TRANSFORMATION DAY

AWS IoT: Services Built for Business Outcomes

Danilo Poccia
Principal Evangelist, Serverless

If you knew **the state of everything** and could **reason on top of that data**…

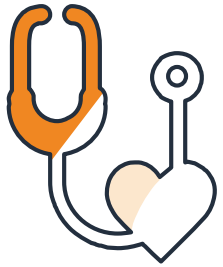
what problems would you solve?

AWS IoT Customers

What Customers Are Doing with AWS IoT

Predictive maintenance

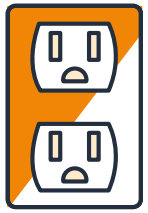
Wellness & health solutions



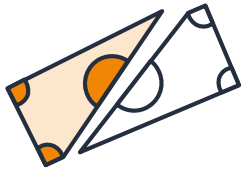
Remote patient monitor

Connected buildings & city systems

Maintain device fleets



Monitor energy efficiency



IoT payment & connected commerce

Safeguard manufacturing facilities

Nobody just buys IoT technology…

they seek business outcomes

Business Outcomes with IoT

New services & business models

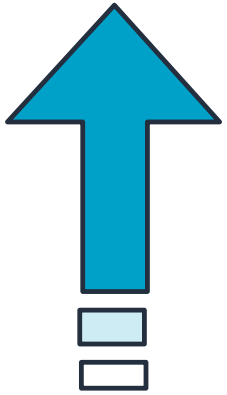
Products that get better with time

Better relationship with customers

Increased efficiency

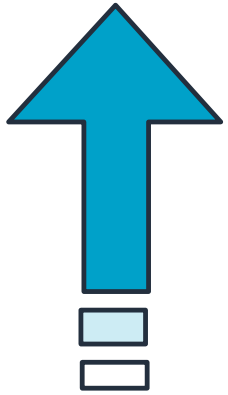
Intelligent decision making

Data driven discipline



Revenue growth

IoT data drives business growth



Operational efficiency

IoT data decreases OpEx

IoT Solutions Are Complex & Multidimensional

Devices & sensors

Onboard, provision, manage

Connectivity & infrastructure

Connect, communicate, secure

Analytics & insights

Analyze, visualize, act

Applications & services

Engage, empower, delight

Change management

Transform, shift culture

Our Concept of IoT

Things
Sense & Act

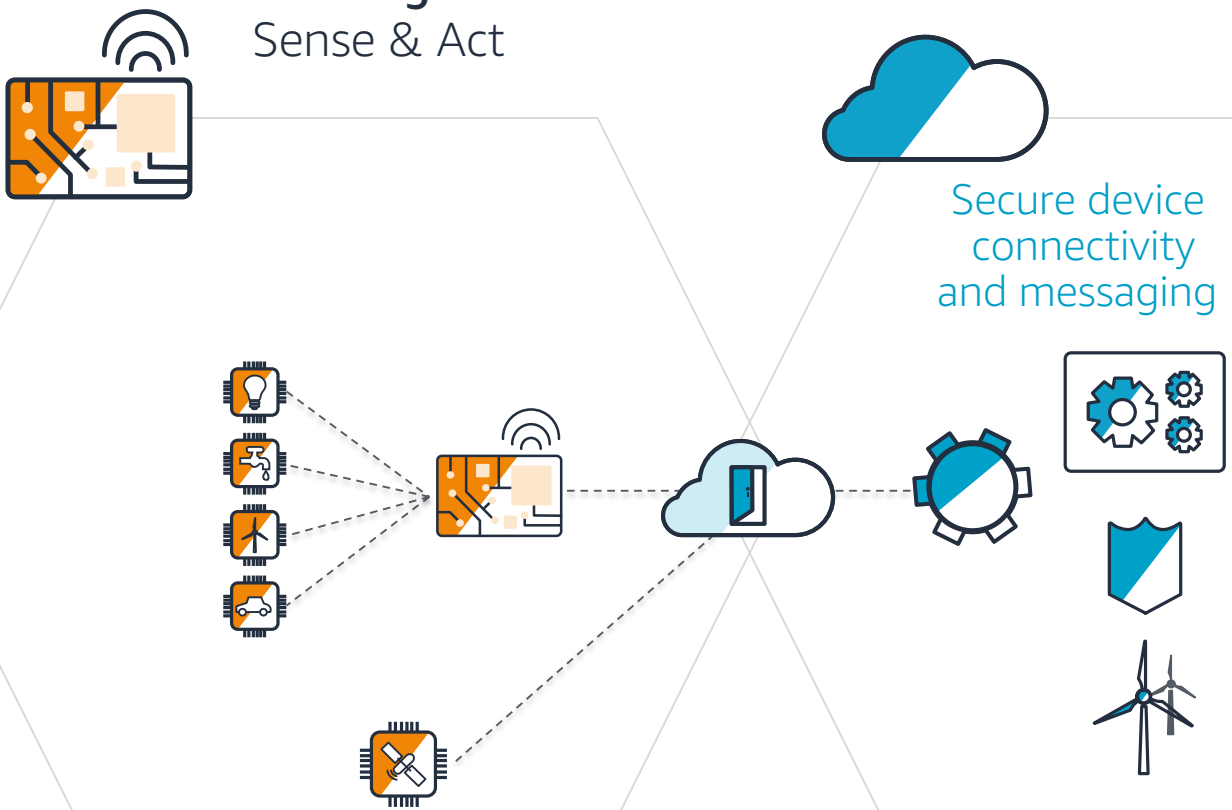
Cloud
Storage & Compute

Intelligence
Insights & Logic → Action

AWS IoT Architecture

Things
Sense & Act

Cloud
Storage & Compute



Intelligence
Insights & Logic → Action

AWS IoT Architecture

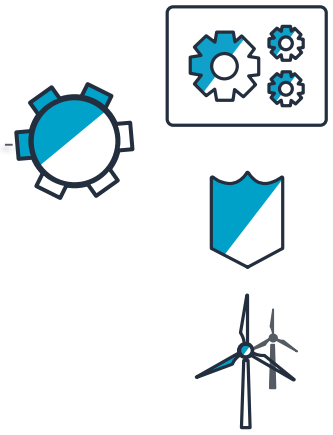
Things
Sense & Act

Secure local triggers, actions, and data sync

Endpoints

Cloud
Storage & Compute

Secure device connectivity and messaging



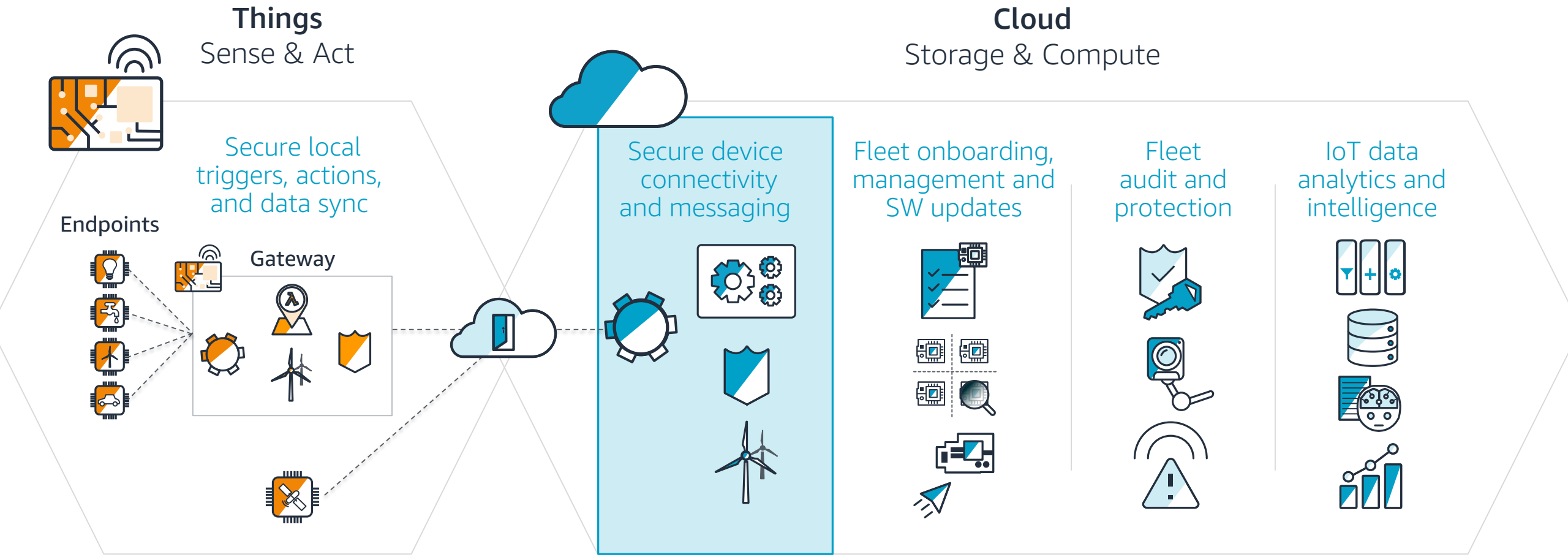
Fleet onboarding, management and SW updates

