

IoT Edge within the IoT Framework

Axel Dittmann

Diplom-Betriebswirt (FH)

Diplom-Wirtschaftsinformatiker (FH)

Global Technical Solution Specialist IOT

CISSP, MCP

Twitter: @DittmannAxel



Waves of Innovation

Cloud

Globally available, unlimited compute resources

IoT

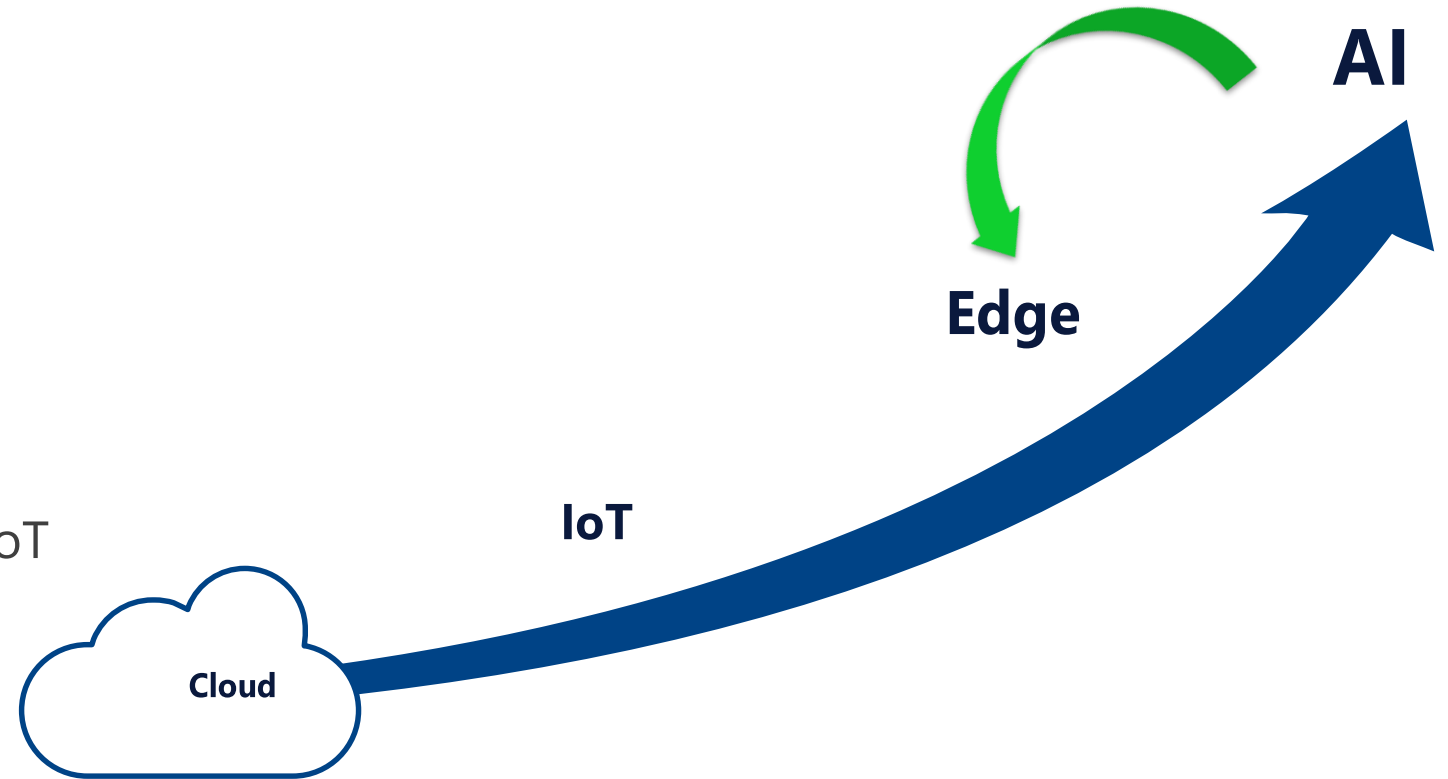
Harnessing signals from sensors and devices, managed centrally by the cloud

