Lecture 2

Solution Architecture

What is IoT Architecture

An IoT architecture is a mix of hardware and software components that interact together to make up a smart cyber-digital system.

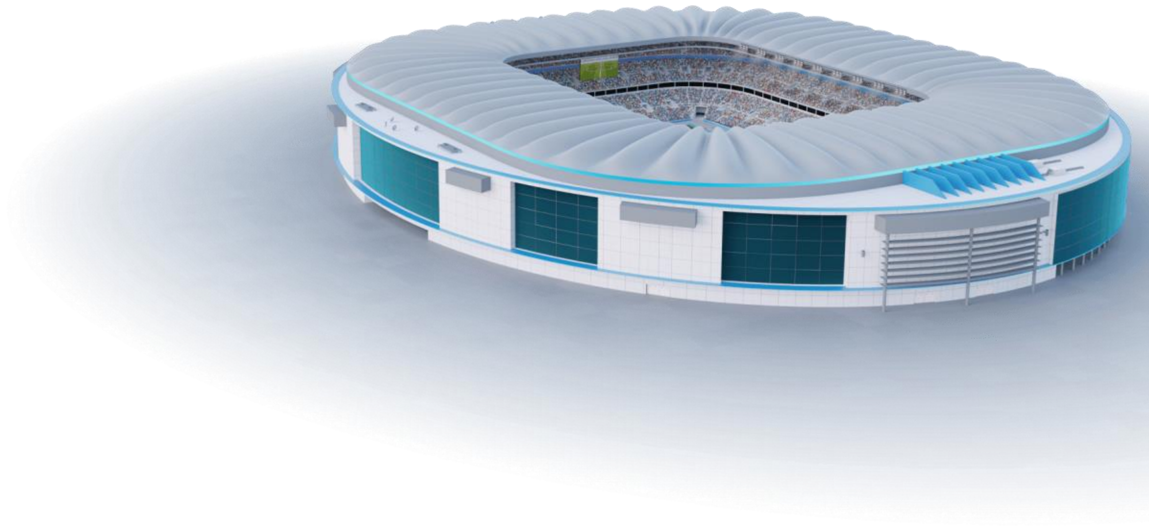
Interoperating with one another, these components make up a base for an IoT solution to be built upon.

- ❑ There's no one-size-fits-all approach to designing an IoT architecture. Still, the basic layout stays largely the same no matter the solution.

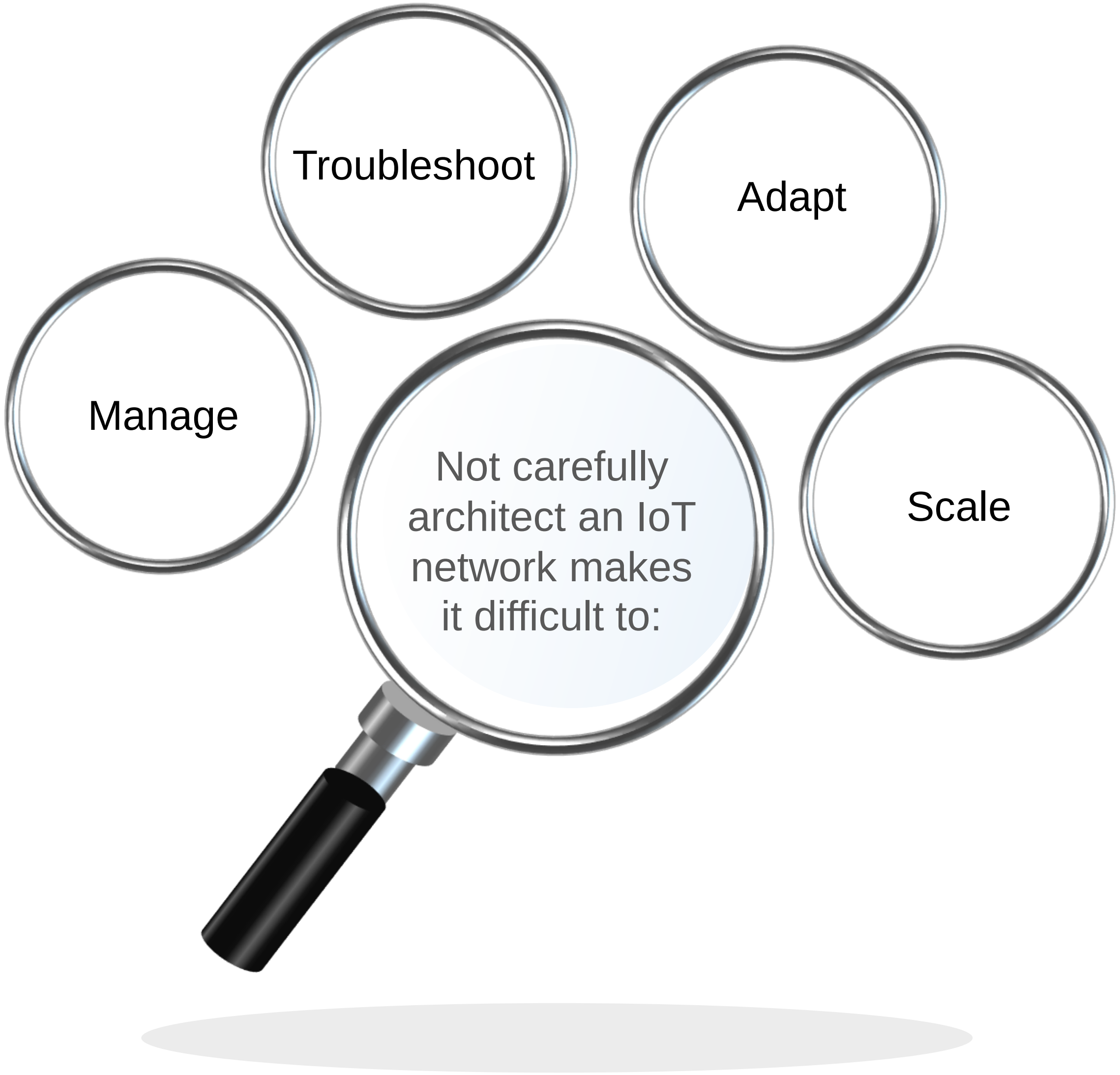
IT vs. IoT Architecture

- The difference between IT and IoT networks is much like the difference between residential architecture and stadium architecture.

- While traditional network architectures for IT have served us well for many years, they are not well suited to the complex requirements of IoT.



Importance of IoT Architecture



IT vs. IoT Architecture

IT

Reliable and continuous support of business applications such as email, web, databases.

IOT

How the data is transported, collected, analyzed, and ultimately acted upon.

The key difference between IT and IoT is the data.

Considerations of IoT Architecture

1. **Scale**
The massive scale of the IoT sensors is far beyond that of typical IT network

2. **Security**
IoT devices are often physically exposed to the world. They lack capabilities to implement security mechanisms.

3. **Limited Resources**
IoT devices and networks are constrained.

4. **Analytics**
IT networks perform scheduled batch processing of data. IoT data needs to be analyzed and responded to in real-time.

5. **Legacy Devices**
Legacy, non-IP devices rely on serial or proprietary protocols.

6. **Big data**
Massive amount of data causes network bottlenecks and slow analytics in the cloud.

IoT Standardized Architecture

Decompose the IoT problem into smaller parts

Identify different technologies at each layer and how they relate to one another

Define a system in which different parts can be provided by different vendors

Have a process of defining interfaces that leads to interoperability

Define a tiered security model that is enforced at the transition points between levels

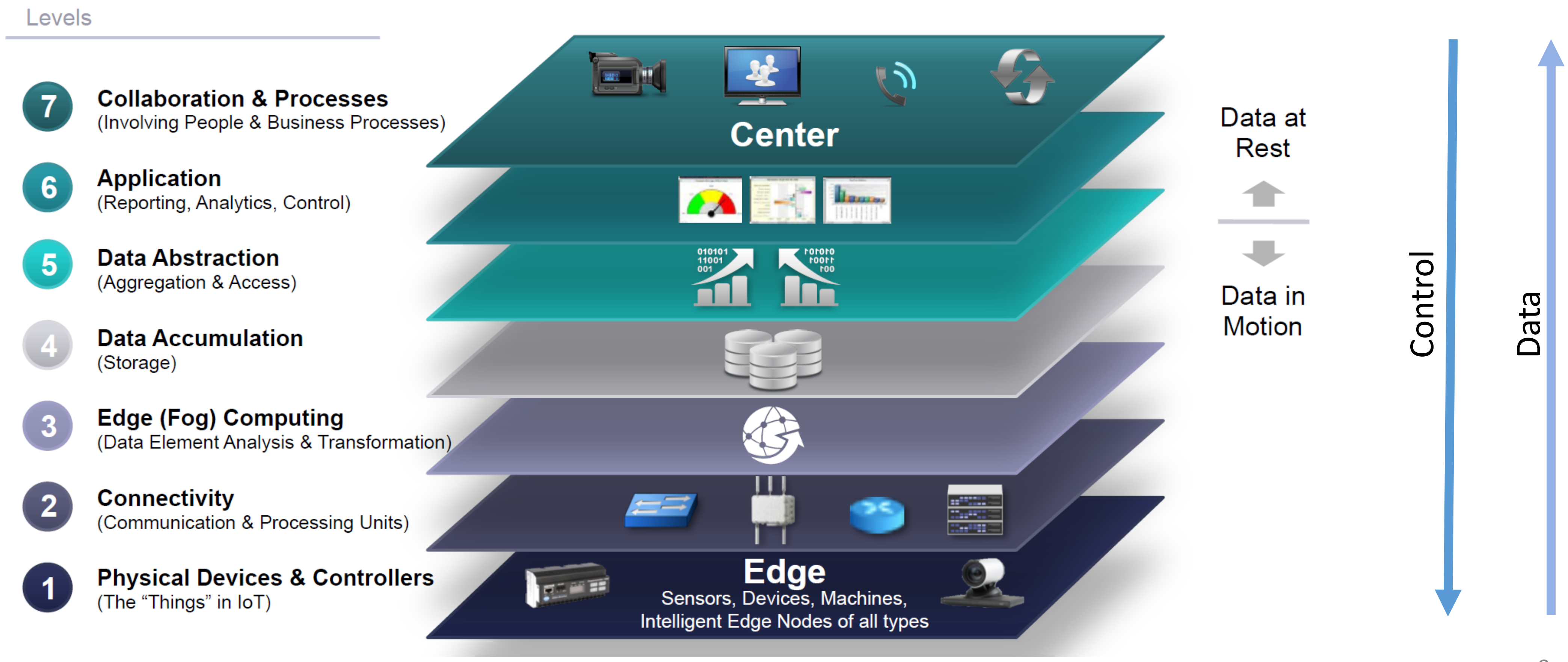
IoTWF

Reference Model

A seven-layer IoT architectural reference model published by the IoT World Forum (IoTWF) architectural committee (led by Cisco, IBM, Rockwell Automation, and others) in 2014.