Fleet audit and protection

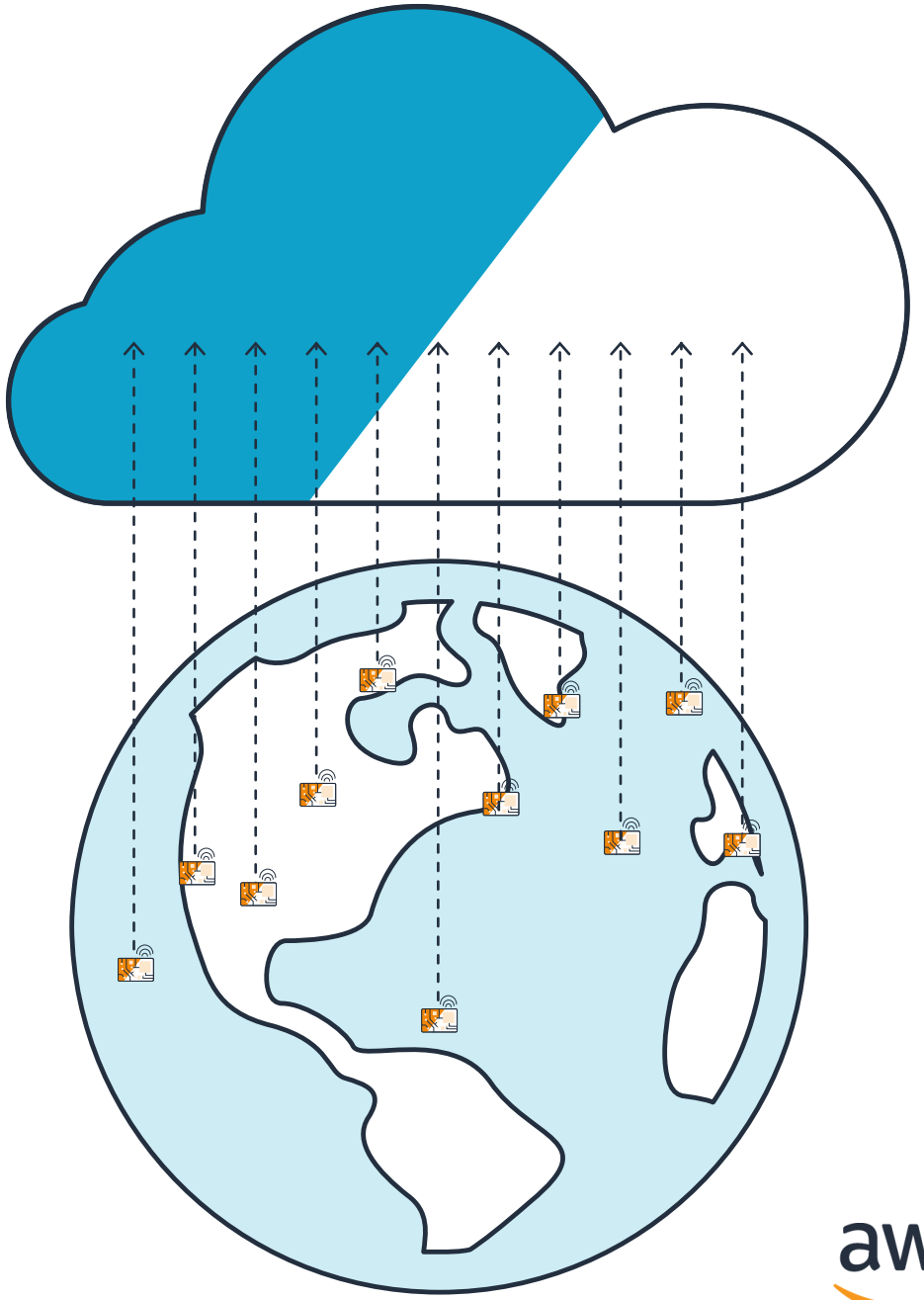
IoT data analytics and intelligence

Intelligence
Insights & Logic → Action

AWS IoT Architecture



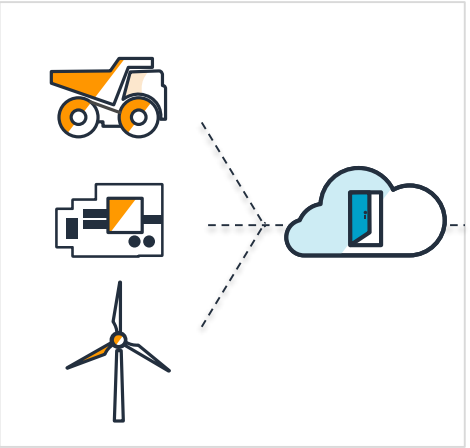
How can I connect my devices securely, and handle the data they generate?



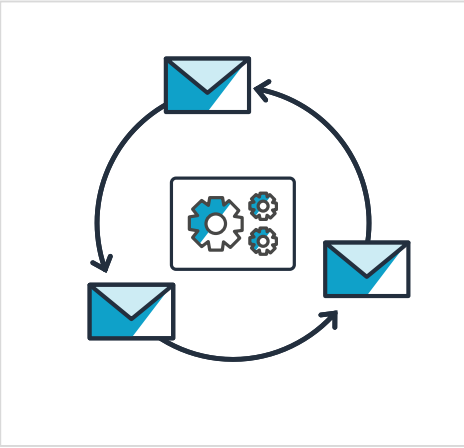
AWS IoT Core

Secure Device Connectivity and Messaging

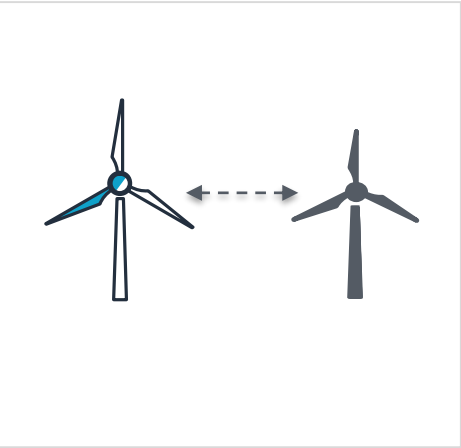
AWS IoT Core is a managed service that lets connected devices easily and securely interact with cloud applications and other devices



To securely connect devices to the AWS cloud and other devices at scale



To route, process, and act upon data from connected devices



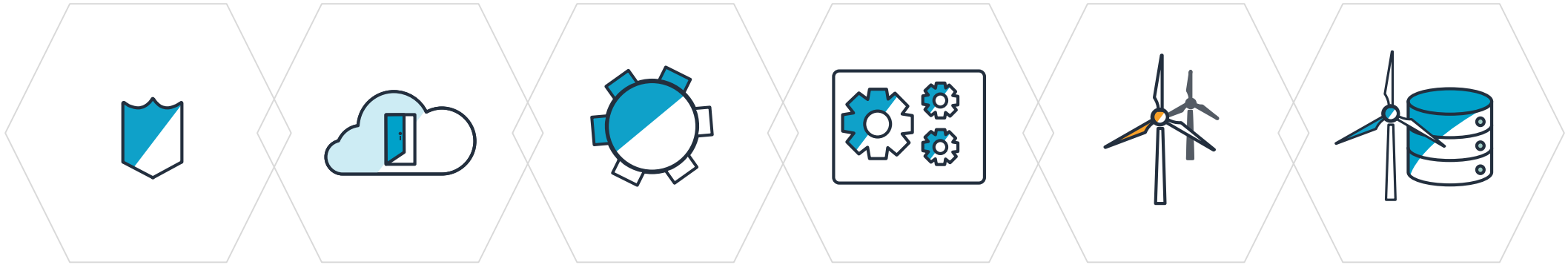
To enable applications to interact with devices even when they are offline

To fully integrate with other AWS service to reason on top of the data
(Analytics, Databases, AI, etc.)

aws

AWS IoT Core

Secure Device Connectivity and Messaging



Identity Service

Device Gateway

Message Broker

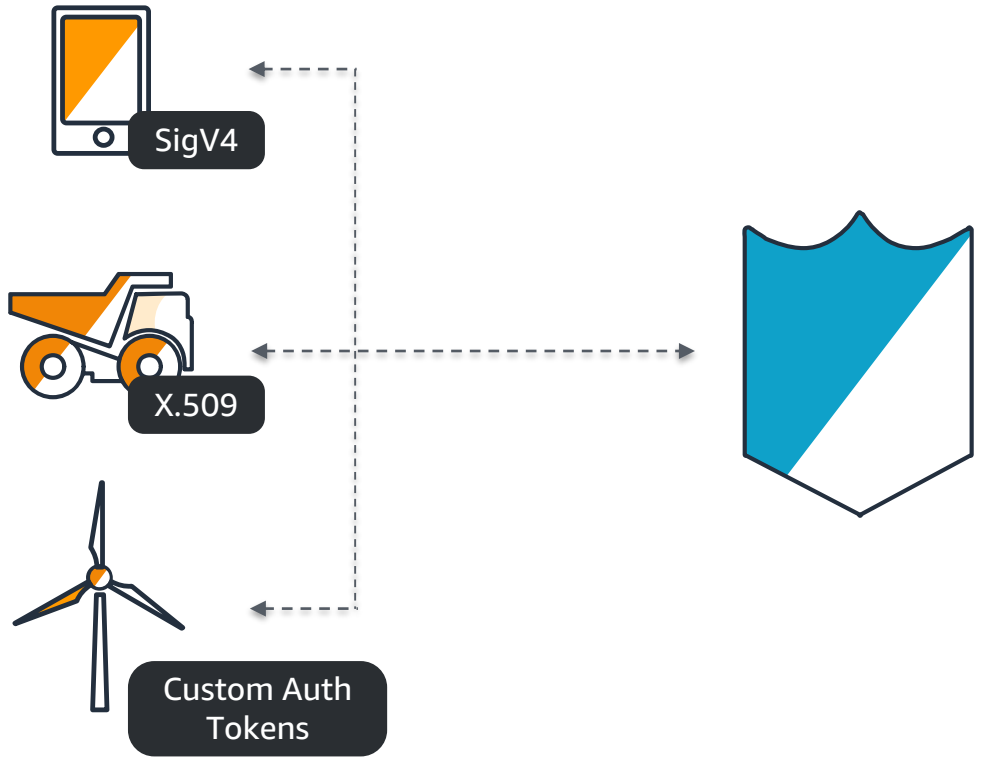
Rules Engine

Device Shadow

Registry

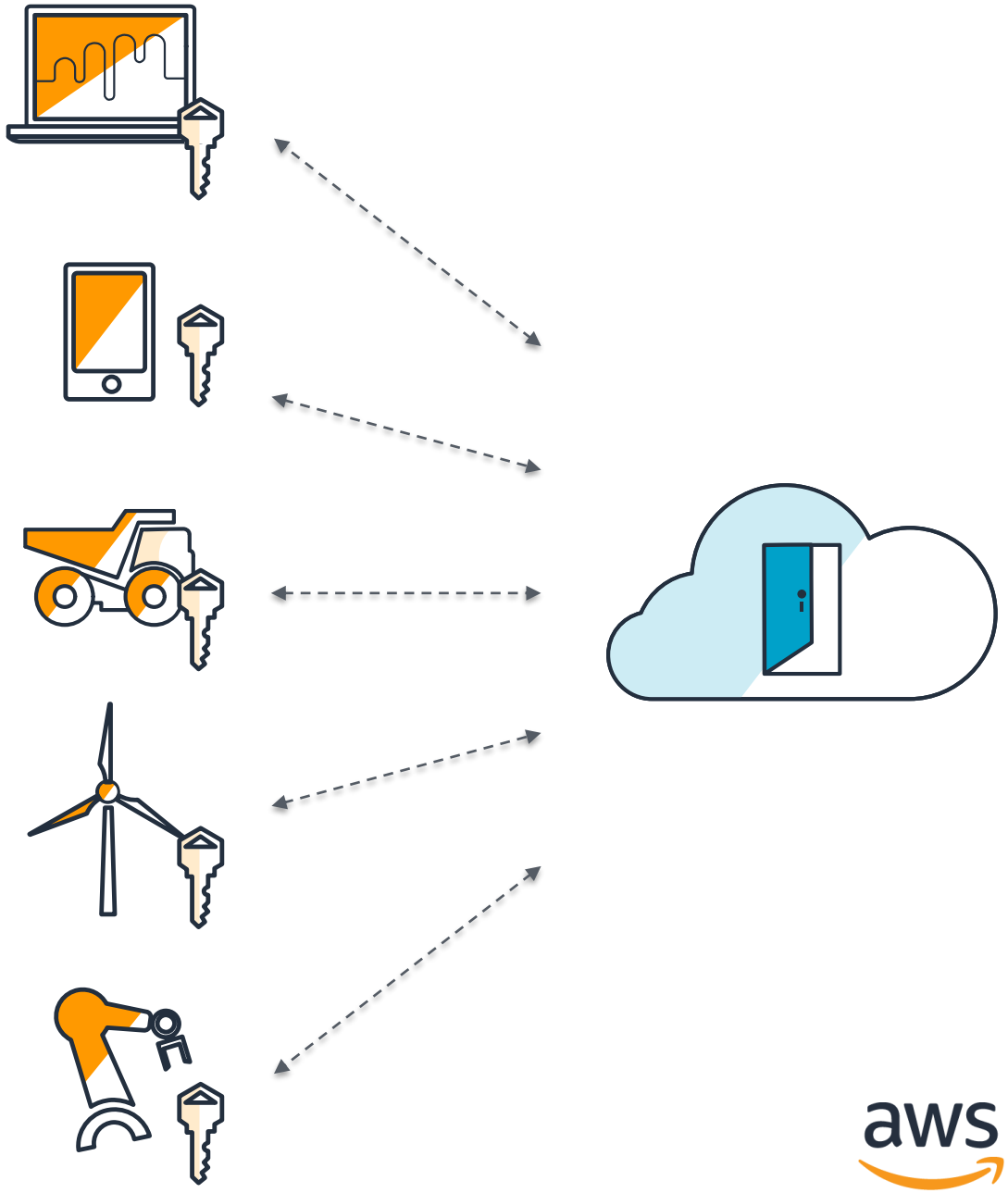
Identity Service

- Bring your own Root CA and certs or let AWS IoT Core generate certificates for you
- Automatic device provisioning with Just-In-Time Registration
- Flexible and fine-grained access control with IoT policies
  - Policies can be associated with identities or registry items
  - Can control access all the way down to the MQTT topic level



