CompTIA

GUIDE

The Six Layers of an IoT Solution

Contents

Introduction

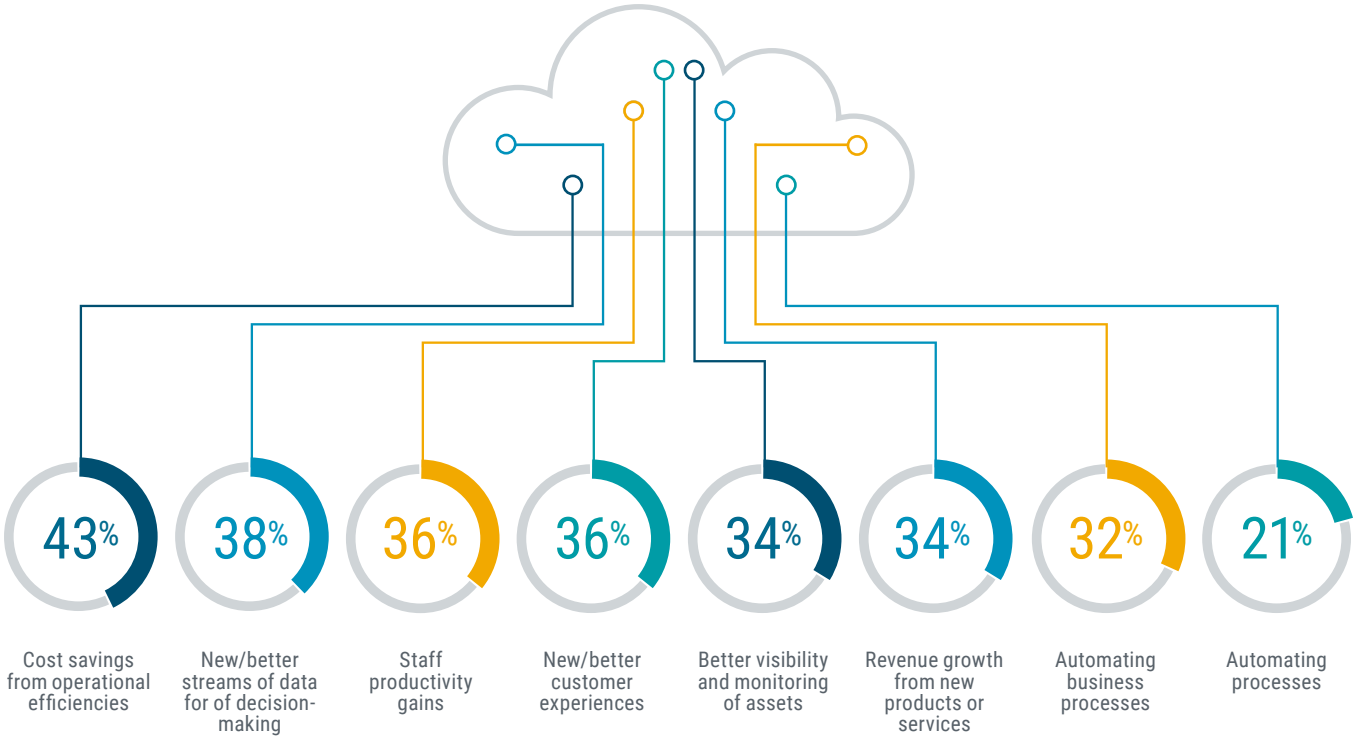
When people think of the internet of things (IoT), they think of a smart device or sensor, but if you want to build an IoT solution, there are six layers that must be considered. Each layer has its own requirements and considerations as well as security ramifications to achieve successful business outcomes and ensure data privacy and compliance. In this guide, the CompTIA IoT Advisory Council has broken these layers down to help enterprise CIOs, IT solution providers, and aspiring IT practitioners understand IoT solutions holistically.

What is IoT?

IoT is the practice of interconnecting the physical world with digital world through the use of sensors to provide data insights. Every physical object can now become a digital device, able to capture data, perform computations, and connect to a network.

IoT applications can be described as using things—or devices—to collect data or events that are then used to generate insights, which typically translate into actions implemented to help improve a business or process. An example is an engine (a thing) sending pressure and temperature data used to determine if the engine is performing as expected (an insight), which is then used to proactively schedule maintenance on the engine (an action). Ultimately, the implementation of IoT can help businesses achieve myriad benefits, from improved productivity and increased revenues to insights into how customers are using products.

Potential Benefits of IoT



Layer 1: IoT Devices

IoT devices are the "things" of IoT. They are the physical presence of the IoT system. IoT devices are as diverse as their applications. They can be incredibly small, low-powered devices that perform limited functionality, such as a temperature monitor. They can also be large, high-powered equipment that collects, processes, and transmits multiple types of data, such as an autonomous vehicle.

The use case of the IoT system dictates the design of the device. Whereas the design of other parts of the system, such as the data management solution, may be driven by cost or organizational systems already in place, the design of the device is tightly coupled to the application. It is strongly recommended that solutions are tested from end-to-end to ensure the desired outcome is achieved. Several factors can impact the data quality for each scenario, which in turn could impact business outcomes.

According to IoT Analytics, the number of connected devices that are in use worldwide exceeds 17 billion, with the number of IoT devices at 7 billion. The number of IoT devices that are active is expected to grow to 22 billion by 2025.

IoT Device Components

5 Primary Components of an IoT Device

Some type of sensor to collect data or indicator/actuator to respond to data

The 'brains' of the device

A way to transmit and/or receive data, whether through a physical or wireless connection

All devices need some amount of power, though how much and where they get it from may differ greatly

A way to protect the device from its operational environment

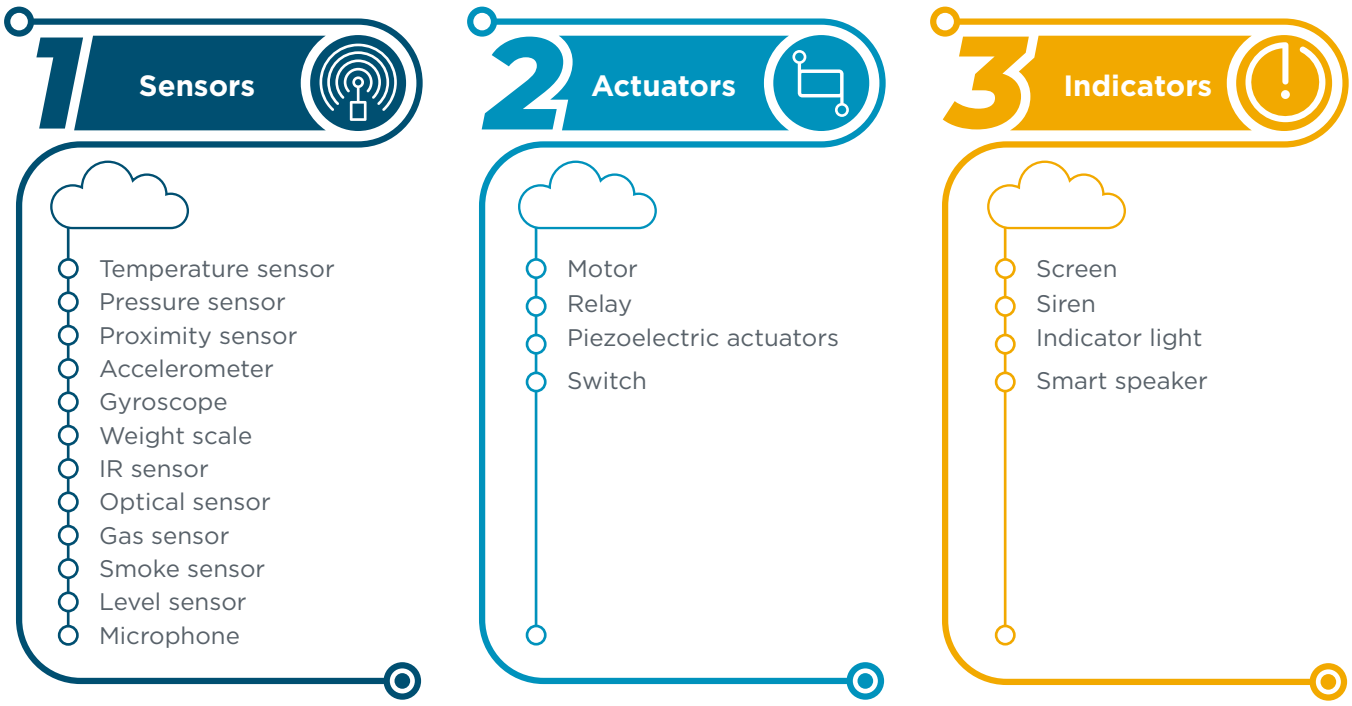
Sensors, Actuators and Indicators

IoT is all about data—collecting it, transmitting it, analyzing it, and acting on it. In order to collect data, you need a sensor. Sensors detect or measure a physical property. They come in a variety of shapes, sizes, and capabilities and can use different methods to detect what they are measuring. For example, there are optical sensors, electrical sensors, and chemical sensors that can detect a wide range of properties such as light intensity, temperature, weight, or salinity.

