Simplifying IoT at scale

Overcoming proof-of-concept purgatory for faster business value

July 2021

Microsoft | Cognizant

Contents

Why are so many IoT projects stuck in proof-of-concept purgatory?

Today, there's no question of the value of IoT. IoT enables connected operations and connected products that increase efficiency and productivity, reduce costs, enhance safety and security, open new revenue streams, and much more. That's why 91% of companies now use the technology and 90% consider it critical to their overall success.[1]

The promise of IoT is clear, yet a recent survey found that only 25% of IoT projects had moved from the proof-of-concept phase to the use phase.[2] At times, a proof of concept may be successful in a limited, controlled environment, but many companies struggle when they attempt to scale a solution to additional devices or sites. Their projects are stuck in what's commonly referred to as proof-of-concept purgatory.

So why are so many organizations failing to scale their projects beyond proof of concept?

A common reason is that they're focused on the quickest way to prove that the technology works, at the expense of taking a longer view to how they will operationalize and commercialize that technology at scale.

To be successful, organizations need to address three dimensions of scale:

- **The operational:** Does the organization have the resources to operate a large-scale IoT implementation or adopt new business processes that the new solution demands? For example, updating devices in the field as needed or deploying solutions at thousands of sites globally.
- **The economic:** Does the organization have the ability to scale the solution in a way that maximizes the business value and ensures the highest return on investment (ROI)?
- **The technical:** Does the organization have the technology foundation to support implementation at scale? For example, connecting millions of devices in the field and managing the enormous amount of data they collect.

During proof of concept, organizations focus on proving the technology:

- ✓ Dashboard
- ✓ Device connectivity
- ✓ Command and control
- ✓ Protocols
- ✓ Visualization
- ✓ Software update
- ✓ Alarms/alerts

At the expense of considerations that help operationalize IoT at scale:

- ✗ Enterprise IT alignment
- ✗ TCO and ROI analysis
- ✗ Business process integration
- ✗ Zero-touch provisioning
- ✗ Over-the-air update at scale
- ✗ Operational readiness
- ✗ Global deployment
- ✗ Security

[1,2] Microsoft 2020 IoT Signals report

At Microsoft and Cognizant, our mission is to simplify not only the technical but also the economic and operational aspects of scaling IoT, so that organizations can focus on business value rather than getting mired in complexity. Here we'll talk about considerations and best practices for every dimension of scaling IoT solutions. The goal is to help organizations scale their IoT implementation to production quickly and easily and realize its full value.

The three dimensions of scale

Operational scaling

Ensuring operational readiness is essential to scaling IoT, yet it's something organizations often overlook in the proof-of-concept phase. Read on for recommendations on how to integrate IoT into existing and new business processes and how to manage operations in the field.

Transforming business processes

When moving beyond proof of concept, the real value of IoT comes from using solutions to modify existing business processes and create new processes. That's because insights from IoT data are only valuable if they're put into practice. For example, a condition monitoring solution only makes an impact if the output from the solution transforms the organization's maintenance program. Changes to business processes should be planned from day one in collaboration with the lines of business and operations teams to ensure they are optimized for the operating environments and poised to contribute the most business value.

Effectively incorporating IoT into business processes typically requires acknowledging and documenting changes to existing business processes and new processes and then training the end users. Users need to understand how to read the new data, whether it's provided in a dashboard or another format, and be able to act on that data as part of their everyday work. Taking again the condition monitoring scenario, the operations team needs to be able to use the IoT data to understand when equipment has failed or is at risk and use that to inform how they're allocating maintenance resources. Cognizant builds end-user education into every project to ensure that users understand not only the technical aspects of the solution, but also more importantly the changes in process that are necessary to realize the full benefits.

Managing operations in the field

The operational dimension of scale also comes into play after the IoT solution is deployed. Every aspect of the IoT solution needs to be maintained, including hardware, edge components, connectivity, and cloud. Organizations can eliminate much of the complexity of field operations by leveraging the right technology from the start—for example, a zero-touch provisioning approach, an over-the-air update system, and a managed cloud service, each of which we'll discuss more later.

