Azure MVP

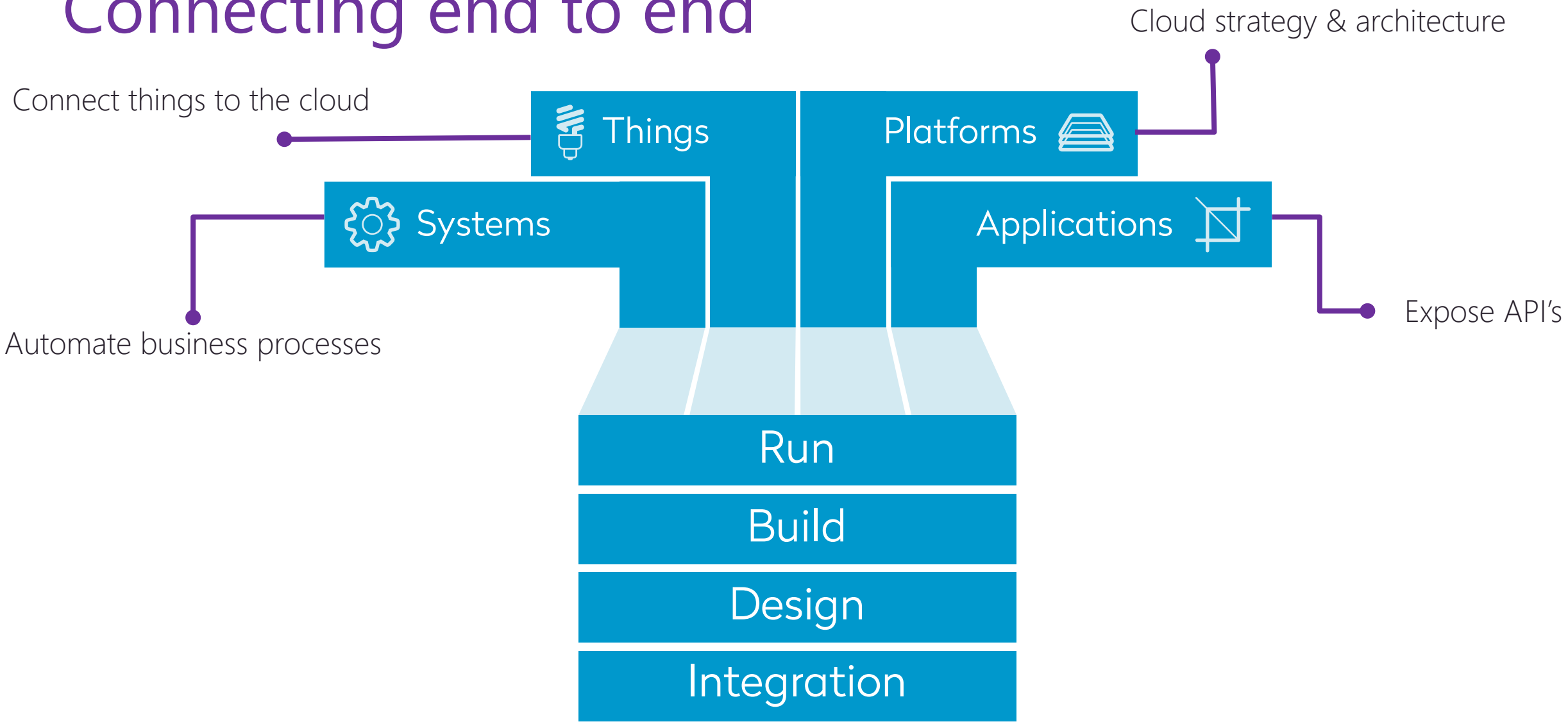
SamVanhoutte

Hi, I am Sam, CTO of Codit

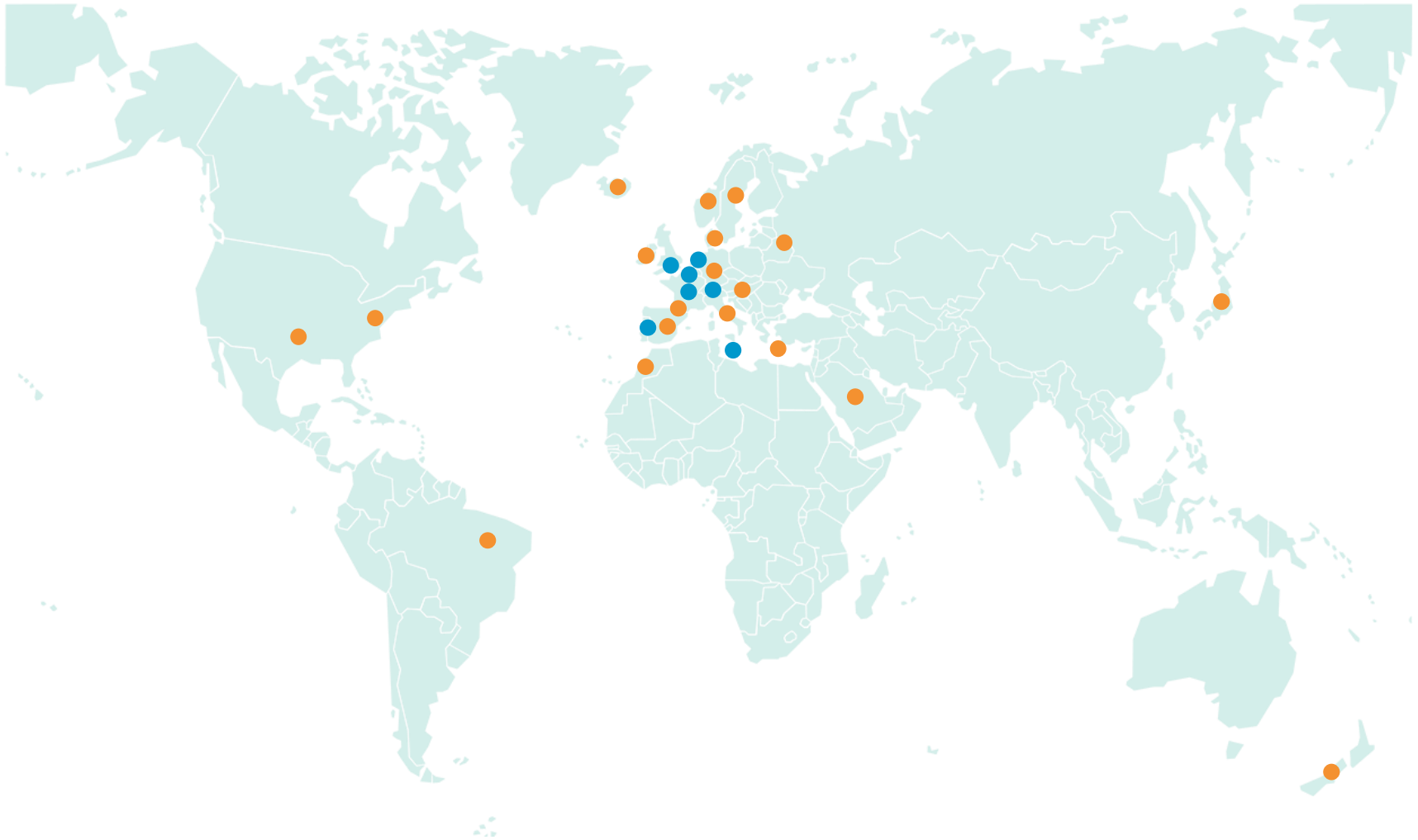
Azure IoT Hub

Deep dive

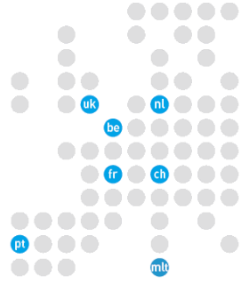
Connecting end to end



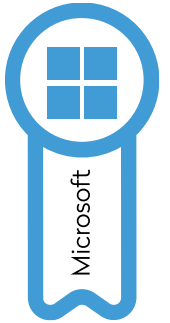
About Codit



2000 Belgium
2004 France
2013 Portugal
2016 Switzerland
2016 UK
2016 The Netherlands
2017 Malta



180
worldwide



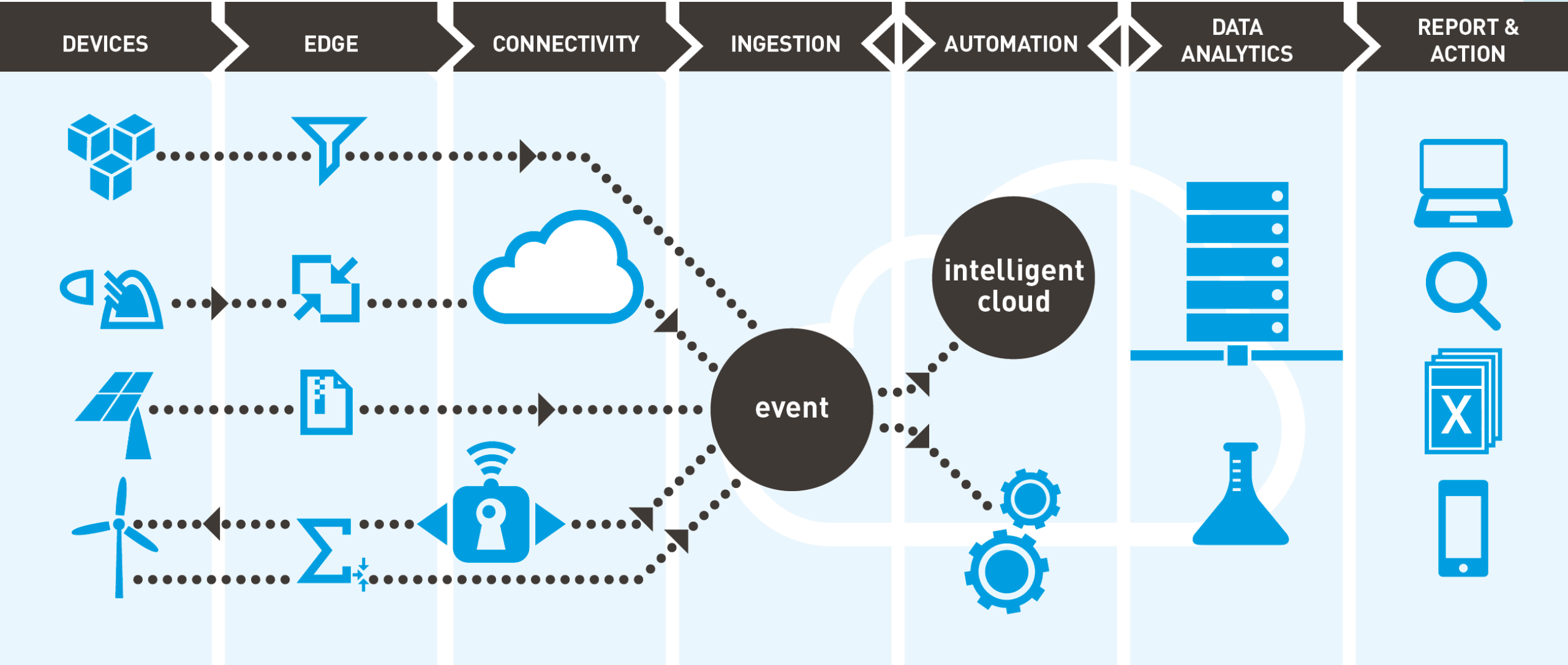
Largest Microsoft partner in Europe for integration, API management, IoT and Azure Solutions

Microsoft Partner
Microsoft

Gold Application Development
Gold Application Integration
Gold Cloud Platform
Gold Data Analytics

Positioning