To automate physical action in response to data, you need an actuator or indicator. Actuators take electrical information and transform it into physical activity to move or control a mechanism, such as a relay or motor. Indicators, like a screen or an LED indicator, display the state of something. They also come in a wide variety of shapes, sizes, and capabilities and can use different methods to take action or display information. For example, actuators could be hydraulic, pneumatic, electric, thermal, magnetic, or mechanical. Indicators could be visual (like a screen) or auditory (like a warning siren).

Sensors, actuators and indicators are not inherently application specific, as the same one could be used for a variety of applications. For example, a temperature sensor may be a critical component in an industrial IoT device to monitor an engine and inform a preventative maintenance system. That same sensor could monitor patient temperature in a telemedicine application or soil temperature in an agricultural automation application.

Examples of Sensors, Actuators and Indicators

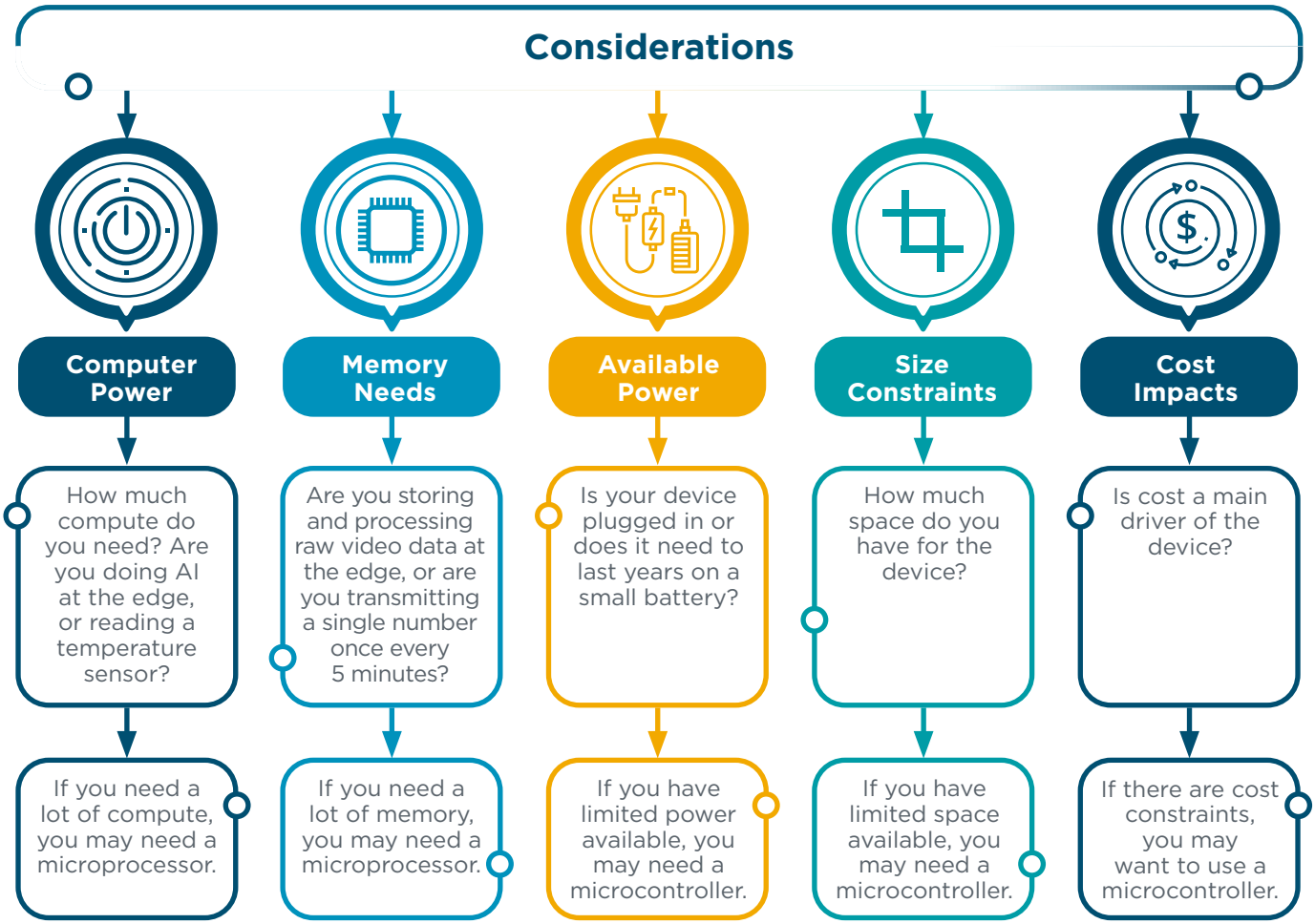


Device Compute

IoT devices need some amount of on-board compute in order to collect, store, and transmit data—how much you need depends on the application. It is important to match the level of compute to your application needs. If your device does not have enough compute power, it will perform poorly. If your device has more compute power than required, it will be larger, use more power, and cost more than required.

At a high level, there are two different compute choices: microcontrollers and microprocessors. They each have different capabilities and corresponding design requirements. In general, microcontrollers have less compute and memory, but need less power, and are cheaper and smaller than microprocessors. We discuss device compute considerations more in the section, Layer 2: Edge Computing.

Do You Need a Microcontroller or a Microprocessor?



Data Connectivity

Every IoT device needs a way to transport data from the device to the data management location, which could be in the cloud or at a data center. This can be done with a physical connection (such as ethernet, electrical cable, or a fiber optic cable) or a wireless connection (such as WiFi, BLE, cellular, or a wireless optical modem).

The best connectivity option for your IT solution depends on many factors, including available power, transmission range, volume of data, and latency requirements. Connectivity considerations are detailed in the section, Layer 3: Connectivity & Data Transport.

Device Power

Every IoT device will need some amount of energy to power its compute, sensors or actuators/indicators, and data transport. It is important to understand the power needs of your device in order to provide the appropriate amounts and types of power, as well as plan for interruptions to power. The biggest question is if your device will be plugged into a power source or if it will need to have a battery. If your device can be plugged into a reliable power source it can remove significant power constraints on your system, but you still have many things to think about, including:

- **Cable robustness:** Will the power cable get damaged by being run over? Chewed on by animals? Exposed to UV and ice?
- **Power transformation:** Often times wall power is provided as AC. You may need to rectify and step down the voltage to power your device. It will be critical to know what voltage and current levels are required by your device and provided by your power source.
- **Power interruption:** What happens when your device gets disconnected from the power source? How does the device get repowered?

If your device does not have access to wall power, you will need to consider alternative ways to power it, such as batteries, solar panels, or piezoelectric generators. It will be critical to understand the power needs of your device to right size the power solution. Aspects that influence the power needs of your device include:

- **Lifetime of device:** How long should the device be operational before needing to be recharged or have its battery replaced?
- **Connection frequency:** How often are you connecting to your data management system and how much data are you sending?
- **Peak power draw of components:** Components like radios can have significantly higher peak power draw than their nominal readings. You'll need to be sure your power supply can handle the peak load and understand its impact on battery life.

On top of being vigilant about power usage, you will need to think about how often the power source will need to be repaired or replaced, how that process works, how to protect the power solution (will the solar panels get covered in dust? Will the battery overheat?), and what happens when power runs out or during a battery replacement.

