your product and your ability to deliver value to your customers.

“When devices go down, it could be because of hardware, the firmware, the network, the SIM card, or any number of things,” said Raniz Bordoloi, Product Marketing Manager at Particle. “And when you’re not working with a full stack provider, it’s harder for you to eliminate all of these possibilities and narrow down the cause of the outage.”

> ”
>
> Managing connectivity means managing a full stack of technologies, even before you get to your own hardware and software that need to be connected.

Security and Certification

Protecting user security and privacy is critical for any IoT deployment, and the penalties for non-compliance with local regulations can be steep. Security is one of the biggest challenges for IoT, and it can significantly slow down your time to market.

In general, you can expect to spend six to nine months and up to $200k acquiring FCC, PTCRB, OTA, and carrier certifications, along with RoHS compliance certifications.

Even those timelines can be pushed out, putting your whole project at risk due to the high rate of FCC certification failure. 80% of all first-time FCC certifications fail.

The first-time certifications are just the beginning. Once your devices are certified, you need to install them safely and avoid installing counterfeit certifications. Additionally, FCC certifications expire, so you'll need to get re-certified over time. As you introduce new connected devices, you'll need to repeat this process.

Setbacks here can easily lead your project to be canceled or delayed if it doesn't go smoothly.

This is where working with a dedicated third-party IoT partner gives you an advantage. A robust platform will include several built-in security features, such as:

- An open-source Device OS where anyone can report and address vulnerabilities.
- Firmware updates over encrypted protocols.
- Frequent testing against OWASP standards.
- Zero open ports so there are no local attack surfaces exposed to bad actors on a network.
- Password-free devices that are managed through the Device Cloud.
- Up-to-date compliance with privacy and security legislation like CCPA, GDPR, and others.
- All communications that occur on the platform use the secure DTLS protocol, which ensures that network communications are always encrypted.
- Public key cryptography, a robust encryption methodology that relies on private and public keys rather than hardcoded secrets, should be used to authenticate a device to the device cloud.

IoT also involves moving significant volumes of data from devices to the cloud. When you build your own infrastructure, you have to ensure that your hardware and cellular vendors can securely integrate with your cloud and that your cloud can securely integrate with business intelligence tools.

Any platform you buy should come fully integrated and secure from edge to cloud and provide secure APIs for connecting BI tools.

Scalability

Scale is a significant factor that has to be considered when deciding whether to build or buy. You might have the expertise to build a POC in-house, but the people who can design and build a prototype may not be the right people to scale it up to a market-ready product.

For example, rolling out firmware updates to 10 devices is a fairly easy task. Rolling out firmware updates to 10,000 devices is a completely different process.

You must be able to assure quality control and checks at scale and remotely upgrade connected devices in a controlled fashion without bricking them or causing downtime. Every new feature or fix that gets pushed must do so seamlessly, without interrupting the end user's experience or the device's performance.

Maintenance and Support

Maintenance and support are an inevitable and crucial part of the IoT lifecycle. An IoT deployment is a complex system involving multiple layers, with much of the complexity coming from the cellular connectivity embedded in the product.

This is to say nothing about maintaining and continually upgrading hardware and firmware and adding new features to the product as the end users' needs change.

Beyond that, tracking issues and resolving them promptly without causing downtime is crucial to maintaining customer satisfaction.

One of the most complex parts of an IoT platform to maintain is cellular connectivity. An issue with your carrier or even a cell tower can cause poor performance and even outages for your end users. When you build your own IoT platform, you'll need several full-time engineers who understand cellular connectivity, can diagnose issues and know how to fix them quickly.

By contrast, buying an IoT platform that manages all of the connectivity for you can shorten the timeframe for fixing end user-facing issues.

For example, in mid-2021, Particle noticed that one of Canada's largest cellular operators with several million subscribers had a longstanding bug that affected all LTE devices nationwide. In certain conditions, servers on the Internet weren't able to send data down to the devices, even though the device had an observably healthy cell connection by all standard metrics.

It made it very hard for an end-user to control a remote device reliably, causing significant frustration. The cellular carrier and several of its partners were unaware of the issue.

However, Particle's cellular engineering team noticed that this was impacting several users across multiple IoT deployments. The team isolated the error conditions, brought all of the relevant partners together, and was able to push a fix in just two months.

An issue like this could potentially take over a year to solve if you cannot convince the SIM manufacturer, the modem manufacturer, the cell carriers, etc., that the issue exists and is worth fixing.

"An in-house IT team probably wouldn't have the expertise and resources to deal with something like this," JT Zemp, Cellular Tech Lead at Particle, said. "They likely wouldn't have the scale of devices in various settings to really dial in on the issue and reduce uncertainty quickly. Nor would they likely have the tenacity and clout to involve each partner at each layer of the "Russian doll" nesting of partnerships."

"Whether you're a small or large company, if you only have a few devices, you likely won't have that kind of access to major cellular carriers who can help solve your problem," Kate said.

A partner that provides and maintains your IoT platform ultimately reduces the amount of maintenance on your stack that you need to handle. Buying a solution that updates its security and privacy protocols - such as GDPR - as they're announced means you don't have to devote headcount to doing it for you.

As it relates to support and upgrades, any platform should also make it easy for you to push over-the-air updates without bricking or interrupting your devices. You can push new features live and not worry about negatively impacting the end-user exp.

Most of all, there's the opportunity cost of devoting resources to maintenance and support. Instead of maintaining systems with an in-house team, a strong IoT partner that manages millions of devices can focus there while you stay focused on your core competencies.

An IoT platform with an entire team of site reliability engineers will have insights and expertise across global deployments. That will give you an advantage over hiring an in-house team that would encounter complex IoT issues for the first time with no frame of reference on how to solve them.

