Whitepaper

From Edge to Center: Key IoT Considerations for Enterprises

For some innovative enterprises, Internet of Things (IoT) is no longer wishful thinking, but a data-driven workhorse that's delivering valuable, real-time insights so they can be smarter, more agile, and more resilient in today's business climate defined by disruption. But many have yet to take the IoT leap; others have not yet transitioned Proof of Concept (PoC) projects to more influential IT initiatives. Before they do either, there are a number of strategic considerations — involving business and technology teams and spanning the entire IT environment — that should be made.

IoT solutions capable of adding real business value will touch technologies and processes that cross the enterprise, including the network, compute resources, storage, data protection, and security. It takes a scalable, interconnected, end-to-end IoT system that not only can securely collect massive amounts of data but also can transform it all into information that improves operations and customer experiences.

Start first with a solid IoT foundation

The amount of IoT devices and the data they generate are growing at an eye-popping yet steady rate.

International Data Corporation (IDC) predicts that "by **2025** there will be **55.7 B connected devices worldwide, 75% of which will be connected to an IoT platform**."

IDC estimates data generated from connected IoT devices to be **73.1 ZB by 2025**, growing from **18.3 ZB in 2019**."[1]

While COVID-19 has impacted many enterprises' ability to invest in anything more than the basics, it has also put into sharp focus IoT's possibilities to better support their employees and customers and create new safety and monitoring applications. IDC states that "enterprises are coming to terms with the current situation and looking for innovative ways to support their disrupted and distributed workforce, customers, and partners, and IoT will play an important role as organizations continue along the journey to recovery and the 'next' normal."[2]

Serving health with IoT

When the COVID-19 pandemic hit, Ignite Brewing Co. was already successfully using an IoT platform built on Microsoft® Azure® to monitor the temperature of beverage coolers and other critical components and take quick action on the information they collected. Ignite decided to use IoT to protect the health of customers and staff, and to help prevent spread of the virus. The brewery worked with Insight to quickly implement a thermal imaging solution. Integrated thermal cameras automate temperature checks for up to 30 guests at once. In the event an elevated temperature is detected, discreet, real-time alerts are securely sent through the IoT platform, and custom workflows help protect privacy, minimizing data collection and delivering notifications only to appropriate parties.

Before any IoT project gets underway, it is necessary to evaluate and thoroughly understand the project's technical and business goals, its expected Return on Investment (ROI), and how the IoT project might evolve in your enterprise. You also need to consider the impact IoT will have on your IT infrastructure — including the network, compute resources, security, storage, and data protection — the downstream consequences, and the challenges that may arise.

It's also critical that a designated team within IT oversees IoT projects within the organization. All too often, IoT projects get their start more like DIY endeavors initiated by lines of business. But much like shadow IT, these disparate and fragmented IoT projects can incur data leaks, potential compliance violations, and more.

Centralizing control and formalizing evaluation and planning to determine the right technologies for your project, combined with a flexible and scalable platform, will ensure your IoT initiative does what it's supposed to do: help you respond smarter and faster to ever-changing business conditions.

There needs to be close coordination with IT operations to prepare the data center and infrastructure, including identifying any legacy devices that might be folded into the IoT initiative, such as SCADA systems or other devices that might need an IP address. Make sure you have the right domain expertise working on the right portion of the project, throughout the lifecycle. Not only does the IoT team need to coordinate with IT operations, but also developers and operations need to work together. Assumptions are often made in a lab, during development, but those assumptions can be significantly challenged when devices are actually deployed into production, out in the field.

Know your IoT devices

Once you've established design goals and defined a strategy that includes specifics about each use case, you need to determine the technologies that will best meet your needs. Here's a basic checklist to consider as you evaluate IoT devices:

- Are the devices built for the environment in which they will operate? For example, are they hardened for industrial use?
- Do they support industry standard protocols?
- Will they have actuators that can do something when instructed by sensors detecting changes, such as a rise in temperature, in the environment?
- Will the devices need to conduct any processing at the point of data collection? For example, will the devices only need to connect and transmit data? Or does the use case require intelligent devices that include a Microcontroller Unit (MCU) so they can compute and perform simple tasks, or a Microprocessor Unit (MPU) for more complex functions?
- How will they be powered?
- What are their connectivity requirements?
- What type of security do the devices feature?

Meaningful IoT outcomes at the edge

When data needs to be collected out in the field, and the information gathered is critical to safety and security, IoT processing at the edge can make all the difference. That's exactly what a railroad company did to enhance maintenance and prevent accidents. A drone-based imaging solution, created by Insight and built on Microsoft Azure, takes images from thousands of miles of track, processes and analyzes the video at the edge, initiates real-time alerts, and then prioritizes images to be sent to a cloud data platform for further analysis and escalation to track inspectors. Workers can then investigate and, if needed, initiate maintenance.

