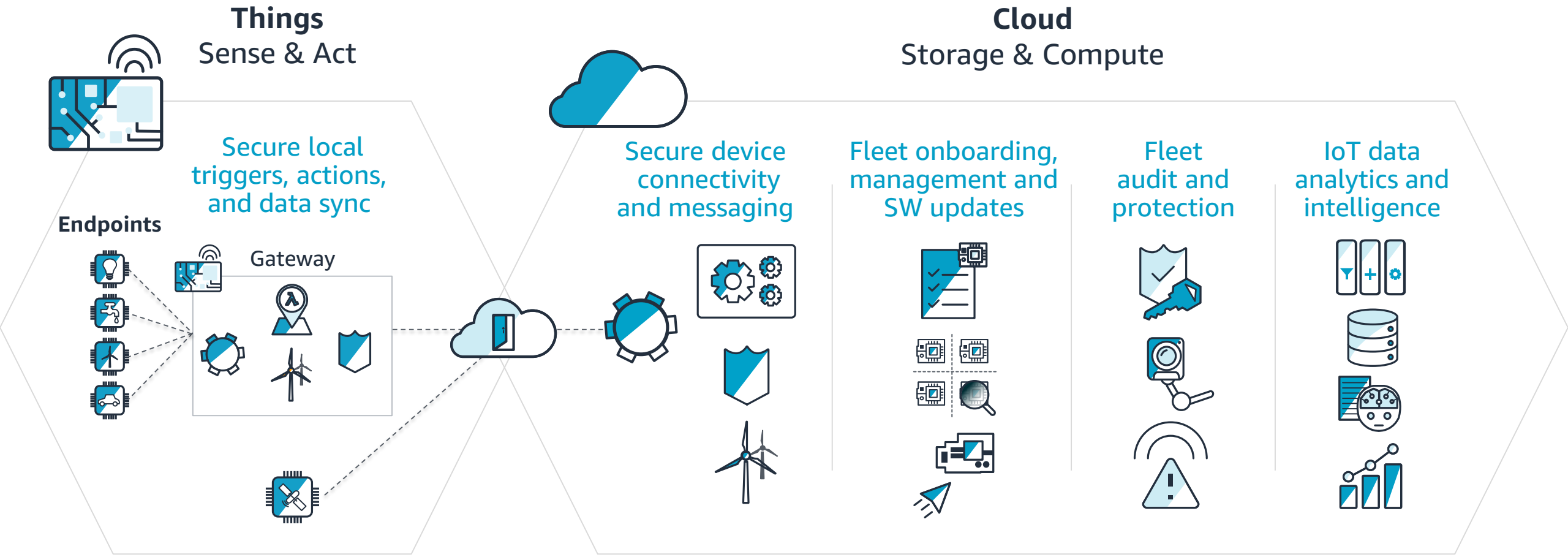
Managing Complexities of IoT Workloads at Scale (Level 300)

Timothée Cruse, IoT Solution Architect

What we'll discuss

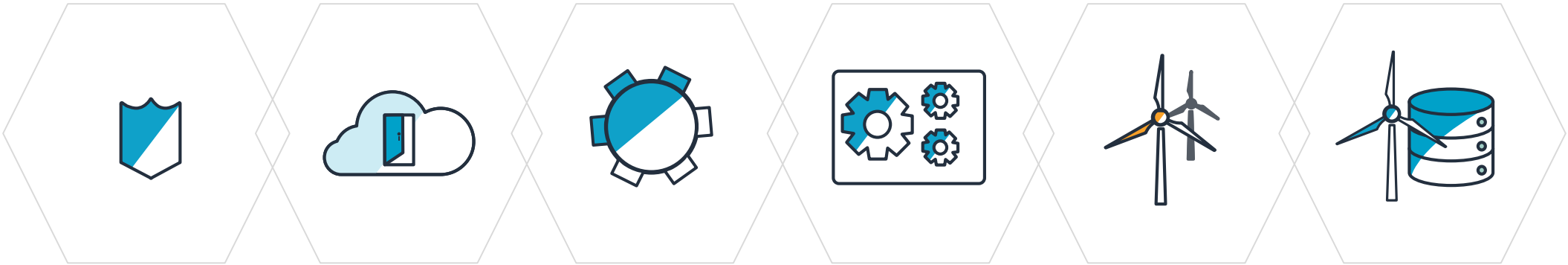
- Quick review of AWS IoT Suite of services
- Security
- Device management
- On-boarding
- Analytics
- Solutions

AWS IoT Architecture



AWS IoT Core

Secure Device Connectivity and Messaging



Identity Service

Device Gateway

Message Broker

Rules Engine

Device Shadow

Registry

Amazon FreeRTOS

IoT Microcontroller OS

Based on FreeRTOS kernel

Amazon FreeRTOS

IoT Microcontroller OS

Local Connectivity Libraries

AWS Greengrass

Cloud Connectivity Libraries

AWS IoT Core

Security Connectivity Libraries

OTA Beta & Code Signing

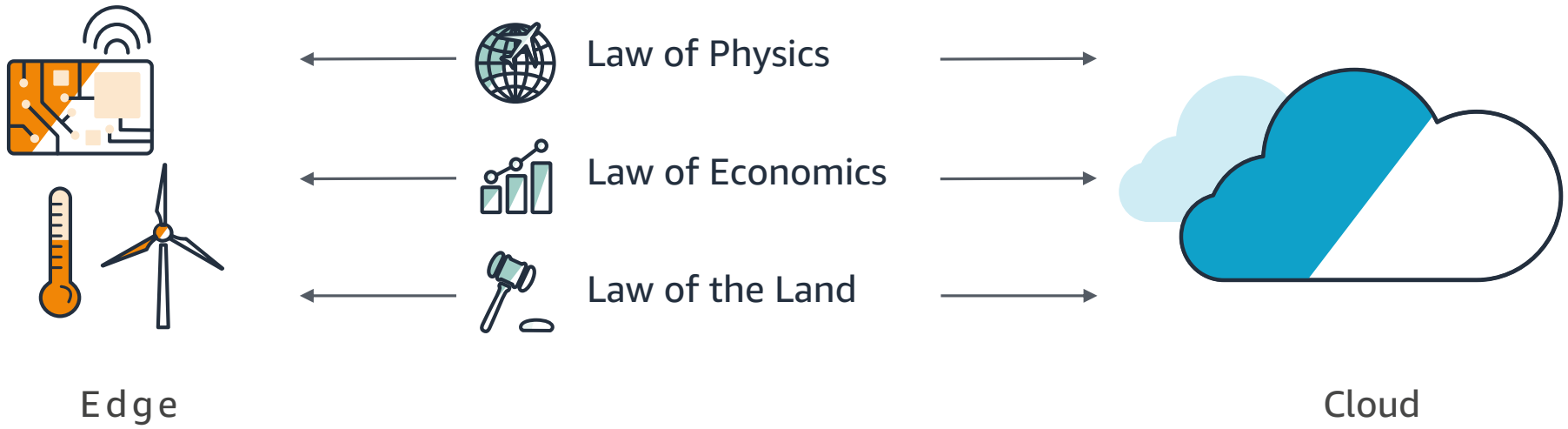
freeRTOS

Based on FreeRTOS kernel

AWS Greengrass

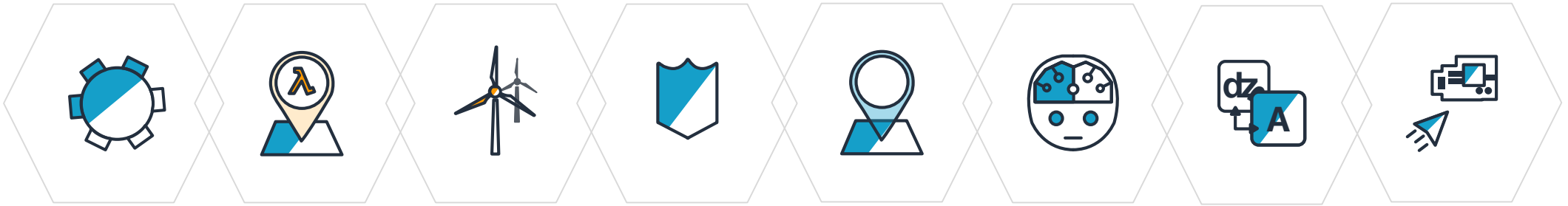
Extend AWS IoT to the Edge

AWS Greengrass extends AWS IoT onto your devices, so that they can act locally on the data they generate, while still taking advantage of the cloud.