Device Housing

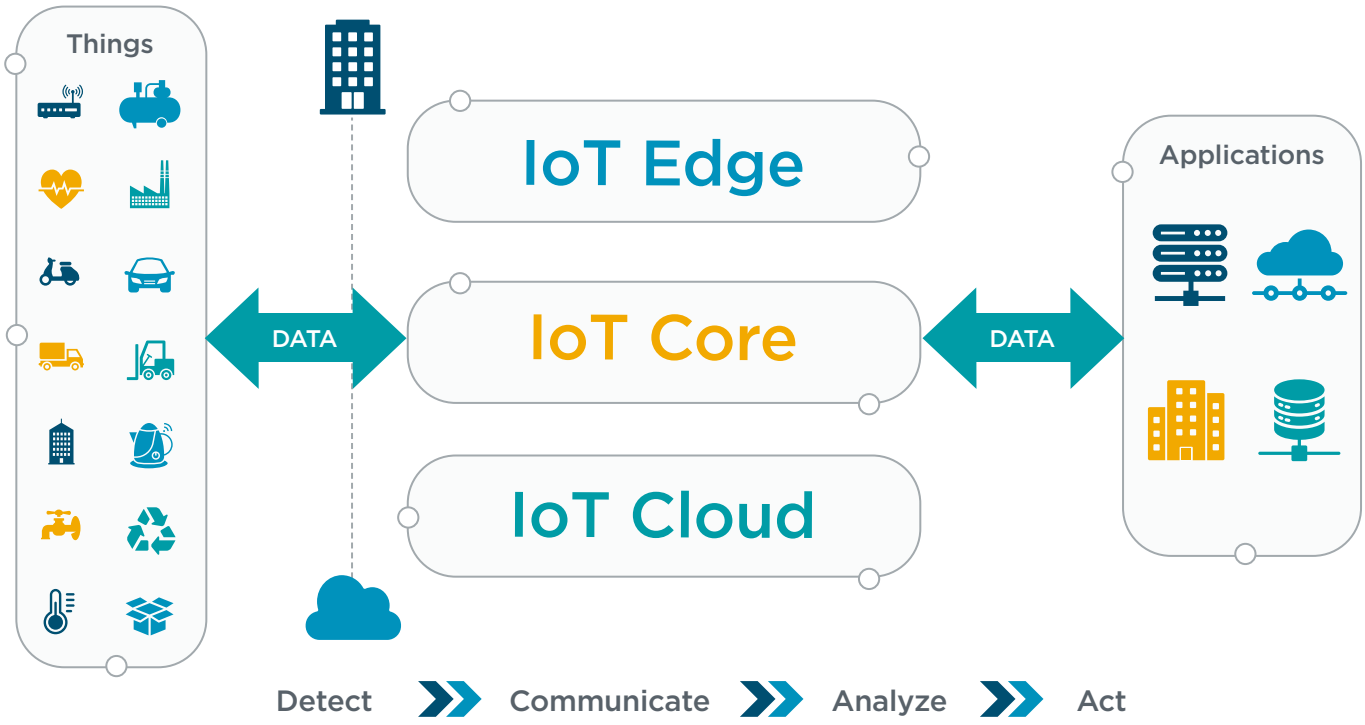
Many IoT devices are deployed to prevent the need for humans to risk accessing dangerous environments, which means devices need to operate in harsh environments. The components that make up an IoT device often have narrow operating parameters and can be easily affected by heat, water, or vibration. Great care and attention should be paid to how the IoT device is housed in order to protect it from its environment. A breadboard solution may work well on a lab bench but will fail quickly in the field. To choose the right housing for a device, you need to know where it is intended to be used; what the normal environmental factors will be in that area; what extremes it might face; and how long it will live there. Things to consider about the environment are:

- **Temperature:** Even in a controlled environment like in a house, the temperature can vary greatly. Uncontrolled environments, such as the outdoors, or industrial environments, such as a freezer or an oven, can be more extreme. Housing that provides thermal insulation is crucial to reliable device operation.
- **Humidity/moisture:** Whether the device needs to survive regular power washing or operate in a steam sauna, appropriate housing can protect against ingress from vapor and liquids that could impact operation.
- **Chemicals:** Appropriate housings must be considered for devices that will be exposed to harsh chemicals. This isn't confined to industrial applications. Consumer devices may need to survive being disinfected with cleaning detergents like bleach.
- **UV:** Devices that must operate outside may have to withstand UV radiation from the sun. Even if it isn't outside, devices may be affected by other sources of UV radiation.
- **Mechanical stresses:** Vibration, shock, and pressure can all adversely affect the operation of electronics. Appropriate housing can help protect an IoT device.

Layer 2: Edge Computing

Edge computing is not always required in IoT solution deployments but can offer several benefits for the right use cases. First, it's important to understand the basics of edge computing. The **edge** refers to the physical location where things and people connect with the digital world. **Edge computing** is part of a distributed computing topology in which information processing is located close to the edge—where things and people produce or consume that information. **Core** is a centralized IoT hub that can be used to collect and aggregate data across multiple edge endpoints.

Is Edge Computing Right for My IoT Solution?



Edge Computing

Edge computing is a distributed computing framework that brings computation and data analytics closer to the source of the data. In the case of IoT that source of data is the sensor.

IoT edges are network hubs that often combine OT data and IT data. These IoT edges are often undermanaged because the responsibility is based in the OT organization and the IT organization. IT edges are common in the telecommunications and media industries for distributed data transfer and processing, as well as distributed computing in branch offices and campuses.

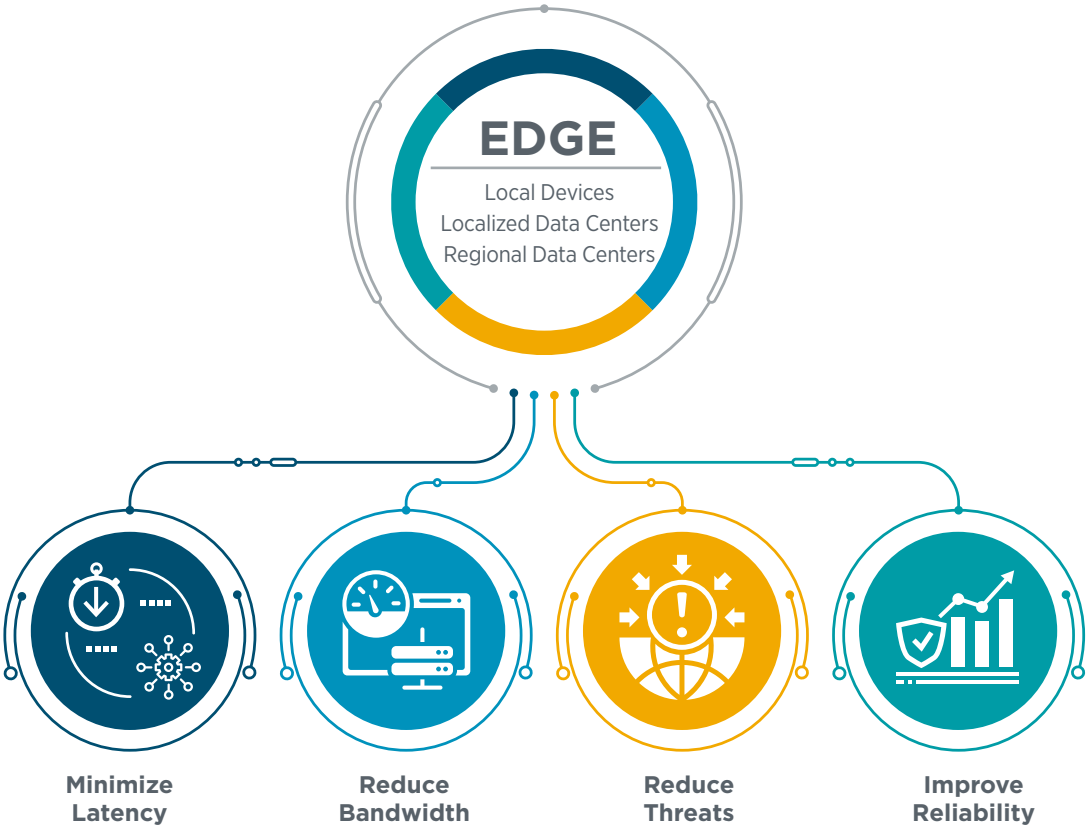
The edge layer includes:

- Large volume real-time data processing
- At-source/on-premises data visualization
- Industrial control systems
- Embedded systems
- Gateways
- Micro data storage

Regardless of the number of layers in your hierarchy, they generally fall within three primary categories:

- **Embedded edge:** Device, sensor, or peripheral that is typically the source of raw data.
- **Gateway edge:** Collector and aggregator of data from multiple peripherals or other gateways.
- **Network edge:** Bridge between the local network and the external internet.

4 Key Benefits of Edge Computing



Edge computing will help you realize the following benefits with your IoT solution:

- **Minimize latency:** There are many applications that require immediate insight and control. For some mission-critical functions, compute must take place at the edge because any latency is intolerable.
- **Reduce bandwidth:** In situations where wireless, i.e., metered, service is the only connectivity option, sending large amounts of data back and forth from things to the cloud can consume enormous bandwidth and greatly increase costs. Edge computing is the most effective solution to this problem.
- **Reduce threats:** When you transfer data across geographies, it is more prone to attacks and breaches. Processing data at the edge can reduce security vulnerabilities.
- **Improve reliability:** Even without any nefarious activity from hackers, data can be corrupted on its own. Retries, drops, and missed connections will plague edge-to-data-center communications.

Layer 3: Connectivity & Data Transport

IoT connectivity is the actual collection and transfer of data between devices and/or systems over a data connection. There are many choices when it comes to connectivity, and the application of your IoT solution will drive the decision.

Connectivity Considerations

There are several facets of connectivity that must be understood and considered as best practices to ensure an efficiently built and successful IoT project. Choosing the best connectivity option will make or break the success of your IoT project. Start by answering the following questions.

- What device am I connecting to/from?
- How much data do I need to transfer?
- How much power do I have available in the hardware device to power data transmission?
- Do I have latency requirements for my application?
- Do I have cost considerations?