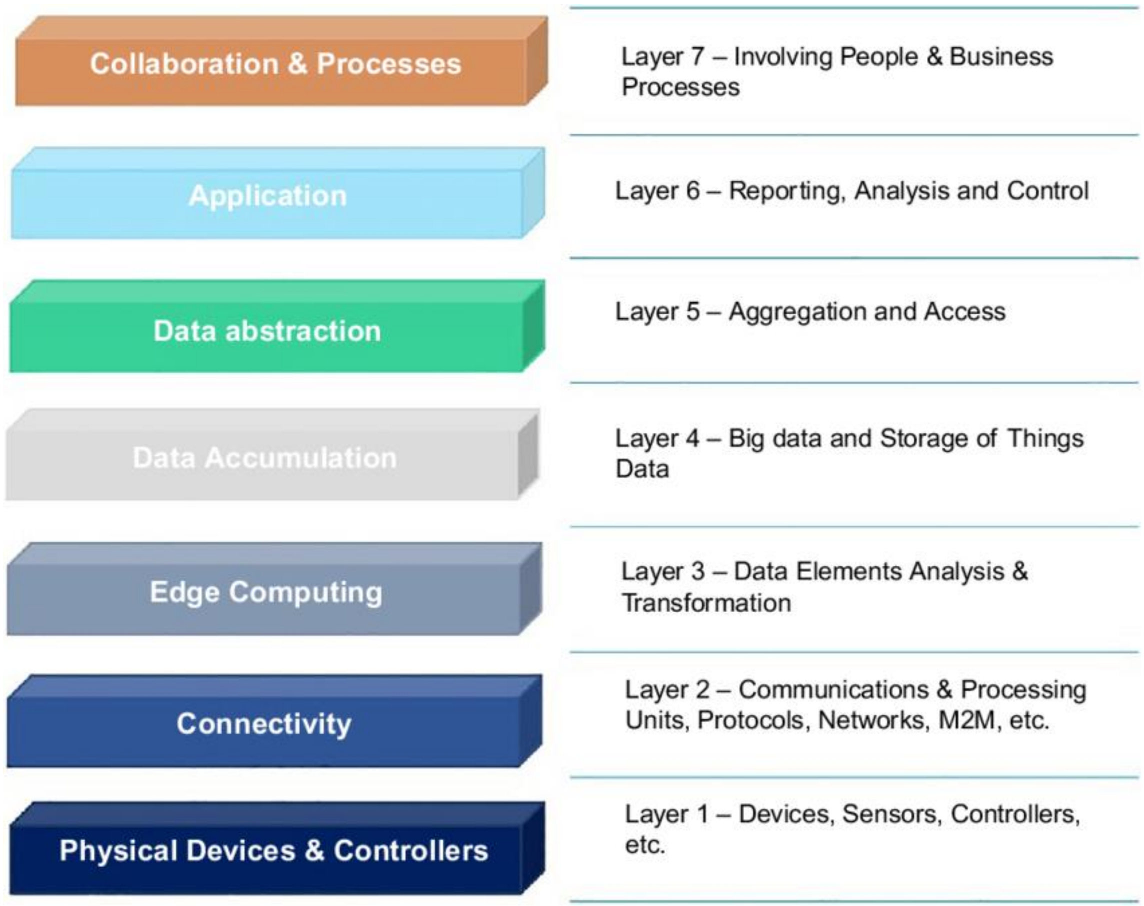
IoT Standardized Architecture

IoTWF



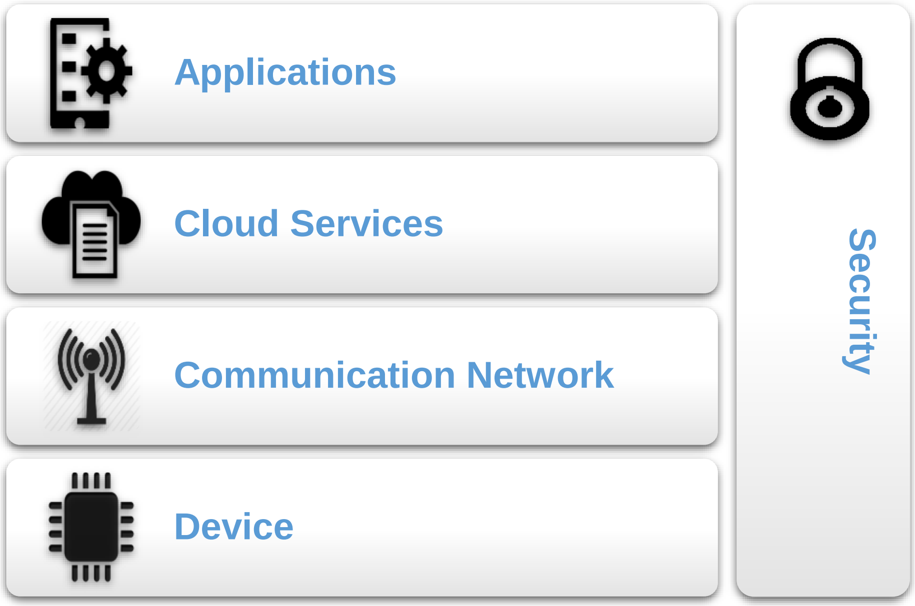
IoT Standardized Architecture

IoTWF – Smart waste management



IoT Architecture Layers

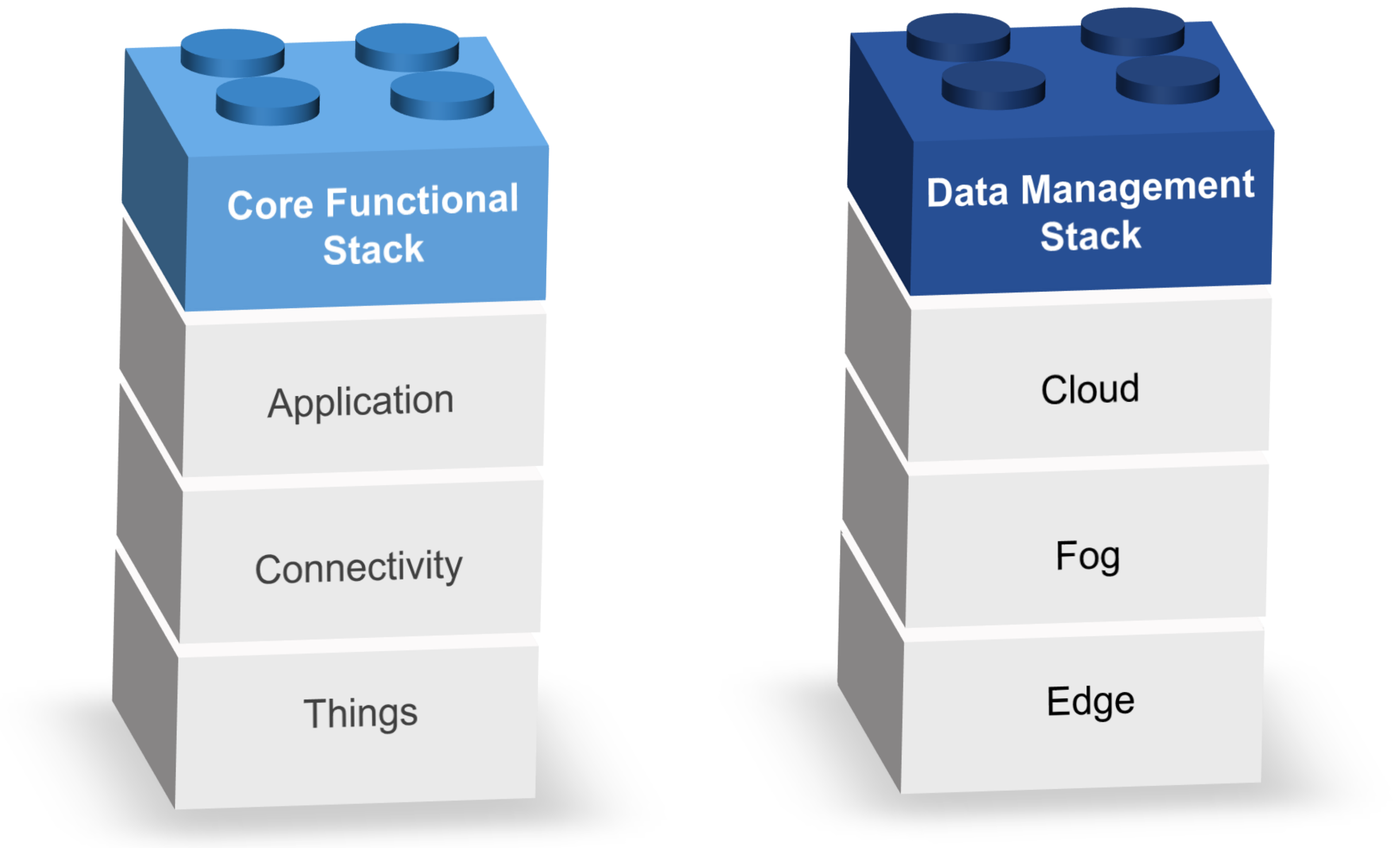
Essential components of an IoT solution architecture