AWS Greengrass

Extend AWS IoT to the Edge



Local Messages and Triggers

Local Message Broker

Local Actions

Lambda Functions

Data and State Sync

Local Device Shadows

Security

AWS-grade security

Local Resource Access

Lambdas Interact With Peripherals

Machine Learning Inference

Local Execution of ML Models

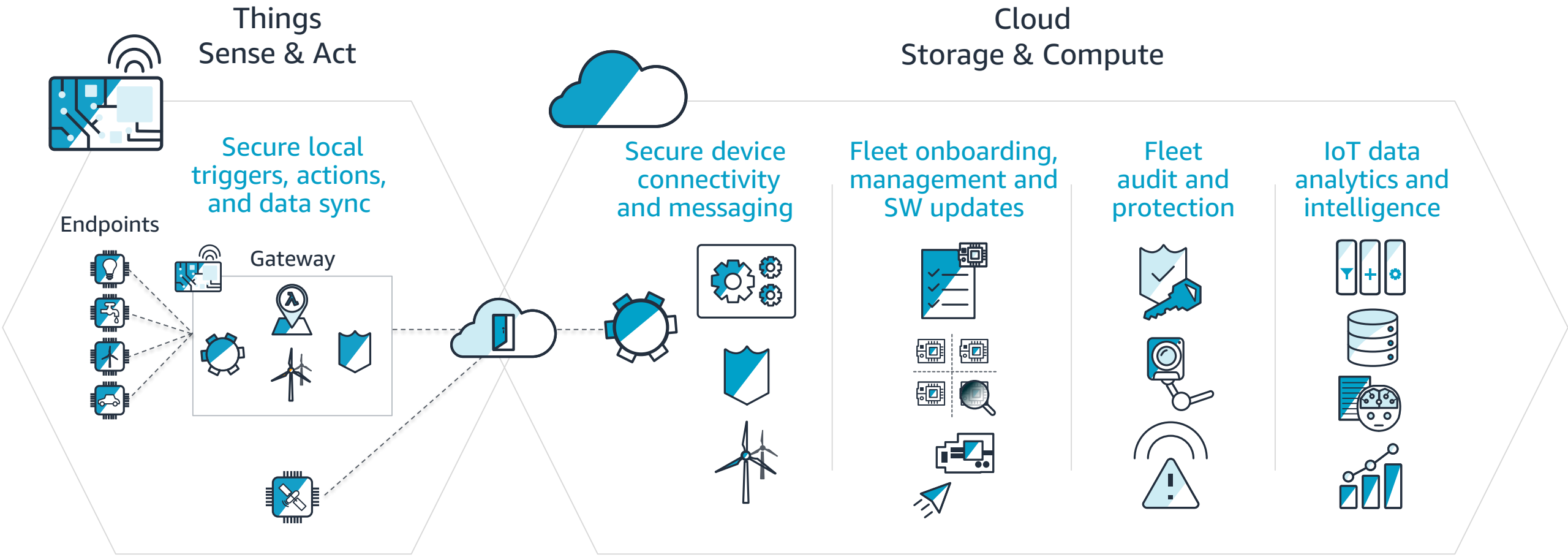
Protocol Adapters

Easy Integrations With Local Protocols

Over the Air Updates

Easily Update Greengrass Core

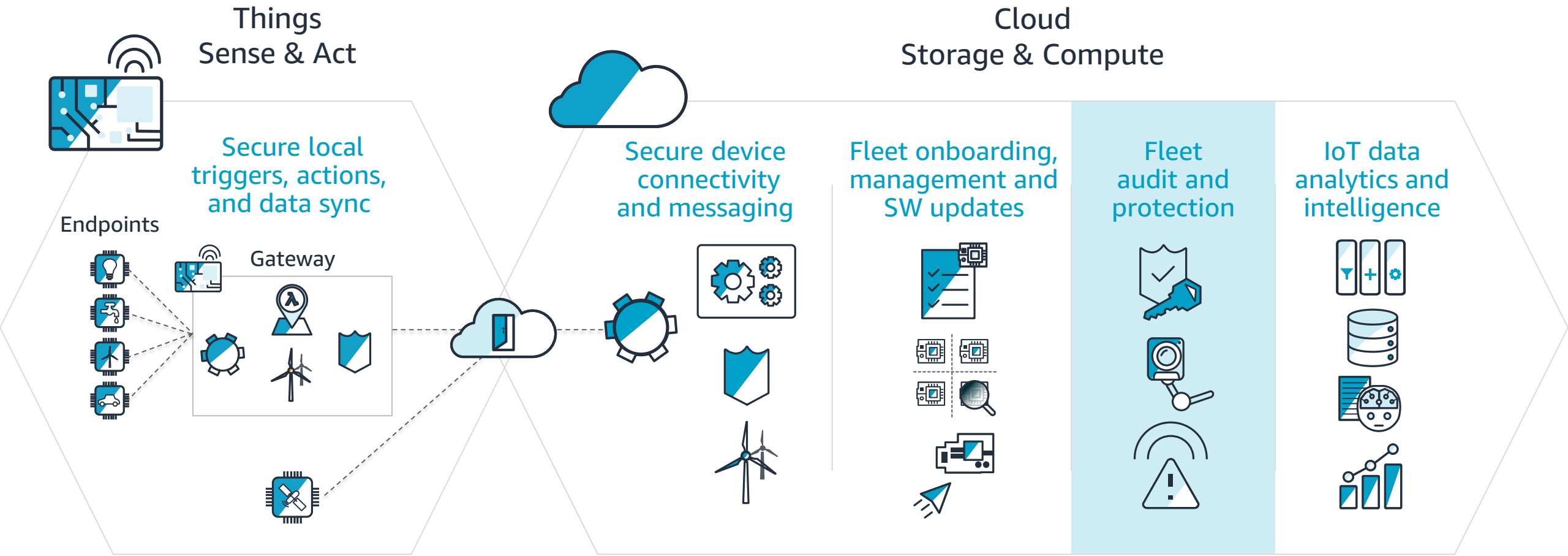
AWS IoT Architecture



“My system DOES NOT NEED security.”

“Security at this level is TOO EXPENSIVE.”

AWS IoT Architecture



AWS IoT Device Defender

COMING IN 2018

Keep Your Fleet Secure

Audit Device Configurations

Monitor Device Behavior

Identify Anomalies

Generate Alerts

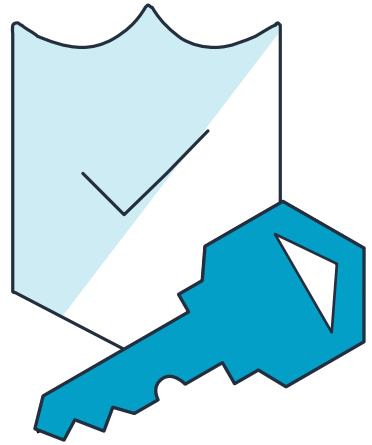
Patch Security Vulnerabilities

Audit Device Configurations

- Ad-hoc and/or scheduled device security policy auditing against best practices

Monitor Device Behavior

- Monitors incoming security metrics and data from connected devices
- Create your own device profile for expected device behavior such as which IP addresses the device can communicate with
- Compares device metrics against expected device behavior such as volume of messages permitted during a 24 hour period



scheduled

Ad-hoc

aws | intel

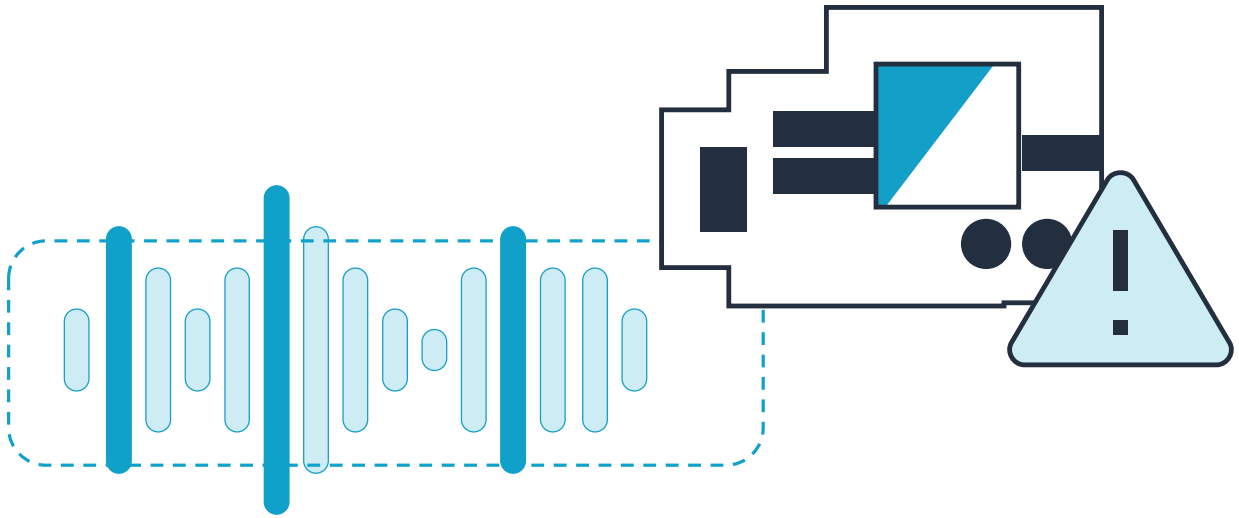
Identify Anomalies

Blacklist/Whitelist behaviors for:

- IP destinations and Geo locations
- Connection IPs
- Open ports

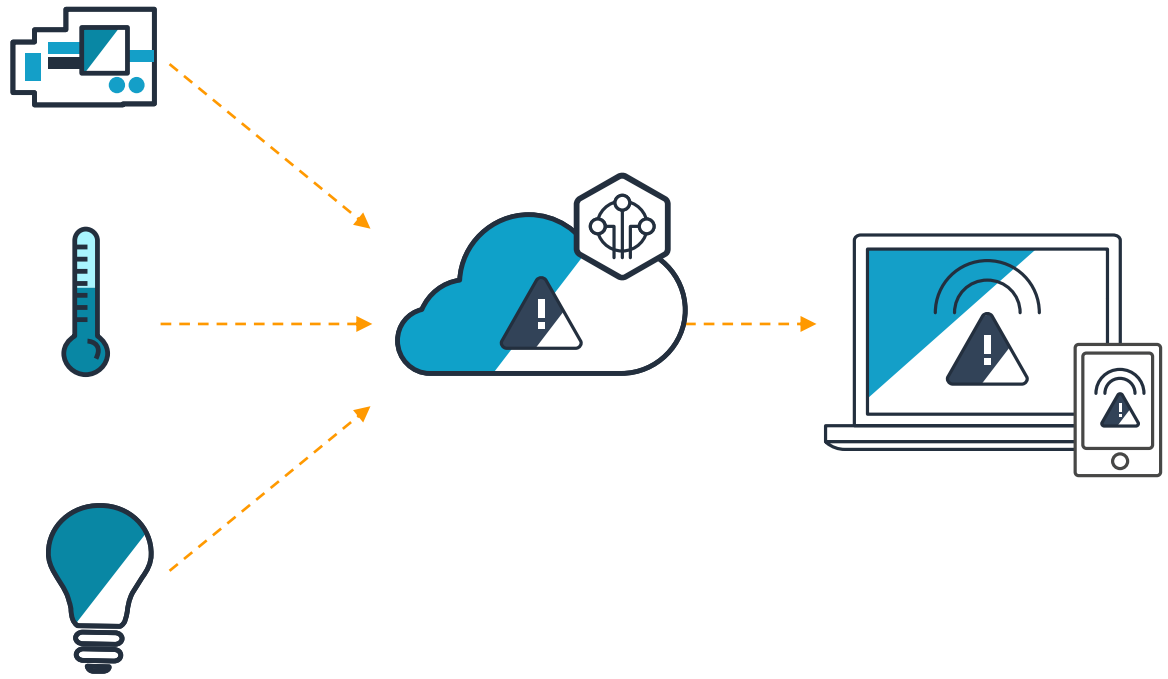
Define thresholds behavior for:

- Number of active connections
- Number of open ports
- Number of outbound packets across all protocols per unit of time
- Number of outbound bytes across all protocols per unit of time
- Number of authorization failures within 24 hours
- Message rate and Message size