Connectivity Types

When choosing how to connect an IoT device, you'll want to factor in placement or proximity of the device to a network. There are two types of connectivity you can consider:

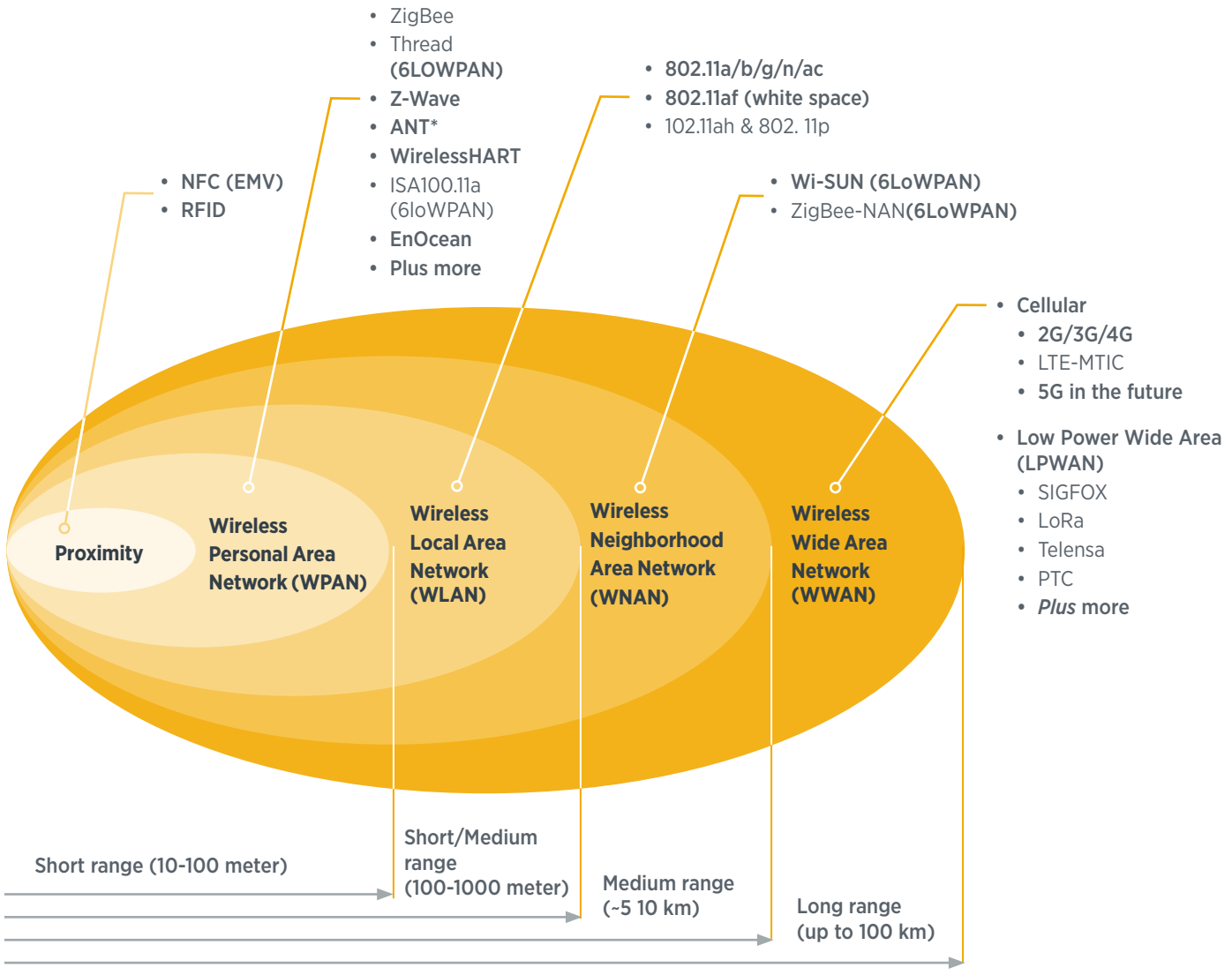
- Short Range – Gateway to Sensor
  - Includes Bluetooth (BLE), Zigbee, Ultra-Wideband, WiFi, LoRa, Z-Wave
- Wide Area Network (WAN) – Gateway to Cloud
  - Include 4G/LTE, 5G, Sigfox, Satcom, Wired Connection

Technology Selection Criteria

Selecting technology should be based on the following factors: range, latency, data throughput, fixed or mobile, and licensed or unlicensed connectivity. The considerations for each are included below.

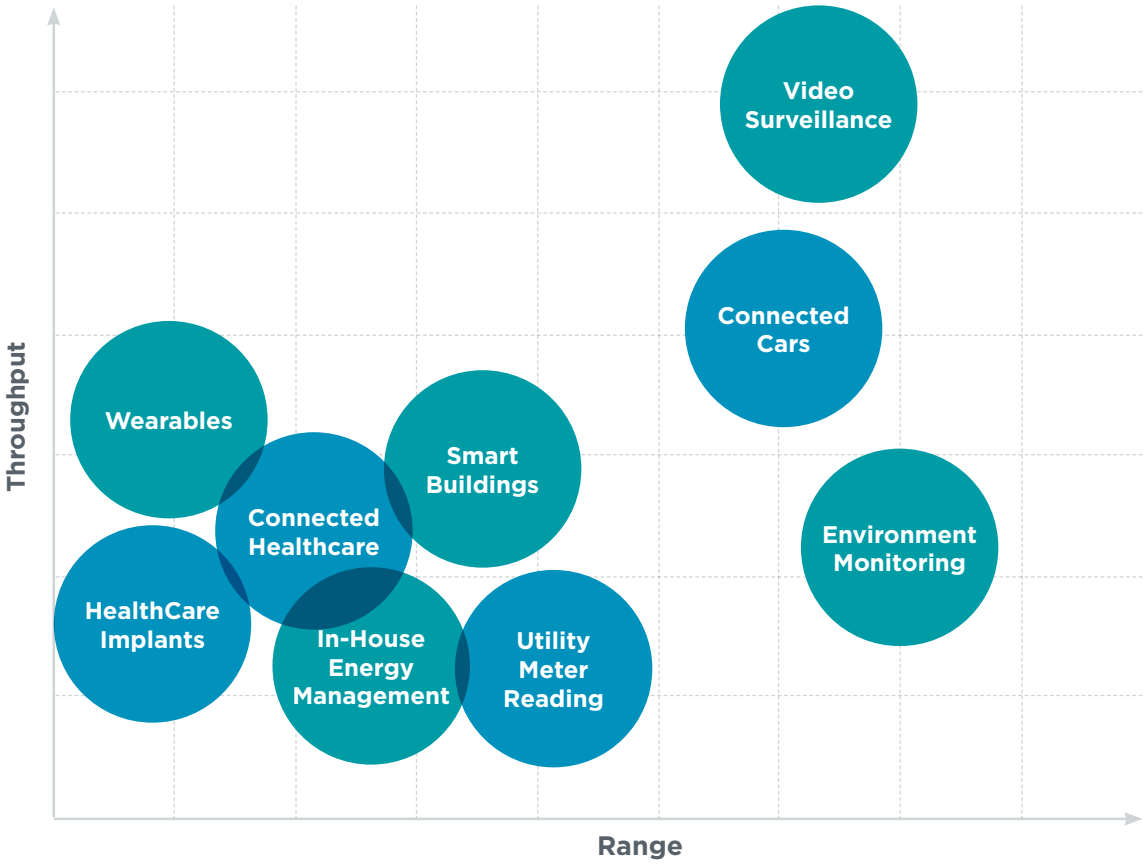
Range

- Target technology should be based upon the nature of the IoT application.
- Range affects throughput, power, and other considerations.
- If transport technology can be localized, costs can be reduced.
  - Example: Metered cellular vs. ethernet
- WWAN - universality
  - Example: Different bands by country can lead to multiple SKUs.
- Deployment density
  - Example: The number of devices by zone may lead to the selection of lower range technology due to device conflicts



Data Throughput

- Based on the use case of the final deployment, multiple technologies may be required.
- Range can affect throughput.
- Throughput may drive costs of edge modules.
- Throughput affects the selection of protocol and network technology.
- Future considerations, projects, or features may drive higher throughput requirements.
- Overhead needs to be considered for highly secure deployments.