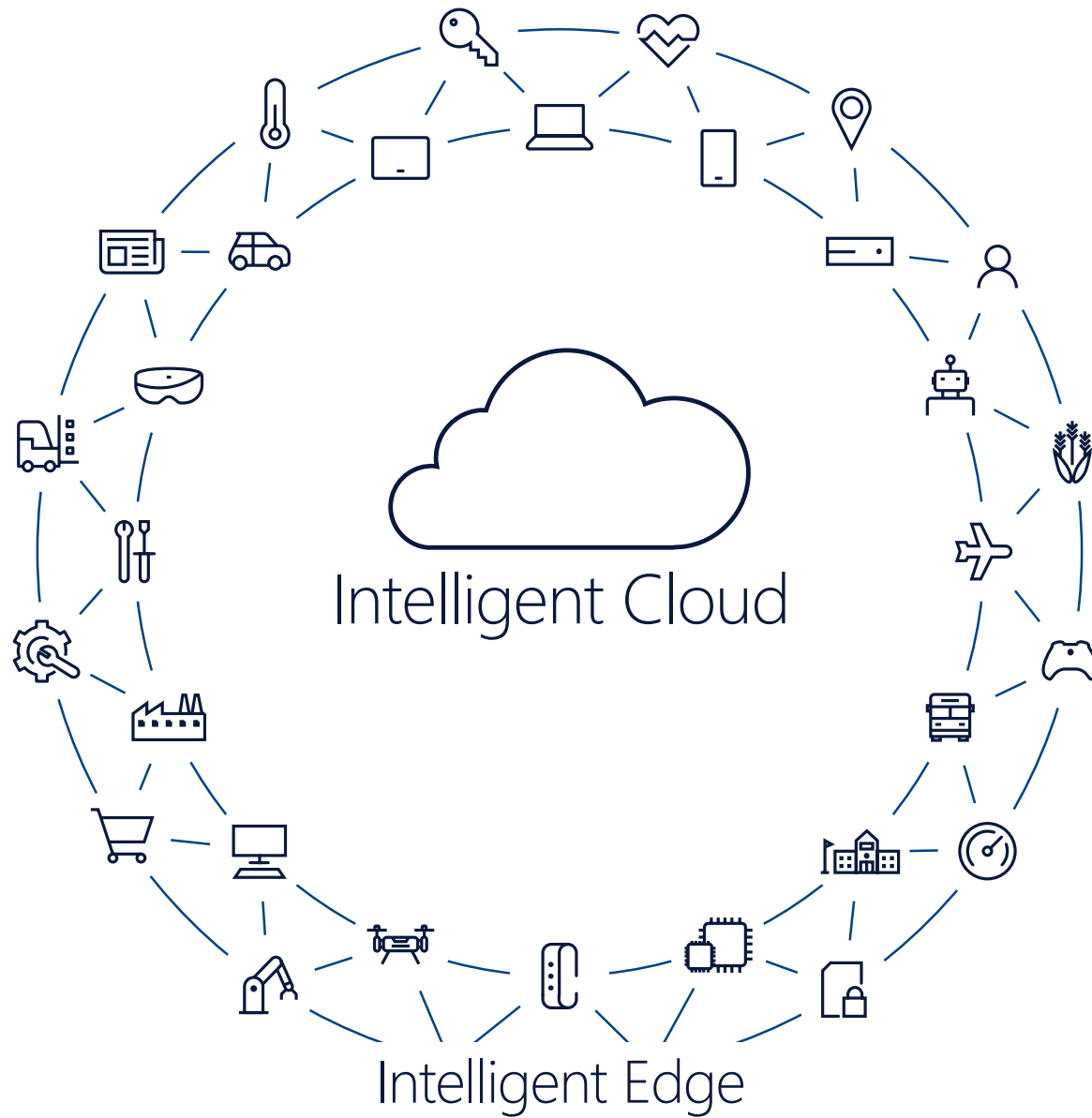
Edge

Intelligence offloaded from the cloud to IoT devices

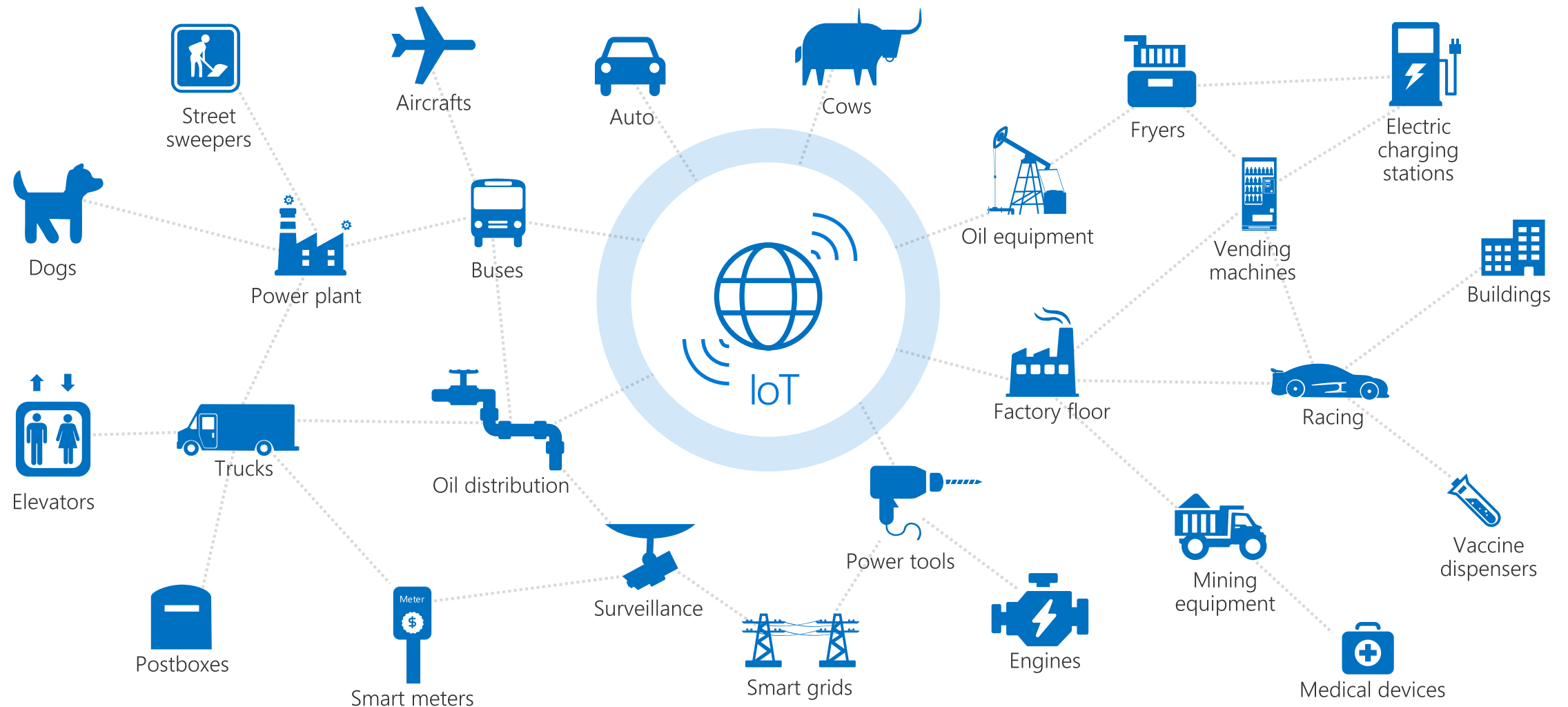
AI

Breakthrough intelligence capabilities, in the cloud and on the edge





When to use edge?



Challenges today create high barriers to entry



Cloud barriers



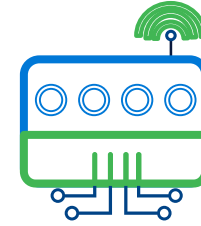
High volume of data collection sources



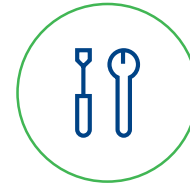
High cost of transporting data to the cloud



Limits to real-time insights



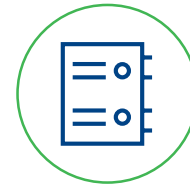
Edge barriers



High developer skillset for hardware, cloud, edge



custom code for everything
= No standardization



Manual set up and integration
= Does not scale

Introducing Azure IoT Edge

A service spanning cloud and edge to run cloud intelligence directly on your IoT devices