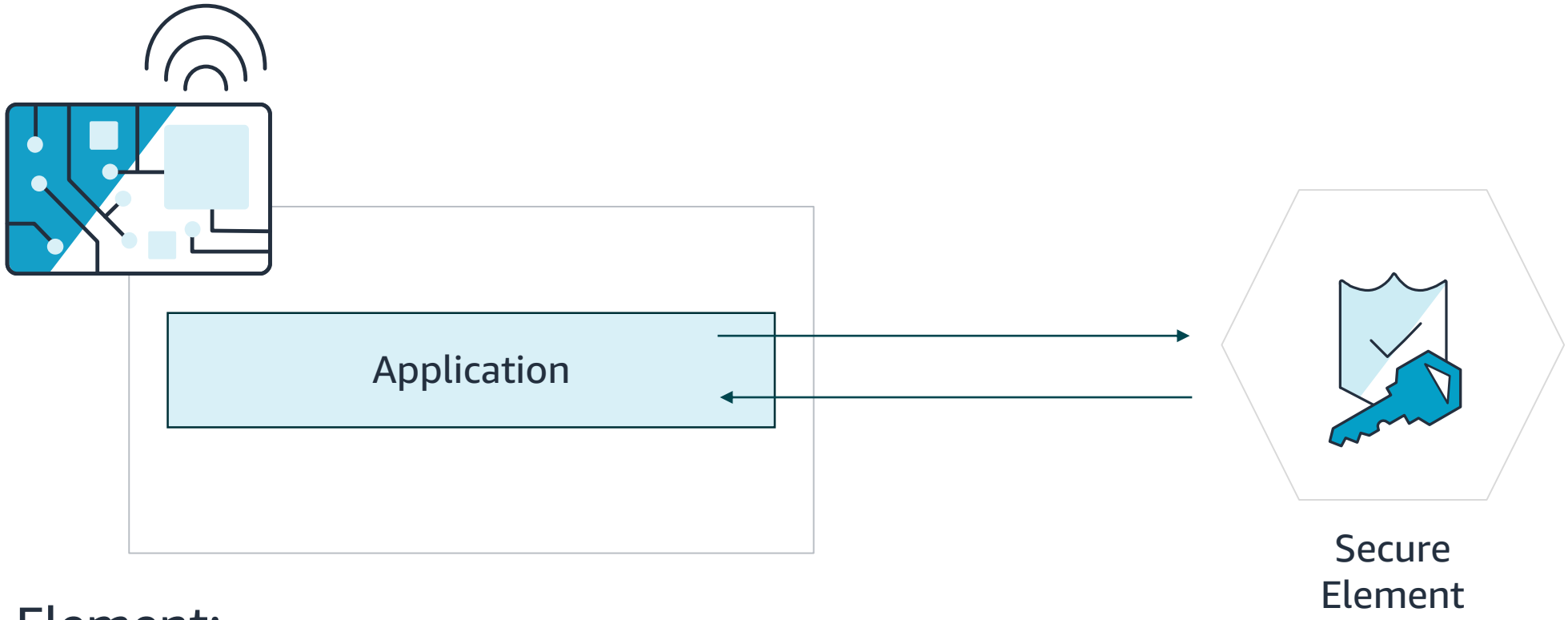


Generate Alerts

- Alerts generated based on identified anomalies and audits
- Alerts sent to AWS IoT Console, Amazon CloudWatch, and Amazon SNS
- Review historical and contextual information about your fleet when it fails an audit or when behavior deviates from what is expected
- View recommended actions to minimize the impact of security issues



Security at the device level



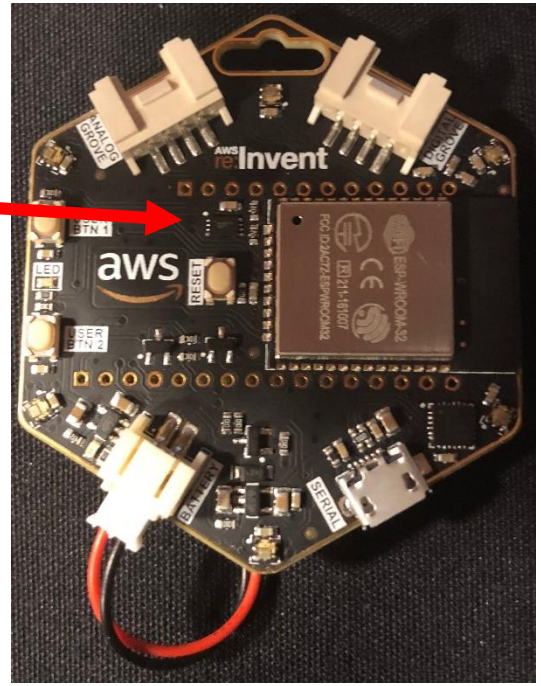
Secure Element:

- Perform cryptographic operations with the private key
- Private key cannot be extracted

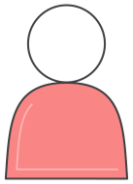
Example: Drink dispenser workshop
AWS Lanyard re:Invent board by Tekt