IoT Architecture Layers

Layer					5 Security Layer
4 Application Layer	Visualization	Business System Integration	Development Environment		Application Identity & Access Management
3 Cloud Services Layer	Storage / Database	Device Management	Event Processing	Advanced Analytics	Privacy Management
2 Network Layer	Licenced Long Range Wireless: 4G LTE, 2G 3G	Unlicensed Short Range Wireless: ZigBee, WiFi, Z-WAVE	Unlicensed Long Range Wireless: LoRa, sigfox		E2E Encryption of Data and Communication
1 Device Layer					Physical Protection, Firmware Attestation

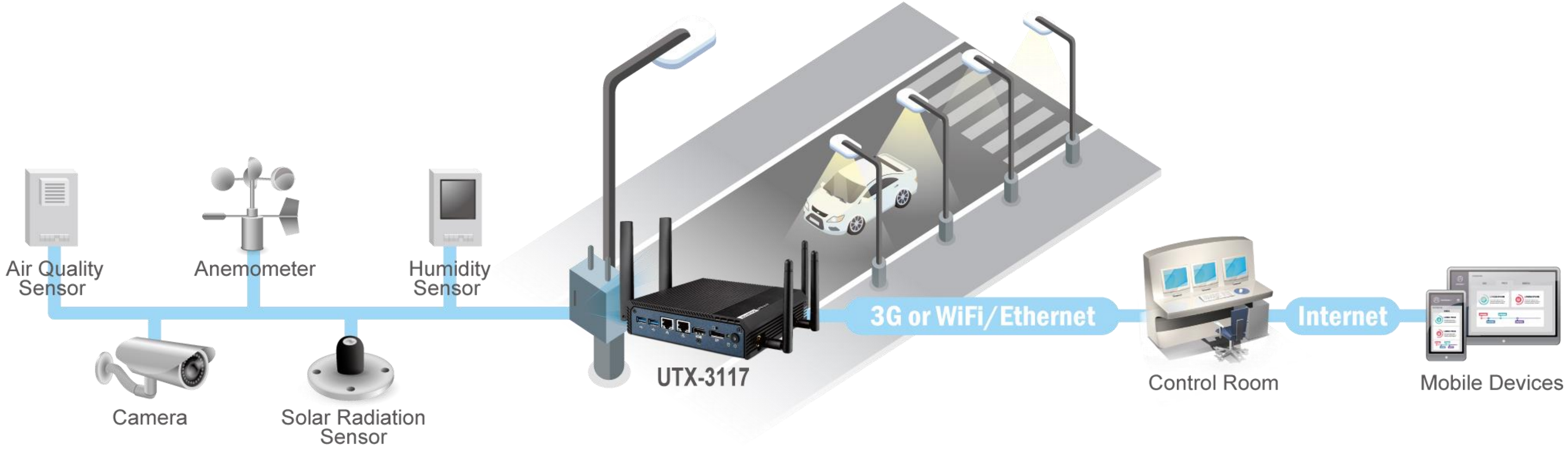
Simplified IoT Architecture



Core Functional Stack

Things

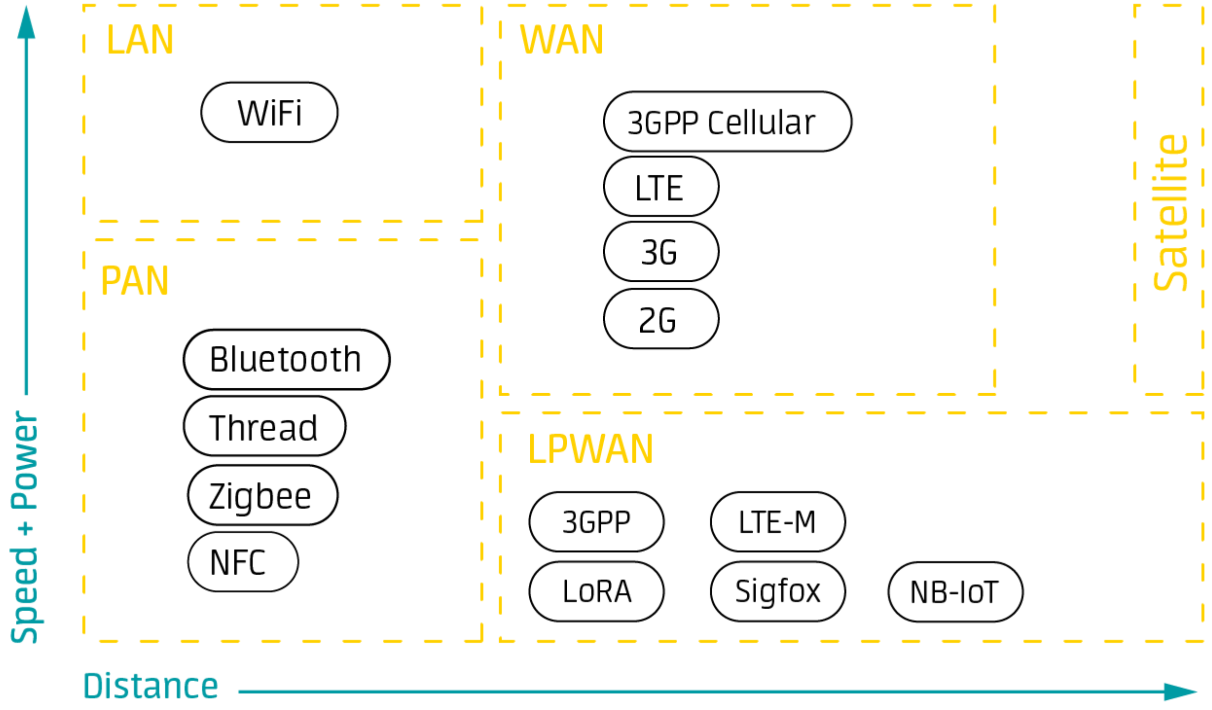
- Battery-powered or power-connected
- Mobile or static
- Low or high reporting frequency
- Simple or rich data
- Report range
- Object density per cell



Core Functional Stack

Connectivity

Once the influence of the smart object form factor over its transmission capabilities is determined, you are ready to connect the object and communicate.



Core Functional Stack

Application

Analytics application

Processes the collected data, and displays the results.

Control application

Controls the behavior of the smart object.

Analytics

Data analytics

Processes the data collected by smart objects and combines it to provide an intelligent view related to the IoT system.

Network analytics

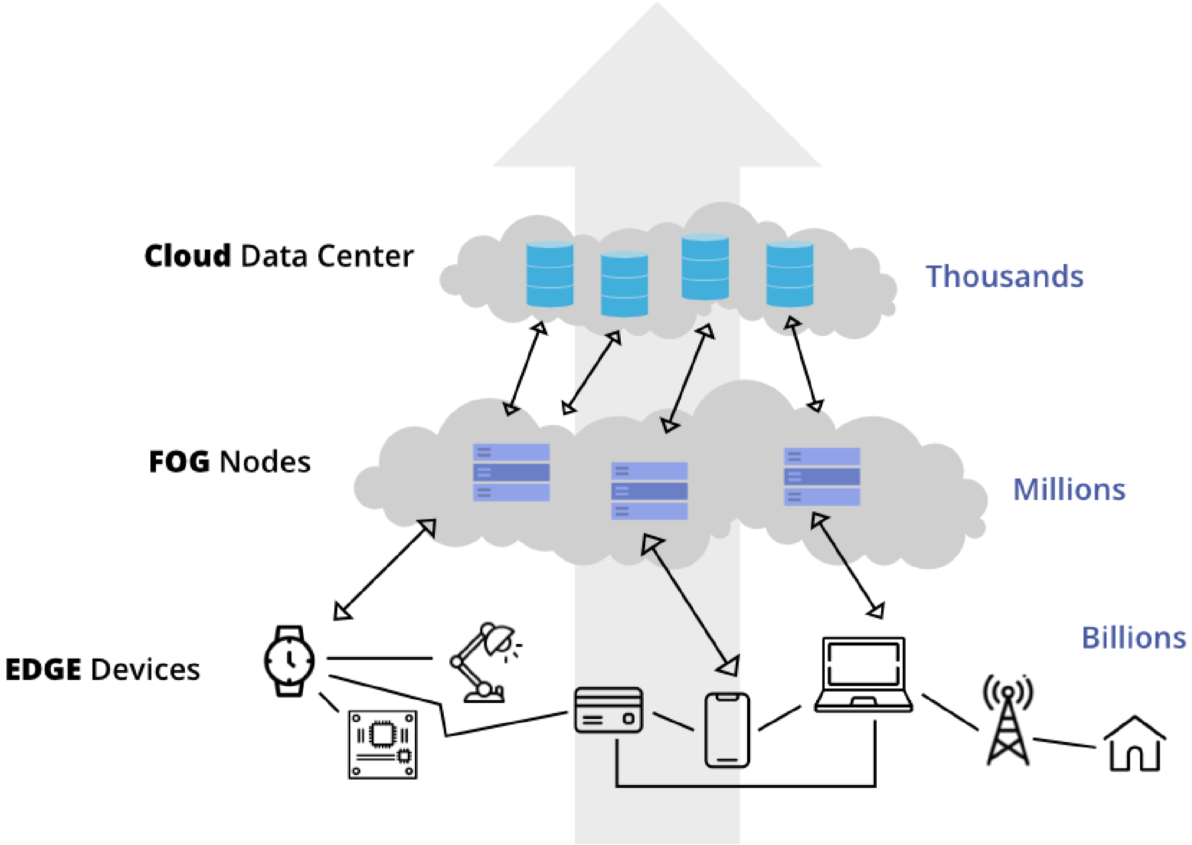
Checks the network connectivity to avoid a loss or degradation of the efficiency of the system.

