Maximizing the impact of your IoT Proof of Concept

Key considerations and best practices to ensure a successful IoT PoC

OAKWOOD

Microsoft

Contents

Introduction

The Internet of Things (IoT) presents a wealth of opportunity. IoT has the power to help businesses completely transform their operations, decision-making, and revenue models—saving money and driving business growth. With a predicted $100M average increase in income for the most digitally transformed enterprises[i], it's easy to understand why IDC projects a compounded annual growth rate of 15.6 percent in IoT spending between now and 2020.[ii]

That doesn't mean, however, that these business opportunities can crop up overnight. Many companies may want to use IoT to revolutionize their entire operations instantaneously, thinking there's an immediate way to realize massive business benefits. Such lofty expectations will most likely leave companies overwhelmed and frustrated, setting them up for costly mistakes. But it doesn't have to be that way.

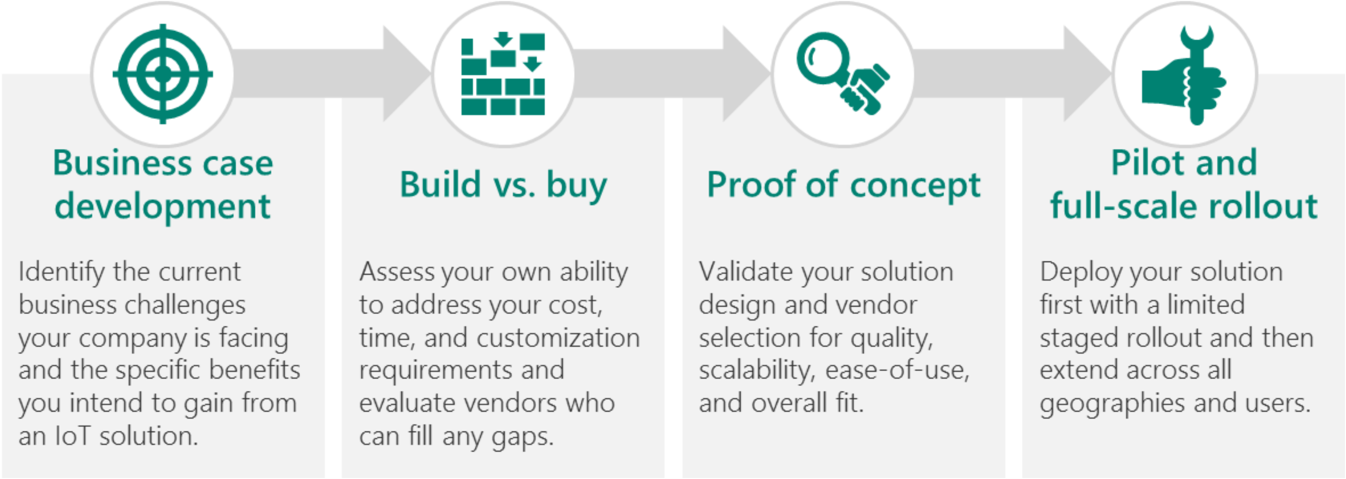
A well-planned proof of concept (PoC) is key to demonstrating the value of your IoT solution before implementing a full-stage rollout. With the right design, you can get results to executive sponsors quickly and iterate on a simple scale, maximizing control of your solution and minimizing the consequences of short-term failures.

Designing an IoT proof of concept may seem like a daunting task, but with the right vision and approach any company can develop a successful IoT initiative. In fact, it's very likely that you already have the pieces in place to get started. The purpose of this paper is to identify the key considerations for each component of an IoT PoC.

Four stages of the IoT journey

A proof of concept is one of four stages in a company's IoT journey. In order to best set up their proof of concept for success, it's critical that a company has first developed a business case and identified the partners and internal teams who will be building the solution.

Figure 1: The four stages of the IoT journey



Business case development

Identify the current business challenges your company is facing and the specific benefits you intend to gain from an IoT solution.

Build vs. buy

Assess your own ability to address your cost, time, and customization requirements and evaluate vendors who can fill any gaps.

Proof of concept

Validate your solution design and vendor selection for quality, scalability, ease-of-use, and overall fit.

Pilot and full-scale rollout

Deploy your solution first with a limited staged rollout and then extend across all geographies and users.