The IoT value chain



Azure IoT Hub

Designed for IoT

Connect millions of devices

Service assisted communications

Devices are not servers

Use IoT Hub to enable secure bi-directional comms

Cloud-scale messaging

Device-to-cloud and Cloud-to-device

Durable messages (at least once semantics)

Cloud-facing feedback

Delivery receipts, expired messages

Device communication errors

Per-device authentication

Individual device identities and credentials

Operations monitoring

Service-side endpoint emitting device connectivity events

Multi-protocol

Natively supports AMQP, MQTT, and HTTP/1

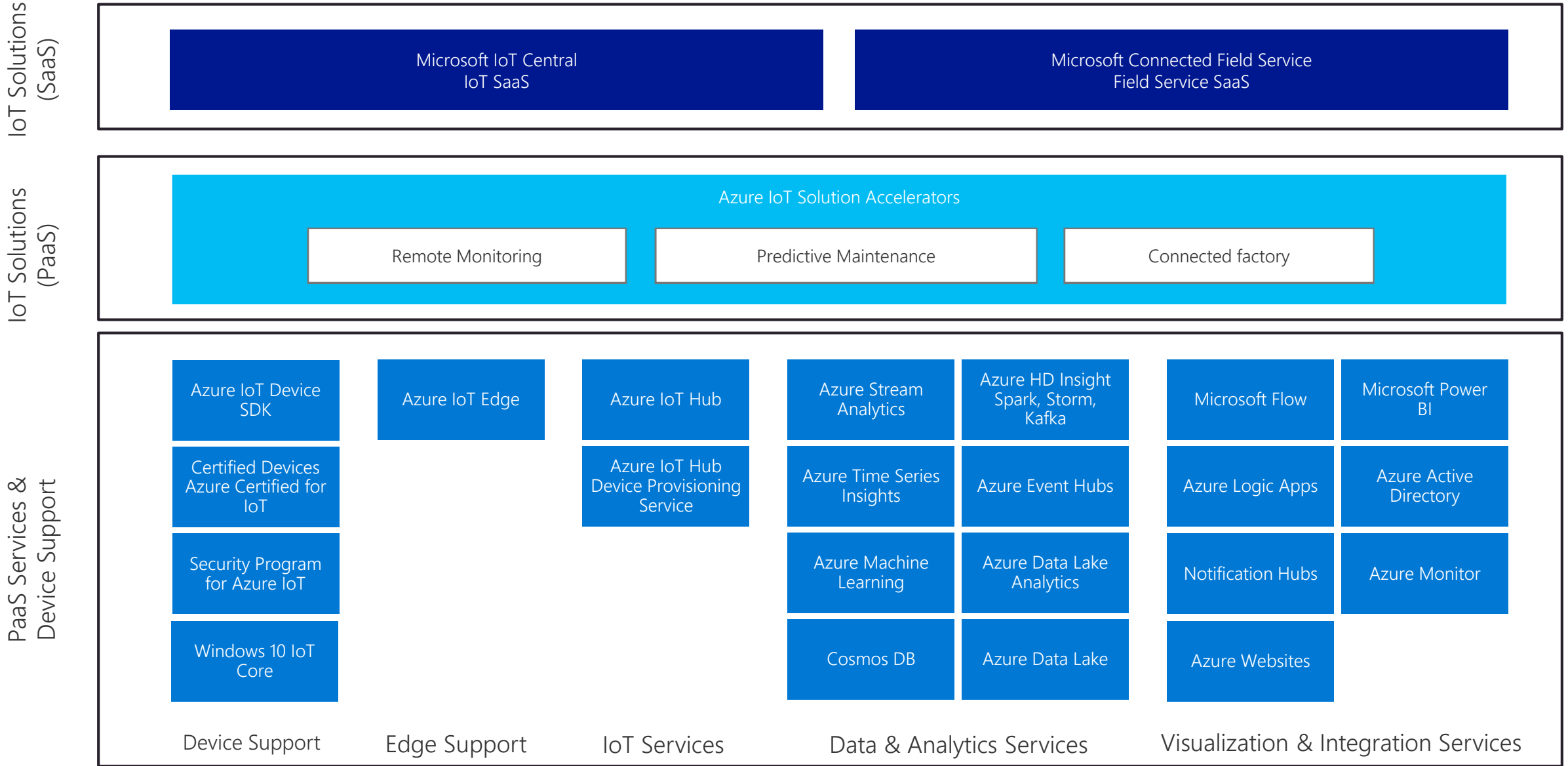
Designed for extensibility to custom protocols