But because IoT involves physical hardware in the field, there are elements that require a human touch. For example, sensors or gateways may need to be replaced. Organizations need to determine who is responsible for replacing these components, whether that be IT or OT. They also need to think about whether they have the ability internally to roll a truck to the site to perform maintenance or replacement or whether it's better to outsource some of this work to external contractors.

If these questions aren't addressed from the start, organizations won't see the value of their IoT solutions. For example, a major fast-food chain developed an approach to transform existing, brownfield fryer equipment into connected equipment with a touch-screen display. The goal was to improve productivity, quality, and employee satisfaction, but ultimately the chain couldn't reach these goals because they hadn't thought through the challenges of deployment and maintenance at thousands of franchise restaurants.

Even more complex is planning operations for connected products, especially consumer products such as connected coffee machines. Organizations need to think about how the product will be provisioned when it reaches the consumer and how to implement new processes for customer support. In addition, they need to think about how to take advantage of cross-sell and up-sell opportunities. This requires comprehensive change management that enables the organization to transition from being a product manufacturer to being a product-as-service provider.

Economic scaling

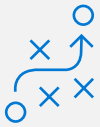
At the end of the day, organizations implement IoT at scale because of the value it will bring to the business, whether that be cost savings or new revenue streams. But it's easy to get distracted from business objectives or to let total cost of ownership (TCO) get out of control when moving to scale. Fortunately, with the right approach, organizations can maximize ROI and contain TCO, reaching their economic objectives.

Delivering return on investment

Often, organizations develop IoT solutions that are disconnected from the heart of the business. Employees are excited by what's possible, rather than what will contribute the most value to the business. The most successful IoT initiatives are developed in response to a business problem or opportunity so that the business outcome is centered from day one. By clearly defining the end goal at the start of the project, organizations can ensure that they don't lose sight of what they're really trying to achieve.

However, because IoT is still fairly new to many industries, it is often difficult or impossible to fully understand the ROI of an IoT project during the planning phase. It can be counterproductive to try to force inaccurate ROI calculations using rough estimates before starting a pilot. As an alternative, organizations can expedite understanding of the potential ROI and value of an IoT project by performing a detailed assessment of the operational environment, which can more accurately identify the potential areas of value, help guide the direction of the proof of concept, and build a more accurate picture of ROI.

Without proof of ROI, it's hard to justify additional investments needed to scale. Organizations should use their proof of concept to not only prove the technology works, but also demonstrate ROI.



Customer story: Engaging a partner to evaluate ROI

Determining which use cases and approaches will maximize ROI is easier said than done. For many organizations it makes sense to engage a partner like Cognizant to perform assessment. Let's look at an example of how Cognizant drove success for a leading kitchen and bath home goods provider.

The organization knew that IoT could unlock new revenue streams and transform their business model, but they didn't know where to start. They engaged Cognizant to perform market analysis to identify the strongest opportunities and create an IoT solution roadmap and complete investment plan to guide IoT initiatives so they could capitalize on key growth areas. With Cognizant's help, the organization aligned every segment of the business around a clear IoT vision and was successful in focusing their efforts on IoT initiatives that maximize ROI.

Managing total cost of ownership

To some degree, organizations can't control their ROI, but what they can control, with the right approach, is TCO. For IoT, TCO primarily comprises the cost of devices, connectivity, and compute infrastructure. When taking IoT from proof of concept to scale, it's essential to have controlled, predictable costs for these elements.

To control TCO, organizations should start by being strategic in where they make investments in connecting devices. For example, most organizations are dominated by legacy, brownfield equipment that requires an investment to enable connection.

While for some devices the complexity and expense of connection are easily justified by business outcomes, for other devices there may be little ROI. It's essential to understand the business case for connecting different devices and prioritize which devices to connect based on what will drive the most value.