ECC508A

MICROCHIP

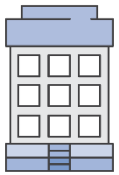


Manufacturing

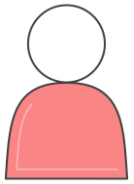


You

Manufacturing

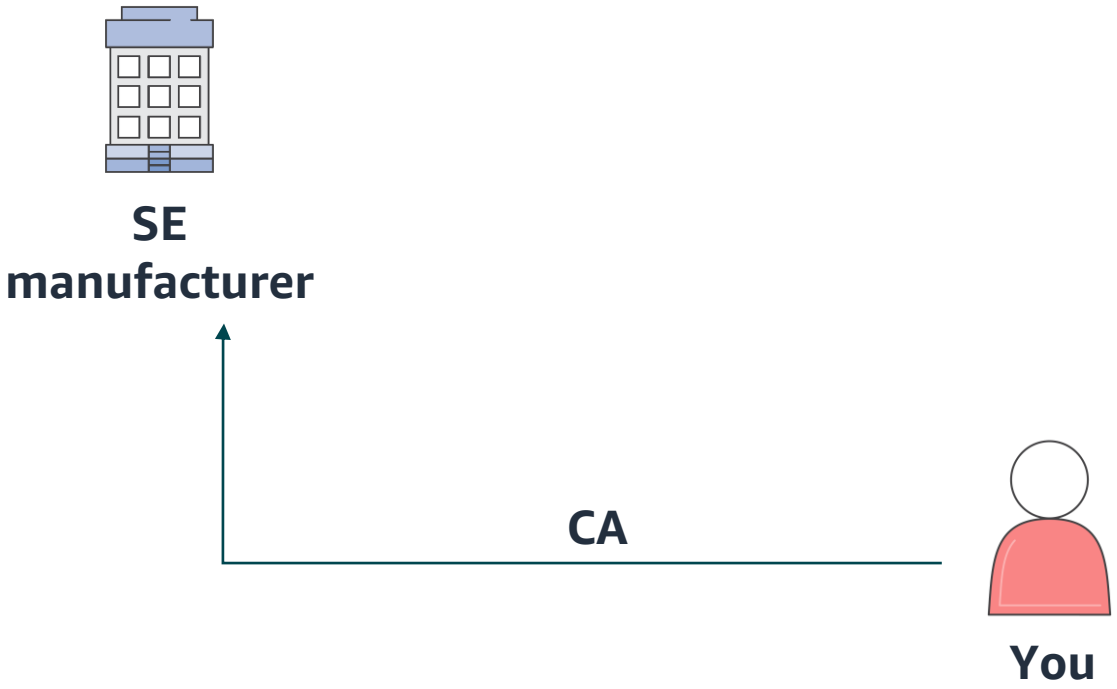


SE manufacturer

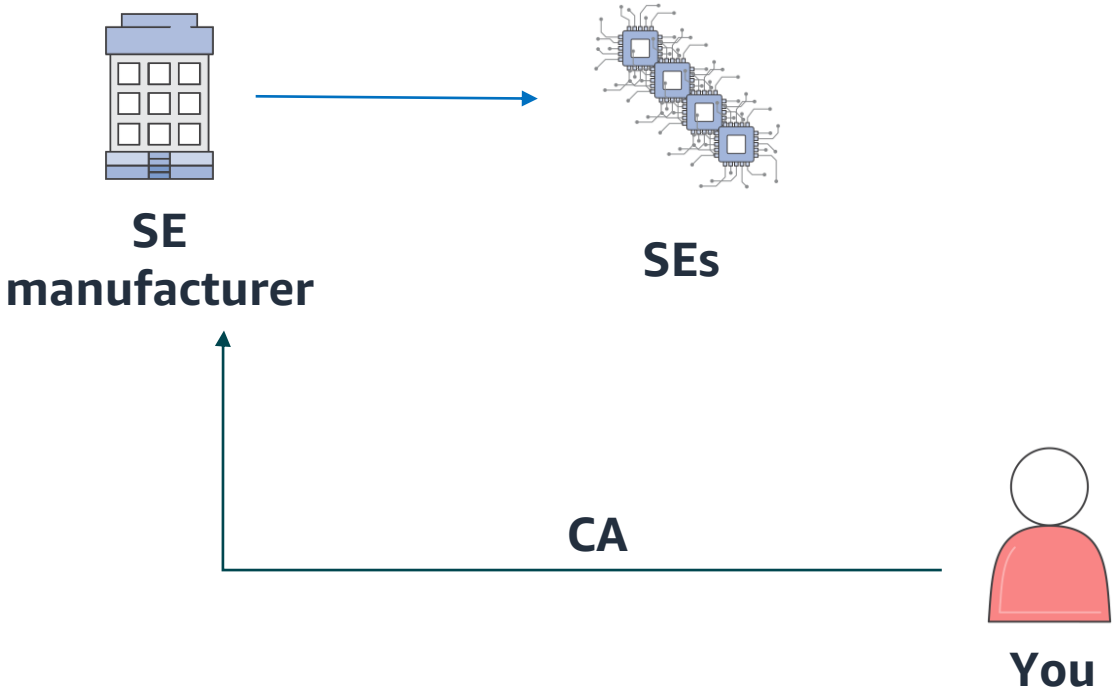


You

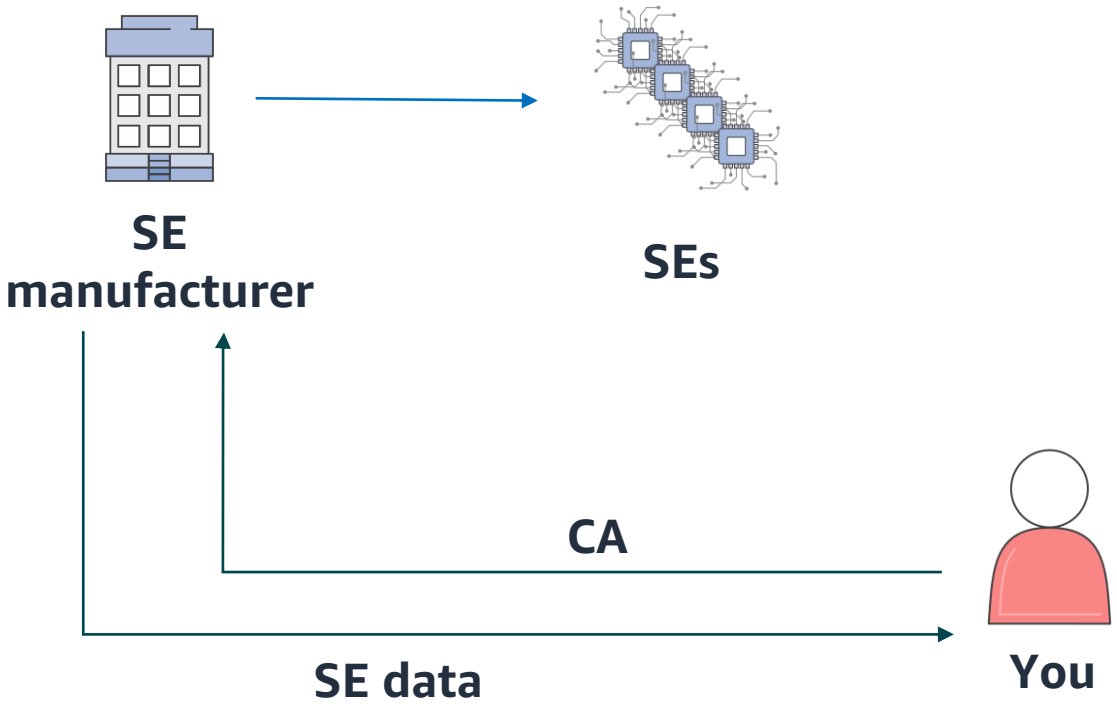
Manufacturing



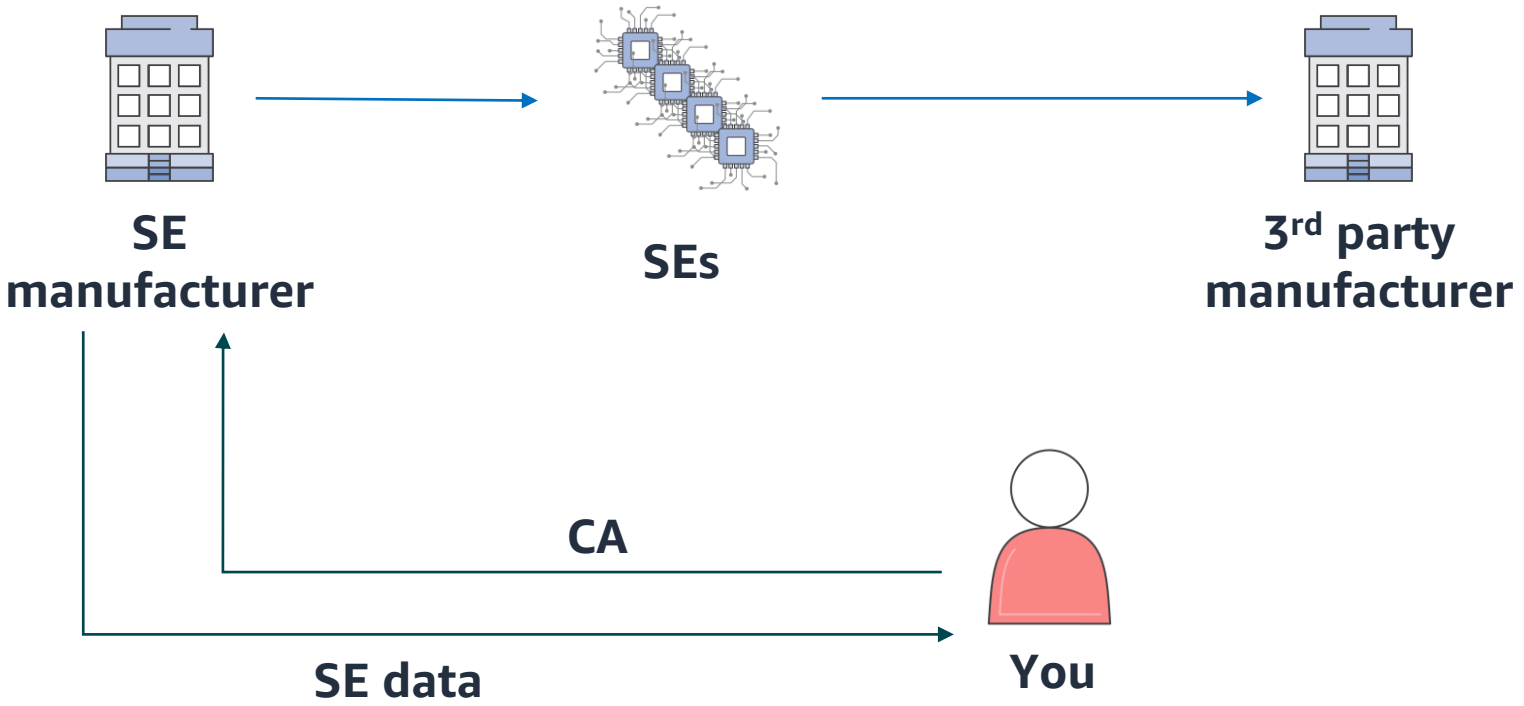
Manufacturing



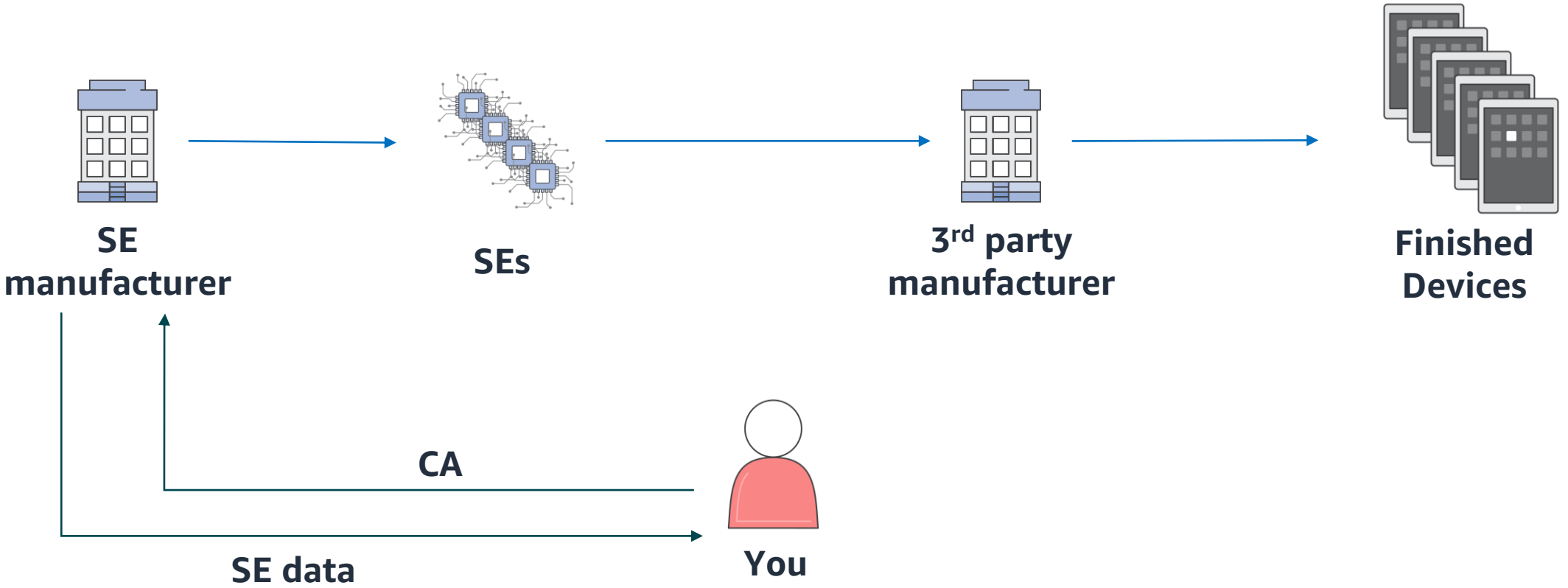
Manufacturing



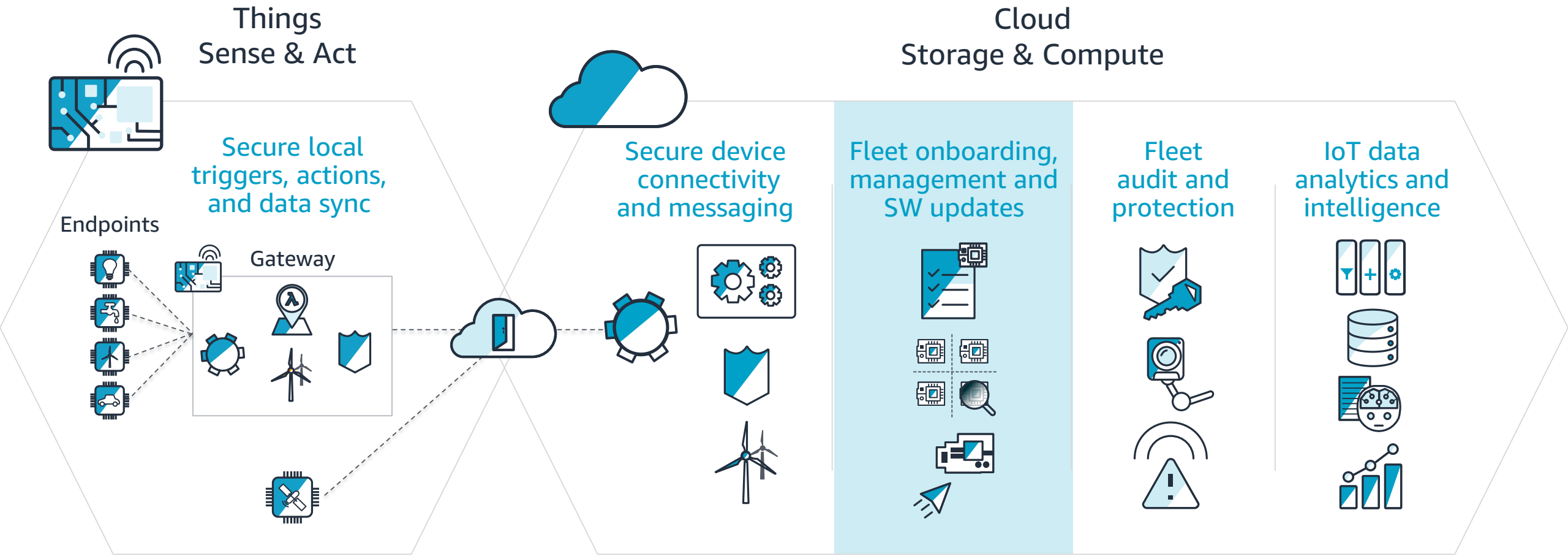
Manufacturing



Manufacturing



AWS IoT Architecture

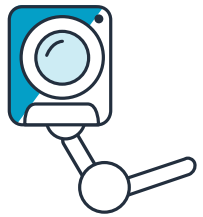


AWS IoT Device Management

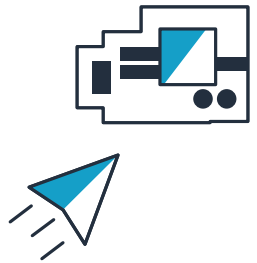
Maintain Fleet Health

Batch Fleet Provisioning

Real-time Fleet Index & Search



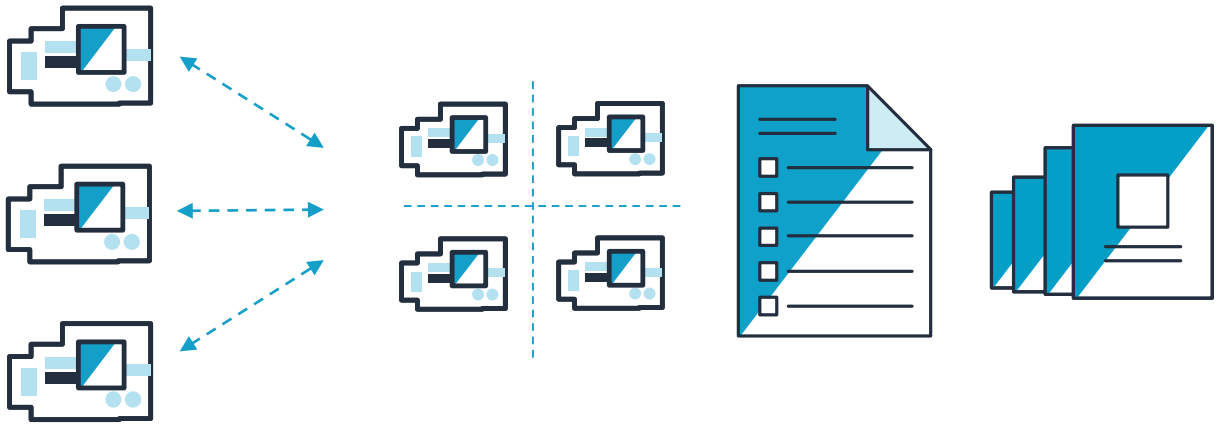
Fine Grained Device Logging & Monitoring