Multi-platform

Device SDKs available for multiple platforms (e.g. RTOS, Linux, Windows)

Multi-platform Service SDK.

The Azure IoT Landscape



Security

Access policies

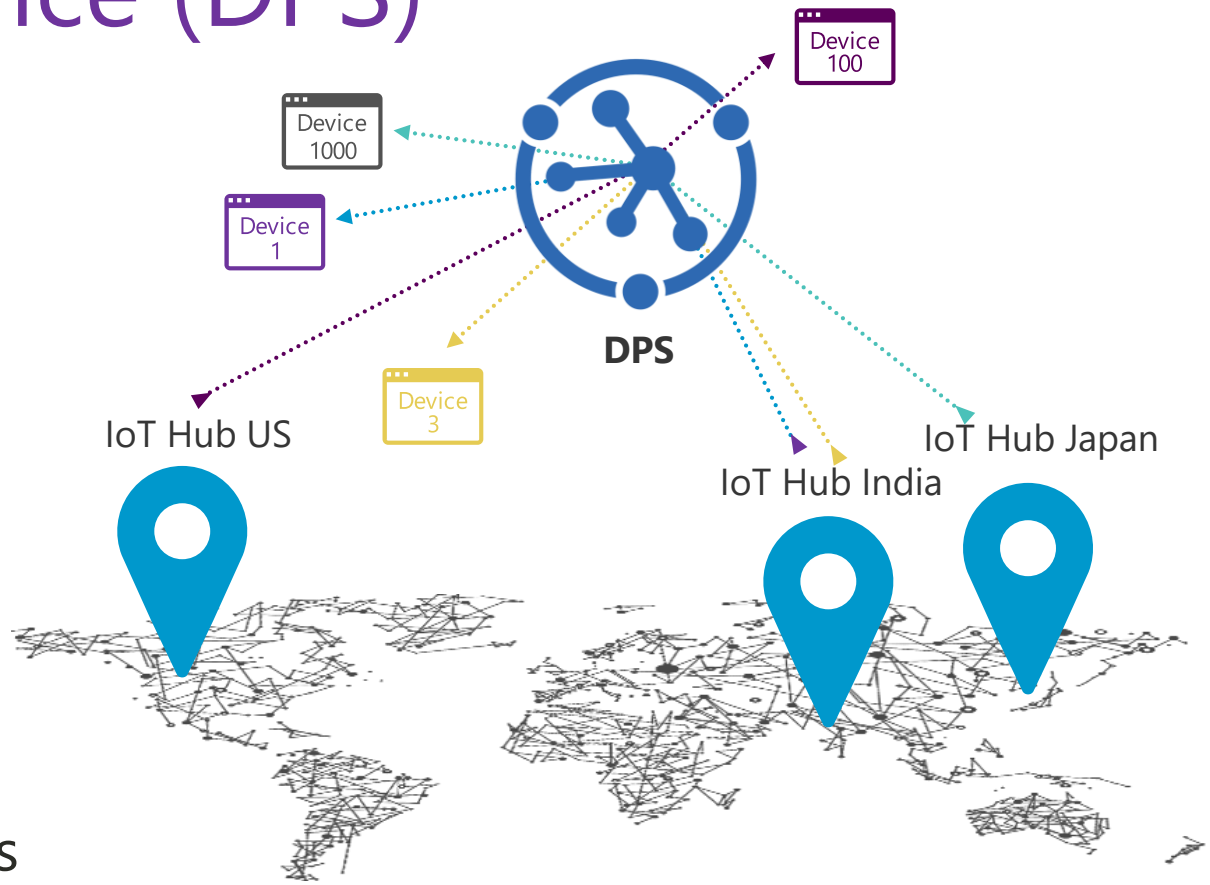
- ServiceConnect (cloud side reading messages)
- DeviceConnect (individual devices – or send on behalf)
- RegistryRead (read only device monitoring)
- RegistryReadWrite (device management)

Authentication support

- Device id + device key
  - Security credentials are never sent over the wire
  - Token transport is protocol specific (MQTT, AMQP, HTTPS)
- X.509 certificates
  - Existing cert
  - Self signed cert
  - CA-signed cert

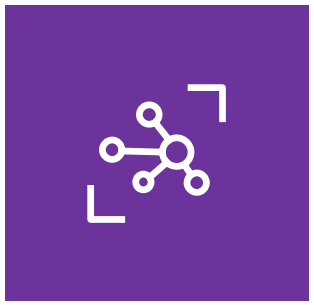
Device Provisioning Service (DPS)

- Simplify with zero touch provisioning
- Supports multiple locations
- Easiest way to mass-provision devices
- URL stability
- Enhanced security through HSM
- For any device compatible with IoT Hub
- Remove human error
- Minimize manual connection requirements
- Multitenancy support