Data Management Stack

Cloud computing
Enables companies to store, process, and otherwise work with their data on remote servers that are hosted over the internet.

Fog computing
Allows data to be temporarily stored and analyzed in a compute layer between the cloud and the edge for cases where it's not possible to process edge data due to edge equipment compute limitations.

Edge computing
Allows the capture, processing, and analysis of data at the farthest reaches of an organization's network: the "edge."



Cloud Computing

Cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale.

You typically pay only for cloud services you use, helping you lower your operating costs, run your infrastructure more efficiently, and scale as your business needs change.

Cloud Computing

Benefits of cloud computing

Cost
Helps companies optimize IT costs by eliminating the capital expense of buying hardware and software and setting up and running onsite datacenters.

Speed
Most cloud computing services are provided self service and on demand, so even vast amounts of computing resources can be provisioned in minutes, giving businesses a lot of flexibility and taking the pressure off capacity planning.

Global scale
Delivering the right amount of IT resources right when they're needed, and from the right geographic location.

Productivity
Removes the need for hardware setup, software patching, and other time-consuming IT management chores, so IT teams can spend time on achieving more important business goals.

Performance
A worldwide network of secure datacenters, which are regularly upgraded to the latest generation of fast and efficient computing hardware.

Reliability
Cloud computing makes data backup, disaster recovery, and business continuity easier and less expensive

Security
Many cloud providers offer a broad set of policies, technologies, and controls that strengthen your security posture overall.

Cloud Computing

Limitations of cloud model

Limited bandwidth

When dealing with thousands/millions of devices, available bandwidth may be on order of tens of Kbps per device or even less.

High latency

Large IoT networks often introduce latency of hundreds to thousands of milliseconds.

Unreliable backhaul

Often depends on 3G/LTE or even satellite links. Backhaul links can also be expensive if a per-byte data usage model is necessary.

High volume of data

Much of the data transmitted over the backhaul may not really be that interesting.

Big data

The concept of storing and analyzing all sensor data in the cloud is impractical.

Cloud Computing

Public cloud

Public clouds are owned and operated by third-party cloud service providers, which deliver computing resources like servers and storage over the internet. Microsoft Azure is an example of a public cloud. With a public cloud, all hardware, software, and other supporting infrastructure is owned and managed by the cloud provider. You access these services and manage your account using a web browser.

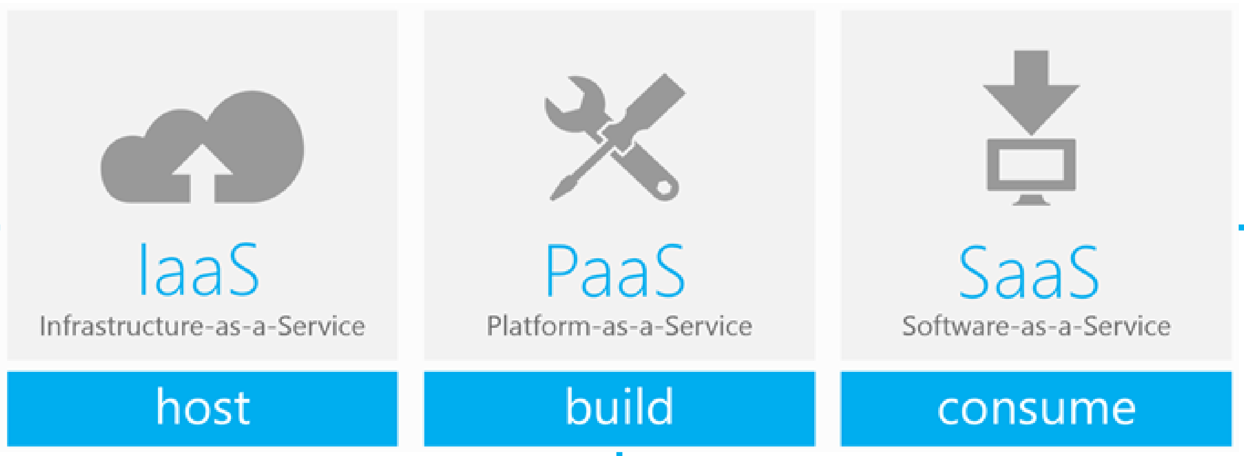
Private cloud

A private cloud refers to cloud computing resources used exclusively by a single business or organization. A private cloud can be physically located on the company's onsite datacenter. Some companies also pay third-party service providers to host their private cloud. A private cloud is one in which the services and infrastructure are maintained on a private network.

Hybrid cloud

Hybrid clouds combine public and private clouds, bound together by technology that allows data and applications to be shared between them. By allowing data and applications to move between private and public clouds, a hybrid cloud gives your business greater flexibility and more deployment options and helps optimize your existing infrastructure, security, and compliance.

Cloud Service Models

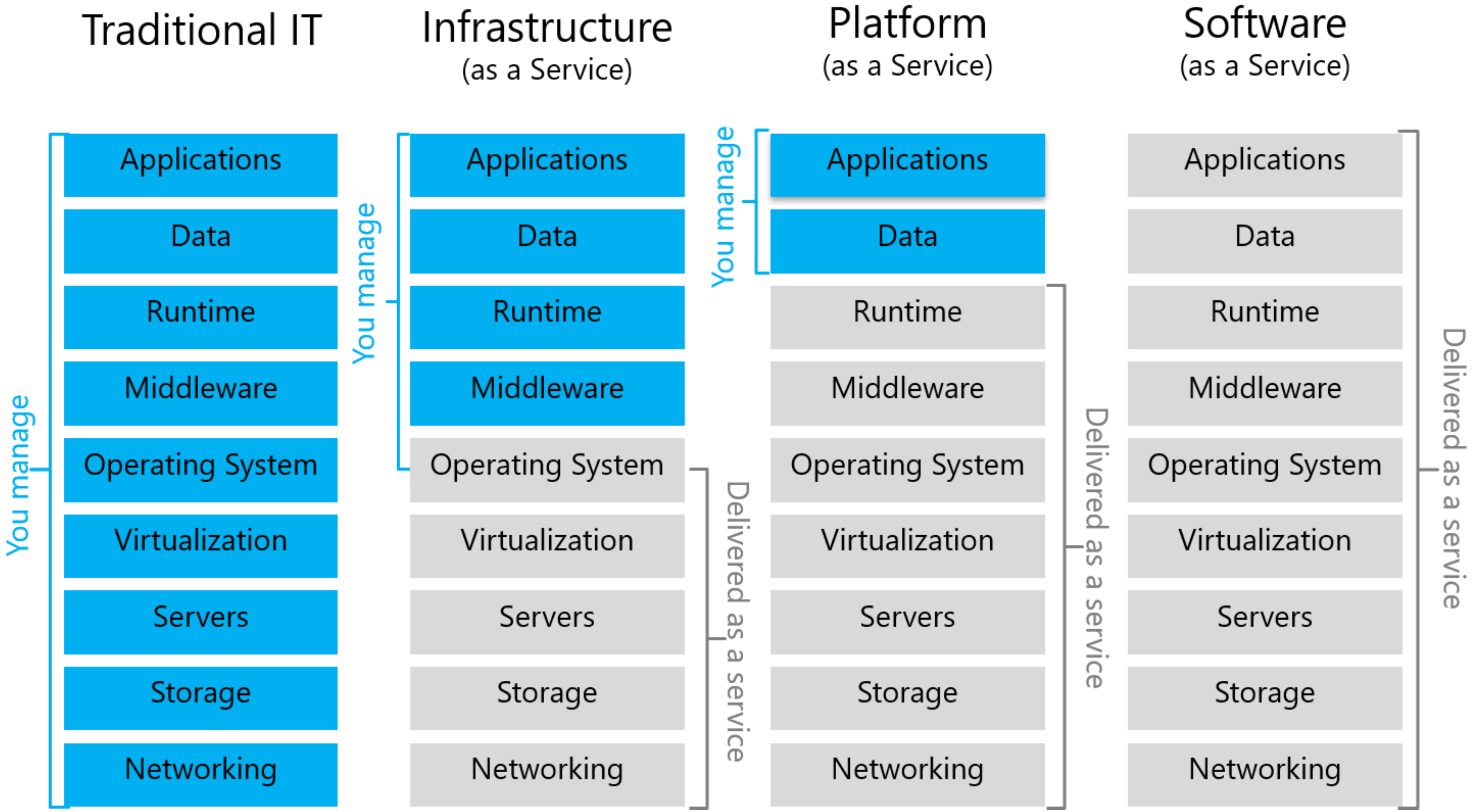


On-demand access to cloud-hosted physical and virtual servers, storage and networking - the backend IT infrastructure for running applications and workloads in the cloud.

On-demand access to a complete, ready-to-use, cloud-hosted platform for developing, running, maintaining and managing applications.

on-demand access to ready-to-use, cloud-hosted application software.

Cloud Service Models



Fog Computing

Any device with computing, storage, and network connectivity can be a fog node e.g., industrial controllers, switches, routers, embedded servers, and IoT gateways.