Over the Air Updates

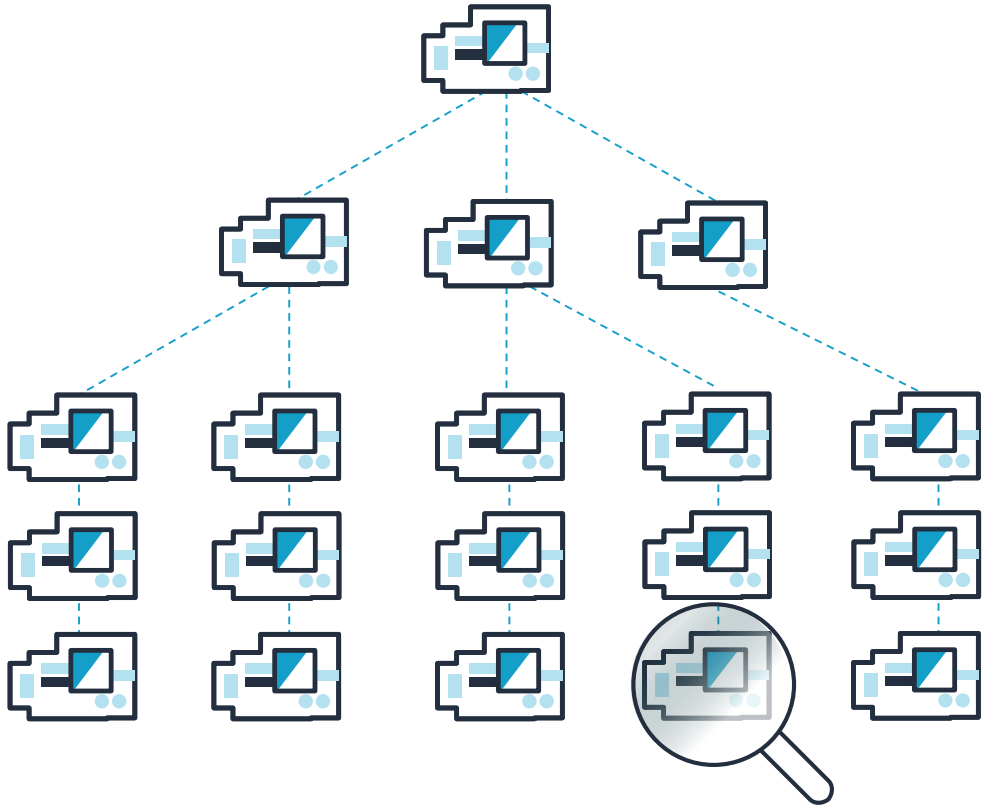
Batch Fleet Provisioning

- Provides provisioning workflows to register device information such as metadata, certificates, and policies for the entire fleet
- JSON template with parameters to define IoT resources (things, certificates, policies) that represent device in the cloud.
- Upload via console or call StartThingRegistrationTask API for registering all devices in bulk
- Track provisioning progress, or download reports for completed tasks
- Can be used for provisioning new devices or re-registering devices (e.g. rotating certificates)



Real-time Fleet Index & Search

- Fast querying across different data sources for your entire device fleet in near real-time
- Currently maintains an index of two data sources (Registry and Shadow) which will allow you to find devices within the fleet based on any combination of device attributes and states
  - “Find all devices manufactured after 2013 with firmware version 1.2 that are connected to a charging station”
- Easy to use – one-click activation via console.
- Support for additional sources (connections, errors, custom data sources) in Q2/2018



Over the Air Updates

- Push over the air updates to your devices after they're deployed to the field to improve device functionality
- Receive notifications on the status of each device update to monitor your updates as they execute
- Target groups of devices to update in bulk, or pinpoint single devices to update
- Control your deployment velocity to reduce the blast radius of any update

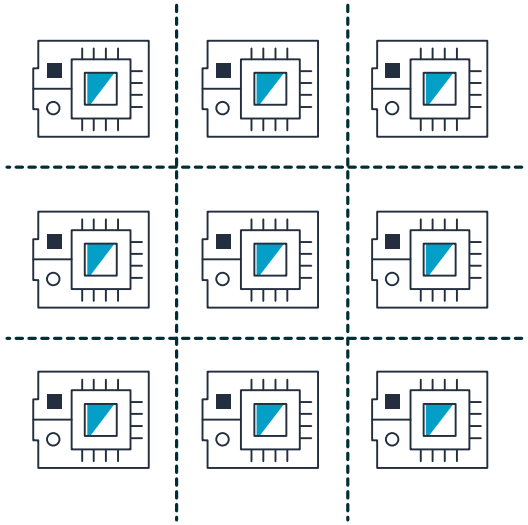
Onboarding of devices at scale strategies

Examples:

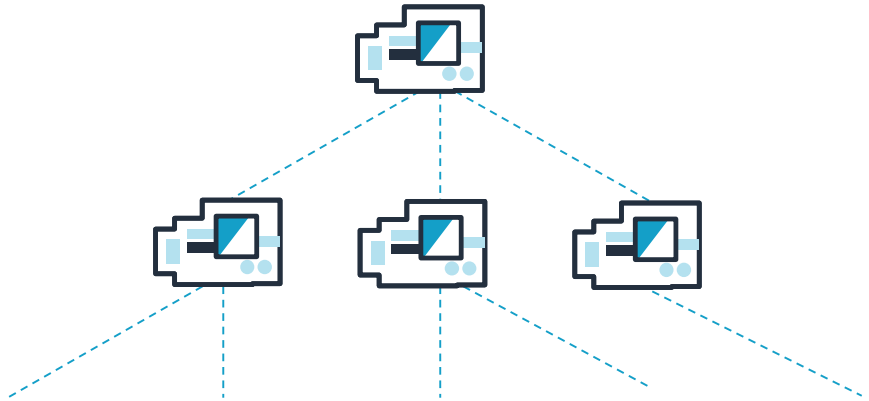
- Pre Registration
- Just In Time Provisioning
- Just in Time Registration
- Certificate Vending Machine

Onboarding of devices at scale: Pre-Registration

JSON description

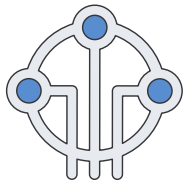


Provision vis
AWS IoT Device Management

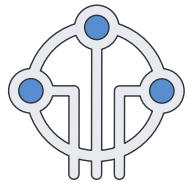


Organized and ready to connect

Onboarding of devices at scale: JITP



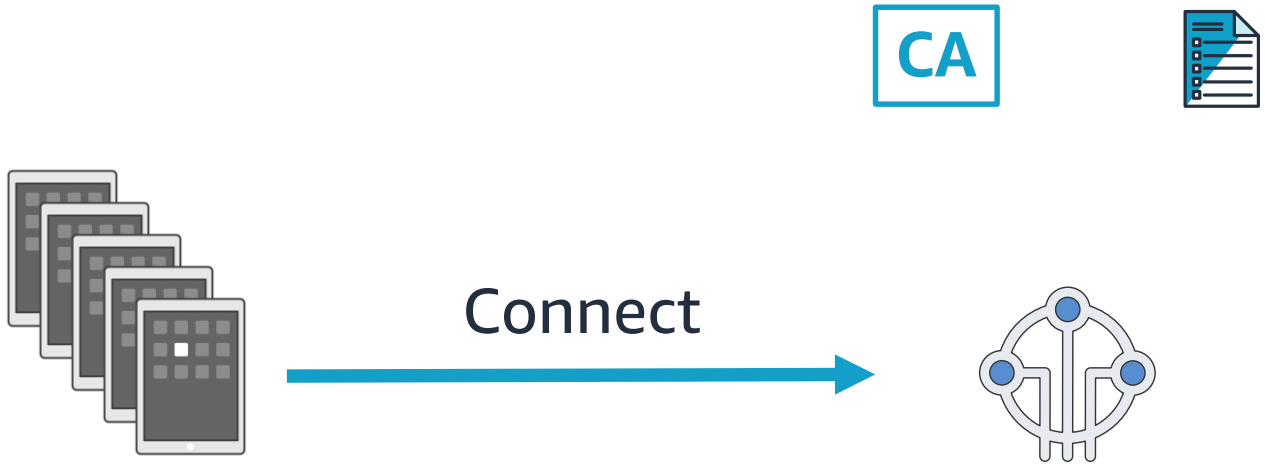
Onboarding of devices at scale: JITP



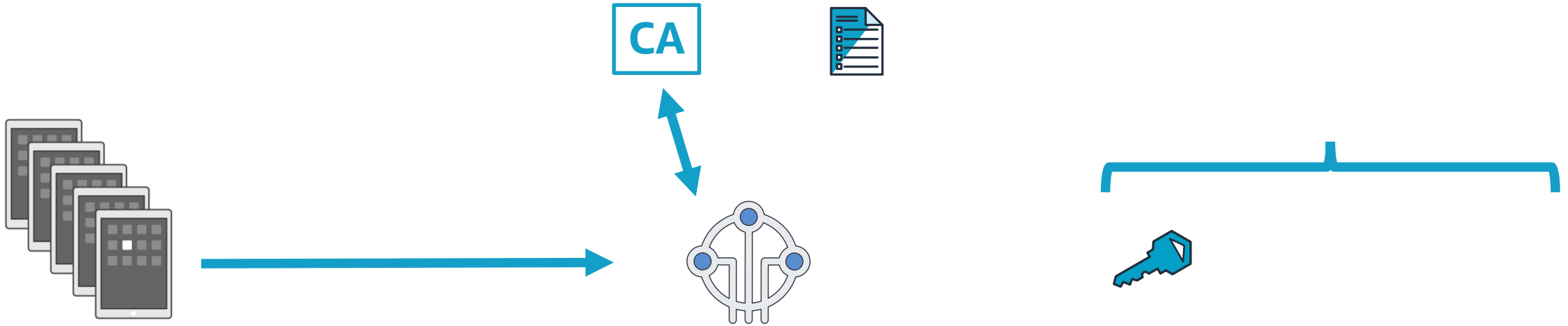
Register your CA, incl. registration template