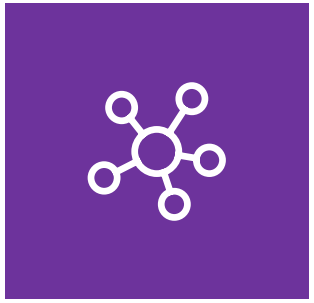


DPS knows exactly which IoT Hub to connect and provision

Device Provisioning Service : concepts



Linking an IoT hub to DPS gives DPS permissions to register devices to the hub



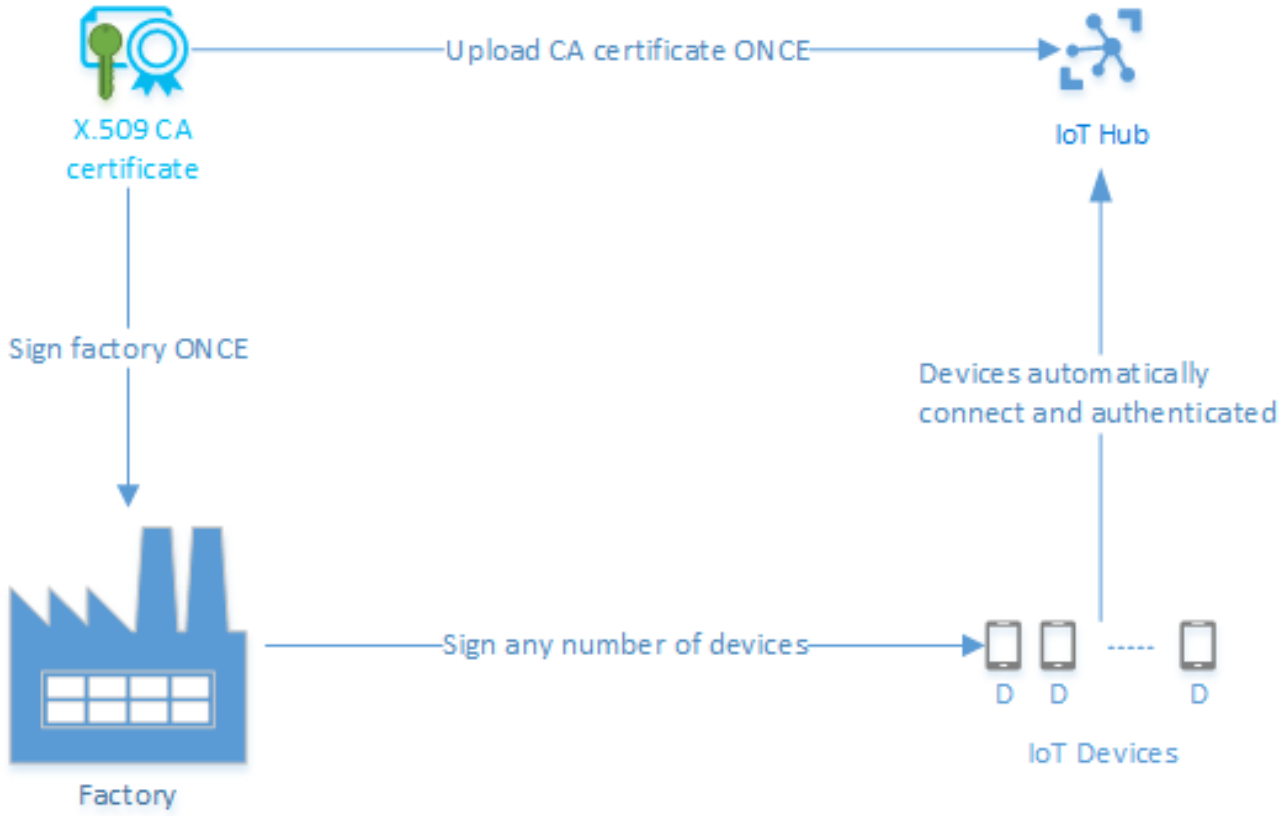
Links can be cross-region or cross-subscription

Determines how DPS assigns devices to linked hubs

- Evenly weighted distribution
- Lowest latency
- Static configuration via the enrollment list

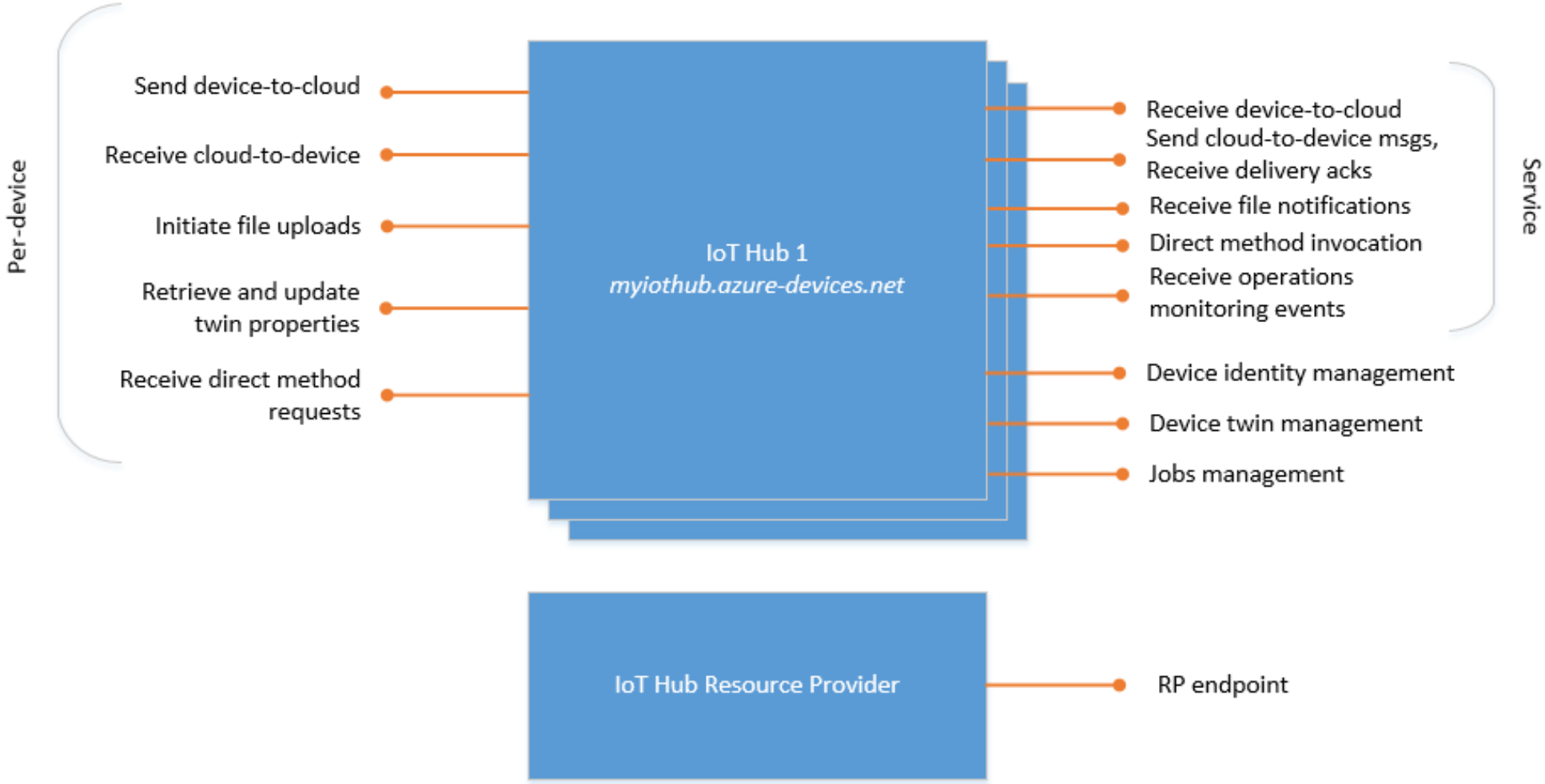
x.509 C.A. Support on IoT Hub

- Configure CA cert (per factory?) on IoT hub
  - Sign all devices once at production time
- Authentication happens through the CA trust
- Can be combined with DPS