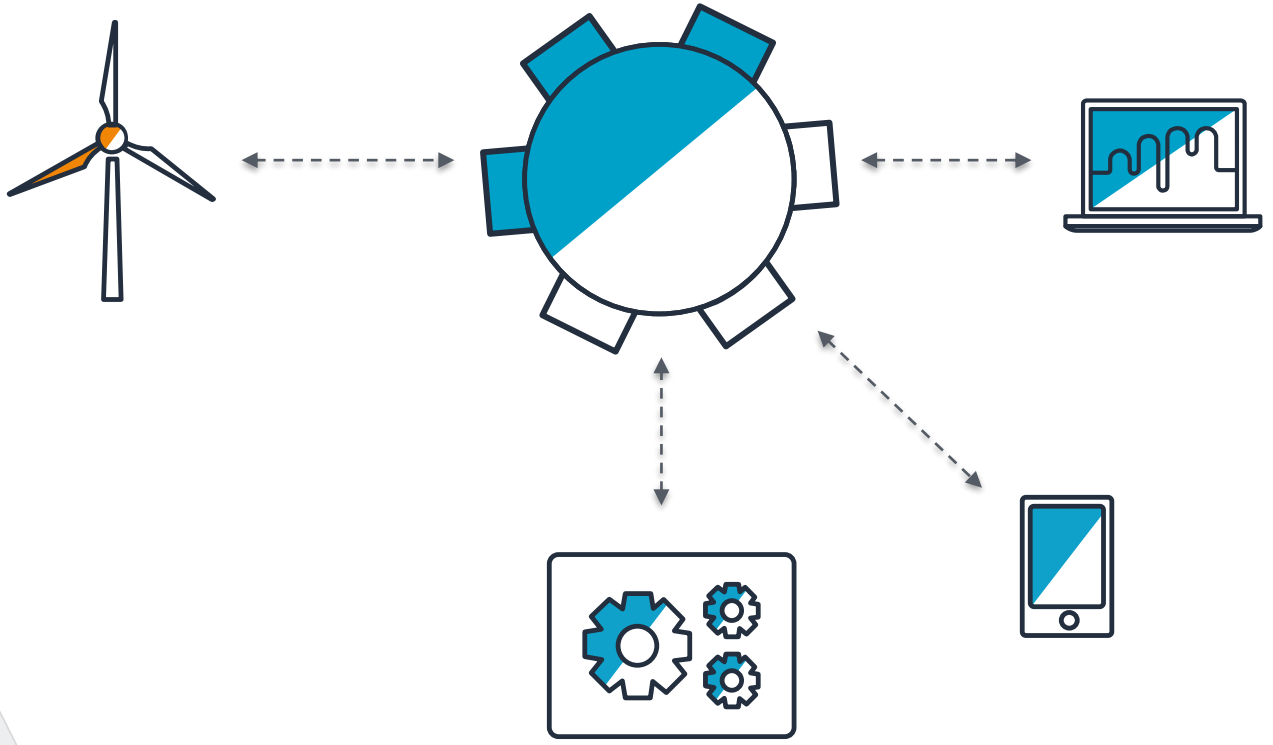
Device Gateway

- Entry point into the cloud for IoT devices
- Long-lived connections for bidirectional communication
- Support for multiple protocols including MQTT, WebSockets, HTTP
- Supports SigV4, X.509 and token based authentication (via Custom Authorizors)
- Secure communications over TLS 1.2
  - Support for numerous AES and ECDHE cipher suites



Message Broker

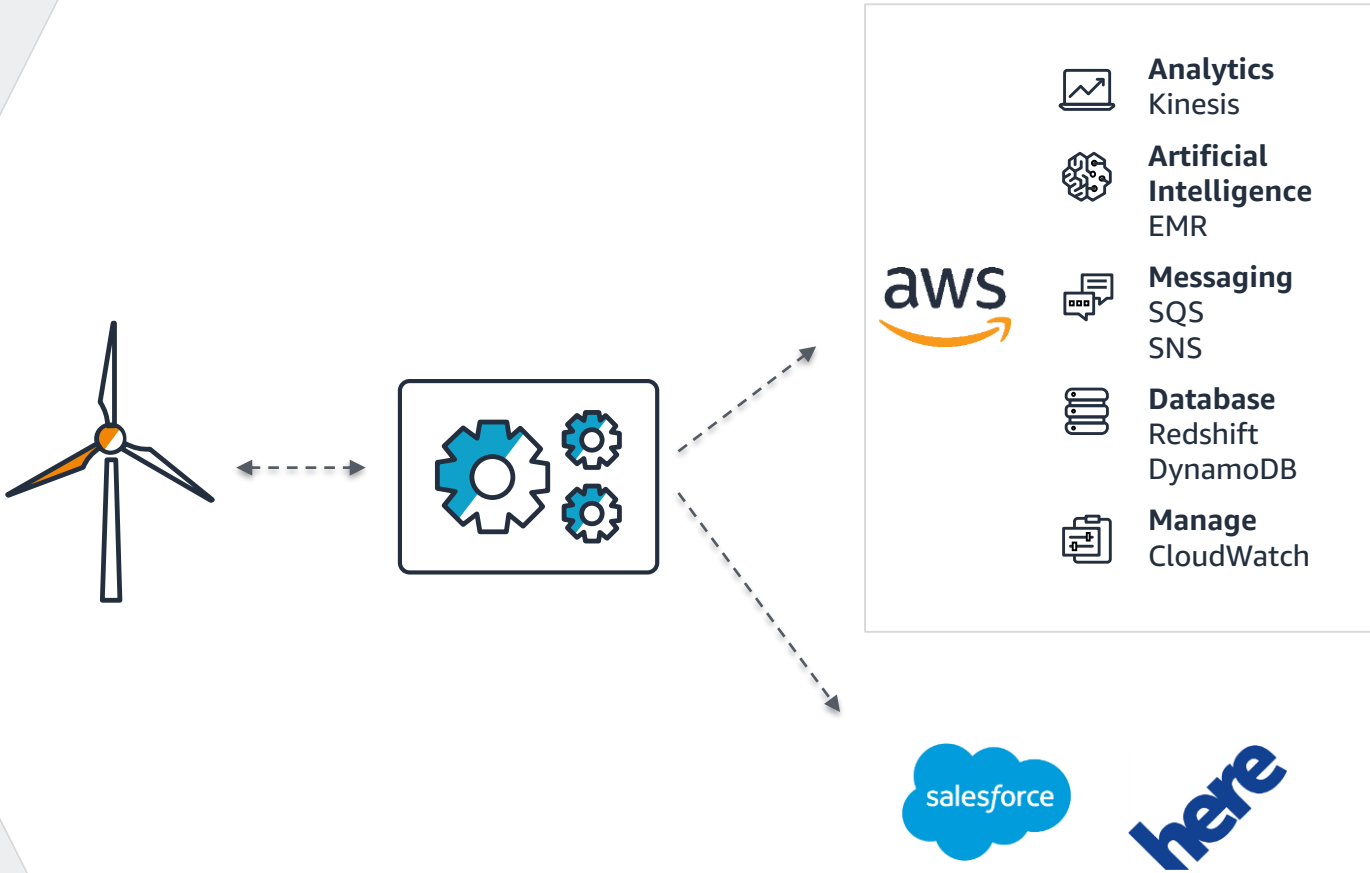
- Scalable, low-latency, reliable message routing based on MQTT protocol
- Two-way message streaming between devices and applications
- Publish/Subscribe for decoupled devices and applications
- Support for QoS0 and QoS1 messaging
- Customizable topic space with support for wildcard topic filters



Rules Engine

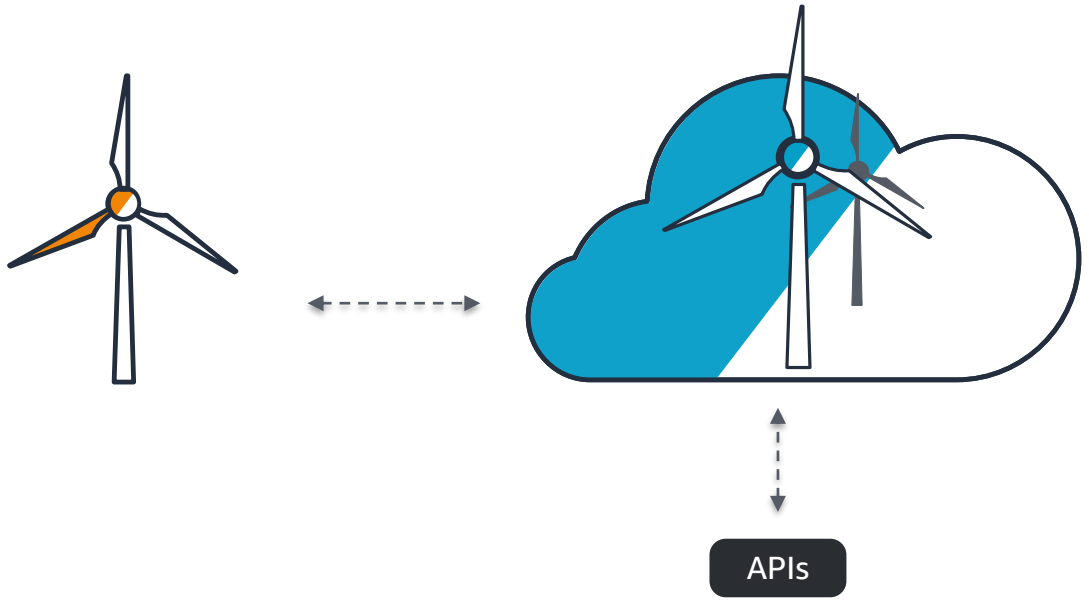
Data transformation and actions

- Easy to use SQL-like language for transforming, filtering and enriching your data
- Transform—built in functions for math, string manipulation, dates, etc.
- Filter—use the WHERE clause to capture only the data you want
- Enrich—bring in context from the Device Shadow and Amazon Machine Learning or from external sources via inline Lambda execution
- Route—send your data to over 10 AWS services and third party services like Salesforce, HERE, etc.