Business case development

The first step in a company's IoT journey is to develop a compelling business case for implementing a solution. This includes identifying the current business challenges you are facing and what opportunities there are for growth. Maybe you are looking for new ways to assess your business operations with the hopes of uncovering inefficiencies. Or perhaps you want to learn more about customer sentiment and how they are using your products. You may even be looking to transform your existing business to create entirely new revenue streams. In this stage, you will need to outline the specific benefits you intend to gain from an IoT solution and get your initial buy-in from executive sponsors.

Build vs. buy

Once you have a clearly defined business goal, the next step is to determine how you are going to develop your solution. At a high level, there are two approaches that companies can take: building in-house or outsourcing to a partner. Most companies will use a combination of these approaches, depending on their capabilities. Some companies who are new to IoT may want to outsource the development and implementation process entirely.

This step requires both an analysis of your cost, time, and customization requirements as well as an internal assessment of your own cloud solution expertise, including skill sets in analytics and security. Companies will need to acknowledge their limitations and evaluate vendors who can address their needs.

Learn more

How to choose an IoT provider

Discover the five questions that any business decision maker should consider before deciding on the right provider for their IoT solution.

Proof of concept

Before rolling out your IoT solution across your entire company, it's important to validate your solution design and vendor selection for quality, scalability, ease-of-use, and overall fit with a proof of concept. Most proof of concepts shouldn't take longer than 6-8 weeks, and some preconfigured software-as-a-service (SaaS) solutions can run in as quickly as 2-3 weeks. A proof of concept is also sometimes known as a proof of value.

Pilot and full-scale rollout

The final stage of an IoT implementation is the production rollout. Typically, this begins with a staged rollout of the IoT solution for specific product lines, geographies, or beta users. Early planning for organizational and process transformation during this pilot phase prevents issues later.

Eventually the solution will be fully rolled out across all geographies and users. This often requires internal training to ensure system acceptance and successful process changes. It's important to regularly analyze the outcome of your solution and continue to build upon it to improve your return on investment.

In this paper, we are focused on the proof of concept stage in this IoT journey. The remainder of this paper outlines the key considerations and best practices for developing a PoC.

Cummins Power Generation

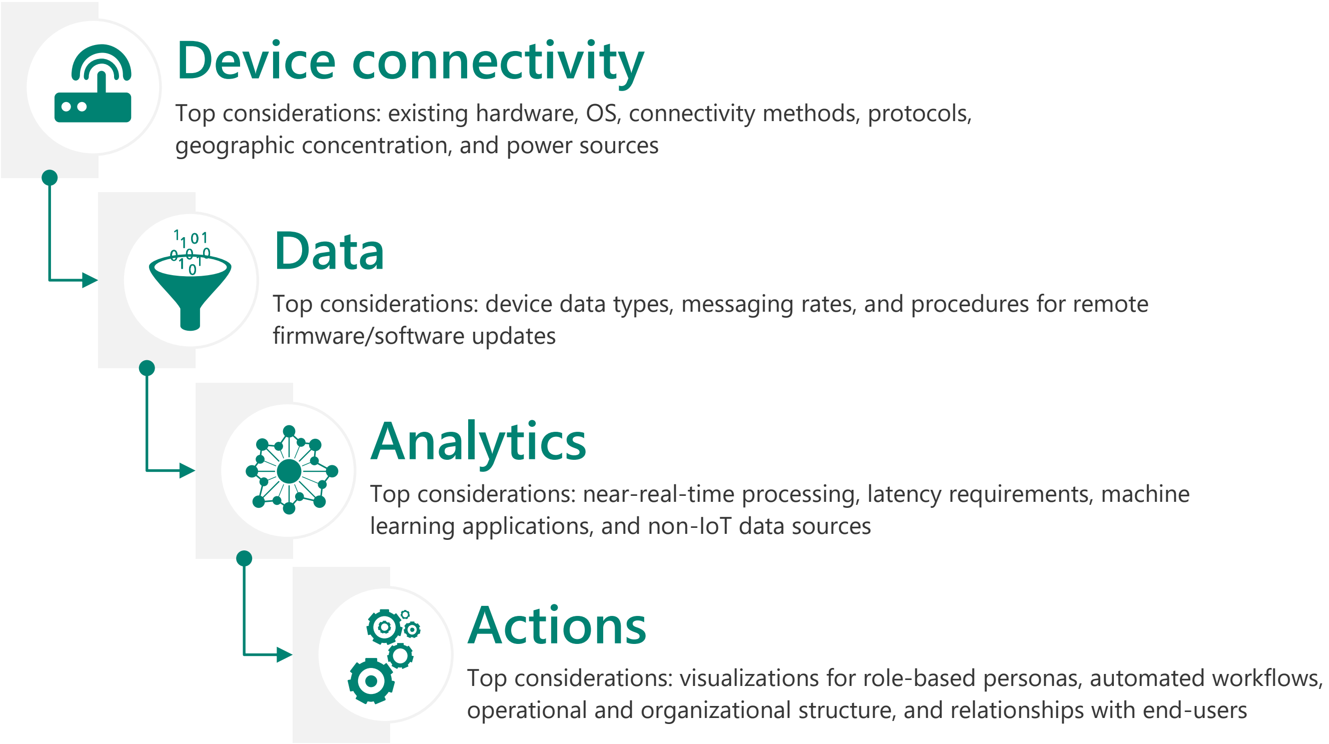
Keeping the Power on When You Need It Most