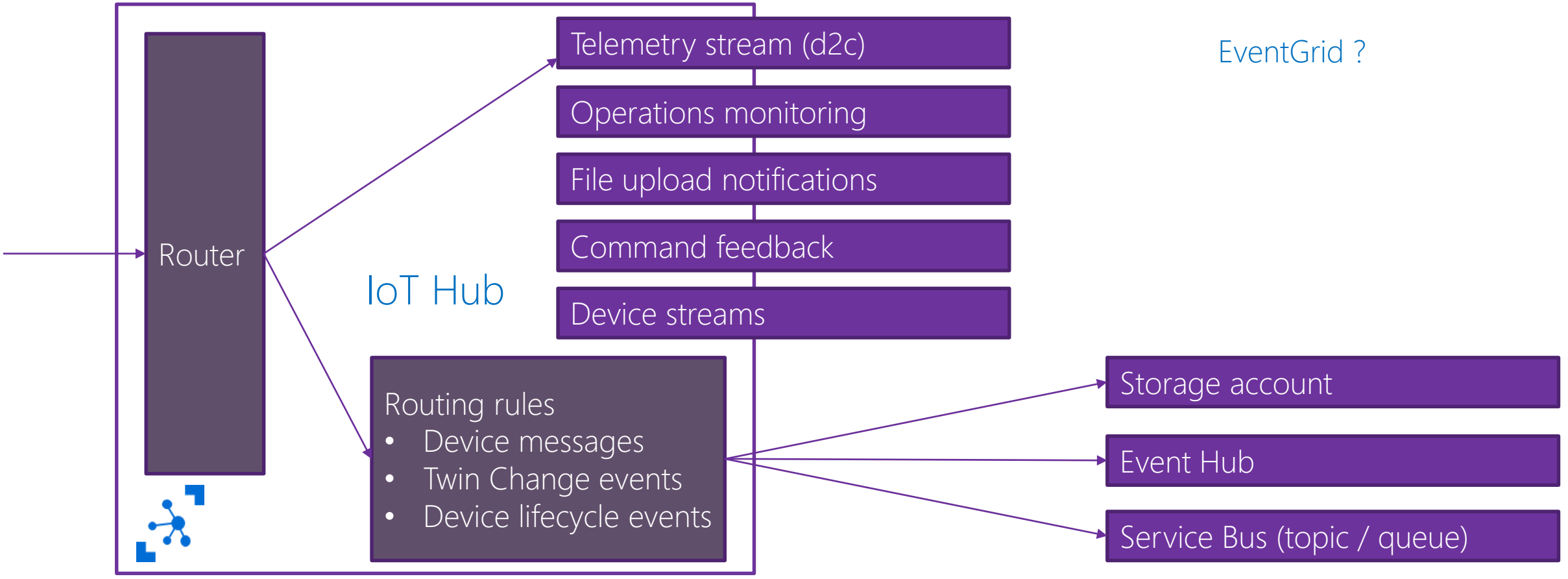


Endpoints & routes

IoT Hub endpoints

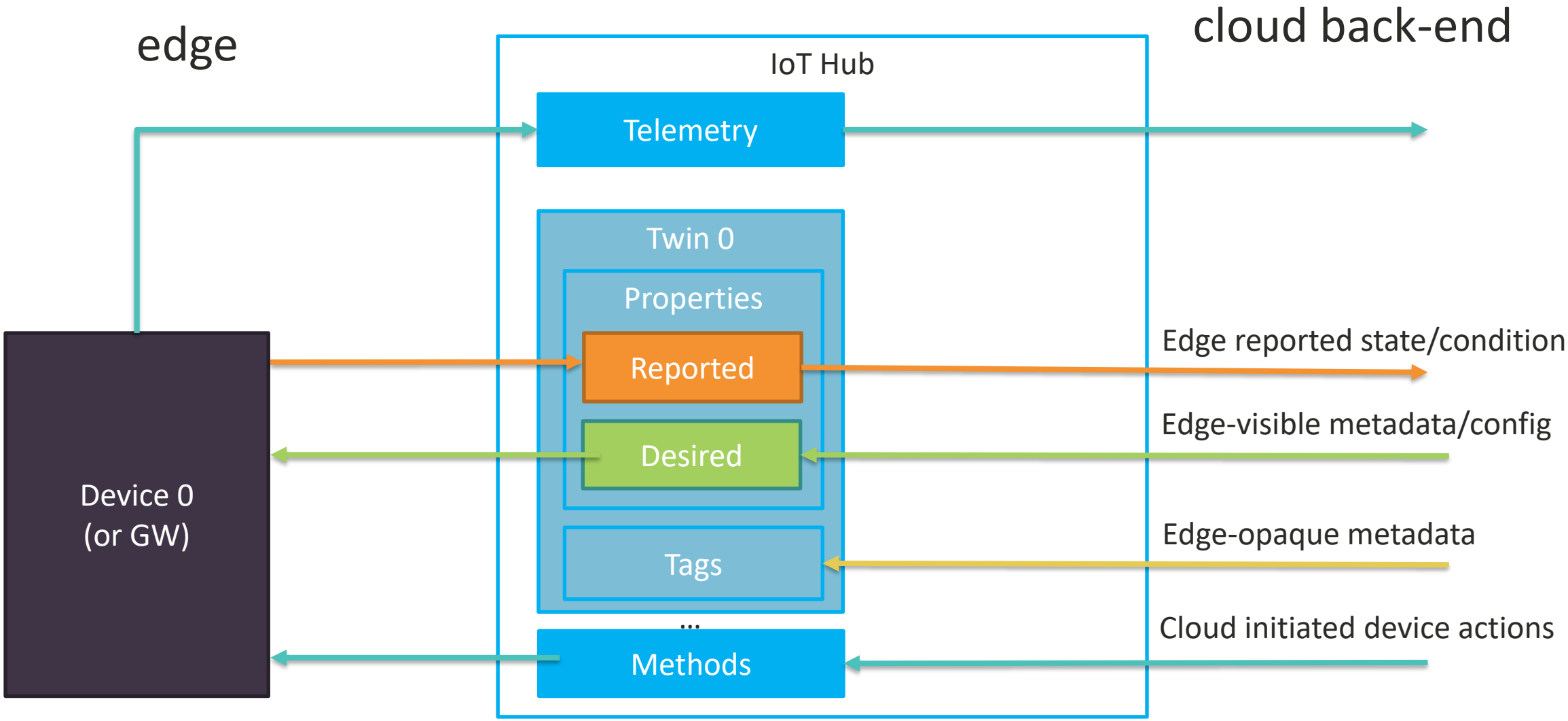


IoT Hub endpoints & routing



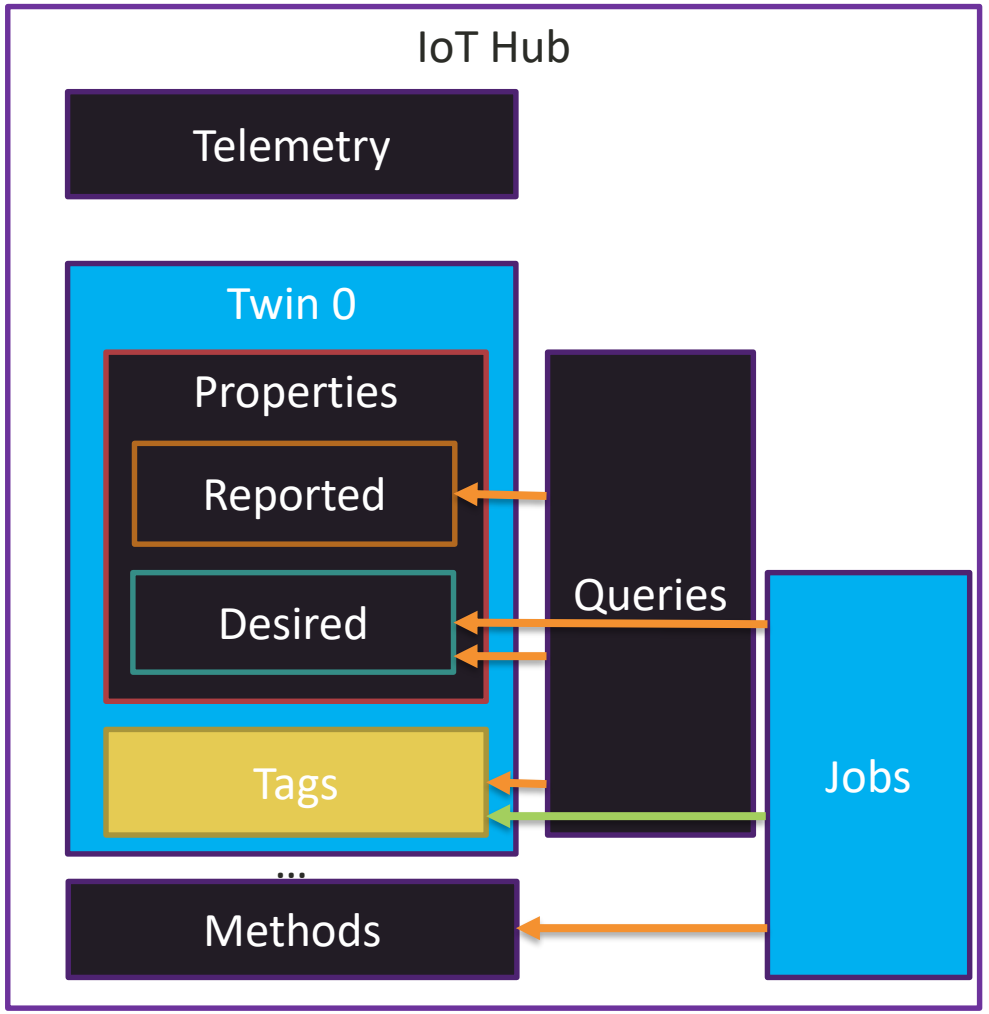
Device twins

Device twins



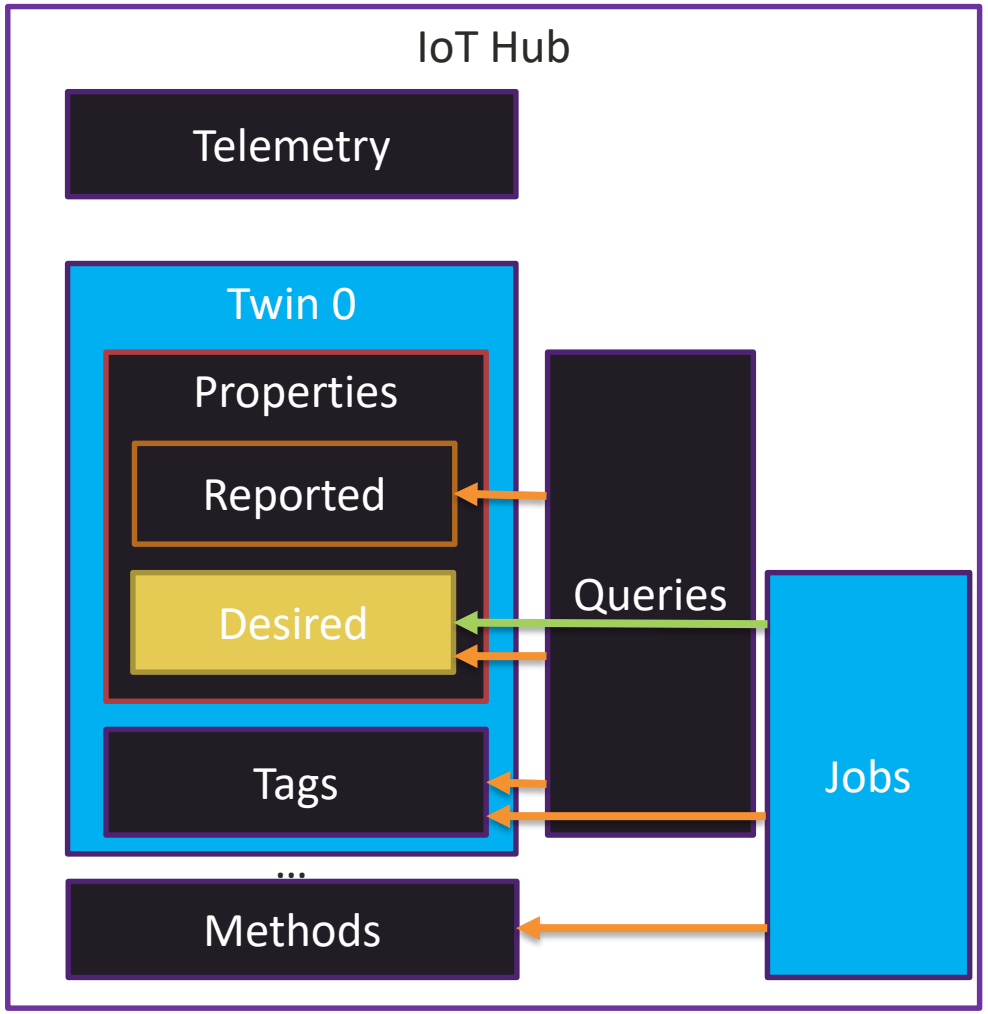