Use existing AI, cloud analytics or create your own code



Deploy workloads as containers via IoT Edge runtime

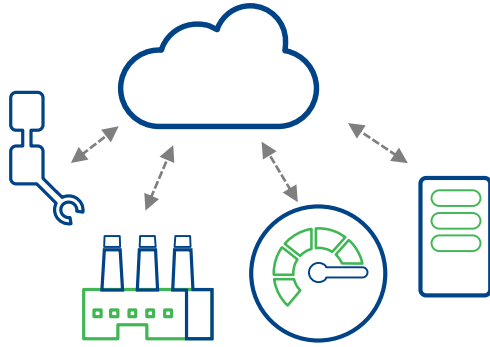


Manage devices and containers centrally in the cloud



Secure solution from chipset to cloud

IoT in the Cloud and on the Edge

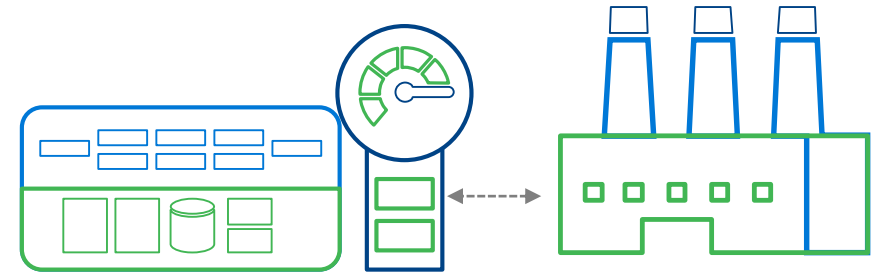


IoT in the Cloud

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

Low latency tight control loops require near real-time response

Protocol translation & data normalization

Privacy of data and protection of IP

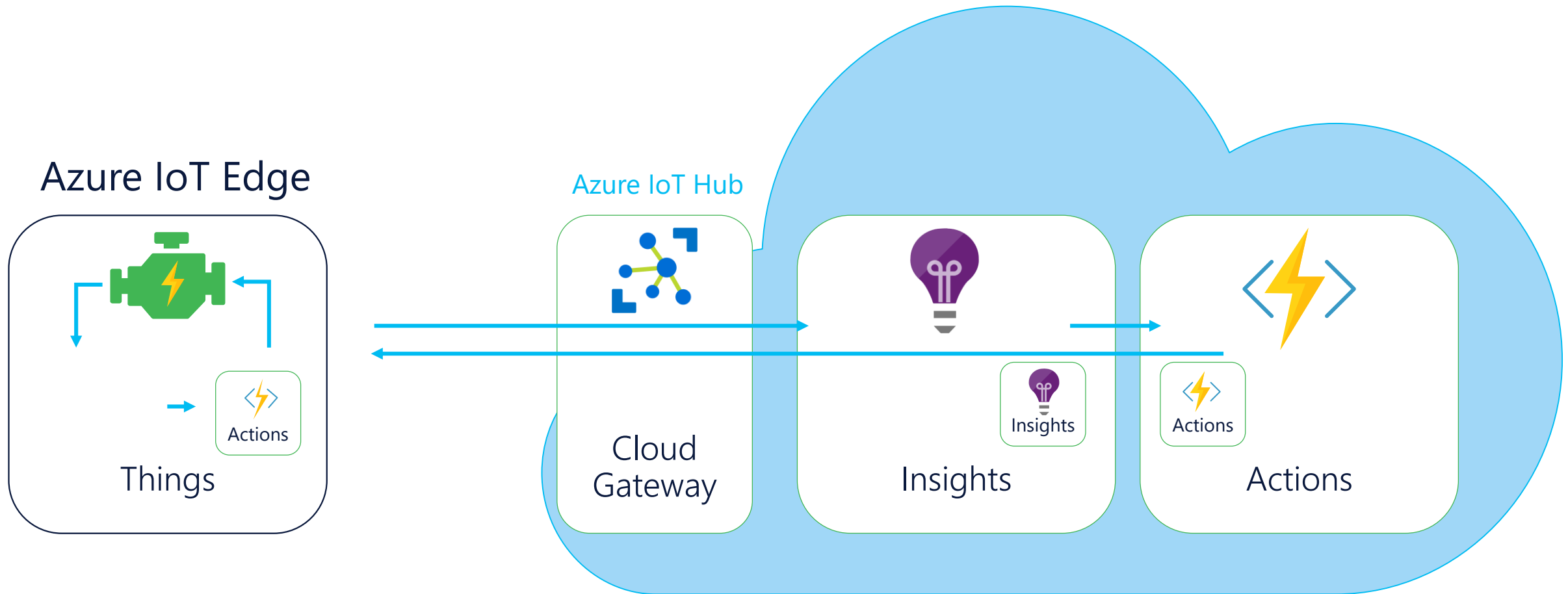
Symmetry

Operational patterns for Azure IoT Edge

- **Protocol translation** – Collect data using any protocol and translate to IoT friendly protocols (e.g. Modbus -> MQTT)
- **On-prem data aggregation and analysis** – Aggregate and save on bandwidth, cost, privacy, IP
- **Offline** – Short or long term
- **Deploy intelligence at the edge** – Azure Machine Learning and AI, Azure Stream Analytics, Functions, your own code