Pros

- Improved bandwidth
- Minimized latency & congestion
- Enabling autonomous operations
- Bolstered security & privacy & regulatory compliance

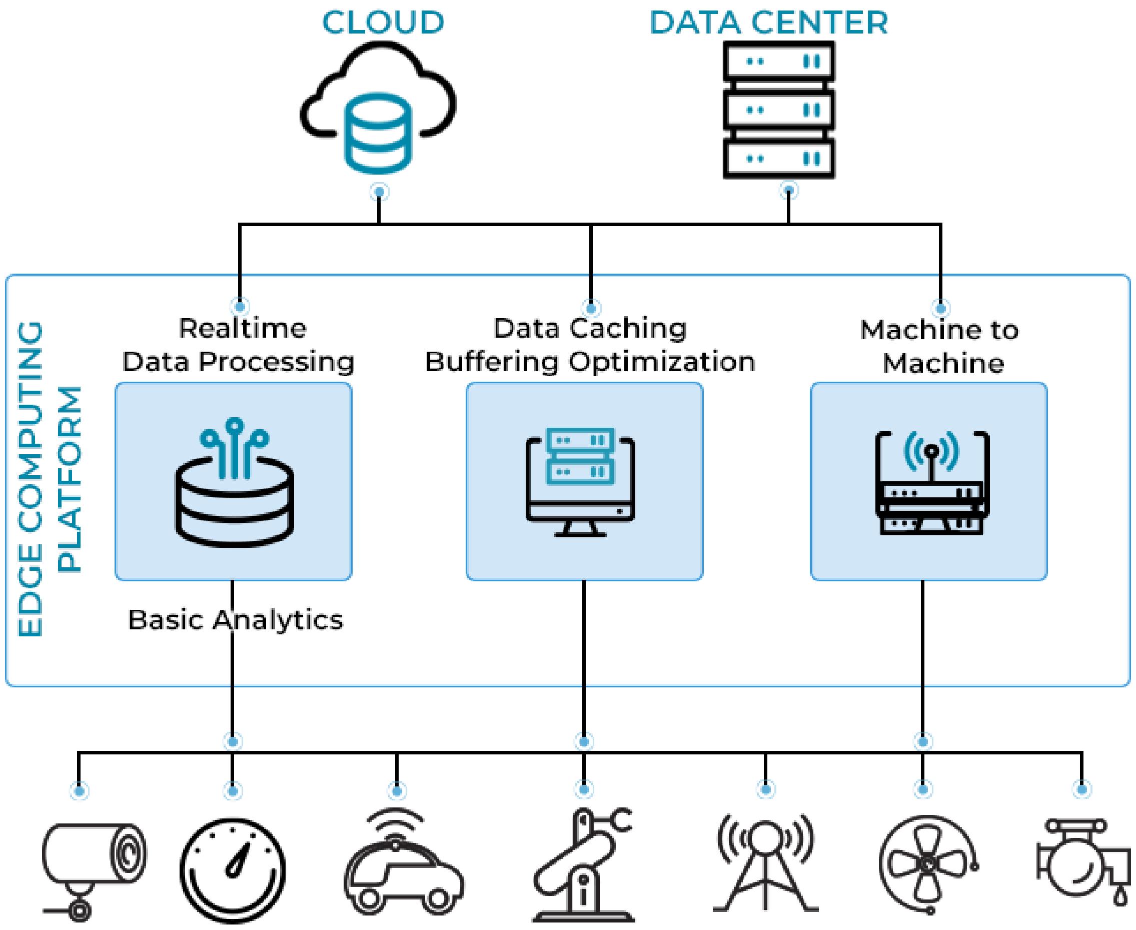
Cons

- Requires additional security
- Not enough protection against failure or misuse
- High maintenance requirements
- High hardware costs

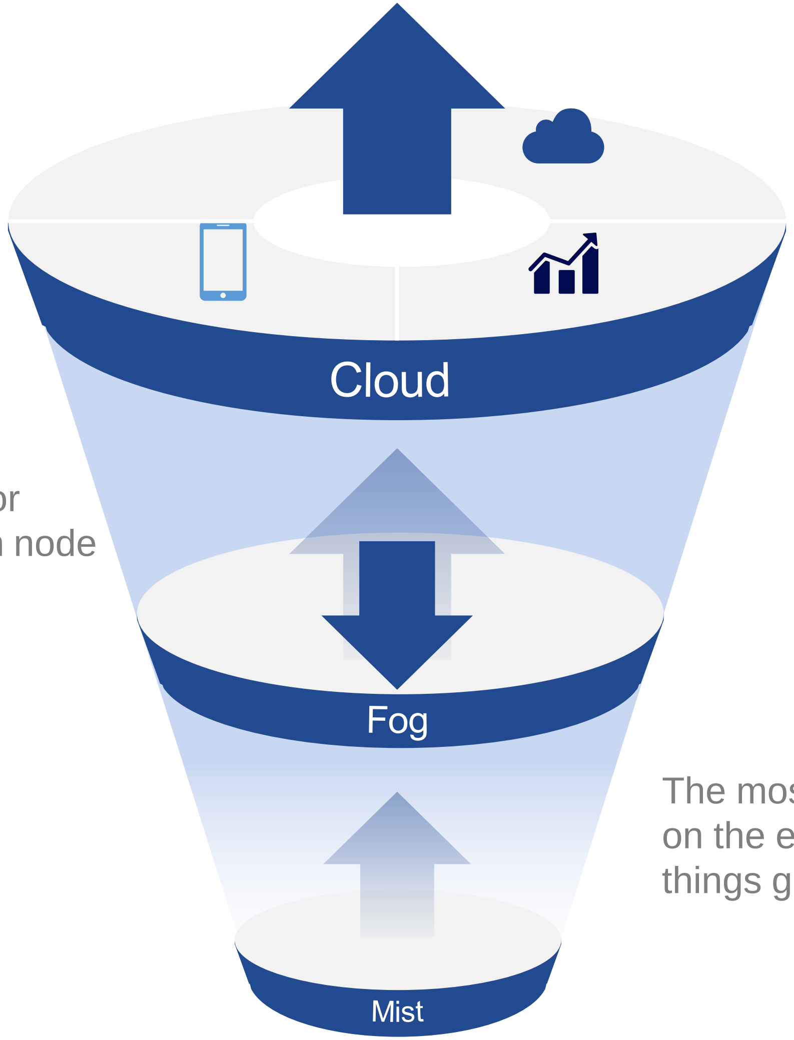
Edge Computing

Edge computing is a distributed computing framework that brings enterprise applications closer to data sources such as IoT devices or local edge servers.

- ✓ Reduced latency and improved response times
- ✓ Better bandwidth availability
- ✓ Improved data security



Hierarchy of Edge, Fog & Cloud

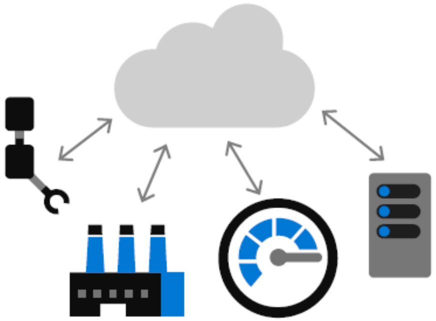


Data that is less time sensitive is sent to the cloud for historical analysis, big data analytics, and long-term storage.

Data that can wait seconds or minutes for action is passed along to an aggregation node for analysis and action.

The most time-sensitive data is analyzed on the edge or fog node closest to the things generating the data.

IoT Cloud or Edge?

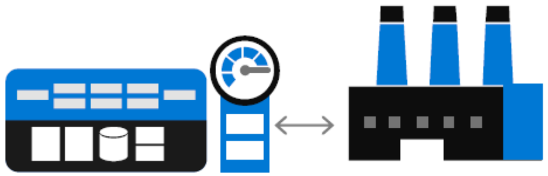


IoT in the Cloud

Remote monitoring and management

Merging remote data from multiple IoT devices

Infinite compute and storage to train
machine learning and other advanced AI tools



IoT on the Edge

Offline operations

Privacy of data and protection of IP

Pre-process data On-Prem, e.g., video streams

Near real-time response, e.g. low latency control loops

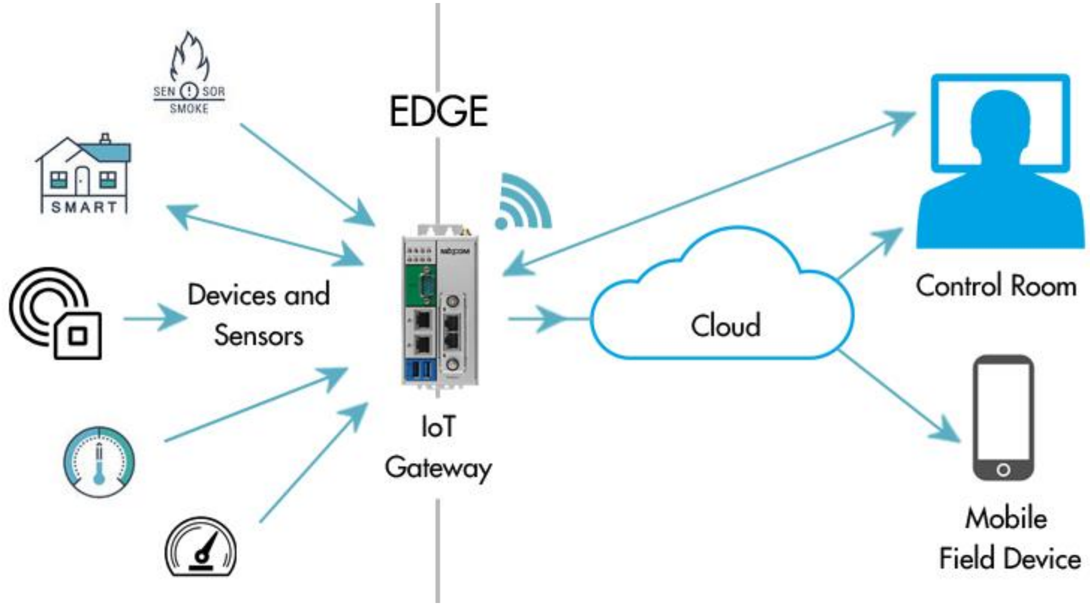
Protocol translation & data normalization

IoT Edge Gateways

IoT devices can connect to the IoT platform directly, or through IoT Edge gateways that implement intelligent capabilities.