There are a few common types of IoT initiatives: one is connecting an organization's own assets, such as creating a connected store, kitchen, or factory. The other is creating connected products. For the former, it's essential to contain the per-facility price to enable scaling to hundreds or even thousands of facilities. For the latter, per-device pricing is key. Understanding the per-facility or per-device price enables organizations to make strategic scaling decisions: they can better predict ROI and choose how and when to scale.

The cost of the necessary hardware should already be predictable, so what organizations need to focus on is controlling the cost of technology services, such as tools for connecting and managing devices. For example, organizations can leverage a SaaS platform like Azure IoT Central, which provides predictable per-device pricing and reduces maintenance costs. They can also control costs by creating an enterprise IoT platform that offers re-usable components, so that costs don't increase dramatically as organizations scale to additional use cases. (We'll discuss enterprise platforms in more depth later in this paper.)

Azure IoT Central: Leveraging a SaaS platform

The simplest approach to connecting and managing IoT devices is to leverage a SaaS solution that offers functionality for every element of the process in a single service.

Azure IoT Central is a SaaS platform that makes it easy to build IoT solutions at scale. Organizations can easily connect and manage devices and because of the integration with Microsoft's certified device catalogue, they even have access to thousands of devices that will connect automatically to their solutions. Plus, organizations can leverage out-of-the-box templates to easily visualize data. Now organizations can spend more time using IoT data to contribute business value, rather than simply collecting it.

Learn more about Azure IoT Central

Technical scaling

For most organizations, the technical challenges of scaling IoT are the first thing that comes to mind. Although the operational and economic challenges are equally important, overcoming technical challenges is necessary to scale your IoT implementation. Two of the key challenges related to scale are connecting and managing devices and managing data.

Connecting and managing IoT devices at scale

Organizations need to plan for the thousands, sometimes millions, of devices required to scale their IoT solutions. During proof of concept, improvised, manual approaches to connecting and managing devices may show the technology is viable, but scaling manual processes won't cut it when dealing with thousands of devices. Below are best practices for connecting and managing devices that work just as well to accelerate a proof of concept as to simplify implementation at scale.

Identifying and onboarding devices

The first step is to establish the connection to the cloud and configure the device to perform its intended task. In a proof of concept with only dozens of devices, it's not hard to onboard devices manually, but at scale it's impracticable. Organizations should take a zero-touch provisioning approach to enable automated provisioning at scale. With zero-touch provisioning, a handshake is triggered when a device is powered on which initiates onboarding and a subsequent automated provisioning process. Because the initial handshake includes authentication of identity, credentialing of trusted certificates, and security of the device and data, zero-touch provisioning not only eases the onboarding of devices, but also supports a strong security posture.

Managing connectivity

To keep IoT solutions running as intended, it's essential to ensure that they are able to connect reliably to the cloud. A best practice for connecting thousands or millions of devices across the globe is to use multiple instances of a core connectivity and device management service like Azure IoT Hub. Organizations should provision devices to connect to the nearest instance of the service to reduce latency. Then, they should monitor the load on the services: as the service nears its load limit, the organization should create new instances. This is the approach that leading car companies use to meet the challenge of connecting millions of cars around the world.

Azure IoT Plug and Play

In the world of personal computers, we're used to plugging in a device, like a USB drive or printer, and being able to use it right away. But to connect an IoT device to a cloud solution, typically you need to manually hard code each device to the solution so they can sync.

Things would be a lot simpler if you could connect your device and have it work immediately. Microsoft makes this possible with Azure IoT Plug and Play, enabling solution builders to integrate devices with solutions without manual configuration by coding both the device and the solution to a common interface, rather than to each other.