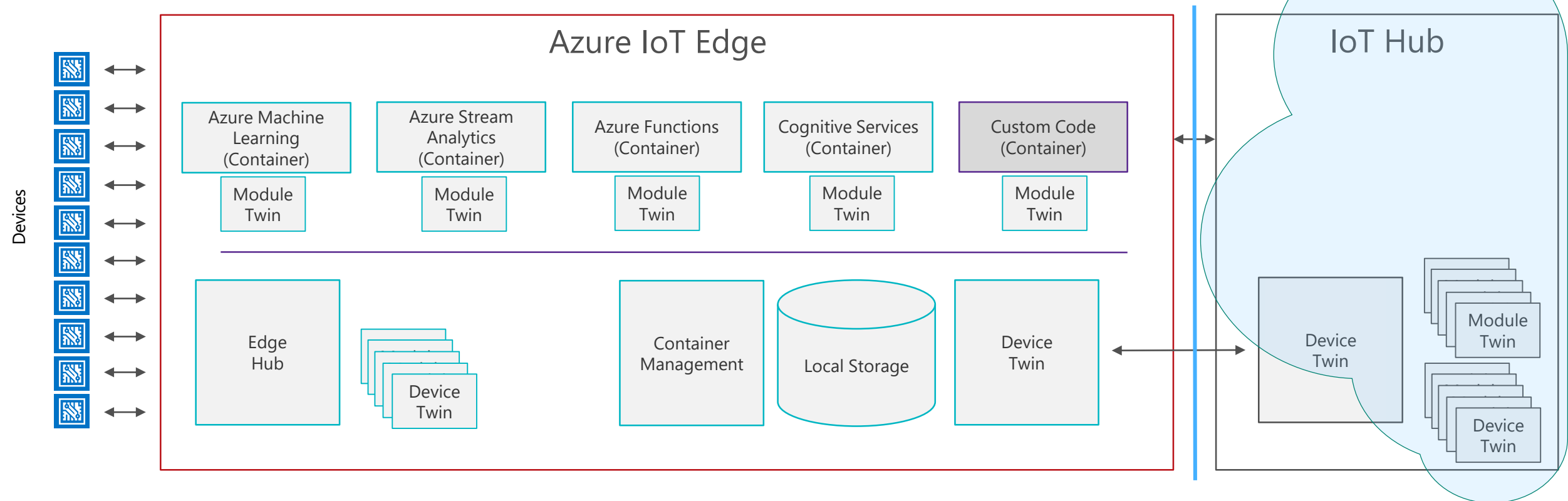


IoT Pattern + Edge



Azure IoT Edge V2 (preview)

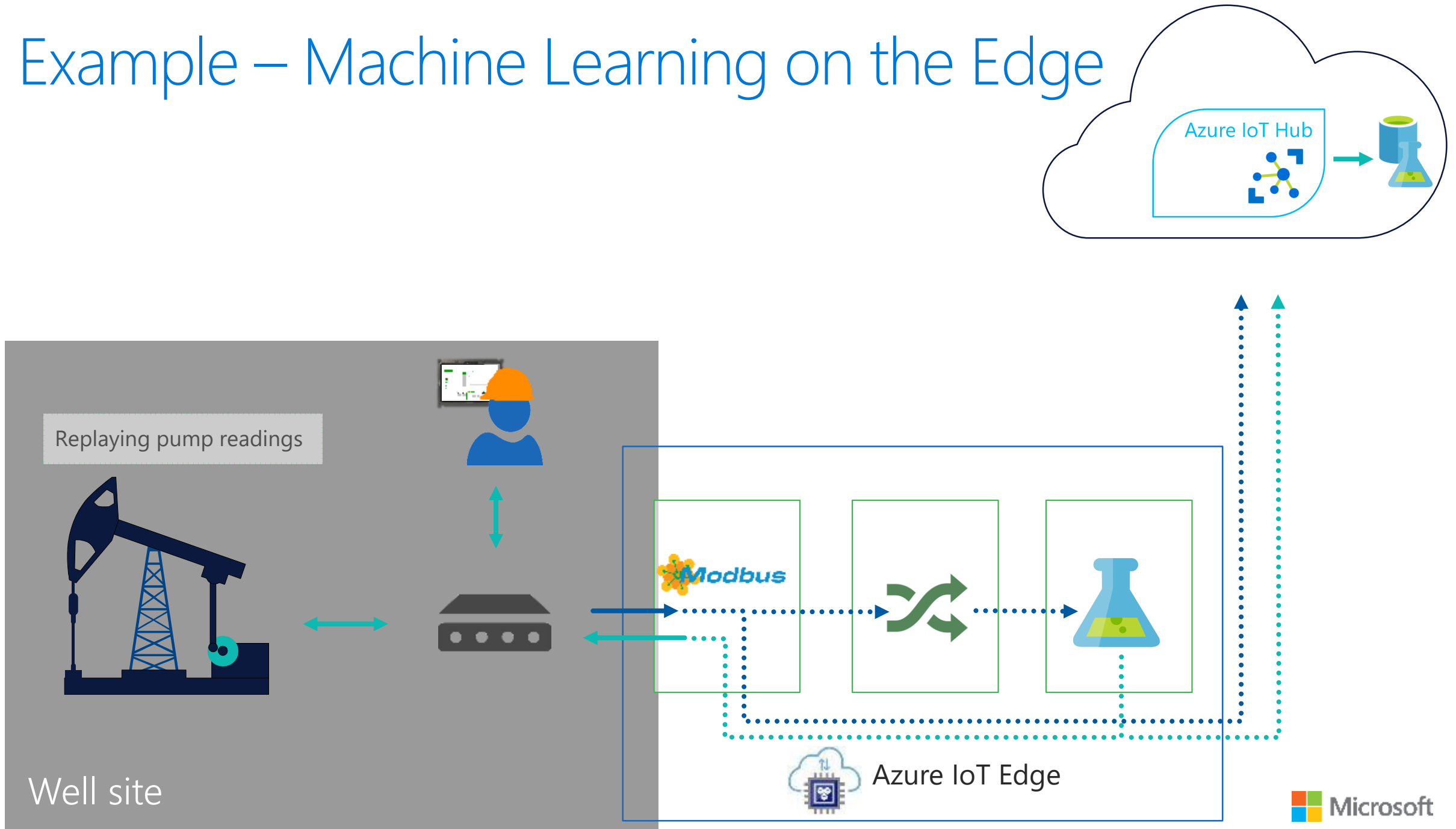
- Container based workloads
- Azure Functions
- Azure Stream Analytics
- Azure Machine Learning
- Cognitive Services
- Offline / Synchronized Device Twins
- Local Storage
- Container Management
- Local "IoT Hub"
- HA/DR, Cloud Dev/Test Support