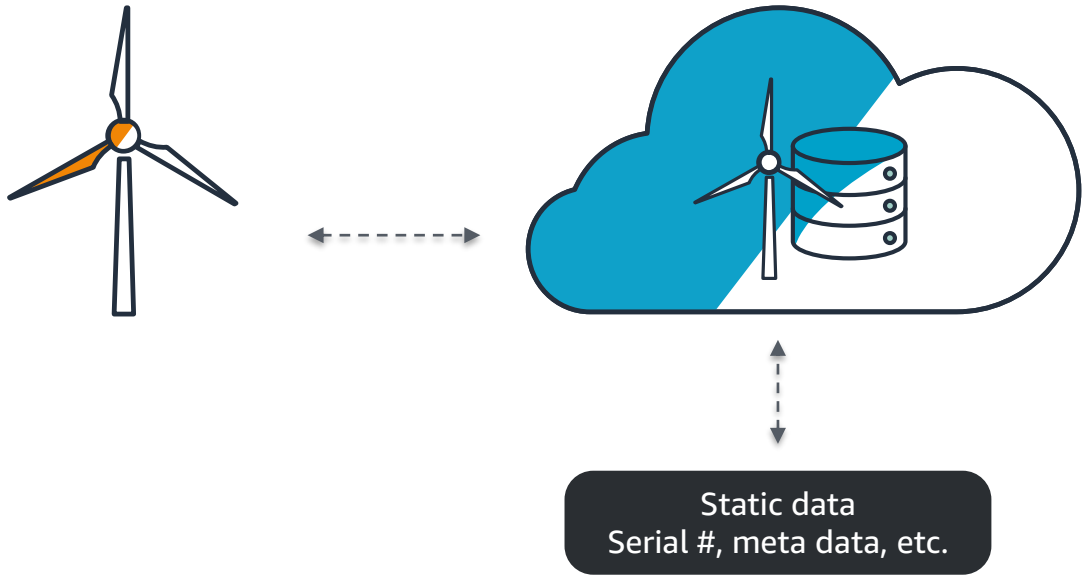
Device Shadow

- Cloud representation of dynamic device state; e.g., temperature or RPM
- Control devices via Shadow updates like volume up or down, on/off, etc.
- Devices and application notified of state change in real-time on dedicated MQTT topics (e.g., $aws/things/thing-name/shadow/update/delta)
- Query last known state for offline devices
- Automatic synchronization once devices connect
- REST APIs for applications to discover and interact with devices
- Device SDK integration for easy integration with devices



Registry

- Cloud catalog of static device meta data (e.g., Serial number, Manufacturer, etc.)
- Things that share common attributes can be associated with ThingTypes (e.g., LightBulb or Thermostat)
  - Simpler searches
  - Policies can be inherited from associated ThingTypes
- Things can be marshaled into Groups for simpler management (e.g., sensors in one building)
  - Policies can be attached to Groups
  - Jobs can be executed on Groups with AWS IoT Device Management



Problem

Pentair provides water filtration systems equipped with sensors to fish farms and large industrial brewing customers. Most of their industrial customers are located in geographies with unreliable internet connectivity. They need to send data from sensors and devices to the cloud while continuously maintaining connection which is challenging in remote areas.

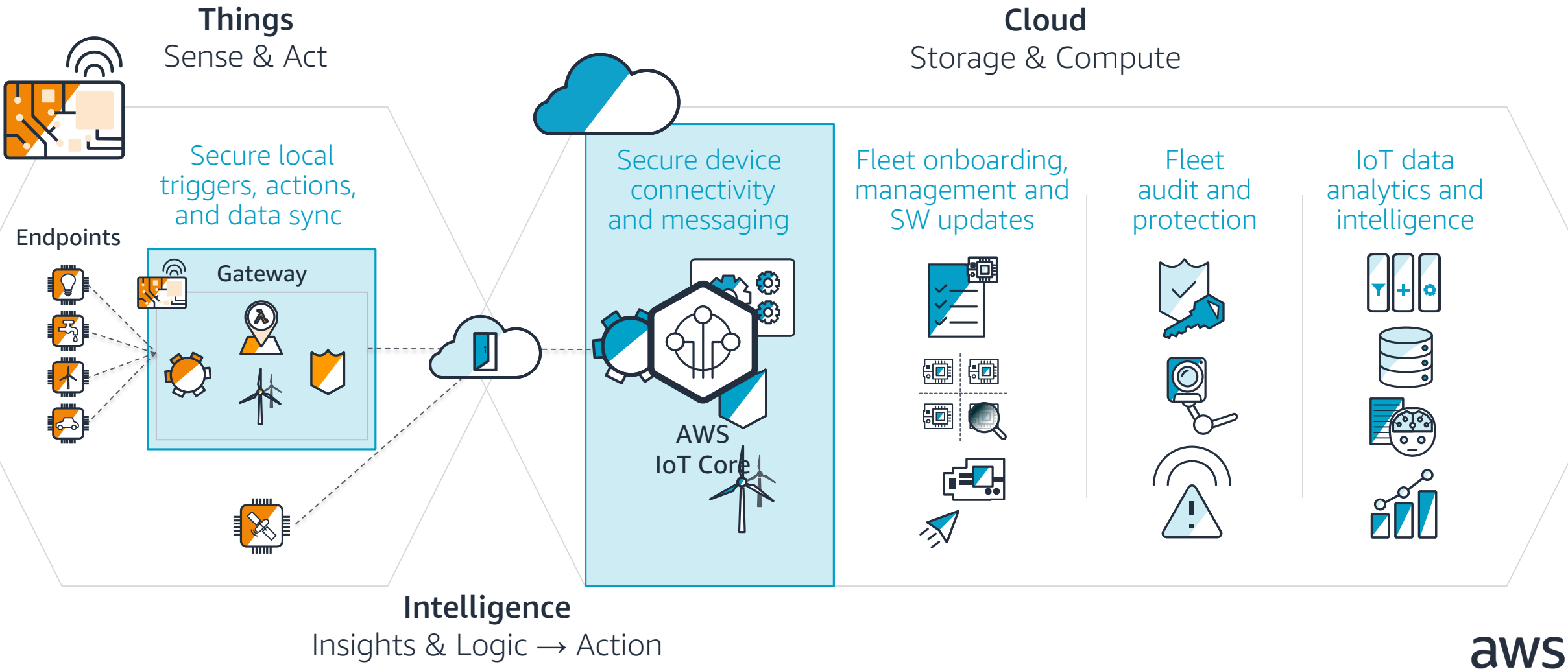
Solution

From Pentair's water filtration systems, data is sent to AWS IoT Core. When connectivity is limited, AWS Greengrass provides Pentair with a local connection so data is never lost.

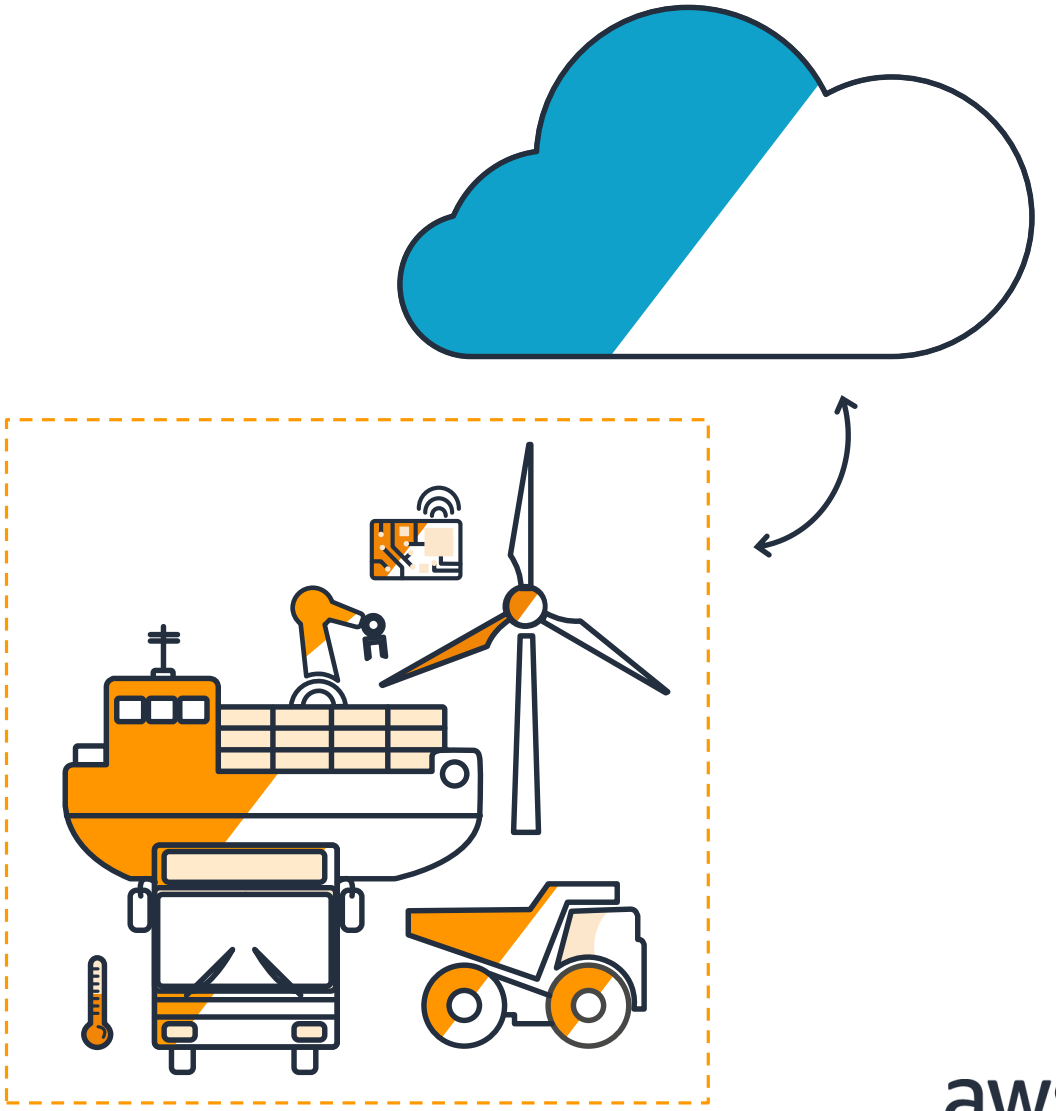
Impact

Pentair can make decisions in near real-time that impact the health of its devices but also the health of the fish which in turn, results in better yields, prevents the spread of disease, and lowers cost of operations.