Learn how the Cummins Power Generation business harnessed the Microsoft Cloud and the Internet of Things to empower its entire ecosystem of customers, dealers, and distributors.

PoC solution considerations

There are four major components of an IoT solution to consider in a PoC.

Figure 2: The four pieces of an IoT proof of concept



Device connectivity

Top considerations: existing hardware, OS, connectivity methods, protocols, geographic concentration, and power sources

Data

Top considerations: device data types, messaging rates, and procedures for remote firmware/software updates

Analytics

Top considerations: near-real-time processing, latency requirements, machine learning applications, and non-IoT data sources

Actions

Top considerations: visualizations for role-based personas, automated workflows, operational and organizational structure, and relationships with end-users

You may not need to do tackle all four of these components right now. For example, if you feel that you already have a reliable device connectivity design, it might make more sense to focus your PoC on an analytics solution.

The following are a set of questions to ask for each component of your IoT proof of concept. These are offered as starting points to help businesses identify the key considerations and decisions that need to be addressed in designing their PoC.

Device connectivity

An IoT PoC starts with the base of devices that must be connected. Typically, companies will have an existing set of devices that they want to connect to the cloud, which may require some retrofitting. This section offers key device connectivity considerations for customers who are making PoC decisions by exploring the following five questions:

1. What hardware and OS are the devices running?
2. What connectivity do the devices have today?
3. What protocols do the devices speak today?
4. Where should gateway devices be deployed?
5. How are the devices powered?

What hardware and OS are the devices running?

A device's hardware and operating system directly impact how easily it connects to the cloud, because connectivity solutions always require some level of software customization. The right combination of hardware and OS will enable you to take advantage of an existing device software development kit. Otherwise, you may need to code your connectivity solution from scratch. Different operating systems require different skill sets and development time, so make sure you identify all your known hardware/OS combinations from the start.

What connectivity do the devices have today?

There are several different connectivity types to consider in an IoT solution, including:

- High-speed connections with low latency, such as Wi-Fi or direct wired connections
- Metered connections, such as cellular and satellite
- Low-Power Wide-Area Network (LPWAN) connections, such as LoRaWAN and Sigfox
- Local, non-reroutable connections, such as Near Field Communication (NFC) and Bluetooth Low Energy

Often a company's devices already connect to the internet via Wi-Fi or a cellular connection. Even if devices are not internet-capable, there are other ways to connect to the cloud. If they have local connection capabilities, you can use an internet-enabled gateway device to bridge the gap to the cloud.

In some cases, you may not want to connect your devices directly to the cloud. For example, your organization may have security specifications that require you to keep all your devices behind a gateway firewall. Another reason may be to reduce the volume of data sent to the cloud. If your existing devices are configured to produce data at very high-frequencies, a gateway can aggregate and filter that data before it is sent to the cloud. Gateways can also offer local storage in the event of transient connectivity issues and provide local edge processing, enabling even faster calculations and workflow automation.

What protocols do the devices speak today?

To connect your devices to your IoT software, you will need to both connect your devices to the cloud an d ensure they speak the same language as your IoT software. Most cloud IoT solutions support secure internet-based protocols like AMQPs, MQTTs, and HTTPs. Typically, AMQPs and MQTTs are preferred protocols for IoT solutions, as they are natively bidirectional.