YOU

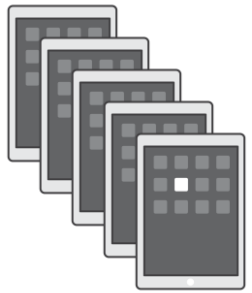
Onboarding of devices at scale: JITP



Onboarding of devices at scale: JITP

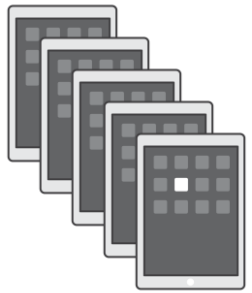


Onboarding of devices at scale: JITP



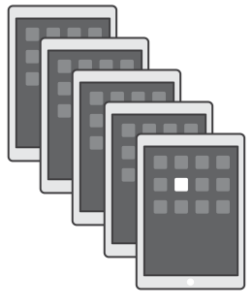
Pending Activation

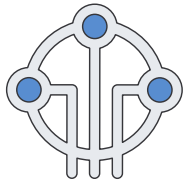
Onboarding of devices at scale: JITP

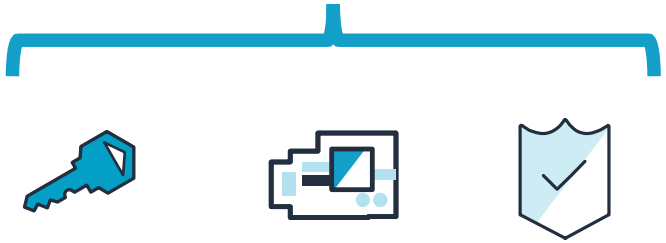


Pending Activation

Onboarding of devices at scale: JITP

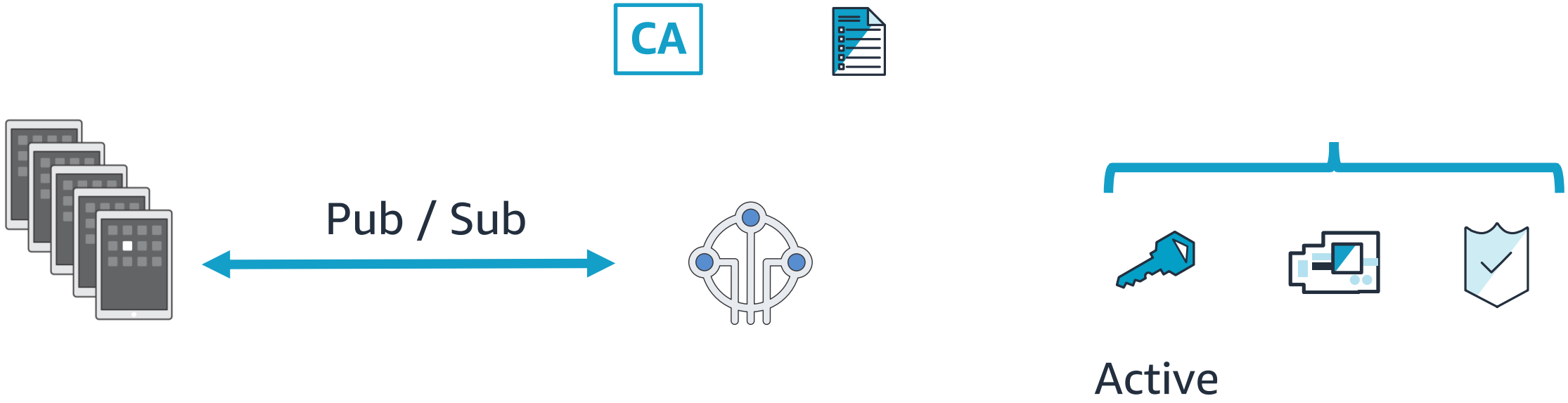






Active

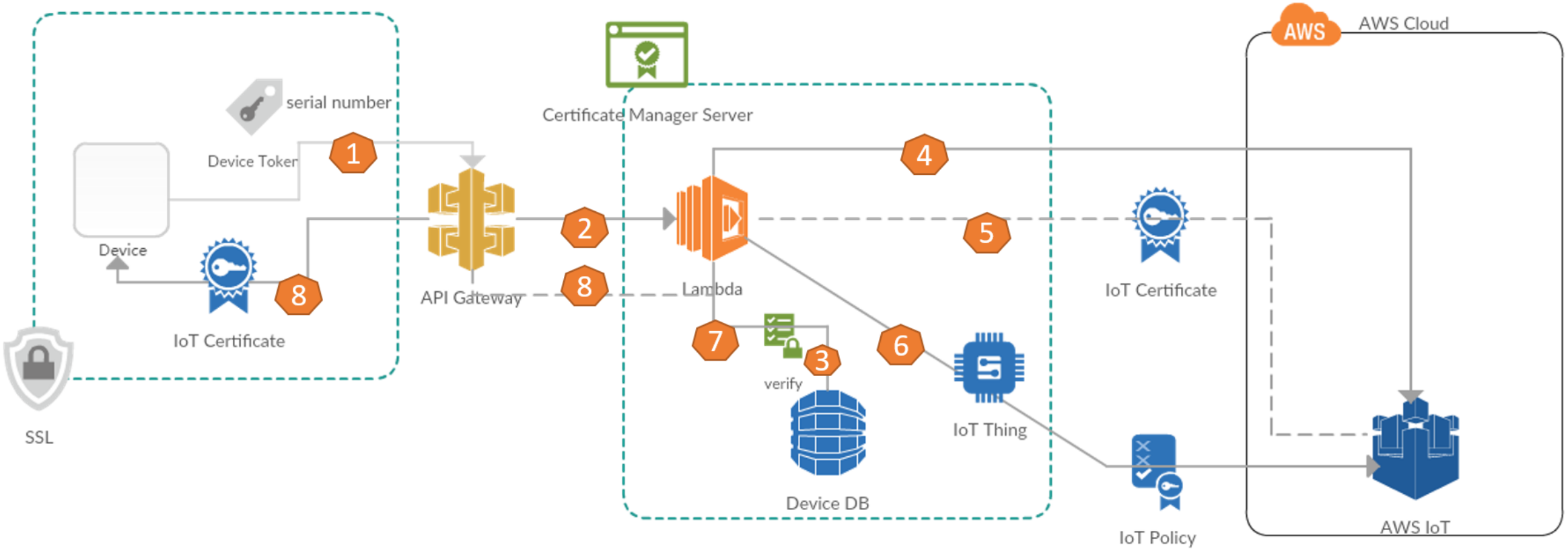
Onboarding of devices at scale: JITP



Onboarding of devices at scale: JITR

- Register your CA
- Devices connect
- Certificate in Pending Activation state
- Lifecycle events get triggered
- User defined Lambda function for creating: Thing, Certificate, Policy
- Certificate in Active state

Onboarding of devices at scale: Example: CVM



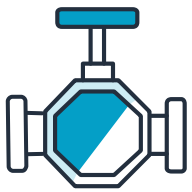
https://github.com/awslabs/aws-iot-certificate-vending-machine

DATA

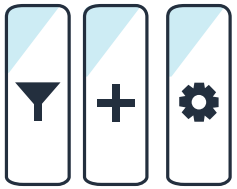
AWS IoT Analytics

Easily analyze IoT data

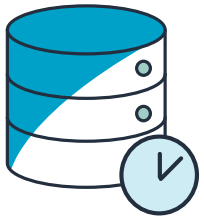
AWS IoT Analytics is a service that processes, enriches, stores, analyzes, and visualizes IoT data for manufacturers and enterprises.