AWS IoT Architecture



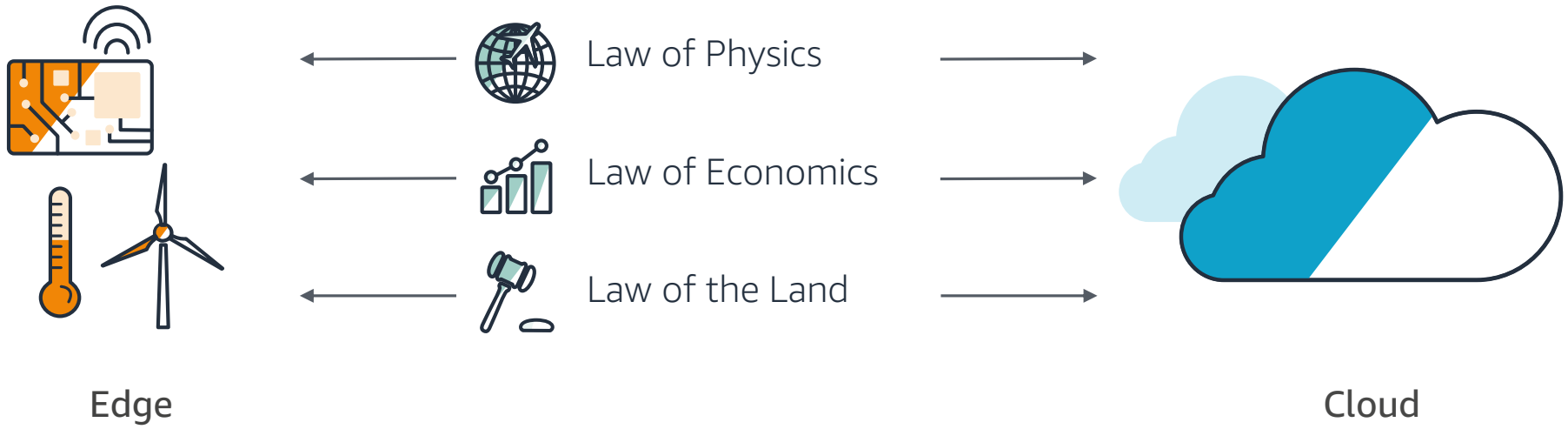
How can I extend AWS cloud capabilities to the edge?



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

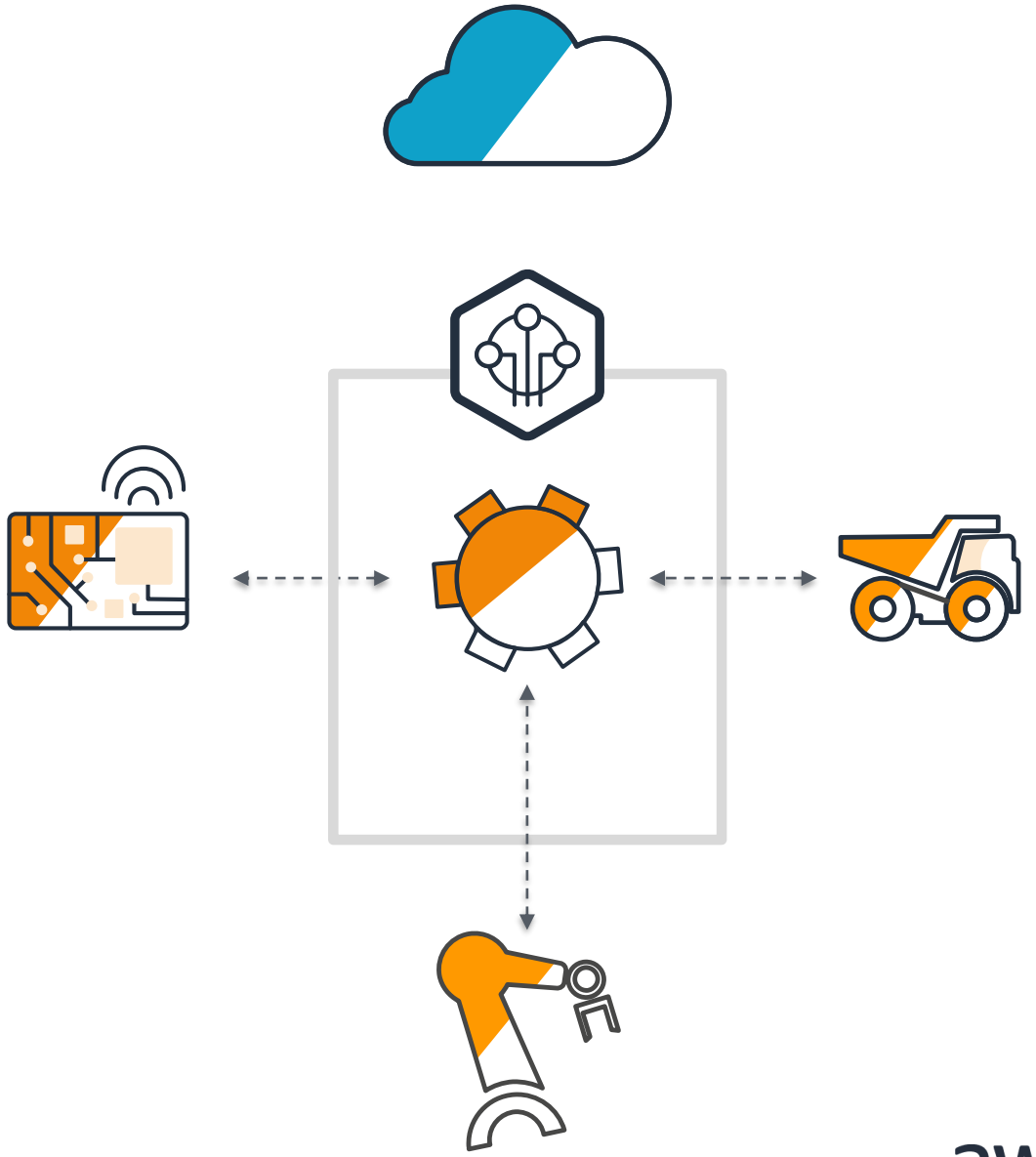
Easy Integrations With Local Protocols

Over the Air Updates

Easily Update Greengrass Core

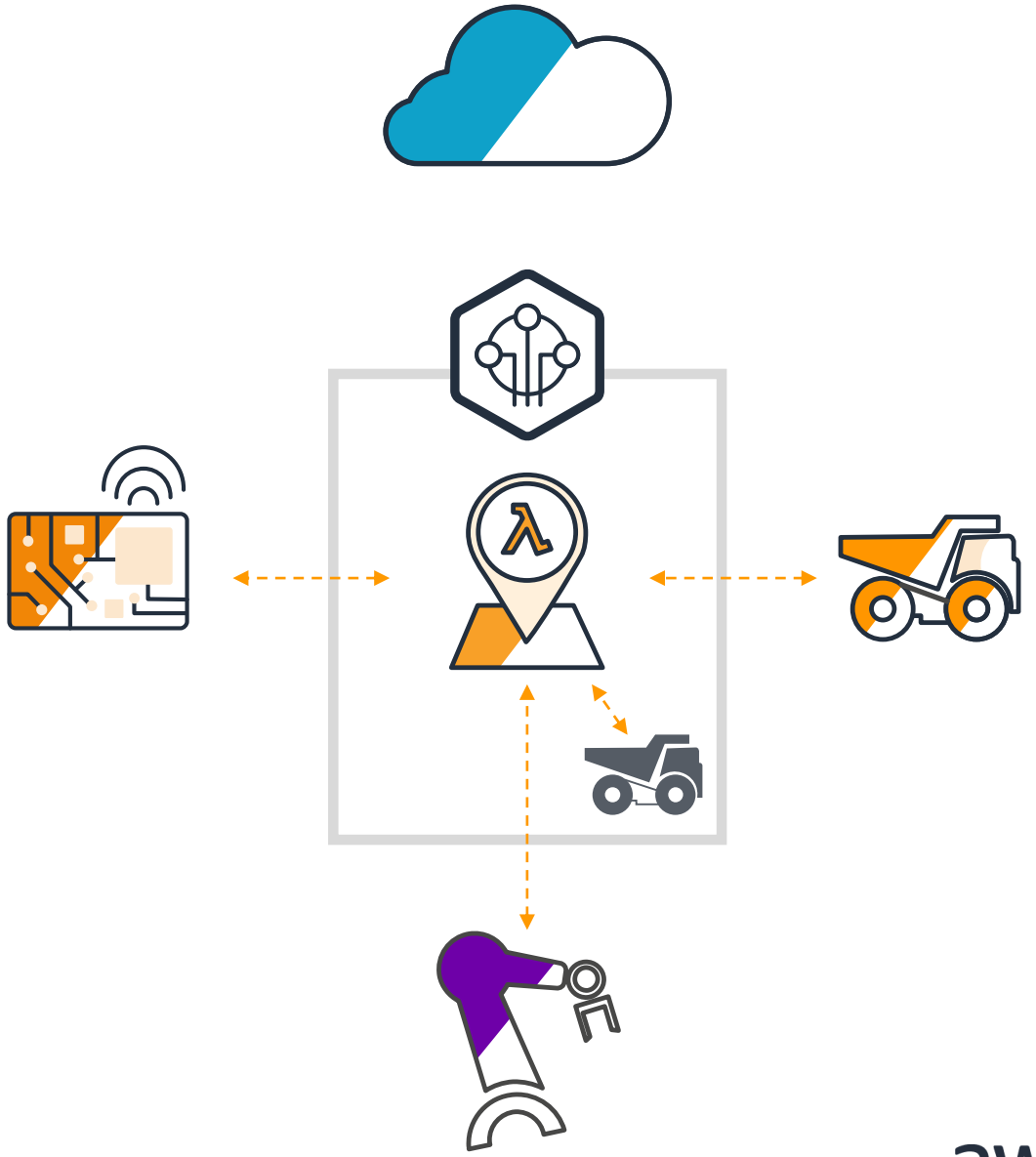
Local Messages and Triggers

- Extends the AWS IoT MQTT pub/sub messaging paradigm locally to the edge
- Allows AWS Lambda functions written in the cloud and deployed locally on the AWS Greengrass core to trigger and respond to events
- Enables offline command and control operations from the AWS Greengrass core and other devices that use the AWS IoT Device SDK
  - The AWS Greengrass core detects low moisture in the soil and in response triggers an action to spray more water in smart greenhouse, without a connection to the cloud



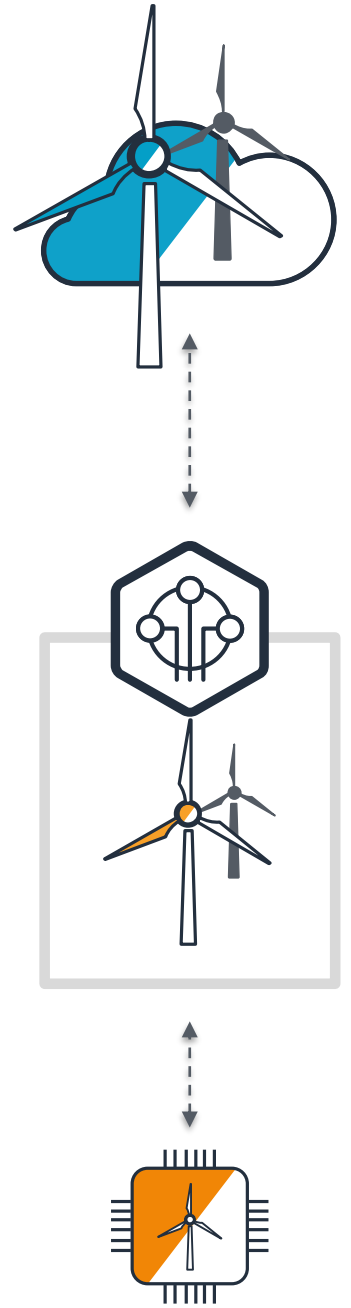
Local Actions

- With AWS Greengrass you can write event-driven AWS Lambda functions in the cloud and deploy them locally
- AWS Greengrass runs AWS Lambda functions written in Python 2.7, Node.js or Java
- Invoke AWS Lambda functions with messaging and shadow updates
- Offline actions and triggers for example, detecting low moisture in the soil and then triggering controls to spray more water inside a smart greenhouse