The wild west of industry standard IoT

Because there are so many IoT devices and sensors on the market, it's easy to end up with incompatibilities, especially if IoT projects are deployed individually, in silos. To avoid incompatibilities, it's preferred to define best practices that call for industry standard protocols. The various protocols that make up an IoT system architecture enable communications between devices, devices and gateways, and gateways to data centers or cloud, as well as communication between data centers.

Turning IoT data into intelligence in the cloud

Newcrest Mining Limited is using an intelligent IoT solution to save money and improve productivity. The solution, built on Microsoft Azure, helps the Australian company track and predict crushed ore in underground bins that feed crushers above ground running around the clock. Insight worked with Newcrest and its partners to create advanced analytics in the cloud that take advantage of hundreds of thousands of data points and a data lake. The solution can predict the level of ore in the bin with 85% accuracy, saving Newcrest millions of dollars, reducing downtime, and boosting productivity.

Standards in the communication channel, designed to enable devices to connect within a specified environment, include:

Bluetooth® Low Energy (BLE)

Like Bluetooth, BLE works with a variety of mobile operating systems for consumer electronics because it is low cost and reduces power consumption, extending the life of the connected device's battery.

Long-Term Evolution (LTE)

A wireless broadband communication standard for mobile devices and data terminals, LTE increases the capacity and speed of wireless networks and supports multicast and broadcast streams.

Near Field Communication (NFC)

Enables two devices to communicate within four centimeters of each other, so it's ideal for contactless mobile payments, ticketing, and smart cards.

Radio Frequency Identification (RFID)

Available as passive (powered by a nearby reader) or active (powered by a battery), these tags transmit digital data such as an identifying inventory number.

Keys to resiliency: Networks, compute resources, security, storage, and data protection

Networks

Because there is such a diversity in the types of IoT devices and their communications requirements, network architects need to consider a variety of variables for power, bandwidth, and reliability, as well as cost and security.

Arguably some of the most critical network requirements for IoT revolve around scalability. Will your network be able to support continuously growing numbers of heterogenous IoT elements? What starts out as only 1,000 devices today can double or triple in no time. Low-cost connectivity will be necessary.

Networks also need to be highly reliable to overcome any potential signal interference and network degradation. The networks will need to provide secure traffic flows. For highly sensitive or mission-critical applications, you may need to establish failover links.

There are numerous networks that can support IoT. Popular, low-power, short-range networks include Bluetooth, which supports voice and data signals up to 10 meters, and Zigbee, ideal for things like tracking medical devices using small, low-power, low-bandwidth IoT devices in close range.

Low-power, wide-area networks include low-cost Cat-0 LTE networks, CAT-1 cellular IoT networks that will eventually replace 3G, and LTE Cat-M1, which is fully compatible with LTE networks. There's also LoRa®, which is gaining traction around the world and is designed to enable data communication over a long range while using very little power, as well as the newer cellular protocols 4G LTE and 5G.

As 5G networks become more pervasive, expect even wider adoption of IoT. That's because the high-speed wireless technology offers high capacity and low latency, supporting much larger volumes of data, connectivity to many more devices, and faster download speeds and response time across mobile networks. 5G will particularly benefit those IoT applications that require data to traverse very long distances; think IoT monitoring key systems on a pipeline.

Compute resources

As your IoT project plans take shape, you need to determine how much compute power you'll need, and where it should reside. In addition, moving away from the traditional data center compute model to the concept of centers of data, and IoT implementations will only further this shift. As you roll out your IoT device and architect the most efficient networking strategy, you'll need to consider what IoT data will be most relevant to your goals. Will that data be filtered and processed out in the field, back on-premises, or in the cloud? Or will you end up with a hybrid model of all these options? Whichever way works best, for an IoT project that's able to scale, you'll need to architect a plan that moves the data from each device to an aggregation site, and that site will need the necessary capacity.

There are numerous products available for processing IoT data at the edge. Inexpensive systems can do the job but may not be powerful enough for video or complex analytics. Newer GPUs are much more powerful and enable PCs, laptops, and servers to effectively and more easily handle videos and other complex, intensive processes.

Using cloud rather than on-premises infrastructure ultimately becomes a financial decision. As you weigh the options, remember to consider your data requirements. If your IoT implementation will generate tons of data, and that data isn't well managed, a public cloud option could become costly.

A critical factor in planning your IoT compute resources will be how to allocate and manage all of it day to day. Initially, take a consultative approach to determine how long you need to keep all your IoT data. Consider any regulations you must comply with, and how the inherent value of some data may not be initially understood but may be extremely important at a later date.

Security

Security is vital. IoT devices, often spread far and wide across an enterprise network, are in effect entry points for any potential attack, so businesses and IT security professionals must be vigilant. Just as you need to leverage scalable networking, your security must also scale with the IoT implementation.

According to a report about IoT security from security firm Kaspersky, nearly a third (28%) of companies with IoT systems faced attacks targeting internet-connected devices in 2019. In the first half of 2019, Kaspersky researchers detected 105 million attacks on IoT devices through honeypots — controlled, safe environments used to lure cyberattackers and expose vulnerabilities.