Device metadata & organisation

Set tags on twins to simplify the task of finding and targeting devices



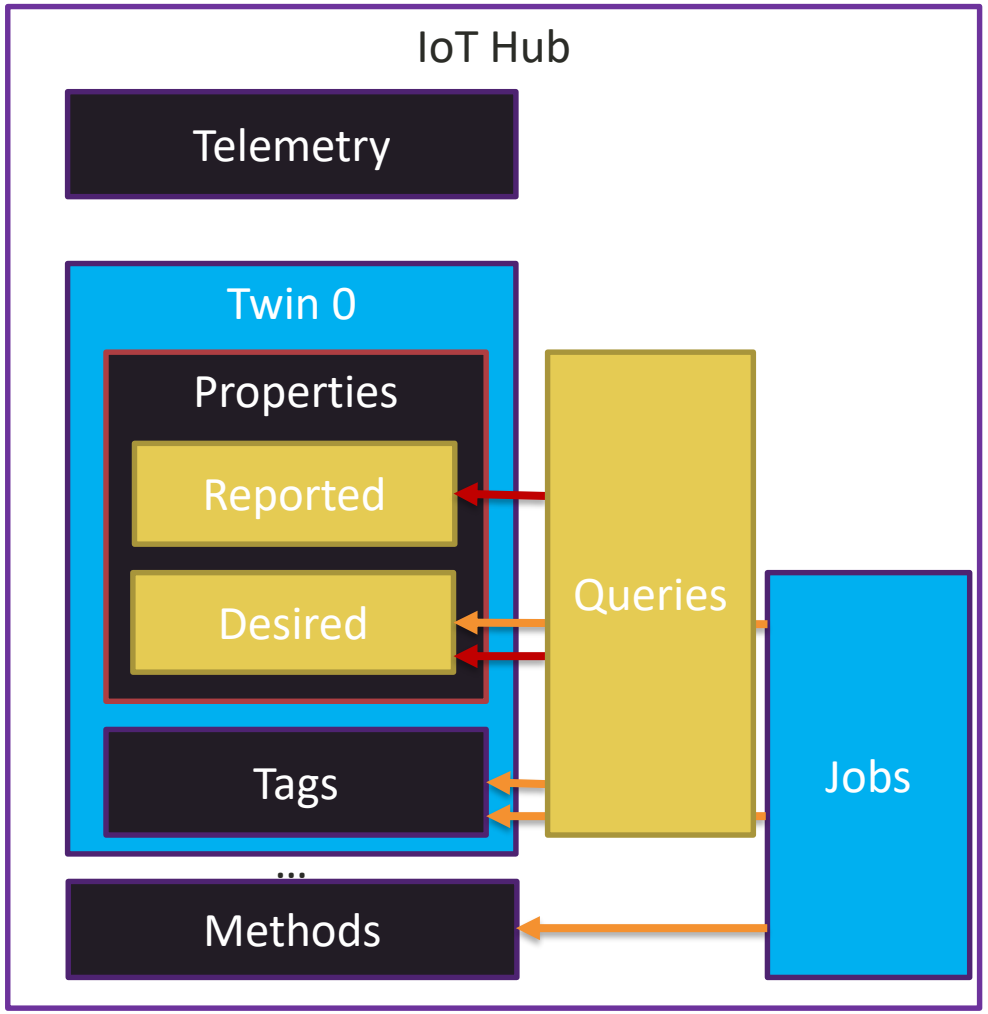
Device management & configuration

Set desired properties on twins to set common policy across a large group of devices