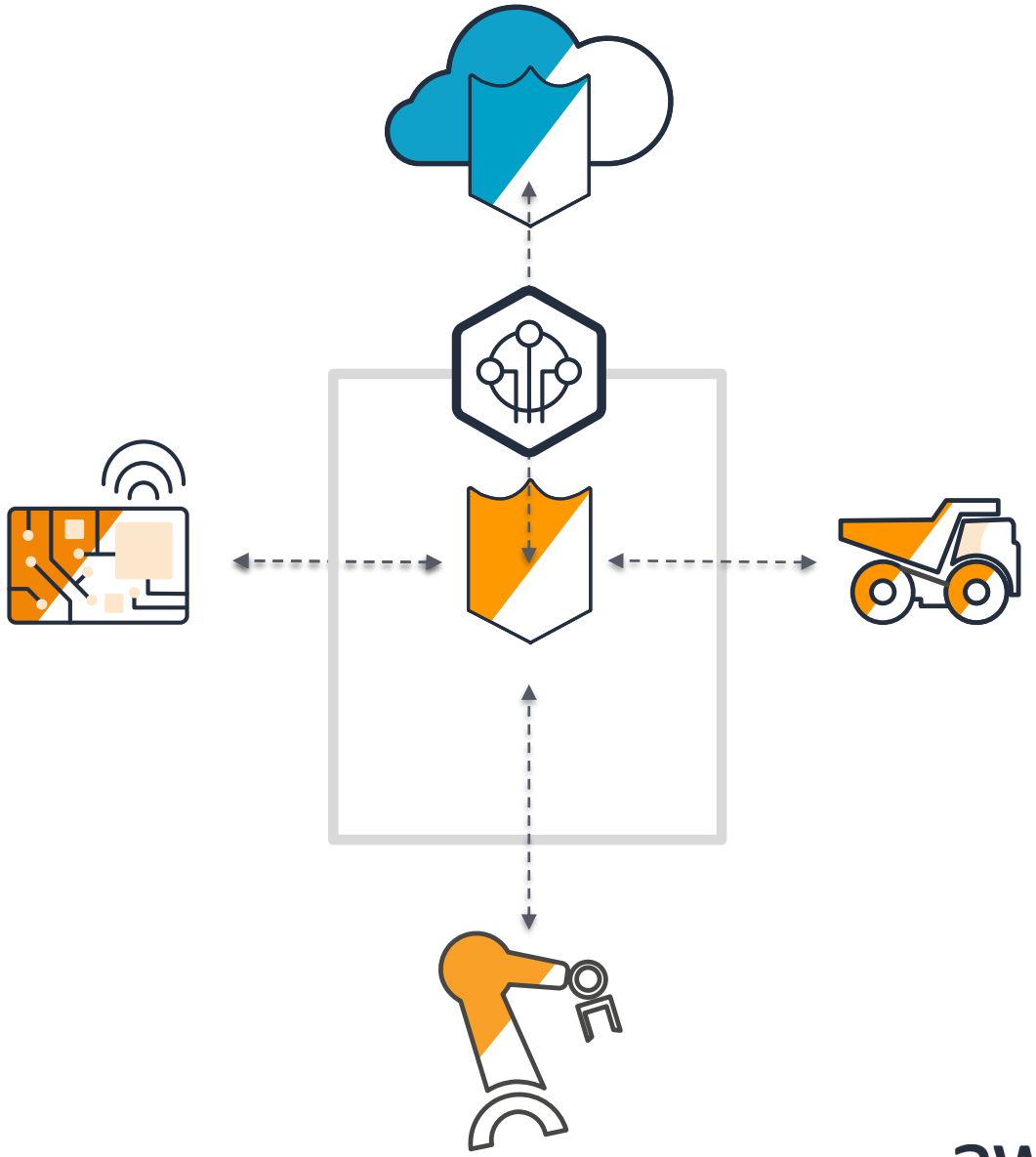
Data & State Sync

- Enables you to define a shadow state for a device as a JSON document in any logical manner—a single wind turbine, a windfarm, or a resource grid
- Allows shadow states to be local or synced to the cloud
- AWS Lambda functions running on the AWS Greengrass core can update shadow states through MQTT messages
  - For example, the AWS Greengrass core can update a tractor's shadow with continuous information on harvest quality, and a snapshot of the data can be synced to the cloud at the end of the day



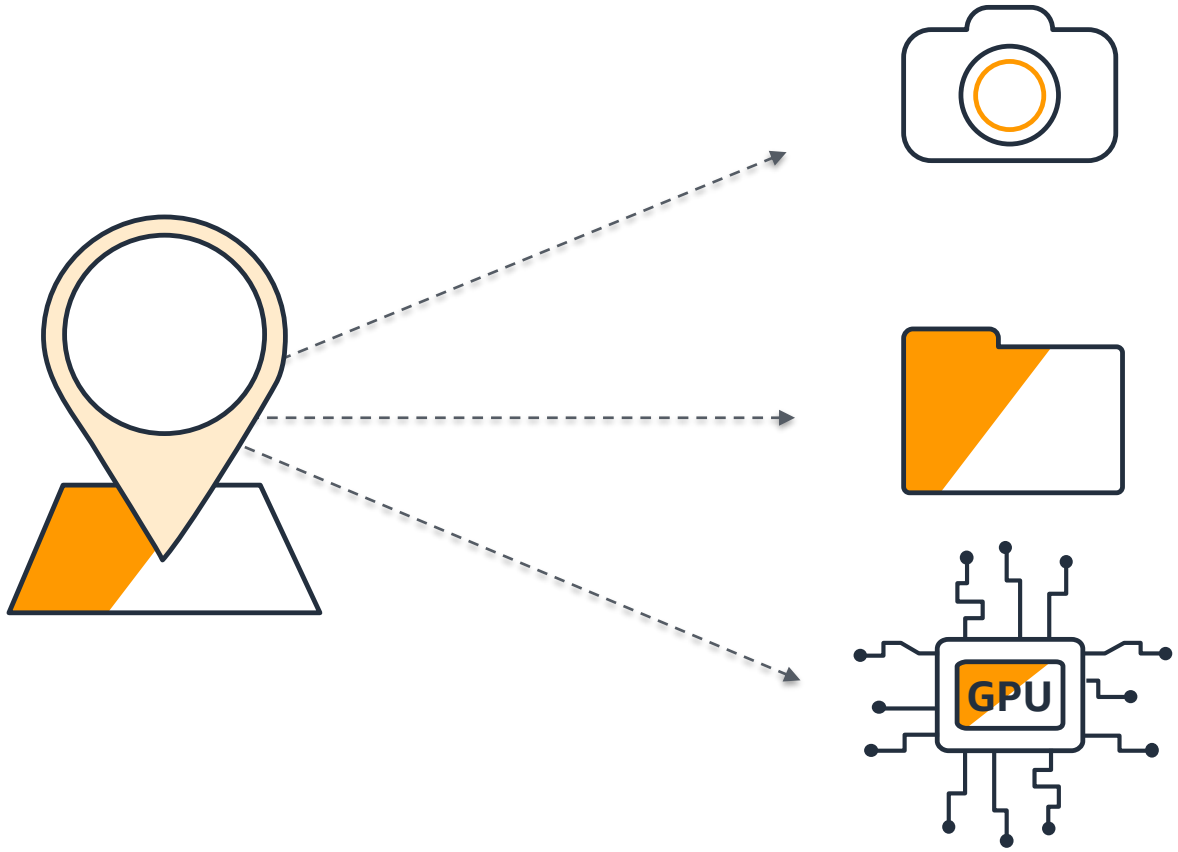
Security

- Supports TLS mutual authentication, both locally and with the cloud
- Certificates on your devices can be associated to SigV4 credentials in the cloud
- Through AWS Lambda running on the AWS Greengrass core, you can easily call any AWS service running in the cloud



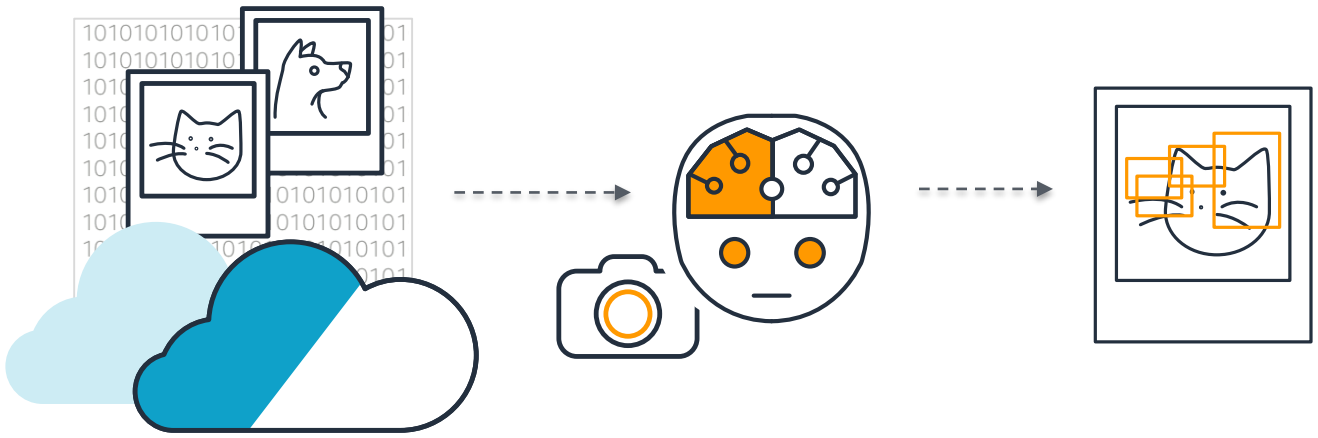
Local Resource Access

- Allows Lambdas to access local resources on a device
- GPIO can be accessed to process sensor and actuator data
- Lambdas can take advantage of the local file system on your operating system
- Lambdas can use GPUs for hardware acceleration for machine learning



Machine Learning Inference

- Train models in the cloud using Amazon Sagemaker or another service using EC2
- ML Inference works with Apache MXNet andTensorFlow
- Transfer your trained models onto your AWS Greengrass device to make predictions based on local data
- ML Inference gives you access to hardware accelerators such as GPUs on your devices