Latency

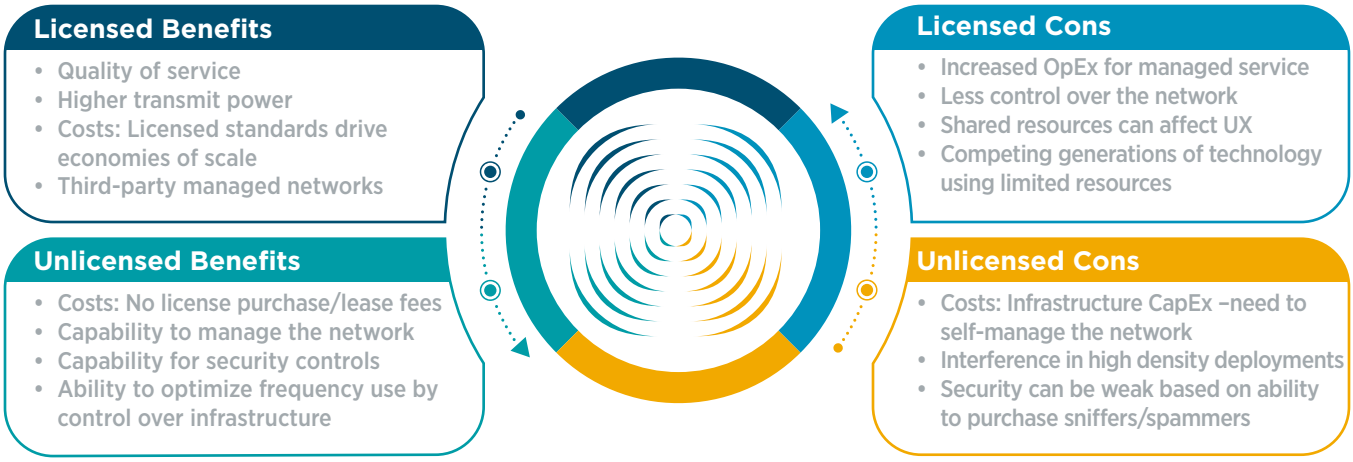
- How important is latency for the application?
  - Email – minutes is fine
  - Self-driving car – seconds could cause death
- How critical is your application?
  - Patient monitoring, fire alarm
  - Hygrometer in a garden, BBQ temperature sensor
- Do you require specific IP addressing needs?
  - Private IP drives control and security but has additional latency.
  - Public IP is geographically optimized reducing latency.
- What range do you require?
  - A higher range means higher latency.

Fixed or Mobile

- Fixed wireless:
  - Point on a map coverage
- Mobile:
  - No single network carrier can guarantee 100% nationwide LTE coverage.
  - Partnerships and cross-carrier collaboration can be required based on use case and geography.

Licensed/Unlicensed Spectrum

Licensed spectrum devices operate within the portion of the radio spectrum designated by the FCC to be reserved for organizations that have been granted licenses. The FCC provides legal protection and enforcement to prevent other operators from transmitting over the same frequency in the same geographic area. Unlicensed spectrum users are competing with other users for priority. As an unlicensed user, you have no protection from interference on the part of other parties. In addition, Part 15 of the FCC regulations limits the time-on-air of most unlicensed transmissions to .4 seconds (400 milliseconds).



Layer 4: IoT Platforms

An IoT platform is the fabric that pulls all the components of the IoT stack together. When selecting a platform, keep in mind that no single universal platform exists today fits all needs. Take some time to evaluate all the considerations brought forth in this document to help drive your selection and approach. Evaluate your options from different perspectives, such as looking at the solution from a vertical or horizontal view.

There is no one-size-fits-all approach to IoT platforms. There are numerous considerations for proper technology selection, and customizability to the use case is key. The right IoT platform should bring many benefits, including:

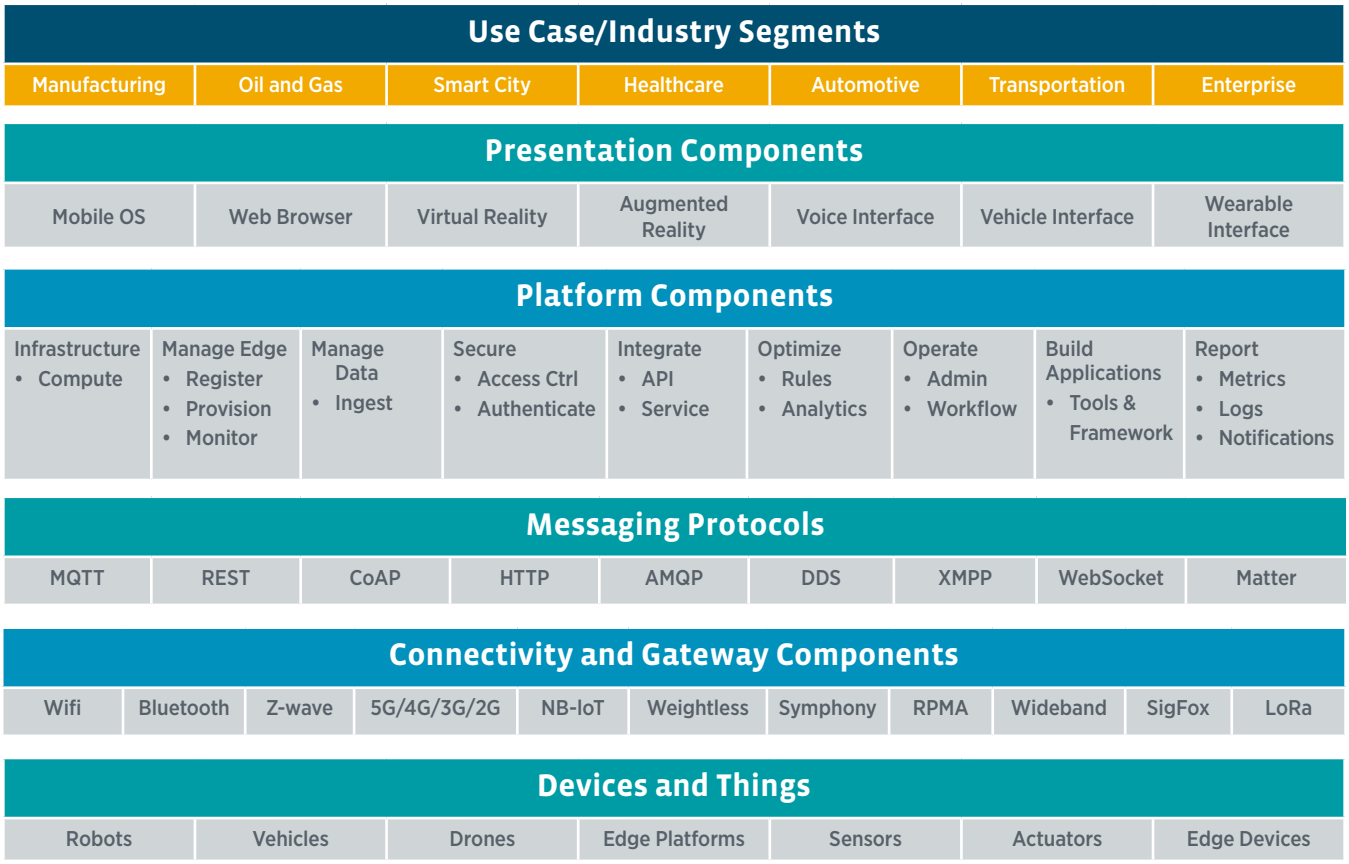
- Connect hardware, such as sensors and devices.
- Handle different hardware and software communication protocols.
- Provide security and authentication for devices and users.
- Collect, visualize, and analyze data the sensors and devices gather.
- Integrate all the above with existing business systems, applications, and other web services.

Once you've considered the components earlier in this guide, these decisions will drive your selection of a platform. Ask yourself:

- What do you want to integrate?
- What does your future look like?
- Where are you going?

According to IoT Analytics, 50% of all profiled IoT platform companies now have a dedicated focus on manufacturing/industrial use.

Typical IOT Platform Components



These are other decisions you should make to guide your direction in selecting an IoT platform. These include:

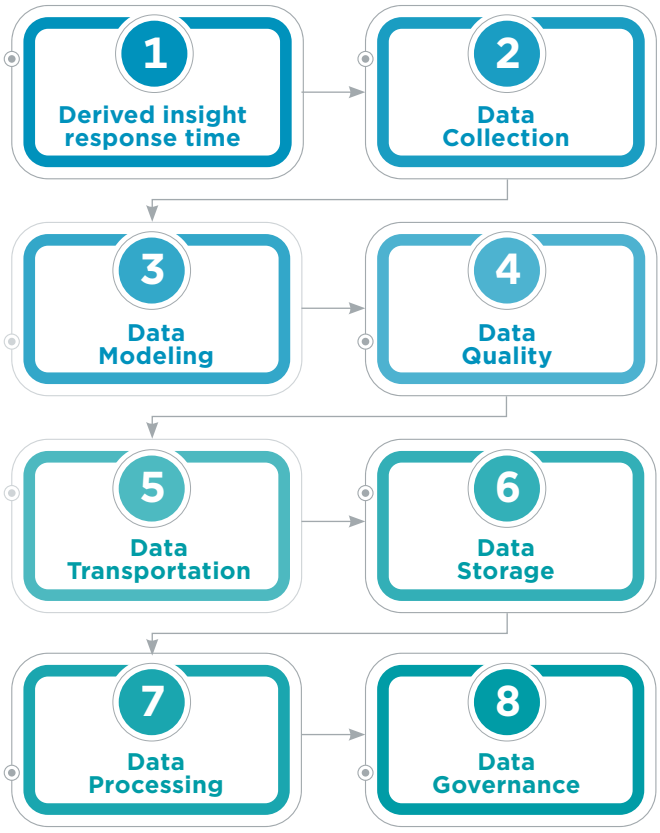
- What is the context (i.e., identify a use case)?
  - Indoor/outdoor
  - Public/private spaces
  - Hazardous area? High-risk factors? Safety controls? Access controls?
- The aspects of a platform:
  - Device and things
  - Connectivity
  - Interaction layer/visualization
  - Information delivery/messaging
  - Storage
- Uptime management and outage remediation
  - What is our uptime requirement? Five 9's or less demanding?
  - How quickly do we need to know about an outage?
  - How quickly do we need to respond to an outage?
  - Who is responsible for identifying and resolving outages?