Azure IoT Edge Design Principles

- **Secure**
Provides a secure connection to the Azure IoT Edge, update software/firmware/configuration remotely, collect state and telemetry and monitor security of the device
- **Cloud managed**
Enables rich management of Azure IoT Edge from Azure provide a complete solution instead of just an SDK
- **Cross-platform**
Enables Azure IoT Edge to target the most popular edge operating systems, such as Windows and Linux
- **Portable**
Enables Dev/Test of edge workloads in the cloud with later deployment to the edge as part of a continuous integration / continuous deployment pipeline
- **Extensible**
Enables seamless deployment of advanced capabilities such as AI from Microsoft, and any third party, today and tomorrow

Example – Machine Learning on the Edge



Next steps

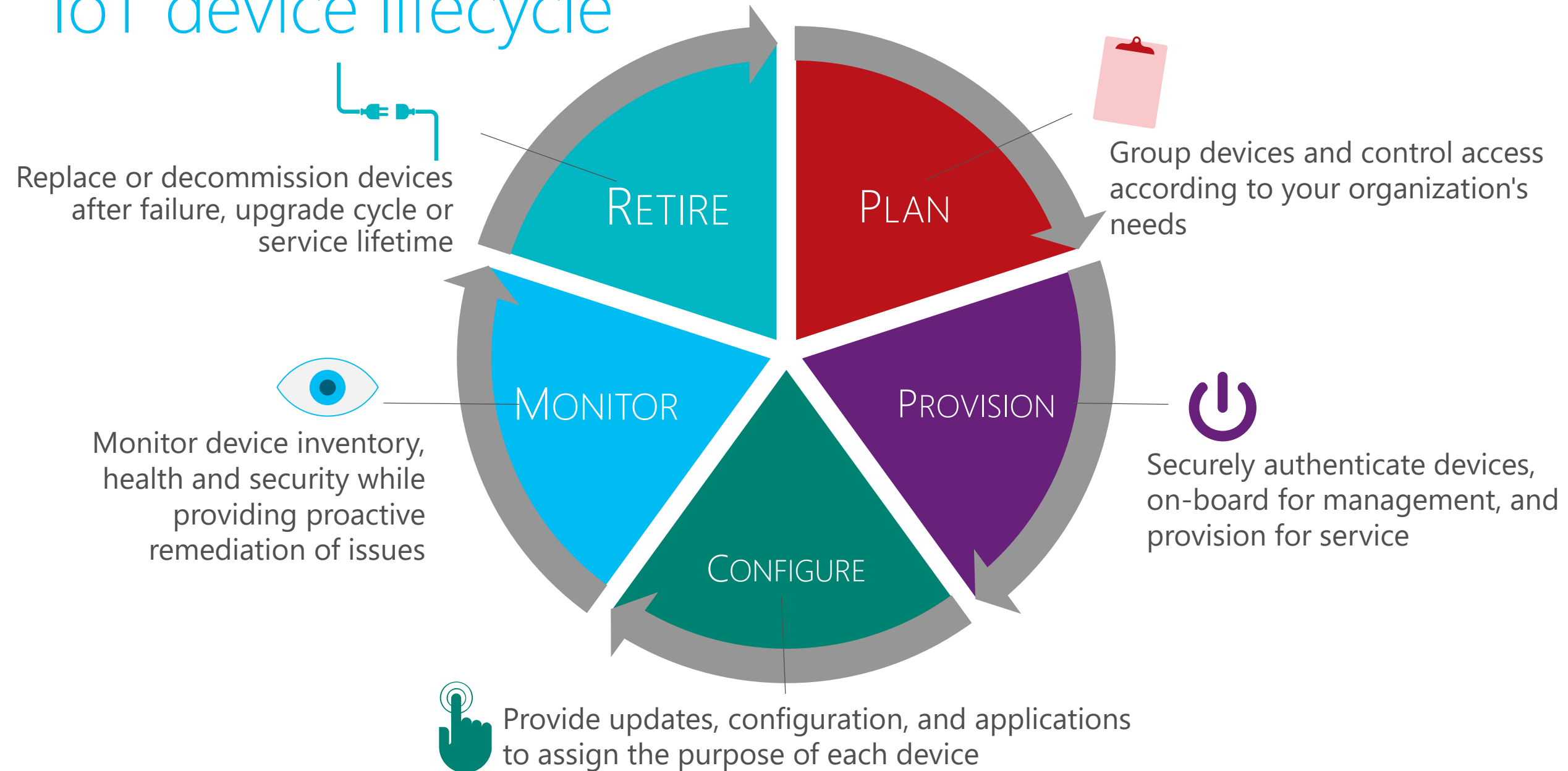
- 1 Learn more
aka.ms/azure-iot-edge
- 2 Get started
docs.microsoft.com/azure/iot-edge