Channels



Pipelines



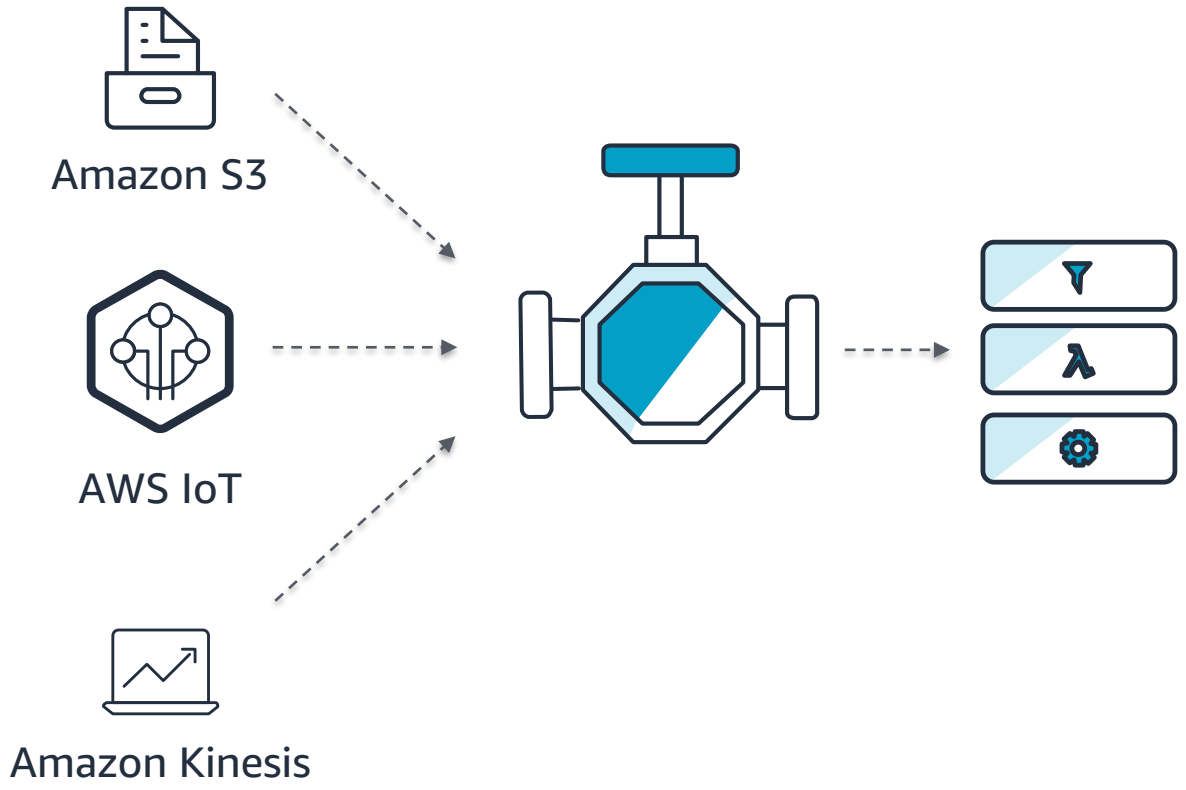
Data Stores

Datasets

Jupyter Notebooks & Templates

Channels

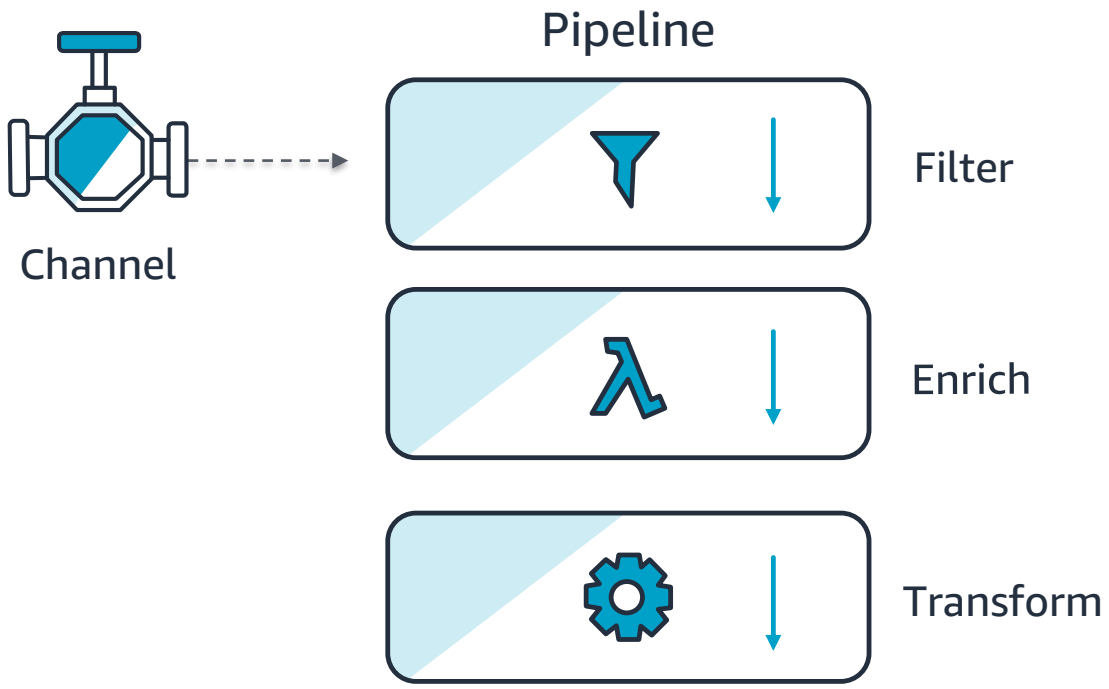
- Entry point to AWS IoT Analytics
- IoT Data Collection from Multiple Sources: IoT Core, Amazon Kinesis, S3, or custom source through APIs
- Data format agnostic
  Binary, JSON
- Elastically scalable



Pipelines

Data (Pre)Processing and Enrichment

- **Filter messages**
  Conditionally purge messages to remove outliers and erroneous/irrelevant data
- **Transform Messages**
  Mathematical and conditional transformations to convert data (e.g. Celsius to Fahrenheit)
- **Enrich Messages**
  Enrichment from MQTT Topic, Device Registry & Device Shadow
- **Custom Preprocessing**
  Customer-defined lambda to add vital context to IoT data (e.g. geo location, weather data)
- **Batches messages prior to enrichment ensures scalability**
- **Easily replicate pipelines using simple API structure as fleets grow from tens to thousands of devices**



Data Stores

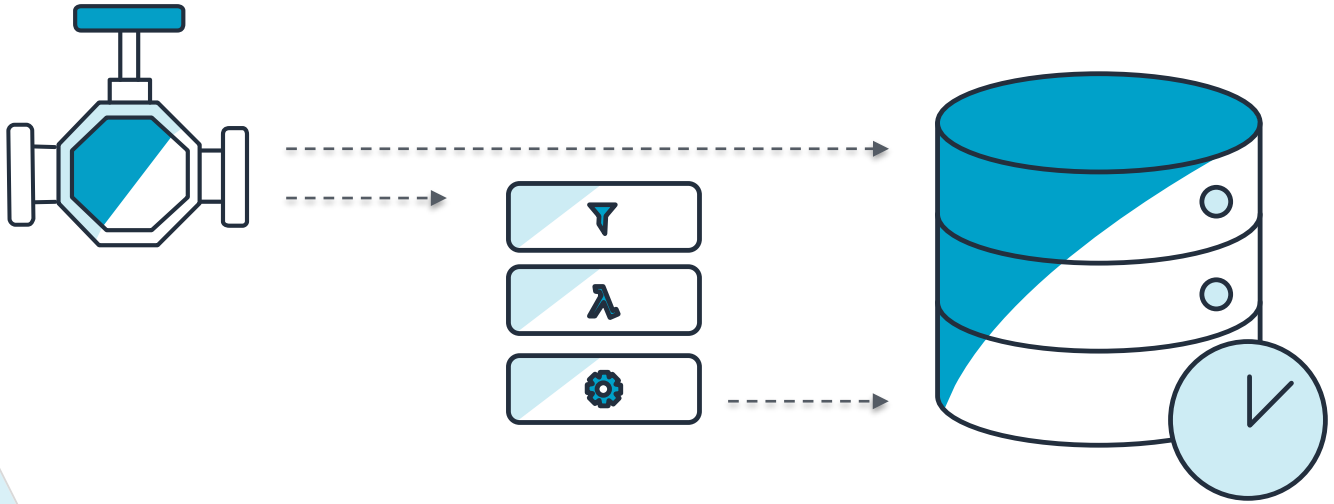
Raw and Processed Data Storage

Authoritative store of raw data from multiple devices.

- Immutably stores raw device data for easily reprocessing using different logic if your needs change

Fully managed and optimized processed data store for time series and IoT workloads

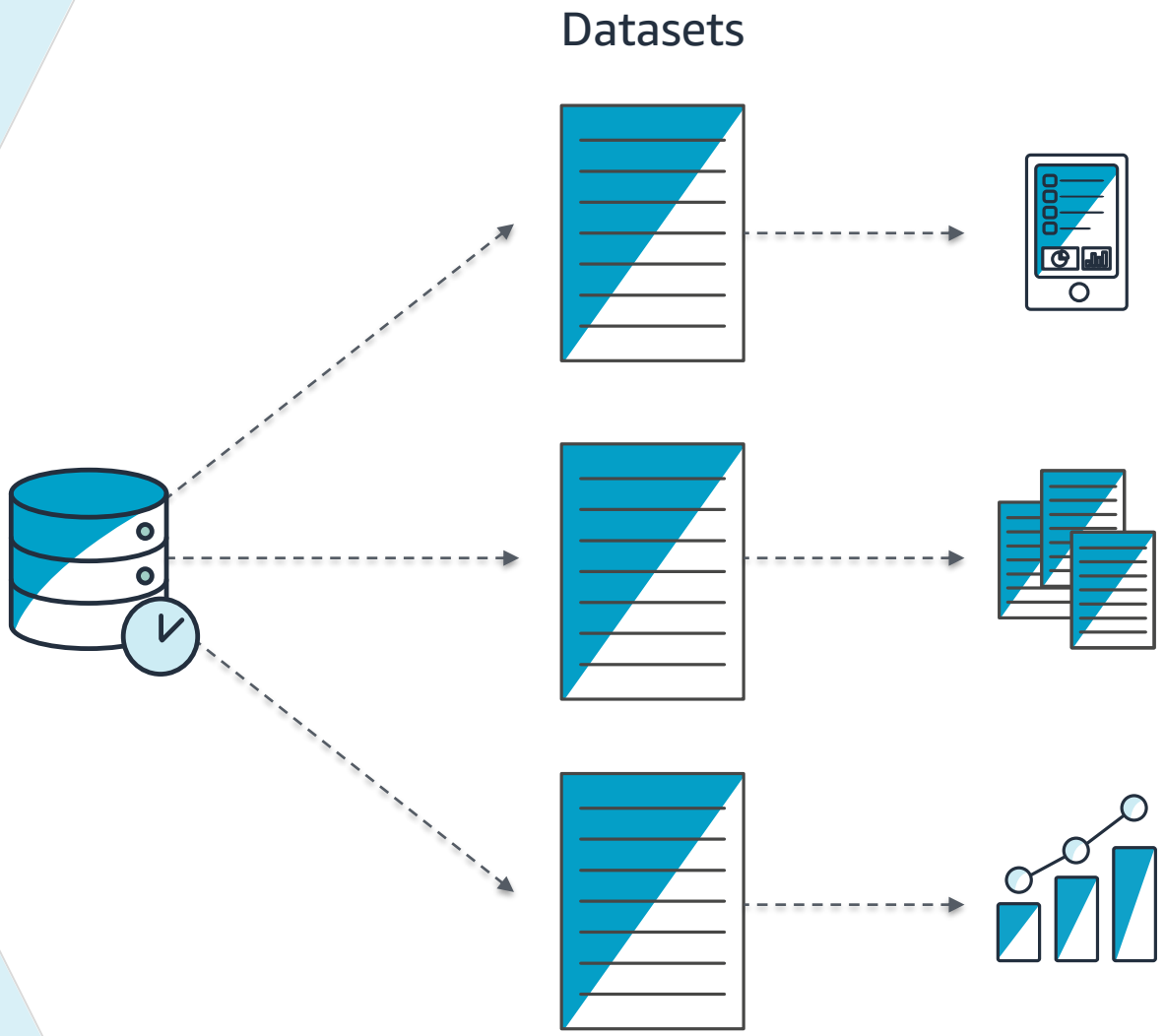
- Partitioned by time
  Supports faster query response on time series data
- More than a single database
  Abstraction on top of several database technologies in a single interface
- Manageable data retention policies