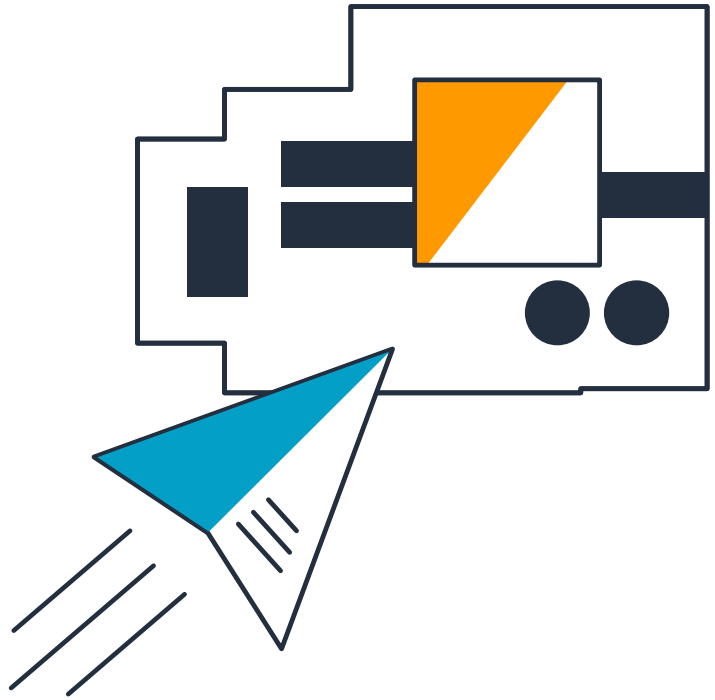


Protocol Adapter for OPC-UA

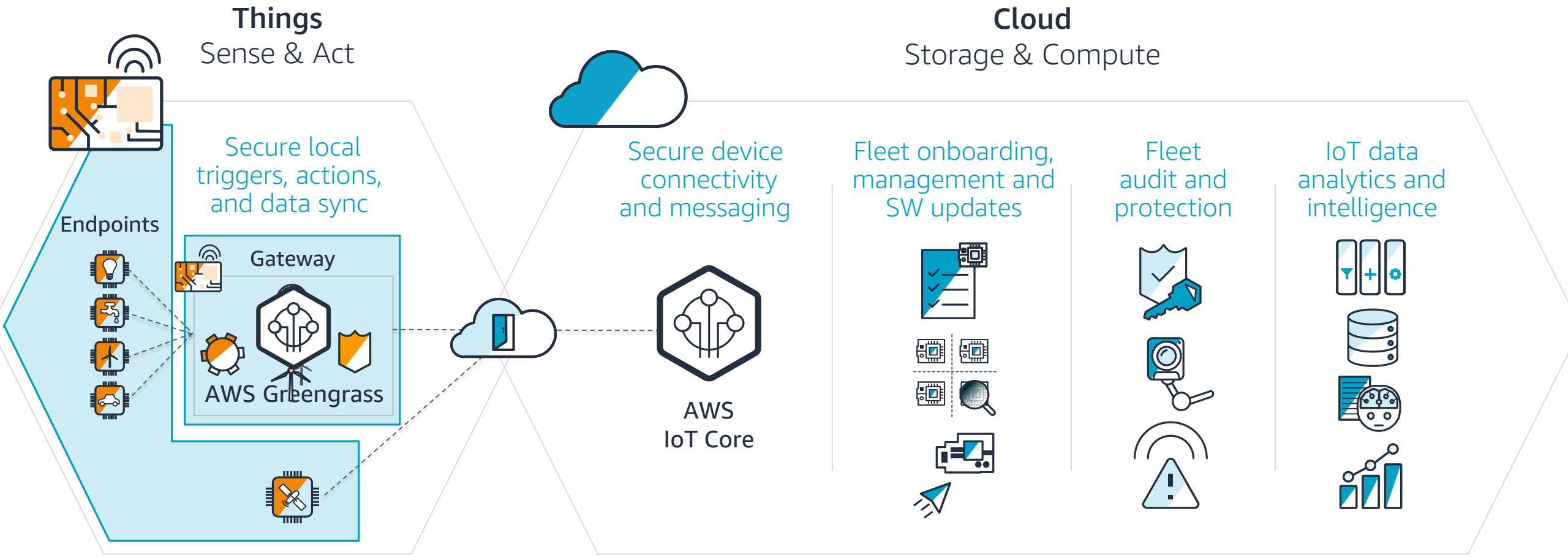
- Allows for industrial machines to participate in the AWS Greengrass programming paradigm
- Brings the robust AWS Greengrass security model to industrial devices that communicate through an OPC-UA server
- Supports certificate-based authentication with industrial OPC-UA servers
- Fully customizable framework to fit other industrial protocols
- Example: an industrial PLC on a machine can send telemetry data to a AWS Greengrass core that in turn controls other machines

Over the Air Updates

- Remotely update an AWS Greengrass core device with the latest Greengrass software, security updates, bug fixes, and new features
- Enables bulk updates of many AWS Greengrass core devices at once
- Updates are fail-safe: any breaking changes will trigger an automatic revert
- Status of updates can be tracked from the AWS IoT console



AWS IoT Architecture

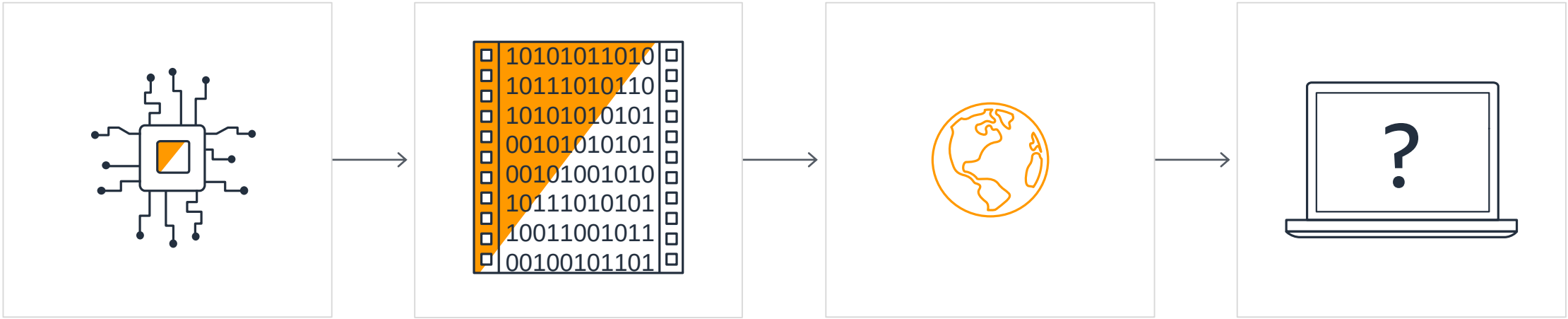


How can I securely connect constrained, microcontroller-based devices?

Amazon FreeRTOS

IoT Operating System for Microcontrollers

Amazon FreeRTOS, based on the popular FreeRTOS, is a microcontroller operating system that makes small, low powered edge devices easy to program, deploy, secure, connect, and maintain



Will it work on my chip?

Does it have the functionality I need?

Where do I get it?

How do I start?

Amazon FreeRTOS

IoT Operating System for Microcontrollers

Amazon FreeRTOS, based on the popular FreeRTOS, is a microcontroller operating system that makes small, low powered edge devices easy to program, deploy, secure, connect, and maintain

Will it work on my chip?

Does it have the functionality I need?

Where do I get it?

How do I start?

aws

Amazon FreeRTOS

IoT Microcontroller OS

Based on FreeRTOS kernel

Local Connectivity Libraries

AWS Greengrass

Cloud Connectivity Libraries

AWS IoT Core

Security Connectivity Libraries

OTA & Code Signing

Based on #1 Real-Time Operating System for Microcontrollers

- 14 years, trusted, and widely distributed
- 40+ supported architectures
- Broad ecosystem support
- Free and open source
- Introducing version 10
- MIT Open Source License
- Improved Inter-Process Communication (IPC) capabilities with stream and message buffers

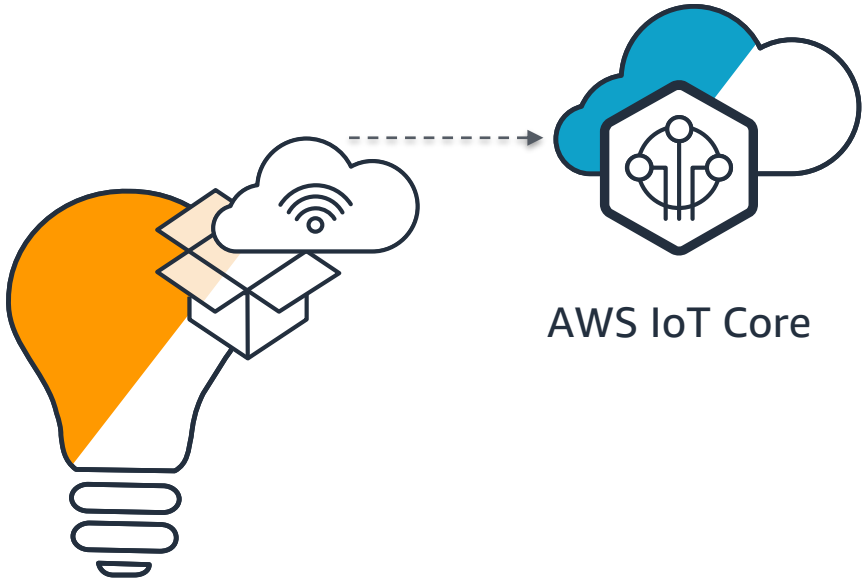
Local Connectivity Libraries

Connect with AWS Greengrass

- Local communication with edge gateways and a Wi-Fi stack, including AWS Greengrass discovery support
- Wi-Fi management library implements an abstraction layer for Wi-Fi features such as setup, configuration, provisioning, security, and power management
- Continue communicating, collecting data, and taking actions without a cloud connection
- Support for many network topologies and use cases

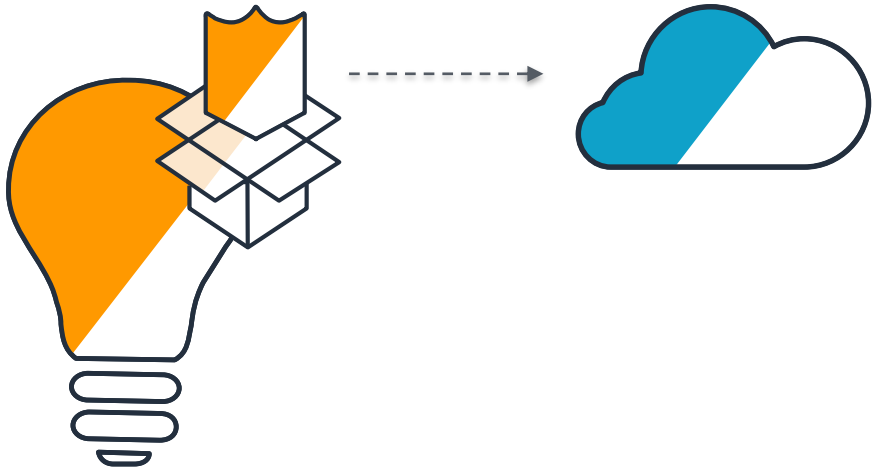
Cloud Connectivity Libraries

- Connectivity to AWS IoT Core
- MQTT Pub/Sub messaging
- Device Shadow support
- Take advantage of IoT Core benefits like IoT Device Management, scalable architecture, and pay as you go pricing
- Fastest way to get started on IoT microcontrollers