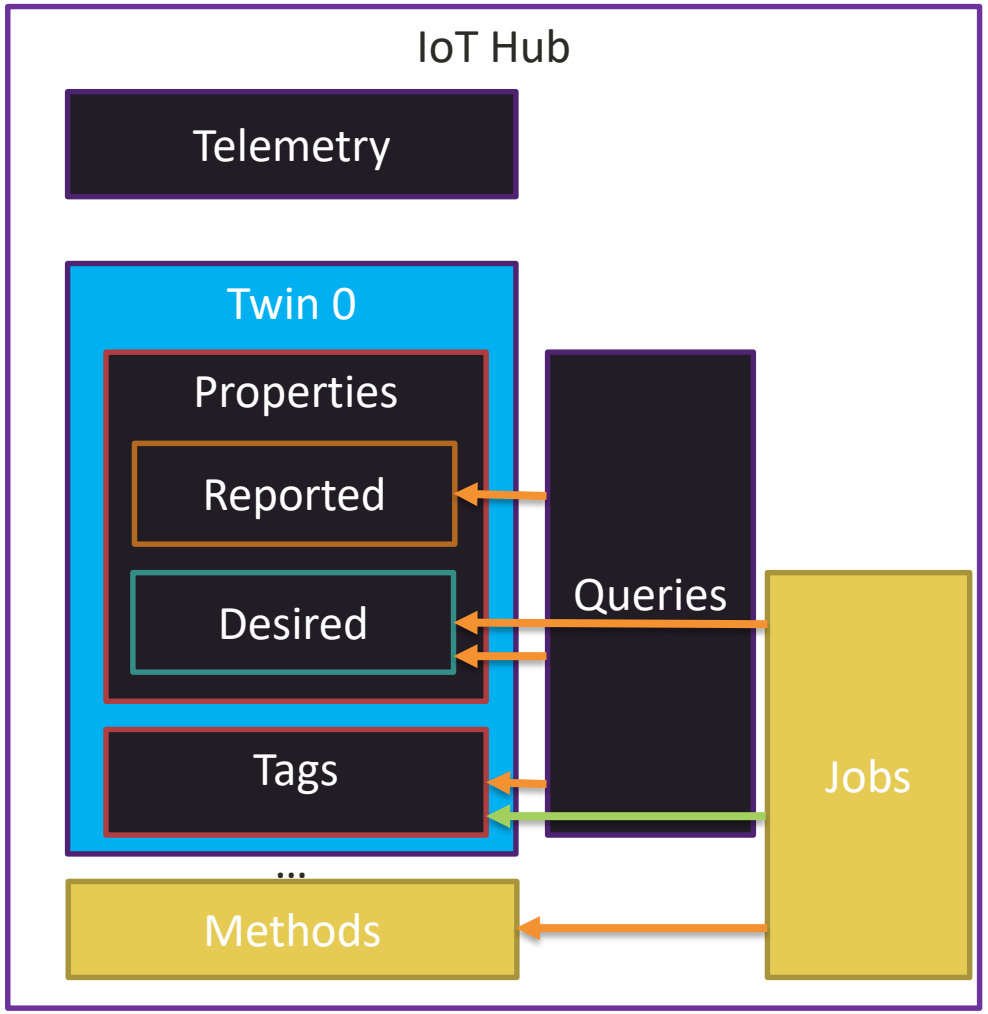
Device querying & compliance

Query desired and reported properties to attest device compliance and surface problems



Device troubleshooting & updating

Initiate an action directly on a device or schedule an action with a job



Messaging & telemetry

Device to cloud messaging

- **Used for telemetry streams**

- AMQP / MQTT / HTTPS
- Send to **/devices/{deviceid}/messages/events**
- Maximum 256 KB
- Body (opaque) + Properties (key-value)
- Partitioning per originating deviceid
- Process with EventProcessorHost (like Event Hub)

Reported properties

- **State information & job status**

- AMQP / MQTT
- Maximum 8 KB
- JSON structure

- Process, using routes on **twinChangeEvents** endpoint

IoT Hub file upload

- Upload abstracted in client SDK
  - `hubClient.UploadToBlobAsync("file.txt", fileStream);`
- Using a claim check pattern
  - Content stored in associated storage account on blob (client endpoint /devices/{deviceId}/files)
  - Event triggered on service endpoint (/messages/servicebound/fileuploadnotifications)

Command & control

Device to cloud messaging

- **Asynchronous operation: device can be offline**

- AMQP / MQTT / HTTPS
- Send to **/devices/{deviceId}/messages/devicebound**
- Maximum 64 KB
- Body (opaque) + Properties (key-value)
- Important to configure TTL (time to live)
- No support for jobs
- At least once guaranteed delivery (device can reject / abandon)

Direct method

- **Interactive (sync) operation: device has to be online**

- MQTT only
- MQTT topic: **$iothub/methods/POST/{method name}/**
- Passing request body, maximum 8KB
- Configurable timeout (default: 30 secs)
- Device disconnected? 404
- Support for jobs