Learn more about Azure IoT Plug and Play

Device Update for Azure IoT Hub

While it is possible to build an update system from scratch, it is extremely challenging, and for most companies impractical, due to resource constraints and ongoing maintenance costs. For most, then, it makes sense to take advantage of a pre-existing solution such as Device Update for Azure IoT Hub. Device Update is a comprehensive platform that organizations can use to publish, distribute, and manage over-the-air updates and it's based on Microsoft's decades of experience rolling out remote updates of the Windows operating system to PCs and other devices.

Learn more about Device Update for Azure IoT Hub

Updating and maintaining devices

A key consideration for IoT at scale is how to efficiently update devices. Devices need to be updated for any number of reasons: to address a security vulnerability, to add new features or turn on existing ones, or to debug and do diagnostic work for customer support. At a small scale, updates can be performed manually, but at a large scale this becomes cost prohibitive. Organizations need a system that can perform updates automatically on everything from the smallest sensor-type device to the largest gateway-class device and work with each device regardless of vendor.

The update system also needs to ensure that updates are being sent to the right devices at the right times. By attaching metadata to updates, an update system will only send updates to devices that have properties that match the properties of the update. In addition, the system should function as an orchestrator to ensure that devices only update at appropriate times and under safe conditions. For example, a medical device manufacturer should schedule updates for when devices are not in use, such as overnight.

Managing IoT data at scale

Your devices are connected and you're ingesting data. Now what? Your data is only valuable if you're able to use it, which means ingesting it, transforming it, and applying rules for data processing. We have recommendations for simplifying data management to ensure that organizations can get what they need from their data without unnecessary complexity, cost, and resource expenditure.

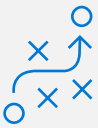
Ingesting data

With IoT at scale, organizations need to be able to handle extremely large quantities of data at a high rate. It's important to use a system like Azure IoT Hub, or even multiple instances of IoT Hub, because it offers data routing capabilities and a strong data pipeline so that there is no throttling and no data is lost.

Transforming and enriching data

In the majority of IoT implementations, the devices involved will be heterogeneous and will likely send data in different formats. A best practice is to use a common data model which provides a shared language for all your devices and solutions, considerably reducing effort for solution developers. A common data model makes it easy to scale to new devices and solutions without challenging data processing and integration work.

Moreover, the data coming from devices will be raw, so it can't be used with your IoT solutions without further transformation. To address this, organizations should enrich their IoT data with contextual or reference data for further processing.



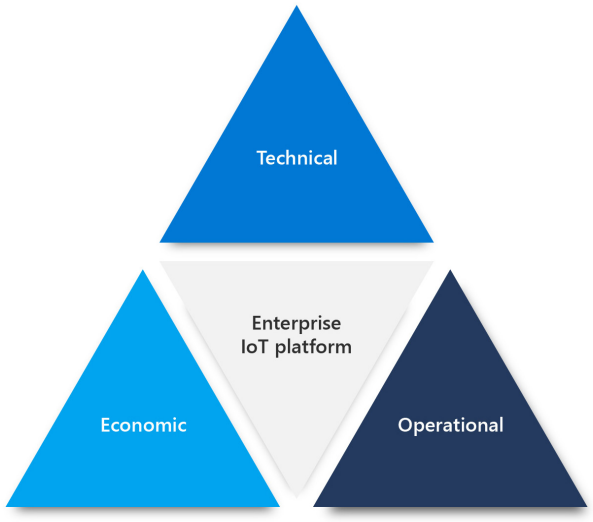
Customer story: Realizing the value of IoT data

A large construction machinery and equipment company has connected products like diggers in the field, some of which are up to twenty years old. Unsurprisingly, the data comes in in different formats, yet the company wanted to do common analysis across all the data. With help from Cognizant, the company transformed their data with a common data model and enriched it with contextual data like product and business data. With the help of unified APIs, that data is available to solutions that serve functions across the business from fleet management to asset management and beyond. Cognizant also provided a fully customizable rules engine so that field users could easily define rules for alerts without coding experience. This data management approach has meant that the company is not just collecting data, but truly extracting the full value of that data for the business.