Layer 5: Data Management

The value of data is at the heart of every IoT solution. This is what drives decisions, creates revenue, reduces cost, and improves quality. There are several planning steps and governance strategies that need to be incorporated into your IoT data management model.

In this section, we cover the necessary functions to ensure the data is being accurately represented, including the governance process for acquiring data, how to secure the data and the teams that need to be involved throughout the process.

8 IoT Data Planning Steps



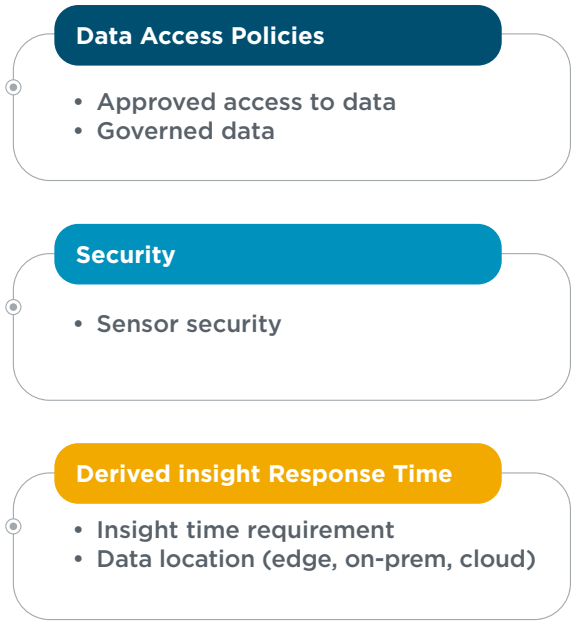
1. **Derived insight response time:** The first step in planning your IoT data strategy is understanding how quickly you need insight from the sensor. This step will help determine what supporting infrastructure you will need to meet your insight requirement. This includes data collection timing, quality, processing impacts. It will also impact your infrastructure choices such as connectivity protocols and battery life.
2. **Data collection:** Data comes from multiple sensors and sensor types. Some of this data will need to be integrated into other systems. IoT often serves as the nucleus to integrate data from multiple sources. IoT data will need to be modeled to achieve your desired outcome.
3. **Data modeling:** Data modeling is necessary to normalize this data across all platforms and sensor groups.
4. **Data quality:** IoT data is often time sensitive. The lifespan of sensor needs to be monitored to ensure time sensitive and reliable data is being captured and delivered. Sensor failures can impact data quality.
5. **Data transport:** Data transport can impact the ROI of your IoT project. It's important to determine what data is relevant and what data is revenue. If you can determine what data is merely exhaust, its best to not to transport this data back to your main data store. The more data you transport, the more your solution will cost you in bandwidth, compute, and storage.

6. **Data storage:** There are multiple options in data storage like SQL, NoSQL, Object/Document DB, etc. There are also multiple locations to store and compute data such as the edge, on-prem storage solutions or a cloud solution. The edge device/sensor needs to be monitored to ensure time sensitive and reliable data is being delivered. The next items to consider are how long to store the data and what other groups within your organization can find value in this data. We call these data value beneficiaries or DVBs.
7. **Data processing:** This is where standardization, filtering, and enriching the data occurs. As each solution varies, so will your data processing needs. Latency impact, volume of data, and timing of insight response will impact data processing. Some responses are real time and may need to be processed at the edge, some data sets can be analyzed in the cloud.
8. **Data governance:** The final item to consider is governing the data to ensure validity. The governing model needs to include how the data is captured, if it is integrated or filtered as part of the process. Data definitions are also key to documenting the data parameters for collection, management and reporting purposes.

Data Access

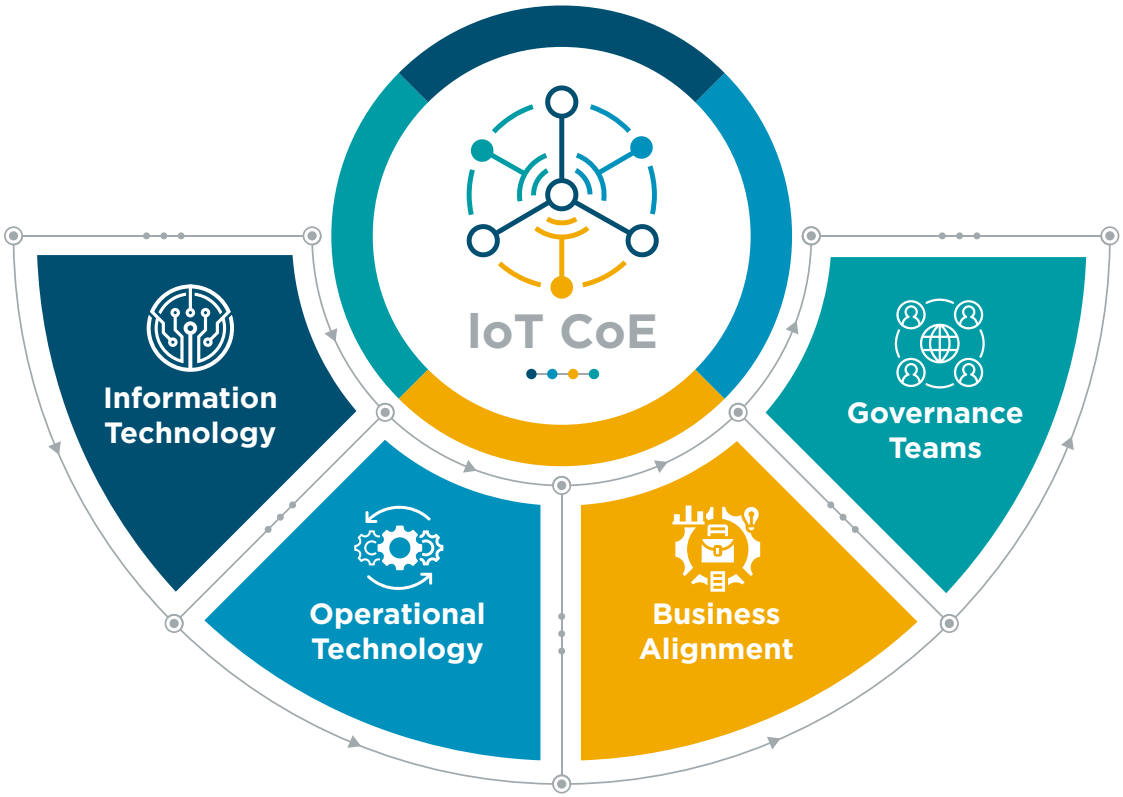
Data upload policies need to address the following considerations:

1. How much of the data being derived from the sensor is relevant to your project? Definition of the intended sensing parameters will help maintain data validity.
2. Thorough investigation and forward thinking are essential to minimize rework. In some cases, other departments may be able to derive valuable insight from this new sensor data. The use cases need to be understood and documented early in the IoT project definition.
3. Data collection security protocols need to be established to ensure that the data received is valid.



IoT Data Governance Stakeholders: Integrating Your Center of Excellence

Cross-practice collaboration between leadership and support teams is essential to drive new revenue streams and create cost-avoidance scenarios.



- **Information Technology and Operational Technology** include IoT liaisons for their respective practices.
- **Business Alignment** includes IoT Center of Excellence liaisons or IoT business analysts.
- **Governance Teams** include data, digital, security, legal, and financial operations.

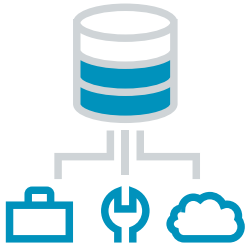
IoT offers a unique benefit to businesses by creating new data streams from previously unconnected assets. As part of the development cycle for IoT projects, it has proved extremely beneficial for organizations to review the new data stream and determine if there are other resources (DVBs) in their organization that can benefit from this new data.

Consider the healthcare industry: As the Internet of Medical Things (IoMT) continues to grow and become more connected, we are seeing more and more people request access to new data. For example, nurses want to know where to find IoT-connected IV pumps; operations wants to know how many IV pumps have recently been used and how many are offline; and facilities wants to know how many need to be purchased, but also need to ensure they are actually necessary. In this scenario, there are three different DVBs for the data derived from IoT-connected IV pumps.

By integrating business units together as part of an IoT Center of Excellence, you can discover additional use cases for these data streams. The key to a successful IoT project is to understand and benefit—specifically in terms of new revenue or cost-avoidance—from the new data streams.

Data Accumulation/Storage

Where is data stored?