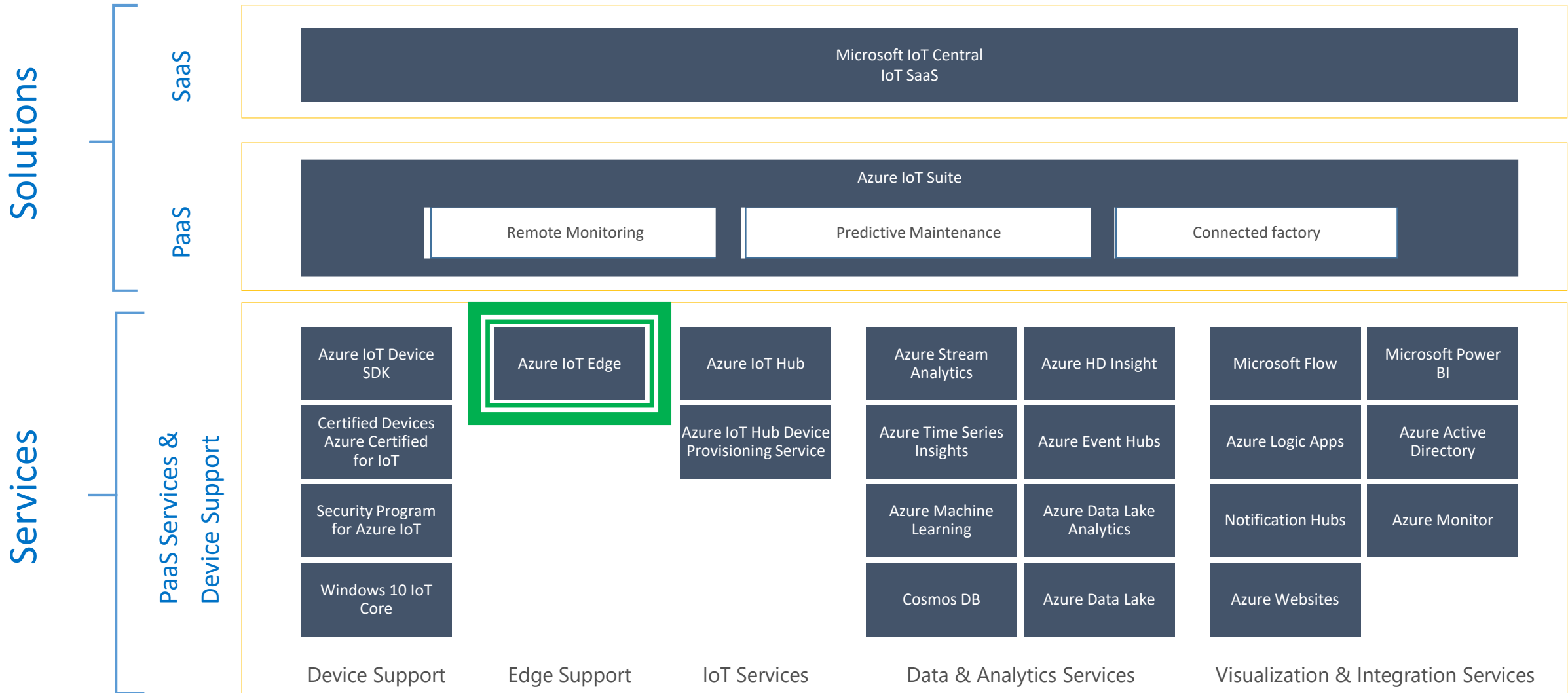


Thank You

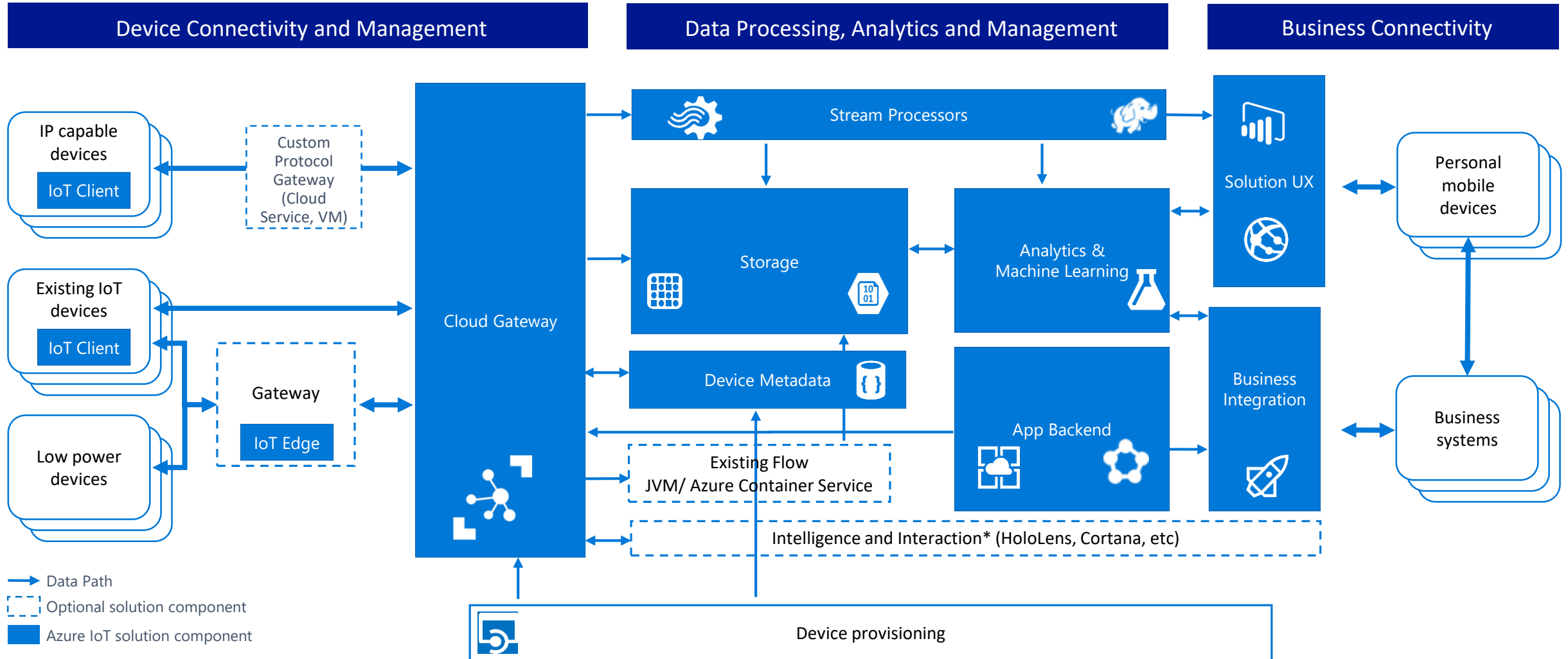
IoT device lifecycle

















Comprehensive Set of Capabilities for IoT Solutions



Azure IoT Reference Architecture



The Seven Properties of Highly Secure Devices:

	Hardware-based Root of Trust		Unforgeable cryptographic key generated and protected by hardware. <i>Does the device have an unforgeable identity, inseparable from the hardware?</i>
	Small Trusted Computing Base		Security enforcement features protected from other hardware and software. <i>Is most of the device's software outside the device's trusted computing base?</i>
	Defense in Depth		Multiple countermeasures mitigate the consequences of any one successful attack. <i>Is the device still protected if the security of one layer of device software is breached?</i>
	Compartmentalization		Internal barriers limit the reach of any single failure. <i>Can a compromised software sub-component be reset & restarted independently?</i>
	Certificate-based Authentication		Trust brokered using signed certificates, proven by unforgeable cryptographic keys. <i>Does the device use certificates instead of passwords for authentication?</i>
	Renewable Security		Device security renewed to overcome evolving threats and security breaches. <i>Is the device's software updated automatically?</i>
	Failure Reporting		Device failures automatically reported to cloud-based failure analysis system. <i>Does the device report failures to its creator?</i>



= Silicon support required.



= OS support required.



= Cloud Service support required.