[Learn about Microsoft's architecture for IoT data analytics]

Applying a rules engine

Users within organizations need to be able to define rules for data processing. For instance, some data needs to be processed immediately to enable real-time use cases (hot path), whereas other data can be sent to storage to be queried later in larger batches (cold path). Users should be able to define rules for data processing using a no-code or low-code experience.



Establishing an enterprise IoT platform

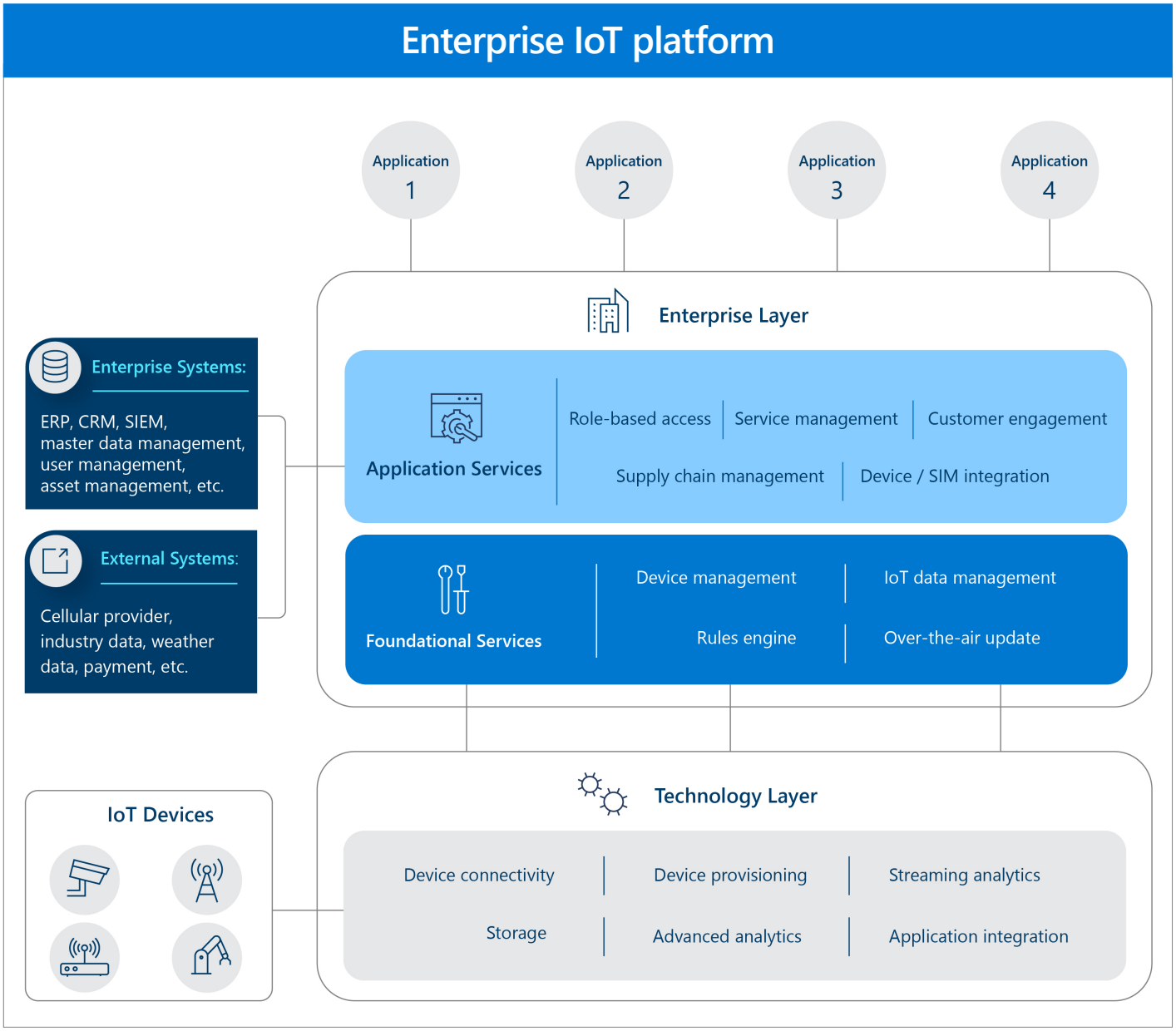
One of the most significant steps an organization can take towards scaling IoT solutions is to invest in an enterprise IoT platform. Such a platform provides all the building blocks for addressing not just the technical challenges of an IoT solution but also operational elements. In addition, it lowers the TCO of IoT solutions by simplifying ongoing