Depending on the protocol that your devices use, they may or may not be able to talk to the IoT software on their own. If your existing devices use a non-IoT protocol, and you cannot make any changes to the devices themselves, a gateway device can also serve as a local translator, speaking to your devices in their local language while using another to talk to the software in the cloud.

Where should gateway devices be deployed?

Broadly speaking, there are two locations to deploy a gateway device: on-premises or in the cloud. The way your devices are deployed is one important factor in where you would host your gateways. While there are exceptions, if your devices are spread out geographically, it's likely you'll have to put any required gateways in the cloud. However, if the devices are concentrated in a single factory building, then it might make more sense to house the gateway on-premises. Other business drivers for gateway location may include messaging rates, local processing needs, the cost of the gateway relative to the cost and number of the devices to be connected, and the ability to update the software of the devices themselves.

How are the devices powered?

A device's power source can have a significant effect on how it can be managed and monitored. If your devices run on batteries, they typically won't be able to run constantly and will therefore only be able to talk to the cloud periodically. Any commands sent to those devices won't be received until they wake up. This also impacts the payload size, since the longer the devices have to be awake to send more data, the faster the batteries burn. Often battery-powered devices will send events in regularly scheduled batches, which affects the format of the data coming in as well. If devices have permanent power, it opens up the opportunity for more immediate command and control.

Data

The second piece in an IoT PoC is the data ingestion and device management component. This involves both streaming data sent to the cloud as well as commands sent to the device.

This section offers key device data ingestion considerations for customers who are making PoC decisions by exploring the following three questions:

1. What kind of data will the devices send?
2. What is the expected or planned messaging rate for the devices?
3. Is updating firmware/software remotely on the devices part of the PoC? If so, do you have a procedure in place for that today?

What kind of data will the devices send?

The data that devices provide in an IoT solution can be grouped into two categories: streaming data and property data. Streaming data, often referred to as telemetry, is provided on a relatively fixed schedule. Property data, on the other hand, may just provide occasional updates. Each data type has its own channel for sending and receiving information.

As an example, consider a battery-powered temperature and humidity sensor. The device sends temperature and humidity readings about every 10 minutes. That would be considered streaming data. Assume you wanted the device to send a signal when the battery power drops below 50 percent. That would be considered property data, since it doesn’t run on a regular schedule.

What is the expected messaging rate for the devices?

The messaging rate, both from device to cloud and from cloud to device, is important to understand, because it has a significant effect on your overall cost. Most IoT offerings are priced by messaging rates. Many of the infrastructure components associated with messaging rates, such as your network bandwidth and cellular satellite connections, can be expensive.

Messaging rates are also important for scalability reasons. Make sure that your solution configurations in the cloud are at the right performance level for the planned messaging rate.

Is updating firmware/software remotely on the devices part of the PoC? If so, do you have a procedure in place for that today?

Many solution providers can orchestrate firmware updates at scale across millions of devices. However, the actual code required to update firmware is typically device-specific.

If you own and can fully control a device, it’s typically easier to modify its native connectivity, protocol, and data output to more easily integrate with your IoT software. If you don’t own the device, it’s likely that you’ll need to either work with the owner of the device to modify the device code or use a bolt-on device as a gateway.

Analytics

Once you have data flowing into your solution, the first thing you do with it is perform analytics. You’ll want to run two types of analytics on your PoC data: near-real-time analytics and deep analytics.

Near-real-time analytics

Near-real-time analytics refers to the basic processing of data as soon as it enters the system. In a PoC, it offers the most immediate value to businesses, with solutions like remote device monitoring. This section offers key analytics considerations for customers who are making PoC decisions by exploring the following two questions:

1. What types of alerting or near-real-time processing are you hoping to get out of the device data?
2. What is the acceptable latency of that processing? Do you need a gateway to perform edge analytics?

What types of alerting or near-real-time processing are you hoping to get out of the device data?
Most of the time, near-real-time analytics falls into three categories:

- **Alerting** lets you know when some piece of your data violates some designated threshold or changes by a certain percentage. This could be a device temperature rising above 100 degrees or a vibration level that is 20% greater than the same time-period yesterday.
- **Aggregation** enables you to perform a mathematical calculation, such as a sum or maximum, on some property over time. This could be the running 10-minute average of a temperature sensor or a count of people who have passed by a motion detector in the last week.
- **Geospatial** analytics can be helpful if you want to know if a device has gone outside of a certain range, such as off a designated job site.