- **Edge: Little integration with other systems, single-use insight, minimal need for storage, quick insight is often needed**
- **On-Prem: Heavy integration with local applications, compliance and privacy is often a factor**

How much data should be stored?

- **Determine how much is required to provide insights.**
- **What data is related to business outcomes? Is there value to storing additional sensor data for another team?**
- **Know your data value beneficiaries (DVB).**

Continuous financial planning for data

- **The longer you store data the more it costs. Determine longevity of data with all stakeholders.**

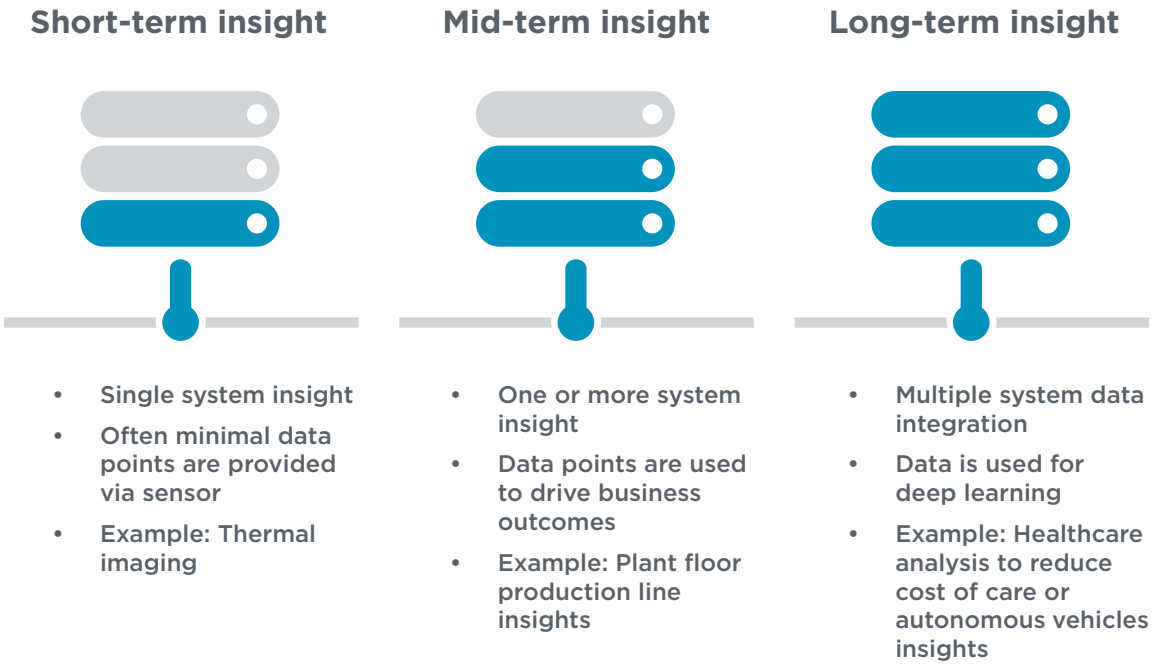
Where is the IoT data stored, how long should it be stored? Is the cloud always the right place to store the data? Not necessarily.

Consider the example of images that come from a moving car or the example of a submarine that collects underwater images. Even a very high-speed internet connection is not good enough to transfer and save the data in real time in the cloud. A local, intermediate storage is required in such scenarios, and then you periodically send filtered data (by preprocessing it, aggregating it, or fusing it) to a central database, which is used for further analysis.

Using intermediate databases is a common strategy in IoT systems. The technology can vary based on the size, type, and speed of the IoT data. When you choose an IoT database, do not start with any preconceived notions. There are multiple options like SQL, NoSQL, Object/Document DB, File Storage, among many others. You can choose one or multiple database technologies based on the storage, access requirements and cost factors.

How much IoT data should be stored? The objective of most IoT systems certainly doesn't include storing precise and predefined datasets. Sometimes the data is not well known before it is stored, and it is fed into unsupervised machine learning algorithms to discover any meaningful patterns. Some amount of redundancy can be allowed, but it should be manageable in terms of disk space requirements.

Data Retention Based on Outcome

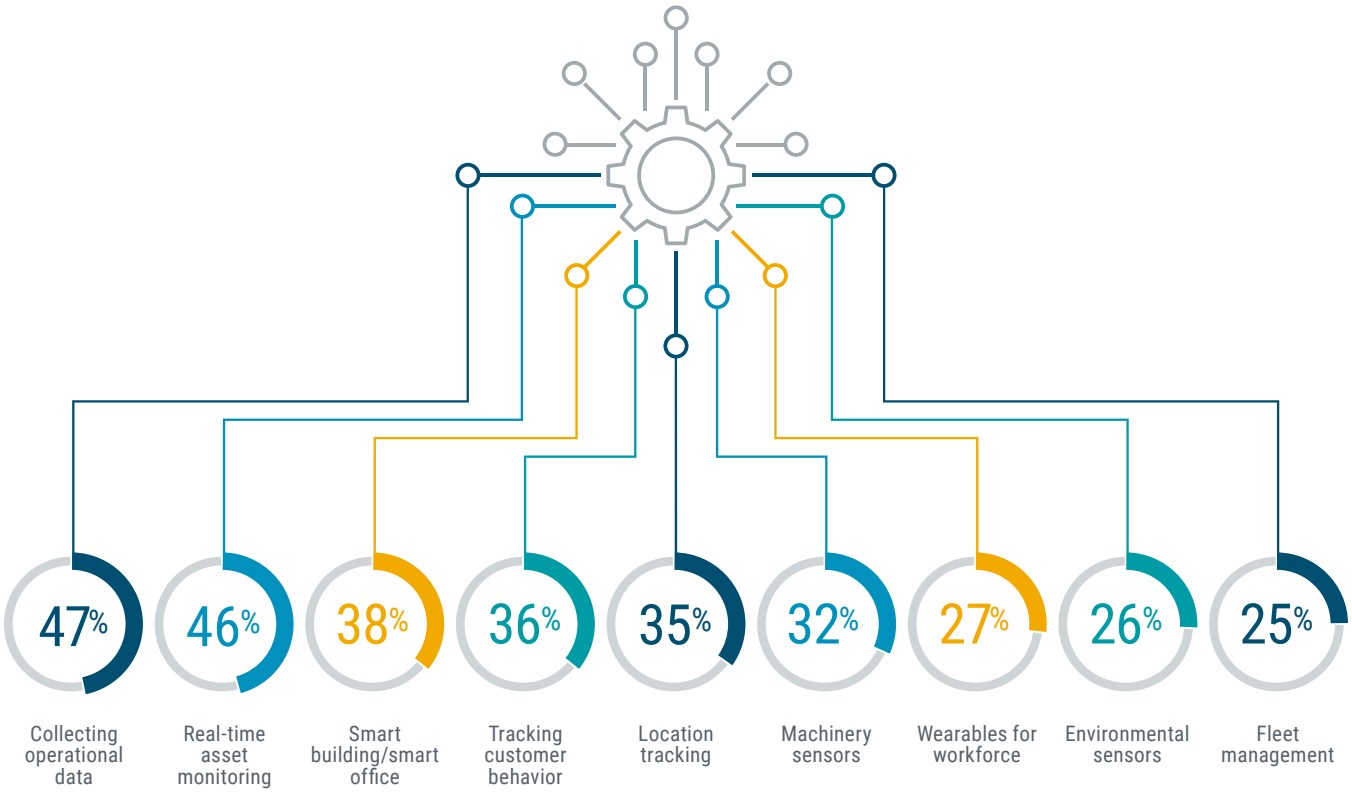


The rapid growth of IoT sensors and solutions is driving higher expectations of IT and supporting systems including networking, storage, analytics, sensors, application, and compute. We must bridge the gap and create avenues for success with newly formed centers of success. Data retention models are often designed based upon the insight from the sensor. Data retention grows from single-system insight to multiple-system data integration points.

Layer 6: Applications

IoT applications may be limited only by your imagination and ingenuity, but there are patterns emerging around typical uses and verticals for this technology. Data from CompTIA's Trends in Internet of Things shows that the most popular use cases among end-user companies are collecting operational data and real-time asset monitoring.

Types of IoT Projects



Popular IoT Vertical Applications

Specialization for a value-added reseller (VAR) helps to narrow down their focus and gives them a better chance to become a trusted partner for their clients.

Technology Selection Criteria: Vertical/Market

1. Understand the market and the vendors working in the vertical.
2. Know the vertical that fits with your expertise and provides the best long-term value and growth.
3. Beware of verticals that are over-crowded—a large vertical may be a poor choice if it's oversaturated with competition.
4. Focus on the vendor selection process (i.e., an established vendor vs. a startup).
5. Understand the typical sales cycle in your chosen vertical.
6. Understand the lifecycle of your chosen vertical.

Technology Selection Criteria: Application Overlap

One use case may fit into multiple IoT categories. This allows multiple vertical entries, IoT categories, and horizontal markets with a single application. For example, personal navigation can be leveraged in consumer offerings, healthcare, and connected cities.