Edge gateways enable functionalities like:

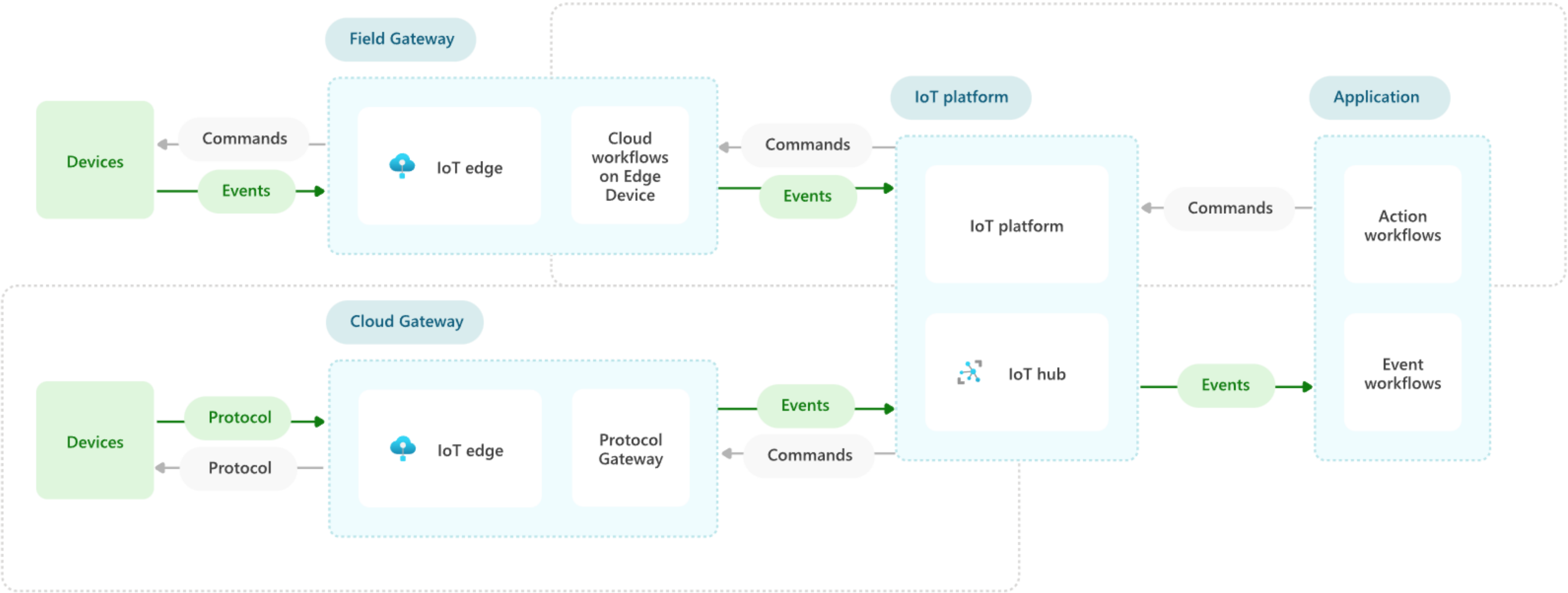
- Aggregating or filtering device events before they're sent to the IoT platform
- Localized decision-making
- Protocol and identity translation on behalf of devices



IoT Edge Gateways

Types: There are two types of edge gateways:

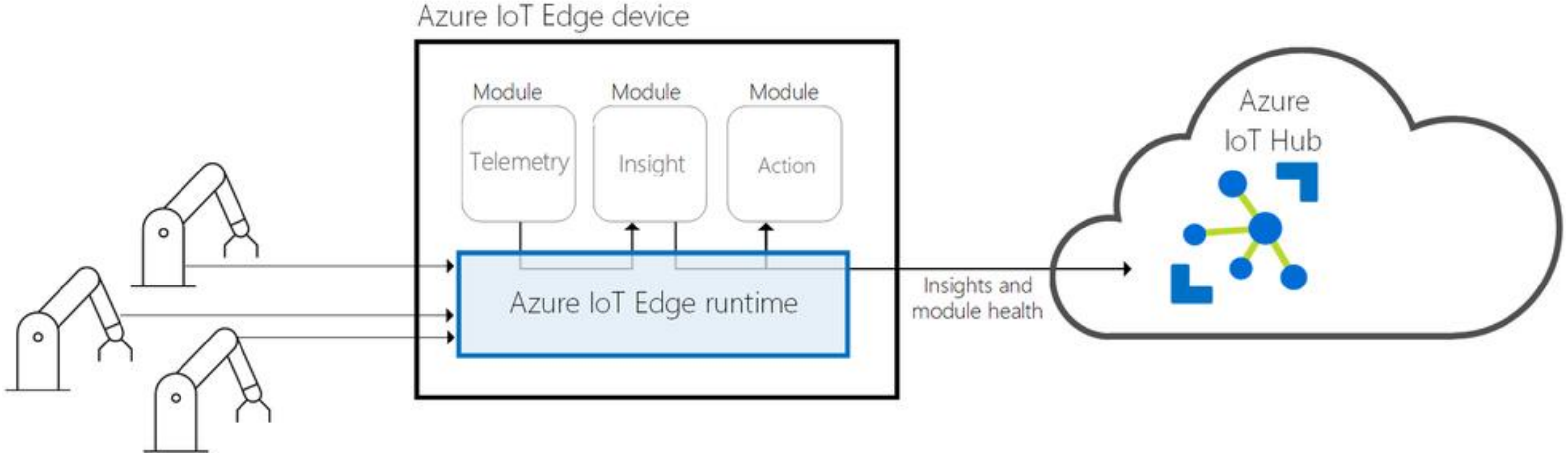
- *Field* or IoT Edge
- *Cloud* or protocol gateways



IoT Edge Gateways

Field or IoT Edge Gateway

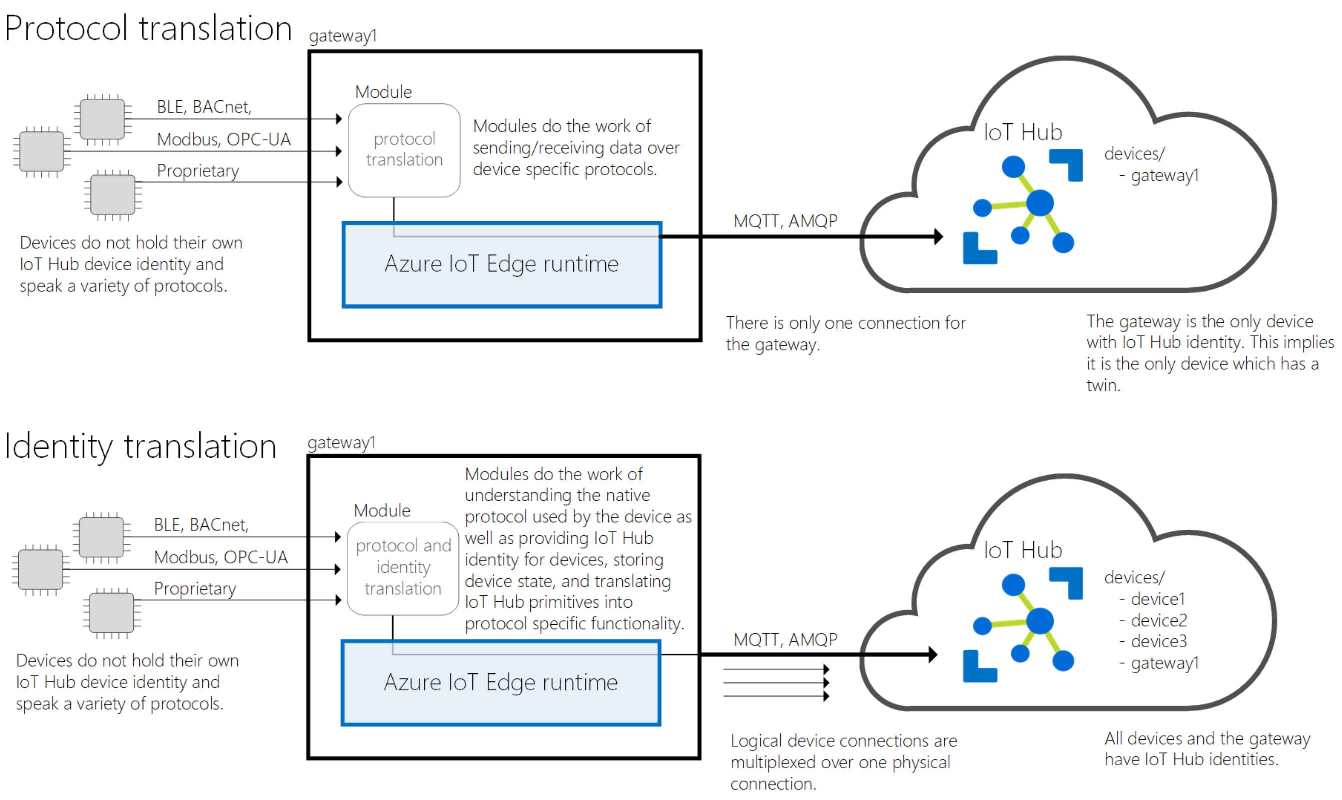
- Located close to devices on-premises.
- Connect to the IoT platform to extend cloud capabilities into devices.
- IoT Edge devices can act as communication enablers, local device control systems, and data processors for the IoT platform.
- IoT Edge devices can run cloud workflows on-premises by using Edge modules.
- Can communicate with devices even in offline scenarios.