What is the acceptable latency of that processing? Do you need a gateway to perform edge analytics?
The speed requirements of your near-real-time analytics will help determine if processing needs to take place on-premises through a gateway or with more powerful analytics tools in the cloud. Sub-second analytics will probably need to be performed on-site with the devices. If processing can take a few seconds or more, this can usually be performed in the cloud.

IoT gateway analytics provide several additional benefits for businesses. They help conserve expensive network bandwidth by significantly reducing the volume of data transported to and from the cloud. They can also add an extra layer of security by isolating devices from the open internet, providing encryption, and securing data that is locally buffered.

Deep analytics and machine learning

Deep analytics and machine learning involve precisely targeted and sometimes complex queries on data sets. While traditional analytics reflect what has happened in the past, deep analytics generate highly accurate predictions about what may happen and ultimately prescribe what you need to do to ensure the optimal result. In a PoC, these kinds of analytics applications can take longer to optimize and begin returning valuable insights.

This section offers key analytics considerations for customers who are making PoC decisions by exploring the following three questions:

1. What longer term insights do you hope to get out of the data?
2. What kinds of predictions would be valuable to your business?
3. What other sources of data do you need to combine with the device data?

What long-term insights do you hope to get out of the data?
You probably won’t be able to answer this question in its entirety up front. After all, when it comes to the underlying value in your data, you don’t know what you don’t know.

However, it can be helpful to start by testing some broader hypotheses and seeing if they produce any valuable insight. Are you looking to increase efficiencies in your operations by identifying anomalies? Perhaps you’re hoping to understand how environmental factors affect the efficiency of your devices? Or maybe you want to see if you have more failures with a specific type of device or with devices from a specific supplier?

What kinds of predictions would be valuable to your business?
IoT machine learning applications are all about making predictions. Typically, machine learning is used to predict some kind of device failure. Other common scenarios include predicting device usage patterns or tracking user location hotspots. Predictive insights can unlock efficiencies, reduce downtime, and enhance revenue streams for your business.

What other sources of data do you need to combine with the device data?
Depending on your solution, you may want to take advantage of preexisting internal or external data sources. These could be legacy on-premises datasets or other cloud-borne sources. A common example of this is using external weather data in analytics models that optimize the efficiency of large outdoor industrial equipment and ensure the safety of any on-site workers.

It's important to consider how these data sources will impact the overall scope of your PoC. You will likely need to determine how to transport that data into the cloud and how to connect it to your device-based datasets.

Action

The final component of an IoT PoC involves converting your analytics outcomes into intelligent action. This includes creating data visualizations and dashboards for the end users in your solution as well as automating processes to improve operational efficiencies and effectiveness. This section offers key considerations for customers who are making PoC decisions by exploring the following four questions:

1. What role-based personas do you want to serve? How do you anticipate users consuming the results of the analytics?
2. What workflows do you want to automate?
3. What is the preferred method of operating the solution?
4. What is your relationship with the end users of the solution?

What role-based personas do you want to serve? How do you anticipate users consuming the results of the analytics?
In any IoT solution, it's crucial to think about who the end users are going to be, what information they need presented, and how they need to consume that information. You may have a wide variety of audiences, such as information workers in the back office, the truck drivers on the road, or the mechanics who keep your equipment maintained.

Understanding how your alerts and processing results need to be delivered to users will help define where and how to output your analytics results. Some users are probably going to need standard operations dashboards. Others will need customized reporting dashboards. Some may want to be able to download the data for their own use. Others may need to consume pre-filtered information via a mobile app in the field.

What workflows do you want to automate?
Beyond basic data visualizations, you may want to use your IoT solution's data analysis to automate specific actions. One common scenario for this is Connected Field Service, which enables organizations to offer their customers a predictive and proactive approach to device maintenance. In this solution, IoT-enabled devices are continuously monitored and anomalies are detected, generating alerts that trigger automated actions or service tickets and workflow according to service level agreements. Availability and proximity of service technicians with the right skills, parts inventory, and tools are then matched against the service requirement and routed to customer locations to take preventive action.