maintenance and enabling foundational components to be reused to support multiple solutions.

An enterprise IoT platform typically has two layers: a technology layer and an enterprise layer.

The technology layer provides core capabilities for an IoT solution, such as device connectivity, device provisioning, streaming analytics, and more. This layer is very complex to develop, so organizations typically leverage offerings from an established IoT platform provider like Microsoft, which offers an extensive set of IoT-specific services in the Azure cloud.

On their own or with the help of a partner, organizations can develop an enterprise layer that's tailored to their requirements. This layer leverages the underlying general-purpose IoT capabilities provided by the technology layer to develop foundational components for IoT solutions, such as device management, a rules engine, and more. Essentially, the nitty-gritty technical elements are hidden behind the scenes, creating well-defined interfaces that simplify application development.



In addition to the foundational services, the enterprise layer offers application services. These are ready-to-use services that application developers can use to enable IoT solutions to integrate with enterprise business processes and comply with enterprise IT guidelines. An example is an application service that enables an IoT solution to interface with a service management tool to create a work order in response to an alarm. A service like this can be pre-built to ease enterprise integration of an IoT solution.

Together, the foundational and application services offer the capabilities that application developers can use to develop IoT solutions quickly without compromising scale.

Benefits of an enterprise IoT platform:

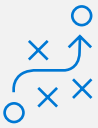
- Provides the "plumbing" for an IoT solution, addressing technical challenges around devices and data by leveraging architectural best practices
- Ensures IoT solutions can easily transition from lab-based proof of concept to being enterprise-ready by helping solutions integrate with business processes and IT standards and compliance
- Accelerates time to market with ready-to-use services
- Offers controlled, predictable TCO with well-defined buildings blocks and optimized use of underlying services
- Drives standardization across various IoT solutions within the organization, improving maintainability

Driving organizational alignment

Establishing an enterprise IoT platform can help address the operational, economic, and technical dimensions of scale, but organizations should also keep in mind that there are significant organizational barriers to scale. IoT projects are typically cross-functional, requiring cooperation among several disciplines, including IT, OT, engineering, and line of business. But given functional silos within organizations, this is easier said than done. Organizations need to consider how to drive alignment across the enterprise.

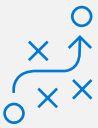
Each group may have their own idea of what the project means, or worse, their own siloed agenda of how the project will benefit their group. A best practice is to designate overarching leadership that has end-to-end responsibility for the IoT initiative. IT, OT, engineering, and the business are effectively peers within an IoT initiative, each responsible for their own defined swim lane. A leader who is responsible for the entire initiative can drive cross-team alignment from the beginning, ensuring that each part of the project is delivering the agreed-upon business case. This leader can be either a new role dedicated specifically to IoT or an existing C-suite member or other leader.

Additionally, it's important to align the project's business objectives with common KPIs that apply to every function. IT is typically considered a cost center and measured on its ability to efficiently provide consistent services across a large number of people. OT metrics are grounded in production—things like overall equipment effectiveness and throughput. The business function is measured on the overall performance of the business and in particular metrics like net margins. Keeping all these metrics in mind and creating common KPIs will build a strong business case to deliver ROI.