Technology Selection Criteria: Integration

In order to identify integration opportunities, ask:

- Can you leverage any existing software?
- Is there support for multiple device types?
- Does it allow for meeting multiple client use cases?
- Is it easy to scale and future proof?
- How complex are management and maintenance?
- Can devices be mapped to objects?
- Are standards present for third-party interoperability?
- Can you easily share the data insights with your consumer and at other levels by access?

Technology Selection Criteria: Make/Buy

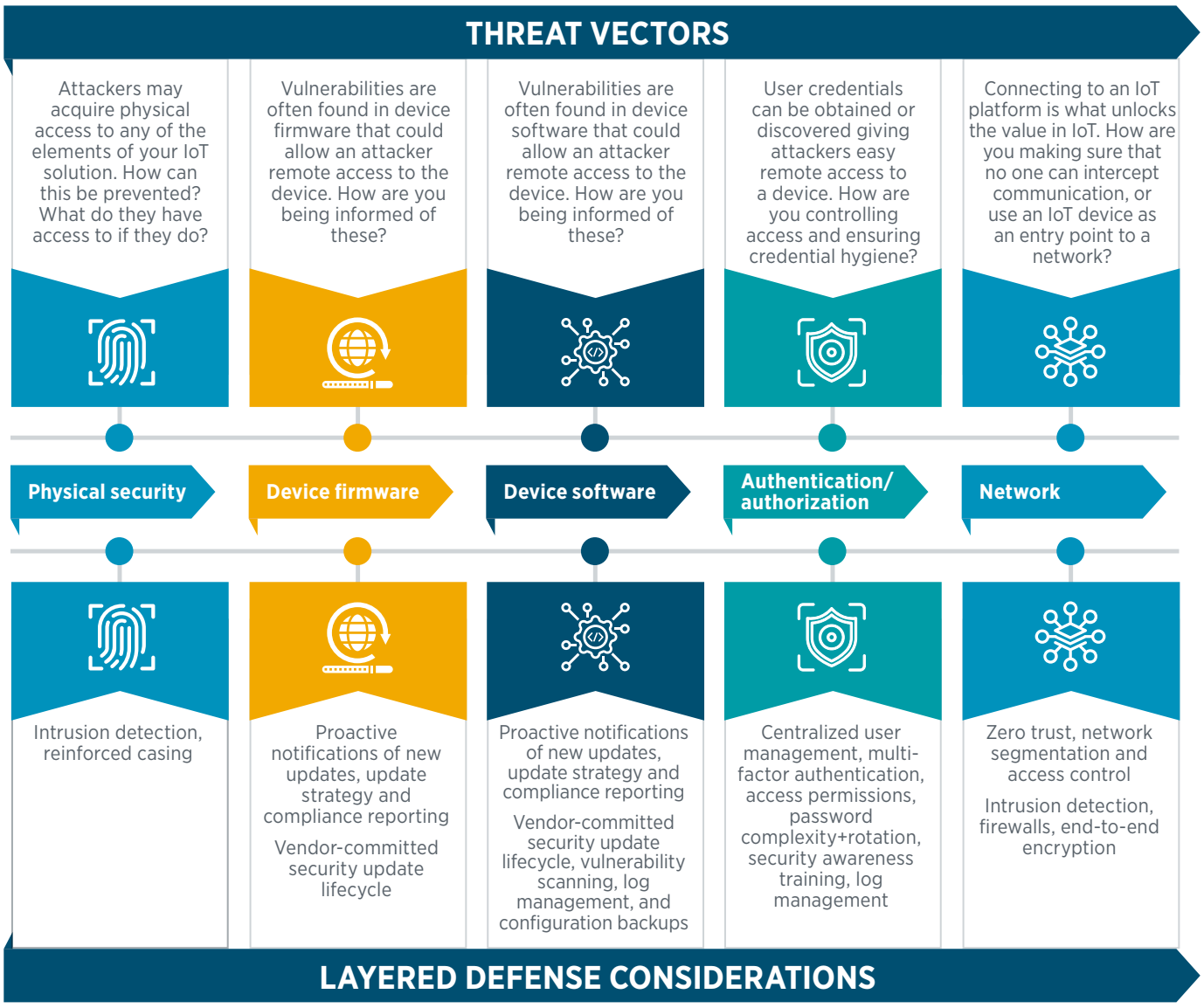
There are pros and cons to developing your own technology vs. buying the technology from a vendor.

IoT Security

Security is relevant at each layer of an IoT solution. No matter the type of device or practical application, IoT security needs to be taken seriously. Much like other asset types, cybercriminals target IoT to get access to sensitive or valuable information, or to take control of an asset or a service. When designing an IoT solution, it's important to consider that the target may be IoT related, or it may simply be the means into a network where another asset is the target.

Threat Vectors and Layered Defense Considerations

The following threat vectors apply to each aspect of your IoT solution (sensor, edge compute, platform, etc.), in addition to the networking infrastructure that supports it. The platform will also have additional considerations such as data residency and data-at-rest encryption, among others.

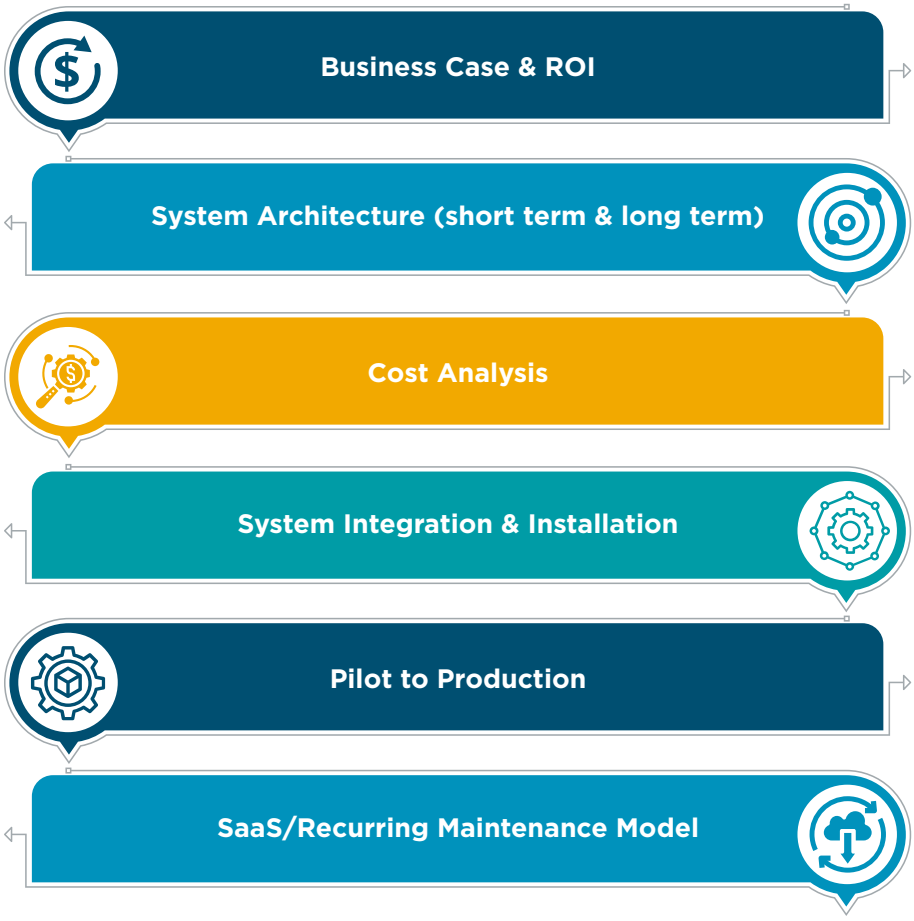


Building Your IoT Solution

Understanding the layers of an IoT solution and choosing the right components is just part of the IoT solution lifecycle, but it is critical to the success of your project. IoT projects can be complex, but the payoff can be huge.

Technology vendors estimate upwards of 50% of IoT projects fail. Utilizing the *6 Layers of an IoT Solution* guide and sharing it with key internal technical, data, privacy, and security stakeholders will bring together the essential input that will lay the preparatory groundwork to build an IoT solution that will deliver a flexible and sustainable framework for success.

IoT Solution Lifecycle



IoT Resources from CompTIA

Business Opportunities in Emerging Technologies: Internet of Things

Turning New Regulations into IoT Opportunity: How to Become a Trusted Business Partner

Emerging Technology Assessment

2021 Emerging Technology Top 10 List: AI and IoT

Internet of Things (IoT) Technology Interest Group

Emerging Technology Community

About the CompTIA IoT Advisory Council

The CompTIA IoT Advisory Council strives to increase the adoption of IoT solutions, promote the concept of smart cities and communities, and create awareness and business opportunities in this rapidly evolving field. We collaborate with CompTIA's other industry advisory councils to present IoT opportunities across the technology ecosystem.

Learn more.

CompTIA.org

CompTIA is responsible for all content and analysis. Any questions regarding the report should be directed to CompTIA Research and Market Intelligence staff at research@comptia.org.