What is the preferred method of operating the solution?
Alongside your technological development, it's important that you also establish an operational and organizational structure that will support your IoT solution. This ensures you have a plan for how you surface any new insights from your data and who is looking at it. For example, some companies may set up operational centers, where employees consume analyzed data from devices in the field, looking for cases where one may fail or is giving anomalous readings.

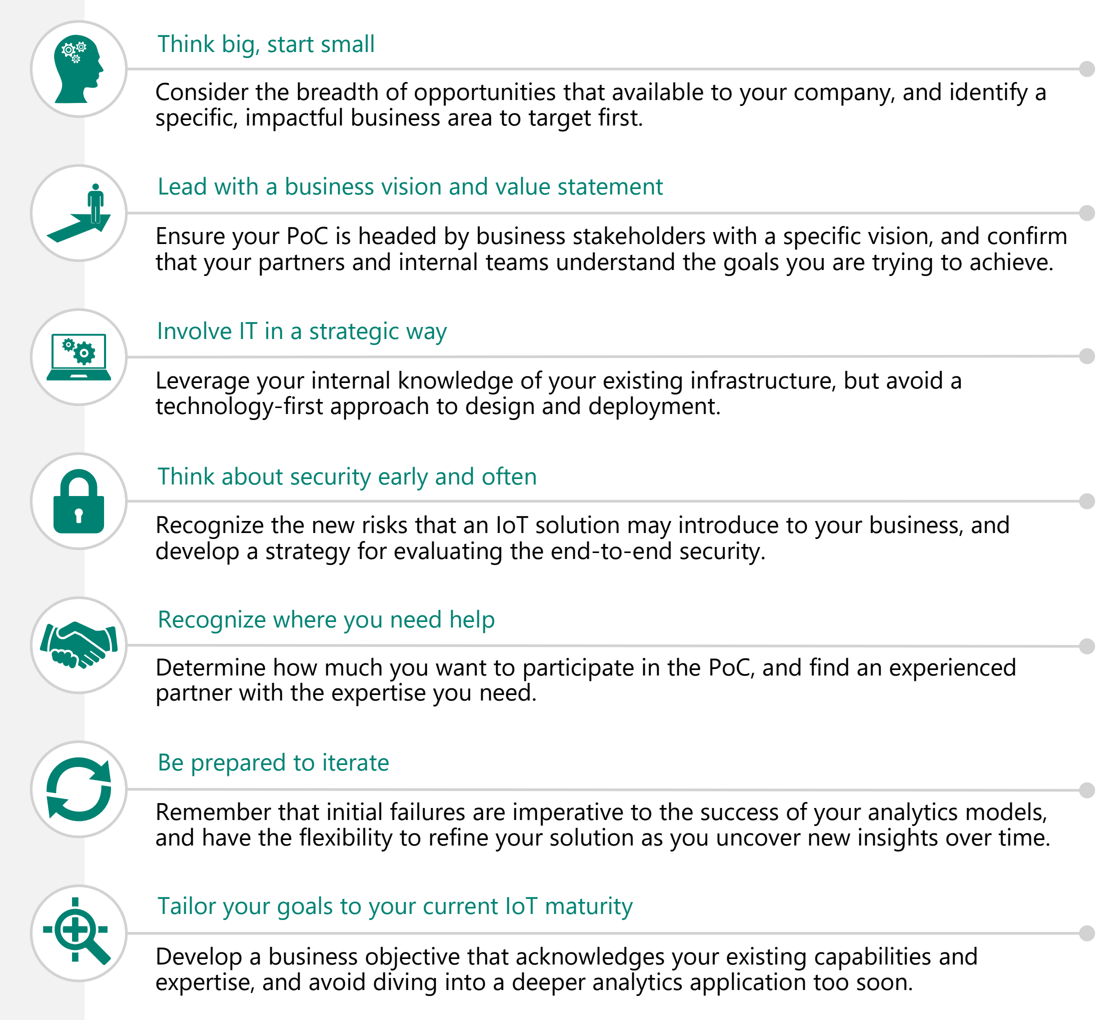
What is your relationship with the end users of the solution?
Your relationship with the end users is important, because it usually defines what control you have over authentication and consumption of your solution. Are your end users employees for whom you provide a mobile app and data plan? Or are they consumers, with whom you have no control over consumption and need their permissions to collect any useful data?