Customer story: Creating a bespoke enterprise IoT platform

A manufacturing giant hired Cognizant to help them build an enterprise IoT platform. Using Microsoft technology like Azure IoT Hub and other Azure services, Cognizant built a common foundation, with services like device management and data management, that can be used for IoT solutions across business lines. For example, the platform is used to enable a use case involving a connected device that improves worker safety for mine workers. And the platform is also flexible enough to support the company's connected consumer products, an entirely different use case. Each use case is supported by the same infrastructure, expediting time to market and reducing maintenance costs and complexity.



Customer story: Building an enterprise IoT platform with Azure IoT Central

A major consumer goods company engaged Cognizant to help them build their enterprise IoT platform using foundational services from Azure IoT Central like device management and rules engine. Building a comparable platform from scratch could have taken well over a year, yet the company was able to start using their platform within months. This vastly reduced time to market for their IoT solutions, enabling them to see value from their investments sooner.

Ensuring security at scale

Another key consideration is IoT security. Security for IoT at scale is fundamentally different from enterprise IT security due to the nature of the devices involved, but there are still concepts from IT security that apply—for example, zero-trust security. Zero-trust security has three principles:

1. The first is to verify explicitly. Whenever a user signs in or a call comes from one service to another or from a device to a service, it should be verified explicitly at the first instance.

2. The second principle is to use least privileged access: give access to a user or a call only for their business function and only when it's needed—what's described as "just-enough access" (JEA) and "just-in-time access" (JIT).

3. Finally, organizations should assume that their infrastructure will be breached and work to monitor it and minimize the blast radius. An approach for minimizing the blast radius is defense in depth, which involves creating an infrastructure that has multiple walls around it and redundancies so that if one feature fails another one can take over.

Building an IoT implementation using a zero-trust security approach will simplify security down the line as you reduce opportunities for security compromises and reduce the impact of compromises when they occur.

Another key to IoT security is a security-oriented approach to zero-touch provisioning. Learn more about the approach Microsoft has developed in collaboration with other domain experts.

Another element of alignment is clearly delineating the role each function plays throughout each stage of an IoT initiative. One team may take the lead in the development of the solution while another will be responsible for the ongoing maintenance of a solution. Successful organizations define roles for each part of development and operation and establish clear SLAs. In some cases, the roles may also include outside vendors—for instance, those that need to replace devices during operation.

Simplifying IoT at scale with Cognizant and Microsoft

Cognizant and Microsoft offer the technology and services to make the best practices we've discussed a reality. To enable the operational dimension of scale, Microsoft offers tools that simplify operations and Cognizant complements these with proven processes and implementation approaches, helping organizations every step along the way. For the economic dimension of scale, organizations can work with Cognizant to perform analysis of TCO and ROI and can depend on Microsoft to offer controlled, predictable pricing through solutions like Azure IoT Central. For technology, Microsoft offers the core services for things like managing devices at scale to quickly set up, update, and replace devices. It also offers services for managing data at scale to store data effectively, access it when needed, and leverage it to make decisions.

Organizations can work with both Cognizant and Microsoft to establish an enterprise platform that supports current and future use cases, so it can grow with their company and

offer the flexibility to meet future needs. To ensure organizational alignment, Cognizant offers change management support. Finally, to create a strong security posture, organizations can leverage best-in-class tools and technologies from Microsoft and work with Cognizant for effective implementation.

Get started today

Scaling IoT isn't easy, but by implementing the best practices above, organizations will find their experience moving from proof of concept to production to be much simpler. One of the common threads in simplifying every element of the IoT lifecycle is to think about scale from day one, whether that means designing how IoT will interact with business processes or implementing a common data model as early as the proof of concept. By planning for scale from the beginning, organizations save themselves from a lot of complexity down the road.

Microsoft and Cognizant aim to help organizations move to IoT at scale as quickly and easily as possible. Learn more about the technologies and services we offer.