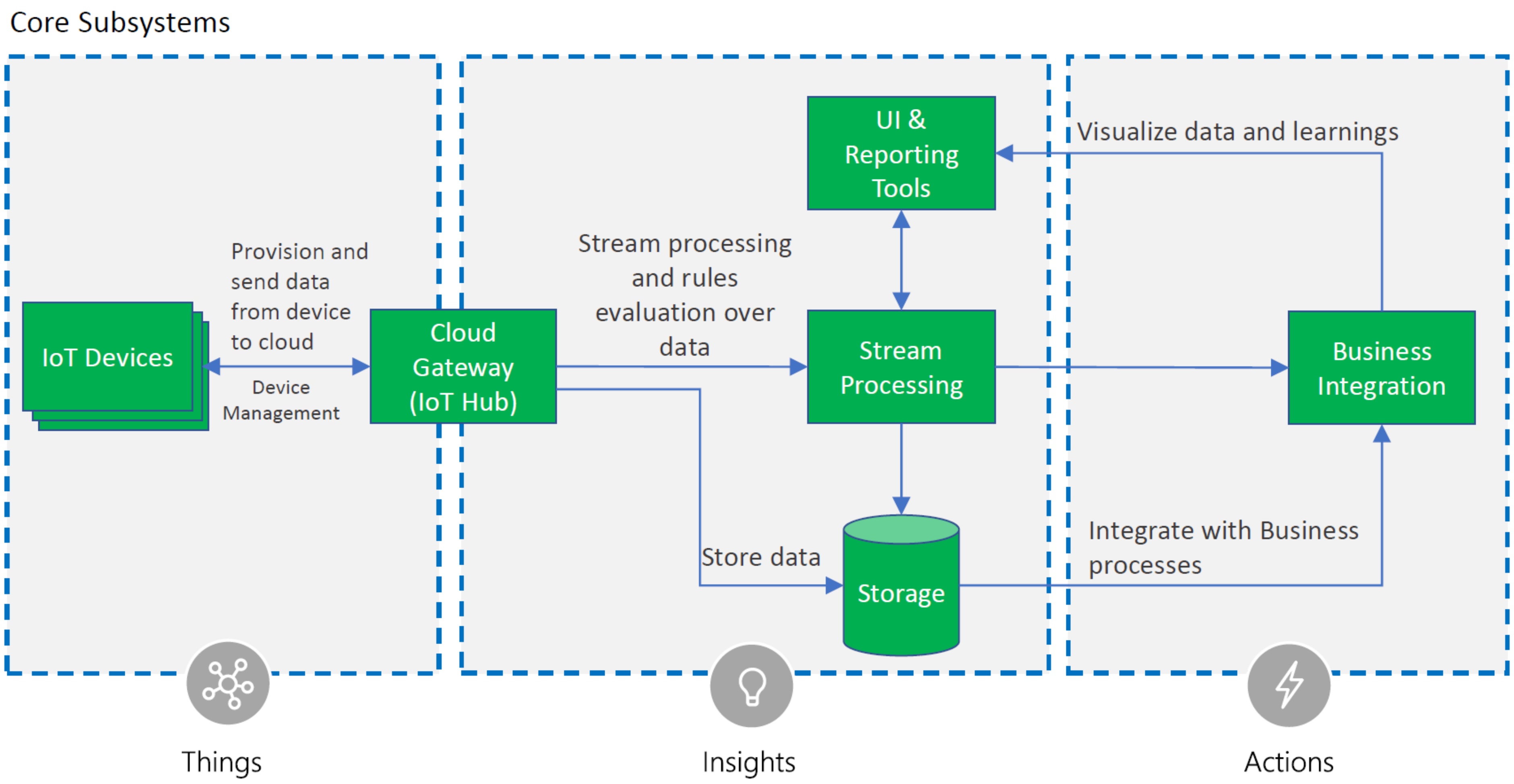
IoT Edge Gateways

Protocol or Cloud IoT Gateway

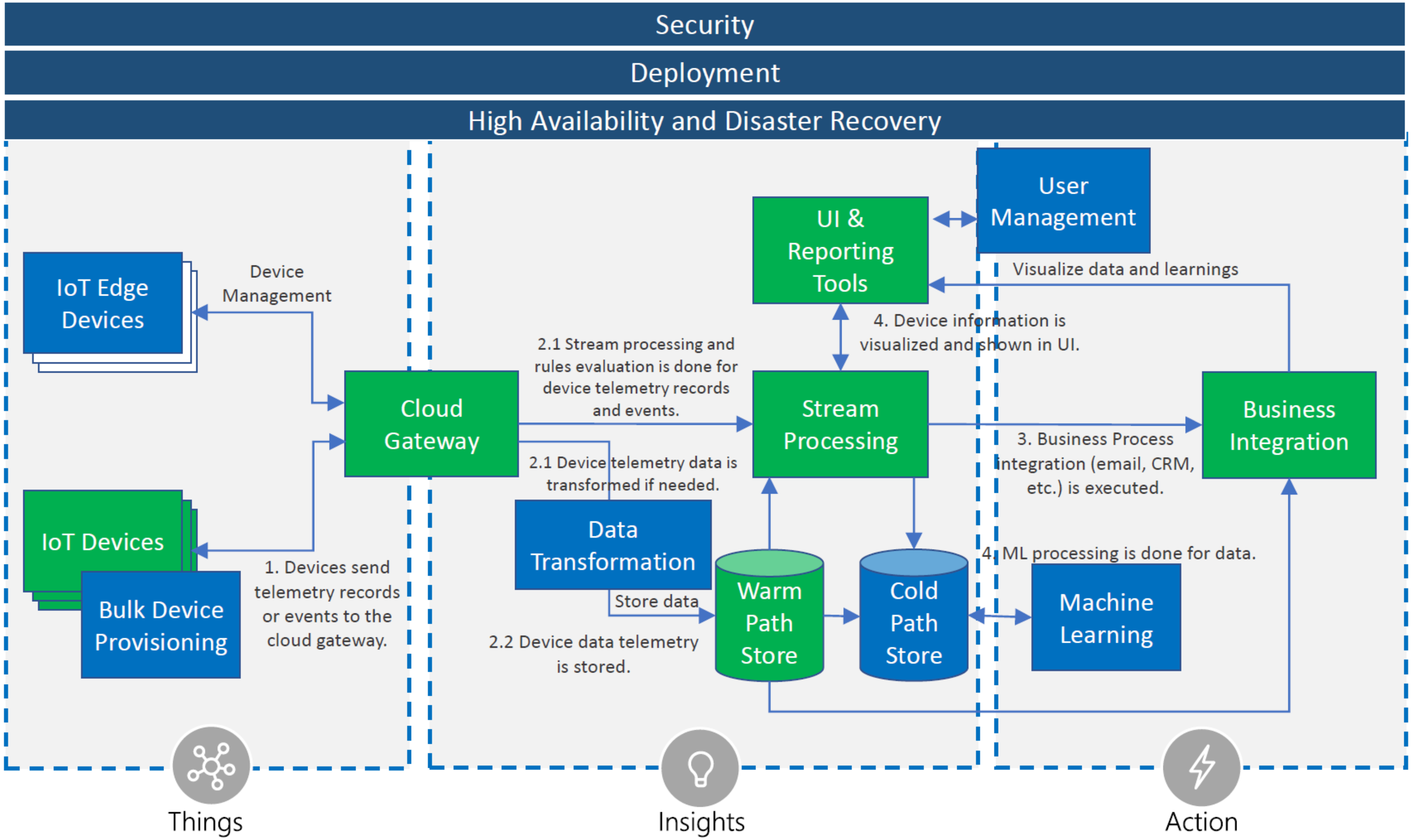
- Enable connecting existing and diverse device populations to IoT solutions by hosting device instances and enabling communication between devices and the IoT platform.
- Can do protocol and identity translation to and from the IoT platform.
- Can execute additional logic on behalf of devices.



Azure IoT Architecture

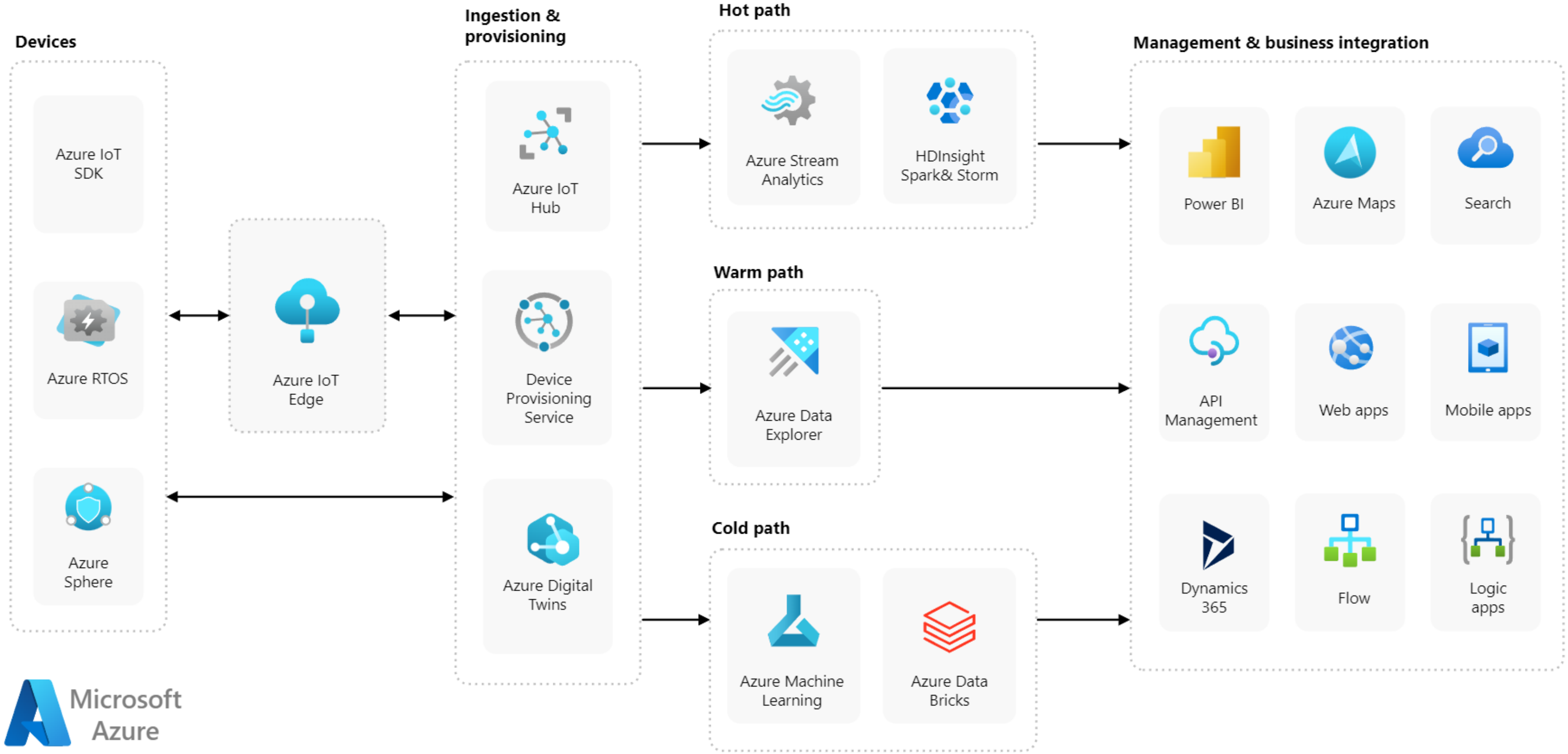


Azure IoT Architecture



Azure IoT Architecture

Custom IoT solutions can be created by assembling Azure PaaS (platform-as-a-service) components.