An effective authentication system is critical to the security and usability of your IoT solution. For company employees, and even partners, you may be able to authenticate via active directory depending on the size of your company. For customers, you might be able to authenticate them via their Microsoft account, social media account, or another web identity provider. Otherwise you may have to manage credentials for all these users yourself.

PoC approach considerations

As you begin to develop your own IoT proof of concept, there are several best practices you should keep in mind. The following key learnings are based on PoC success stories and failures from real companies around the world.

Figure 3: Key approach considerations for an IoT proof of concept



Think big, start small

Consider the breadth of opportunities that available to your company, and identify a specific, impactful business area to target first.

Lead with a business vision and value statement

Ensure your PoC is headed by business stakeholders with a specific vision, and confirm that your partners and internal teams understand the goals you are trying to achieve.

Involve IT in a strategic way

Leverage your internal knowledge of your existing infrastructure, but avoid a technology-first approach to design and deployment.

Think about security early and often

Recognize the new risks that an IoT solution may introduce to your business, and develop a strategy for evaluating the end-to-end security.

Recognize where you need help

Determine how much you want to participate in the PoC, and find an experienced partner with the expertise you need.

Be prepared to iterate

Remember that initial failures are imperative to the success of your analytics models, and have the flexibility to refine your solution as you uncover new insights over time.

Tailor your goals to your current IoT maturity

Develop a business objective that acknowledges your existing capabilities and expertise, and avoid diving into a deeper analytics application too soon.

Microsoft can help make your proof of concept a success

IoT offerings for any business

Whether you are a small developer with extensive cloud solution expertise or a large company with no former IoT experience, Microsoft has an IoT offering to help deepen your IoT maturity.

For companies with minimal in-house cloud solution and device expertise, Microsoft IoT Central takes the complexity out of the Internet of Things with an end-to-end IoT software-as-a-service (SaaS) solution. With Microsoft IoT Central, you can create new revenue opportunities and accelerate innovation through smarter products—helping you better engage customers by understanding their real needs. Connect your products using industry-leading technology and the enterprise-grade security features you need to stay in control of your IoT data.

For companies that need to fine-tune their services with a high degree of control, Microsoft Azure IoT Suite provides the building blocks to construct customized IoT solutions. Integrate your existing devices and systems with IoT solutions that can be tailored to your specific needs, helping uncover data and insights that transform your business and bring new opportunities. Collect and analyze your device data with advanced analytics to reveal previously hidden insights that lead to more informed business decisions.

For businesses looking for a hybrid cloud and edge IoT solution, Azure IoT Edge enables your devices act locally based on the data they generate, while empowering you to configure, deploy, and manage them securely and at scale with the cloud. Azure IoT Edge provides easy orchestration between code and services to distribute intelligence across your IoT devices. Reduce data transmission costs, operate with intermittent connectivity, and enable artificial intelligence and advanced analytics capabilities at the edge.

Industry-leading platform

Microsoft's IoT solutions run on the most trusted cloud, with the most comprehensive compliance coverage of any cloud provider. Get started quickly with preconfigured solutions, and accelerate the development of your IoT solution. Connect practically any device using software development kits (SDKs) for multiple platforms, including Linux, Windows, open-source, and real-time operating systems. Extend your global reach with the cloud service that offers more countries and regions than any other provider. With a worldwide network of Microsoft-managed datacenters across 38 announced regions, Microsoft Azure enables companies to easily scale from just a few sensors to millions of simultaneously connected devices, with reliable global availability—no matter how large or small your project.

Conclusion

A proof of concept is an instrumental step in a company's IoT journey. It allows organizational leaders to take real action on their business visions, by testing and refining the most important characteristics of a solution. It is where a company may begin to see firsthand the value and transformative power that the Internet of Things can bring to their business.

At Microsoft, we want you to feel empowered to make the best decisions in your proof of concept planning. This paper is intended is to help you jumpstart your thinking around the strategic and technological requirements for your IoT PoC. If you have further questions about developing your own proof of concept, please reach out to **Oakwood Systems Group** to learn more about how our offerings, platform, and partner ecosystem can help your business start realizing the incredible potential of the Internet of Things.

Learn more

- Connect with Oakwood Systems Group today to begin a PoC conversation.