Datasets

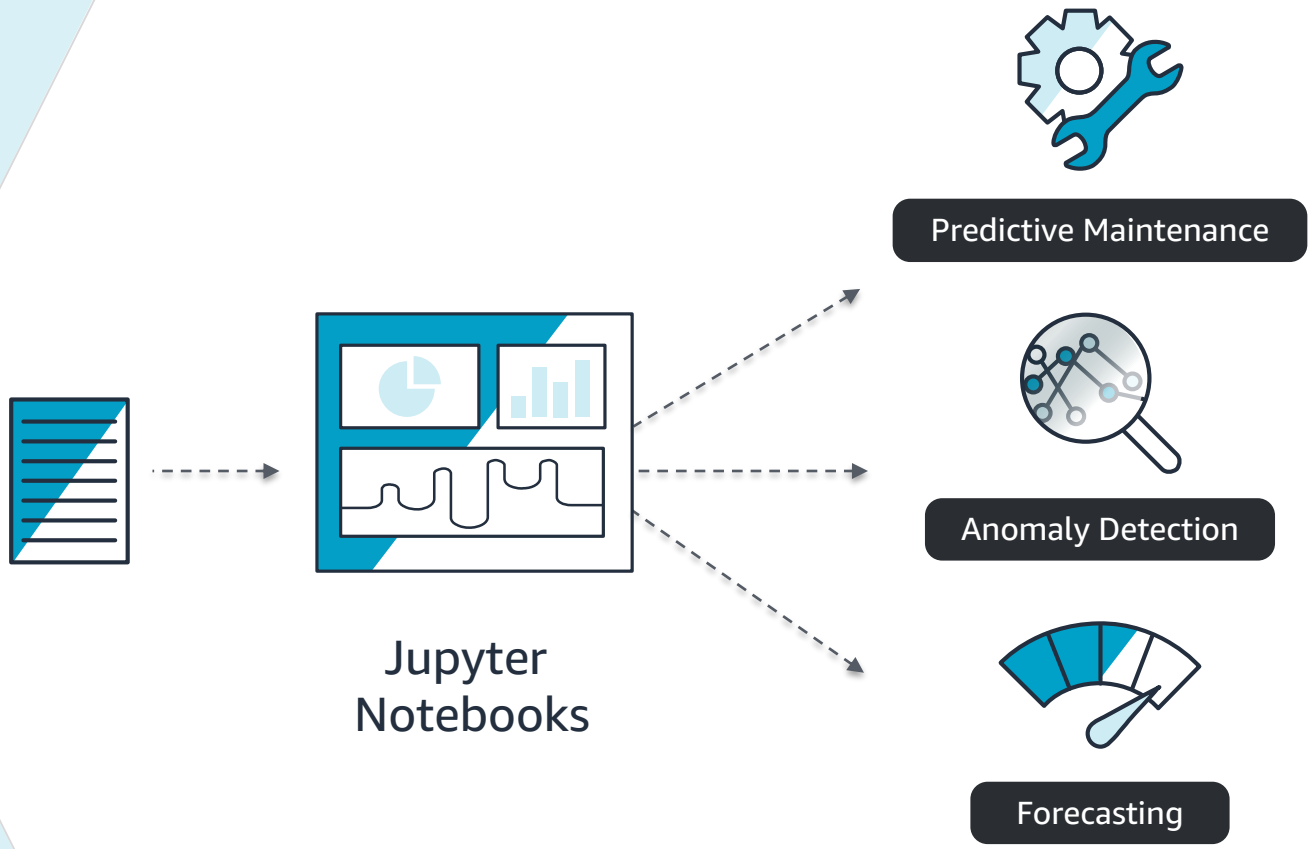
Queries on Data Store

- Query IoT Analytics Data Stores using standard SQL
- Queries can be run ad hoc, or scheduled
- Popular tabular format
- Visualize in QuickSight dashboards
  Native QuickSight Connector to easily build metrics or inspect datasets
- Available via API, console download, or within Jupyter Notebooks
- Console Query Editor
  Edit and schedule your queries from console



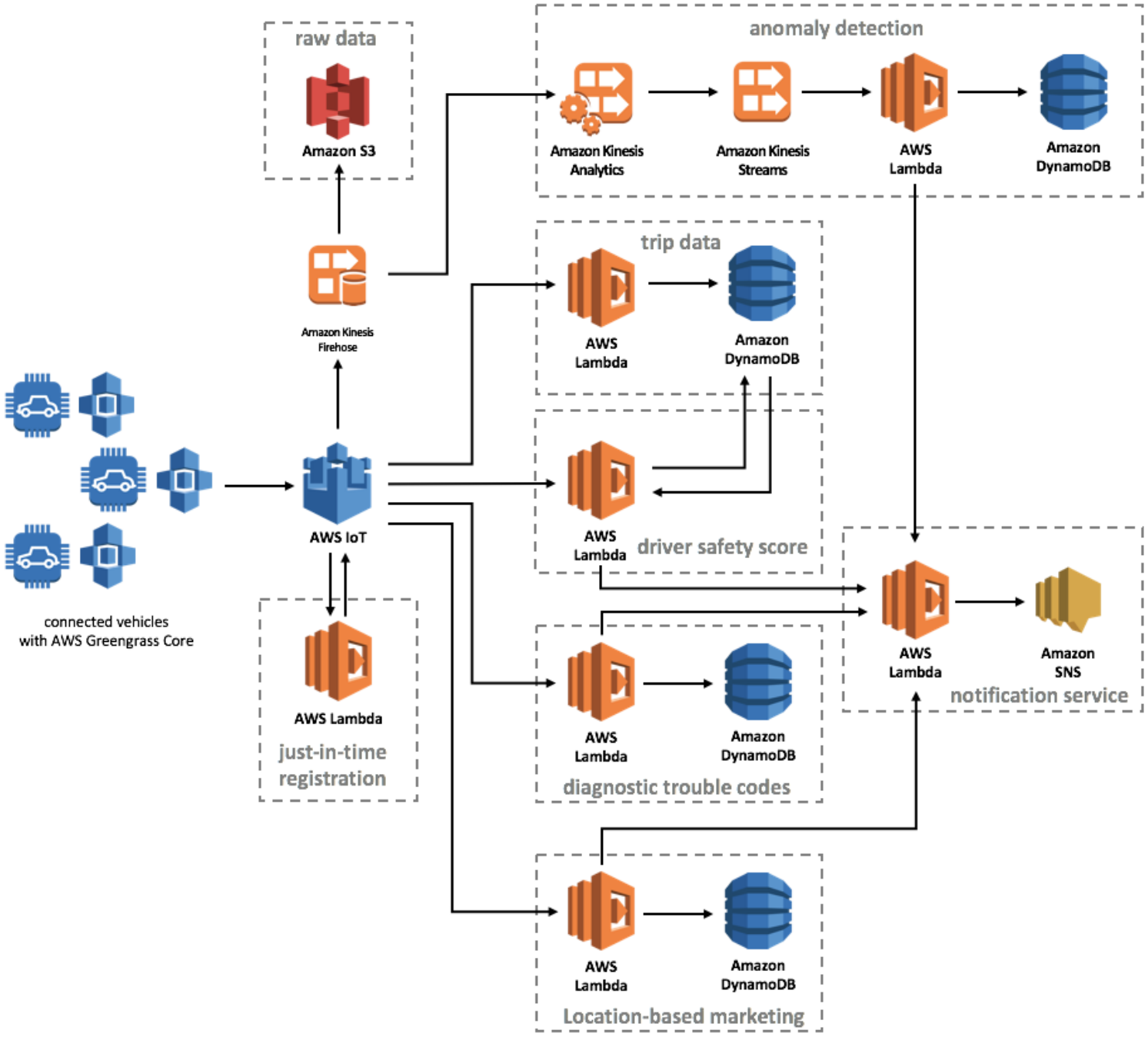
Jupyter Notebooks & Templates

- **Custom author Jupyter-based machine learning notebooks**
  Allows you to build sophisticated ML models on IoT data using popular libraries such as Sci-Kit-Learn and TensorFlow.
- **Built in ML Notebook Templates**
  Get started faster with pre-built notebook templates for common IoT use cases:
  - Predictive Maintenance
  - Anomaly Detection
  - Fleet Segmentation
  - Forecasting
- **Integrated with Amazon SageMaker**
  Use your SageMaker Notebook Instances to run notebooks



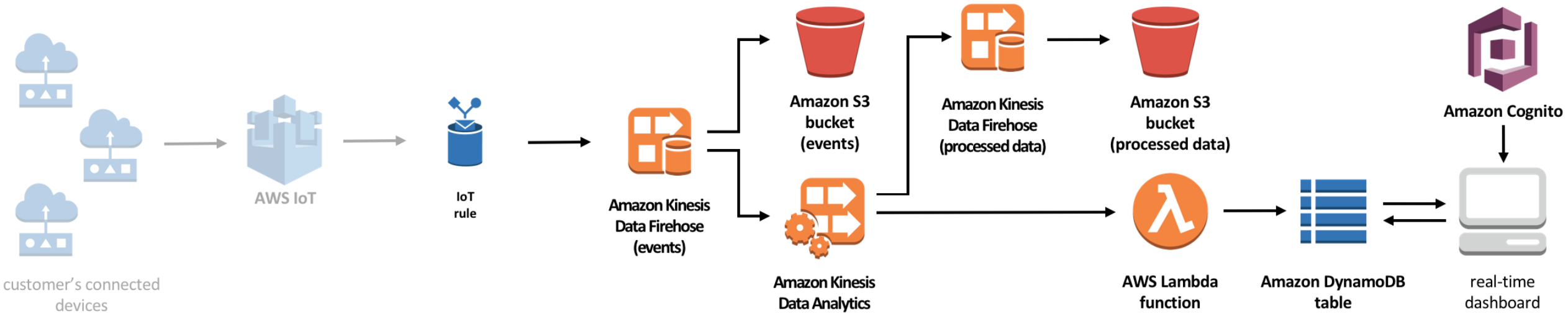
Example Solutions by AWS

AWS Connected Vehicle Solution



https://aws.amazon.com/answers/iot/connected-vehicle-solution/

Real-Time IoT Device Monitoring with Kinesis Data Analytics



https://aws.amazon.com/answers/iot/real-time-iot-device-monitoring-with-kinesis/

Learn from AWS experts. Advance your skills and knowledge. Build your future in the AWS Cloud.

Digital Training

Free, self-paced online courses built by AWS experts

Classroom Training

Classes taught by accredited AWS instructors

AWS Certification

Exams to validate expertise with an industry-recognized credential

Ready to begin building your cloud skills?
Get started at: https://www.aws.training/

With deep expertise on AWS, APN Partners can help your organization at any stage of your Cloud Adoption Journey.

AWS Managed Service Providers

APN Consulting Partners who are skilled at cloud infrastructure and application migration, and offer proactive management of their customer's environment.

AWS Competency Partners

APN Partners who have demonstrated technical proficiency and proven customer success in specialized solution areas.

AWS Marketplace

A digital catalog with thousands of software listings from independent software vendors that make it easy to find, test, buy, and deploy software that runs on AWS.

AWS Service Delivery Partners

APN Partners with a track record of delivering specific AWS services to customers.

Ready to get started with an APN Partner?
Find a partner: https://aws.amazon.com/partners/find/
Learn more at the AWS Partner Network Booth

Thank You for Attending AWS Innovate

We hope you found it interesting! A kind reminder to **complete the survey.**

Let us know what you thought of today's event and how we can improve the event experience for you in the future.


aws-apac-marketing@amazon.com


twitter.com/AWSCloud


facebook.com/AmazonWebServices


youtube.com/user/AmazonWebServices


slideshare.net/AmazonWebServices


twitch.tv/aws