Industrial IoT (IIoT), which includes such use cases as remote monitoring and control of critical infrastructure such as energy grids, may need even more hardened security. Some are exploring the use of blockchain or Distributed Ledger Technology (DLT), although that technology is still in the early stages of development. An Industrial Internet Consortium paper notes that blockchain could help overcome challenges around provisioning, usage tracing, and asset decommissioning, and could enable tamper-proof chain of custody, as well as trace important events and structural changes in a heterogeneous IIoT ecosystem.

Storage and data protection

The primary function of an IoT device is to collect data and pass it along, resulting in a lot more data. How do you store it all and make sure it's available for processing, whether at the edge, in a data lake, or elsewhere? How do you protect and secure all the data? Fortunately, the sky is the limit for securely storing data at the edge — in everything from a simple SD card to a wide variety of storage arrays.

You have to evolve your data protection and storage strategies, and that includes protecting IoT data while in storage and strengthening backup and recovery. Simply backing up all the data won't be enough — you have to also be able to recover it.

If there are transport constraints or insights are needed where the data is collected, traditional data center practices and technologies won't necessarily work. For example, environments at the edge are often hostile, so hardened systems are needed. You also need to lock down access controls, so only the people who are supposed to see the data and insights can see them.

Underpinnings of a connected IoT platform

More and more enterprises are looking to IoT platforms to help them launch and build IoT projects. The goal of an IoT platform is to provide a single service for managing all the hardware and software protocols, integrate security and authentication, and provide user interfaces. IoT platforms can include gateways, cloud infrastructure, device management, Application Programming Interfaces (APIs), and an ecosystem of integrated third-party apps.

Creating a single view for a comprehensive solution

With an integrated platform, organizations can manage multiple IoT devices that are interconnected to deliver a comprehensive service. For example, Insight and BeSafe Technologies have partnered to create an IoT-enabled alert and emergency response system built on the Microsoft Azure platform. With this single service, a school system can aggregate information such as virtual digital twins of floor plans and monitor staff and facilities by pulling data from cameras, motion sensors, and alarms — all from a single view. The platform also can send automated and real-time alerts in the event of an emergency and provide real-time access to information to third parties, such as police, fire, and emergency medical personnel so they can accelerate response times and save lives.

When your numerous IoT devices are scattered broadly, collecting copious amounts of data and streaming that data across the network, gateways are crucial. These essentially hardened PCs collect the data from IoT devices and process it at the edge before sending it on to the data center or a private or public cloud, depending on preference and how you've set it up.

Of course, not all of the data will need to be sent on, so the IoT implementation will need to include efficient ways to store the data. For example, in an IIoT application on an oil rig, some of the real-time information collected might be consumed on-site, so secure storage will be needed.

Gateways also can prolong the battery life of devices, protect data as it travels, lower latency, and reduce transmission sizes.

Get started with Insight

Now that IoT has proven its worth in numerous PoC projects — and even in enterprise-wide projects — it may be the right time for your organization to get started. As you begin, though, remember to consider the impact IoT will have on the technologies and processes throughout your IT environment. Be sure to thoroughly assess the technical and business goals, expected ROI, and the IoT project's evolution. Designate an IoT team to spearhead the work and be sure to include business and technology leaders who will collaborate with others across your organization to ensure IoT delivers. Insight is ready to partner with your organization to help you lay the groundwork for an IoT implementation that is ready to scale for future needs, minimizes development costs and risks, and will quicken the time to value of new business solutions from years down to months.

Review the following related resources:

You can visit the links below to learn more about how Insight can help you on your path to practical, transformative IoT.

- Solution brief: Insight Connected Platform for Detection and Prevention
- Webcast: Providing Secure Infrastructure for the Future of IoT
- Webcast: Securing the Edge: Connectivity, Access, and Security in a Dispersed Environment
- Webcast: Intelligence and Innovation at the Edge: Effective Compute for IoT
- Webcast: How to Handle Dispersed Data: IoT-Specific Data Storage Considerations
- Webcast: IT Considerations for IoT Deployment: Devices, Data, Connectivity, Security, and More
- Webpage: Security and Networking Solutions for the Internet of Things (IoT)

[1] IDC. (2020, July 27). IoT Growth Demands Rethink of Long-Term Storage Strategies, says IDC.

[2] Dickson, F. and Richmond, C. (May 2020). COVID-19 Impact on IT Spending Survey: Expectations for Increased Security Spend Due to COVID-19 Have Waned. IDC.

Meaningful solutions driving business outcomes

We help our clients modernize and secure critical platforms to transform IT. We believe data is a key driver, hybrid models are accelerators, and secure networks are well integrated. Our end-to-end services empower companies to effectively leverage technology solutions to overcome challenges, support growth and innovation, reduce risk, and transform the business.

Learn more at:
insightCDCT.com | insight.com