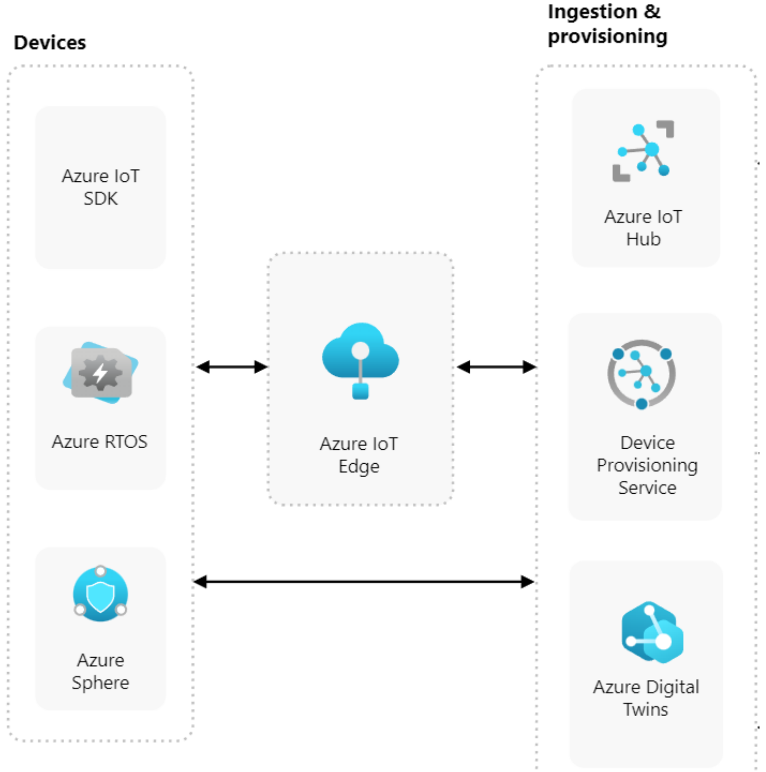
Azure IoT Architecture

1. Devices

A large range of devices, from microcontrollers running **Azure RTOS** and **Azure Sphere** to developer boards like MX Chip and Raspberry Pi.

Devices might perform some local processing through a service such as **Azure IoT Edge**, or just connect directly to Azure so that they can send data to and receive data from the IoT solution.

- **Azure IoT Hub** is a cloud gateway service that can securely connect and manage devices.
- **Azure IoT Hub Device Provisioning Service (DPS)** enables zero-touch, just-in-time provisioning that helps to register a large number of devices in a secure and scalable manner.
- **Azure Digital Twins** enables virtual models of real world systems.



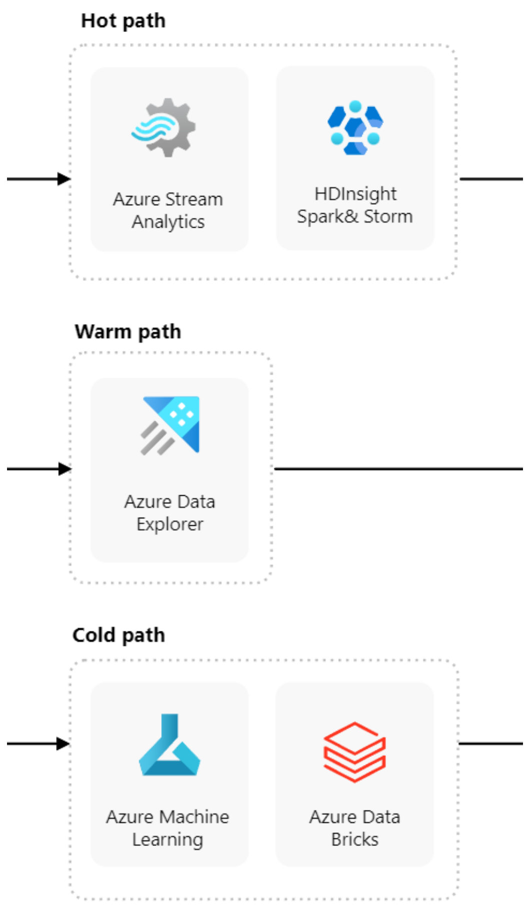
Azure IoT Architecture

2. Insights

- **Hot path** analyzes data in near-real-time as it arrives with very low latency.
  - The hot path typically uses a stream processing engine such as Azure Stream Analytics or Azure HDInsight.
  - The output might trigger an alert, or be written to a structured format that can be queried using analytical tools.

- **Warm path** analyzes data that can accommodate longer delays for more detailed processing.
  - Consider Azure Data Explorer for storing and analyzing large volumes of data.

- **Cold path** performs batch processing at longer intervals, like hourly or daily.
  - The cold path typically operates over large volumes of data, which can be stored in Azure Data Lake Storage.
  - Consider using Azure Machine Learning or Azure Databricks to analyze cold data.



Azure IoT Architecture

3. Actions

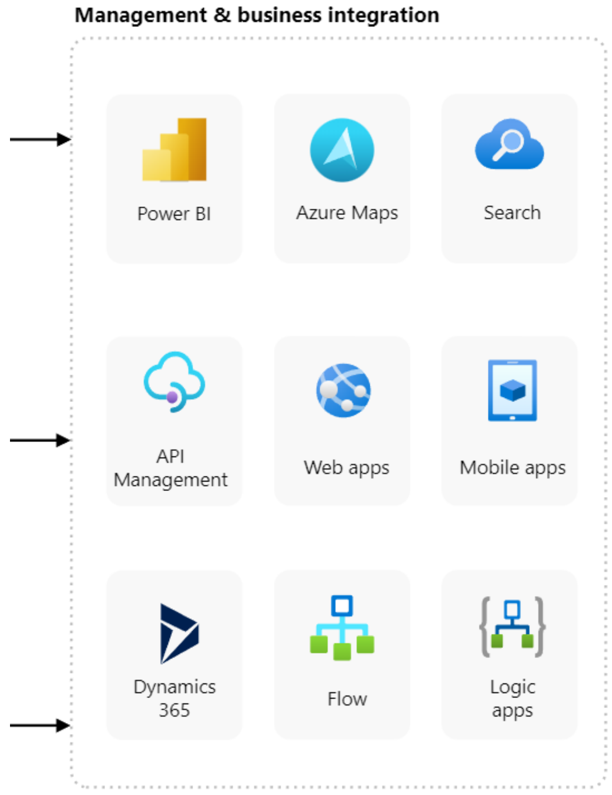
- **Power BI** connects to, models, and visualizes data and lets you collaborate on data and use artificial intelligence to make data-driven decisions.

- **Azure Maps** creates location-aware web and mobile applications by using geospatial APIs, SDKs, and services like search, maps, routing, tracking, and traffic.

- **Azure Cognitive Search** provides a search service over varied types of content. Cognitive Search includes indexing, AI enrichment, and querying capabilities.

- **Azure API Management** provides a single place to manage all of your APIs.

- **Azure App Service** deploys web applications that scale with your organization.



Azure IoT Architecture

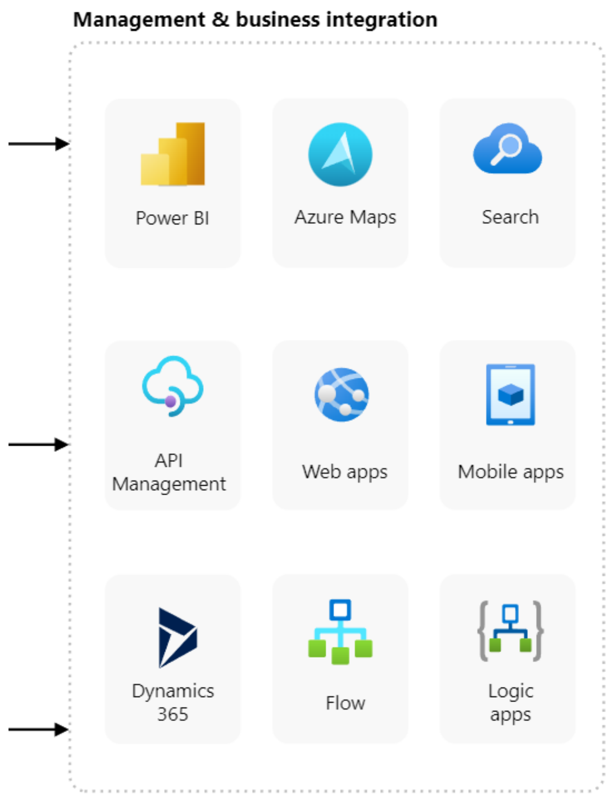
3. Actions

➢ **Azure Mobile Apps** builds cross platform and native apps for iOs, Android, Windows, Mac.

➢ **Dynamics 365** combines CRM and ERP in the cloud.

➢ **Microsoft Flow** is a SaaS offering for automating workflows across applications and other SaaS services.

➢ **Azure Logic Apps** creates and automates workflows that integrate your apps, data, services, and systems.




Thank You