Desired properties

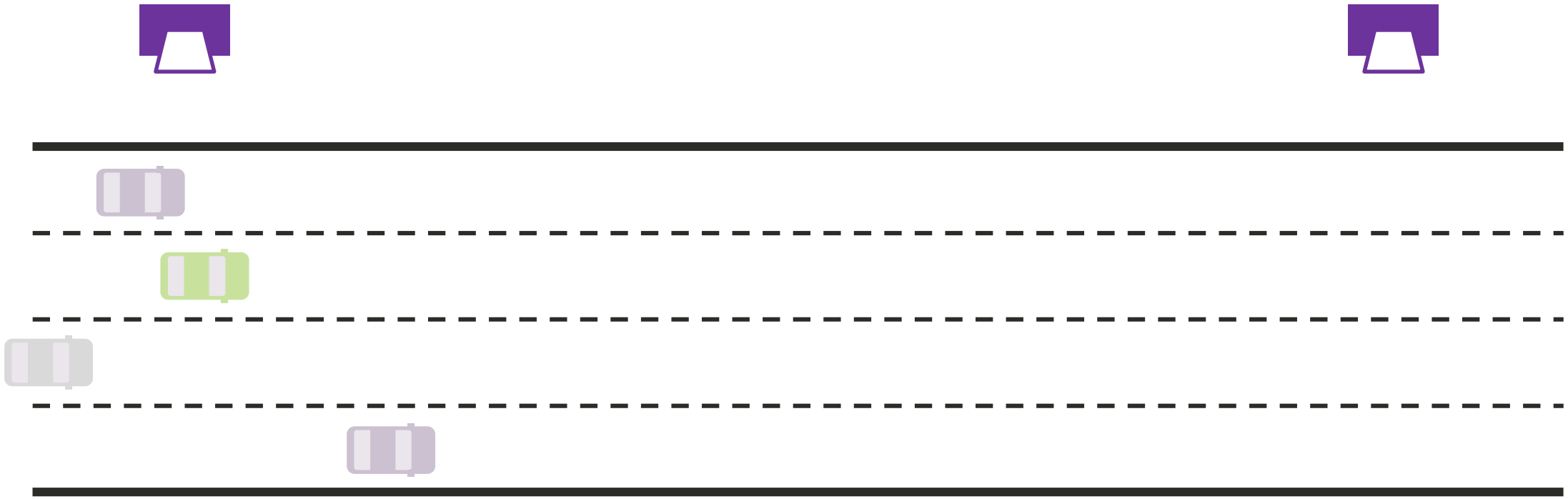
- **Set configuration**

- AMQP / MQTT
- Maximum 8 KB
- JSON structure
- Support for jobs

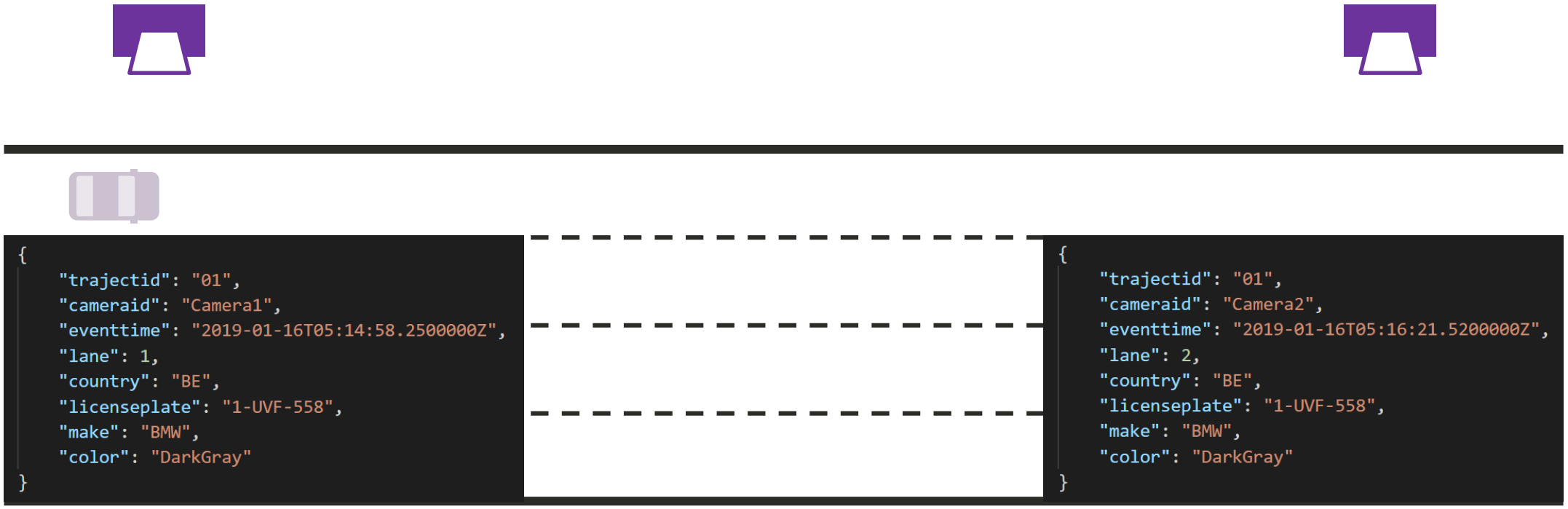
- Durable (persisted in twin).

Configuration management

Traffic camera scenario



Traffic camera scenario



Device jobs

- **Schedule updates or commands for selection of devices**

- Selection: based on device query
- Actions:
  - Update desired properties
  - Update tags
  - Invoke direct methods
- Query on job status, using job id

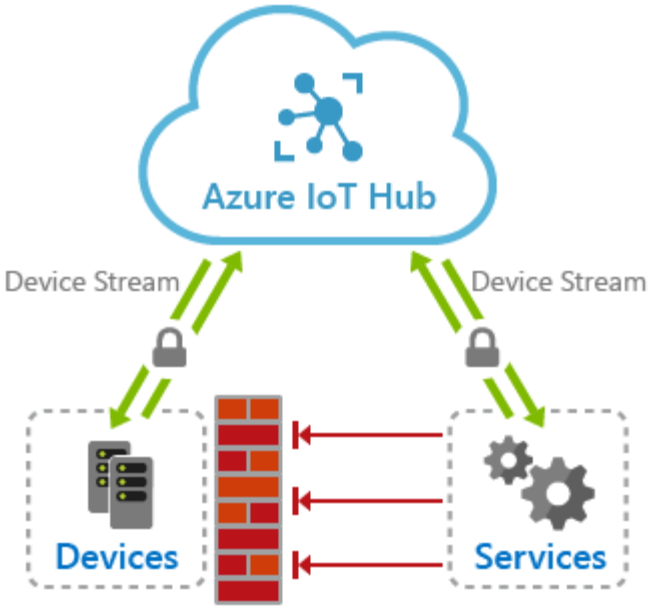
IoT Device configurations

- Apply configurations to multiple devices, based on metadata
- Define settings in device twin
- Add metrics (optional)
  - through SQL Query against Twins
  - Example: SELECT deviceId FROM devices WHERE properties.reported.statusCode = 0
- Set target devices
  - Priority (higher number = highest priority)
  - Target condition, using tags.
  - Example: tags.country='Belgium'

Recent additions

IoT Device streams

- Bi-directional, firewall friendly FTP tunnels
  - TCP compatible web sockets over 443
  - TLS enabled
- Cloud to device, mediated by streaming endpoint
- Scenarios
  - RDP, SSH
  - Proxy

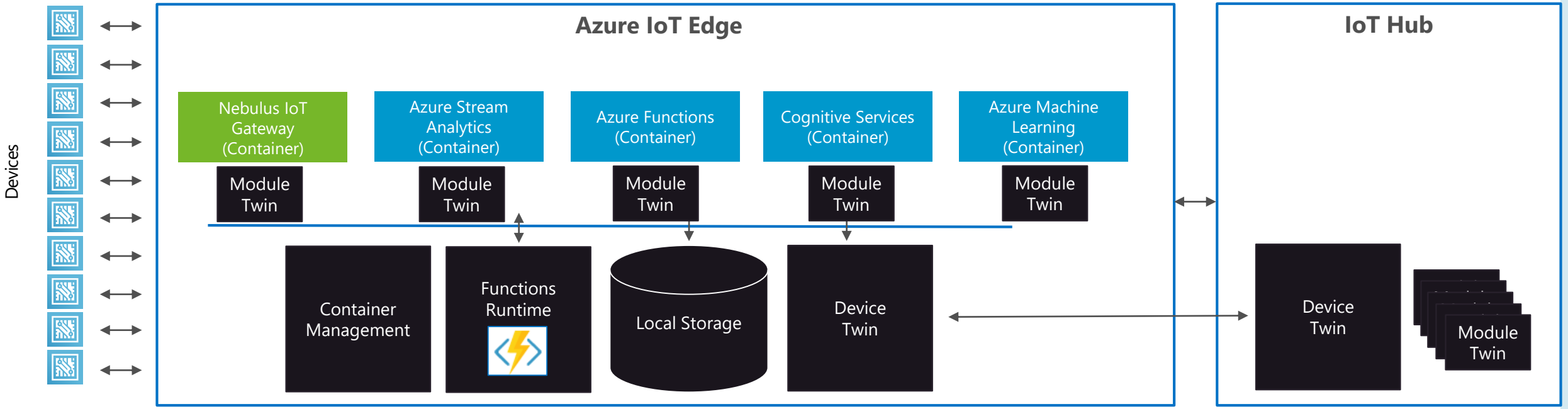


Edge

Azure IoT Edge

- Container based modules
- Azure Functions
- Azure Stream Analytics
- Azure Machine Learning
- Cognitive Services

- Offline / Synchronized Device Twins
- Local Storage
- Cloud Management & Deployment
- High Availability / Fault Tolerance
- Cloud Dev/Test Support



Thank you. Let's connect!