CONCLUSION

Between validating your business case, managing the technical requirements of building and maintaining the infrastructure, and radically changing how your teams work with connected products, IoT is a massive undertaking.

It's tempting to look at the various parts of an IoT ecosystem and think that your team can build them exactly to your specifications. But just because you can build something, it doesn't mean you should.

Buying an IoT platform gives you the full technology stack you need, comprising hardware, an operating system, connectivity, and software to accelerate your time to bring an IoT-connected product to market. IoT is a technical solution to a business problem, and devoting your resources to the technical side can often come at the expense of staying aligned with your business value.

WORK WITH PARTICLE

Particle has helped market leaders and innovative new companies alike bring IoT projects to life for over a decade. What makes our platform different?

- **Secure and reliable:** End-to-end encryption from hardware to connectivity to cloud, with SOC II and GDPR certifications, public/private key authentication, open event logging framework, encryption at REST, encrypted API messages, and firewall protection.

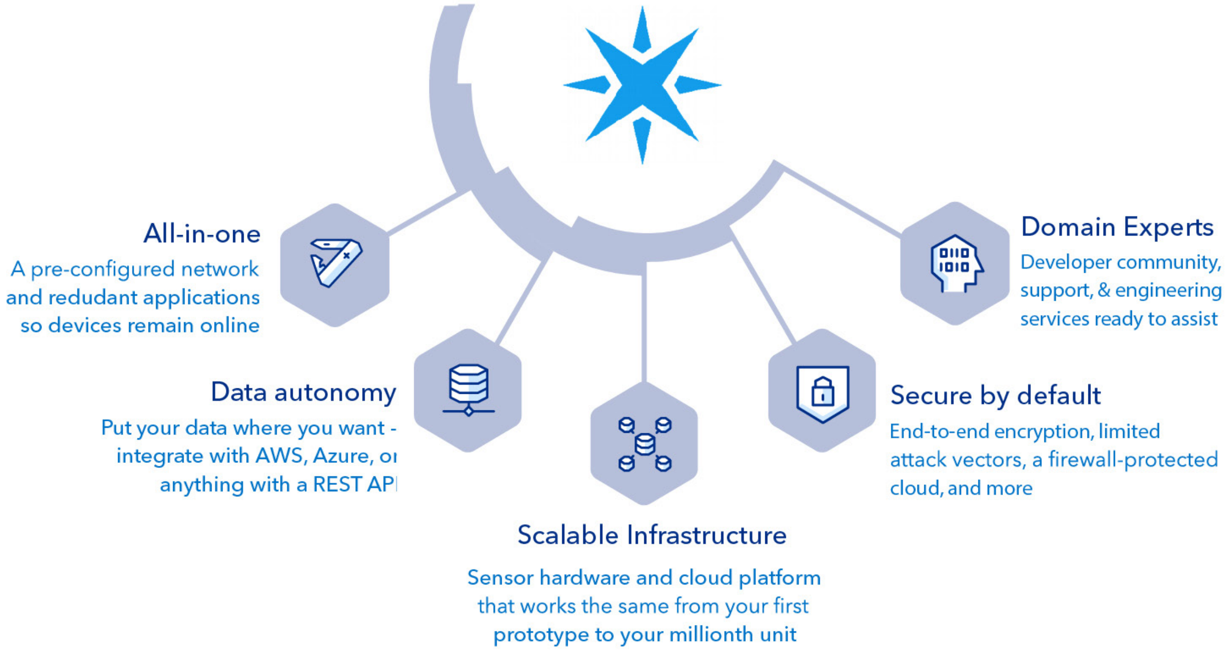
- **Scalable:** We've helped connect and launch hundreds of thousands of devices, with a fully managed cloud infrastructure processing billions of messages a month and zero planned downtime.

- **Upgradable:** Wirelessly reprogram your fleet of vehicles in the field with our over-the-air (OTA) software updates without any hardware or software scalability issues, and add product features, improve bugs, and avoid vehicle disruption with the push of a button.

- **Open:** Use our APIs and open, referenceable system architecture to access and share vehicle data to multiple different stakeholders of your choosing or integrate seamlessly into existing software architecture without any security hassles.

- **Plug and Play and Customizable:** Use our Tracker One hardware for immediate deployment as an off the shelf solution or our Tracker SOM hardware as a fully certified system on module foundation for a more customized solution. With both choices, you inherit a fully integrated, pre-certified solution, with configuration services and an open firmware application framework for differentiation.

- **Global Connectivity:** Our IoT-specific SIM card is built into our hardware and is powered by over 350 carriers around the world that automatically connect to the best networks across 2G, 3G, and LTE technologies, designed to make IoT cellular management simple and unified.



All-in-one

A pre-configured network and redudant applications so devices remain online

Data autonomy

Put your data where you want - integrate with AWS, Azure, or anything with a REST API

Scalable Infrastructure

Sensor hardware and cloud platform that works the same from your first prototype to your millionth unit

Secure by default

End-to-end encryption, limited attack vectors, a firewall-protected cloud, and more

Domain Experts

Developer community, support, & engineering services ready to assist

Contact a Particle expert to start your project.

SOURCES

Microsoft Azure, IoT Signals Edition 3, October 2021
https://azure.microsoft.com/mediahandler/files/resourcefiles/iot-signals/IoT%20Signals_Edition%202_English.pdf

PTC, LiveWorx 2019

IoT Analytics, Guide to IoT Solution Development,
https://iot-analytics.com/guide-to-iot-solution-development/?

IoT Analytics, Current State of IoT Platforms

Particle