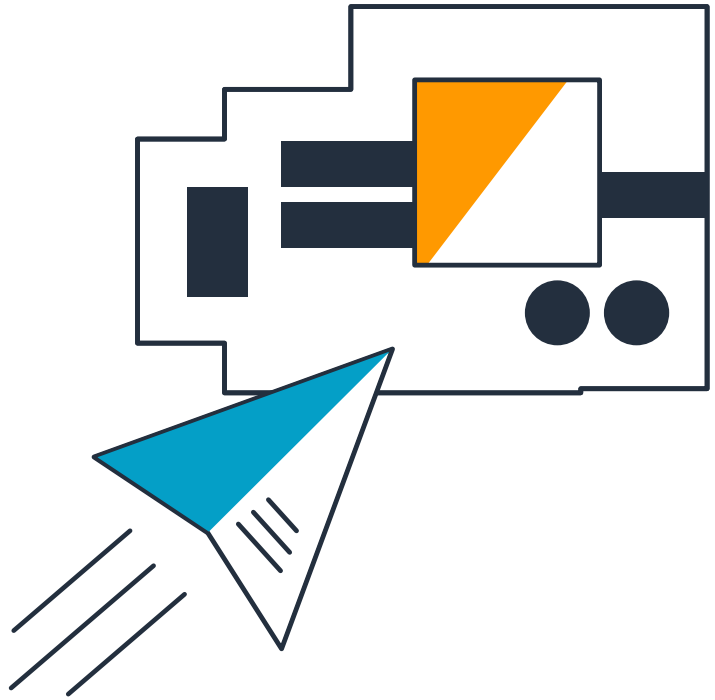
Security Connectivity Libraries

- Secure sockets using TLS
- Certificate-based authentication
- PKCS#11 interface for key management
- Secure by default
- No open network ports
- Only run trusted code
- Clear, modular implementation

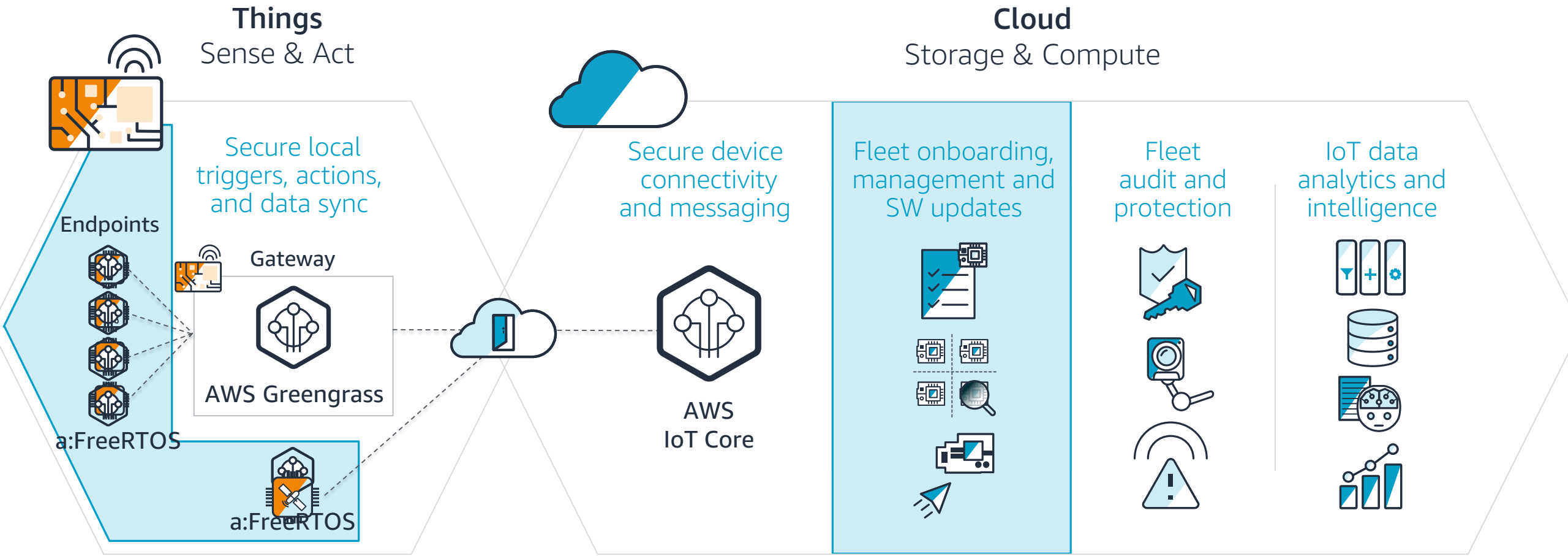


Over-the-Air Firmware Updates

- Use AWS IoT Device Management to assign updates to groups
- Code sign new firmware images
- Stream updates to your device over MQTT
- Validate signature on device
- APIs to control installation and reboot logic
- Simple to manage groups
- Control authorship and ensure devices only run trusted code
- Memory efficient updated client

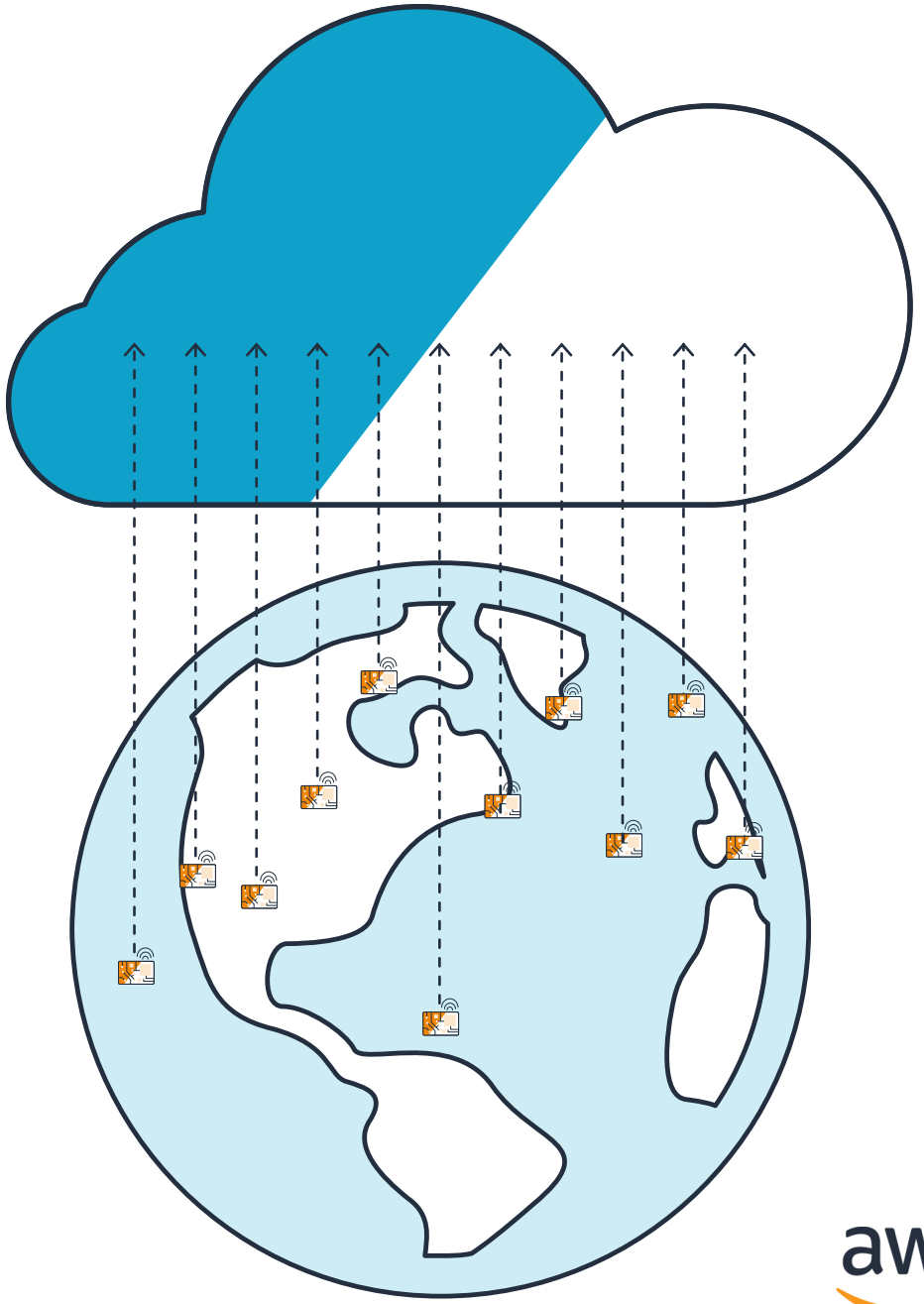


AWS IoT Architecture



Intelligence
Insights & Logic → Action

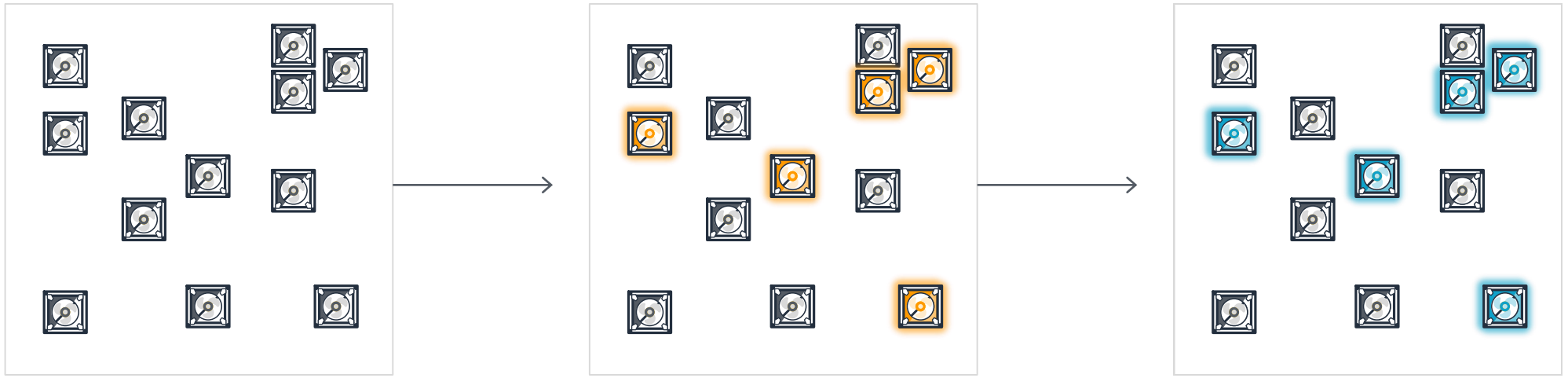
How can I manage my growing number of connected devices?



AWS IoT Device Management

Device Management Service

AWS IoT Device Management helps you onboard, organize, monitor, and remotely manage your growing number of connected devices



Fast device onboarding at scale

Real-time fleet indexing and search

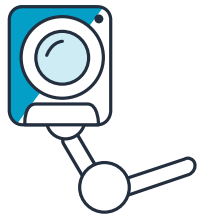
Monitoring and updating devices

AWS IoT Device Management

Maintain Fleet Health

Batch Fleet Provisioning

Real-time Fleet Index & Search

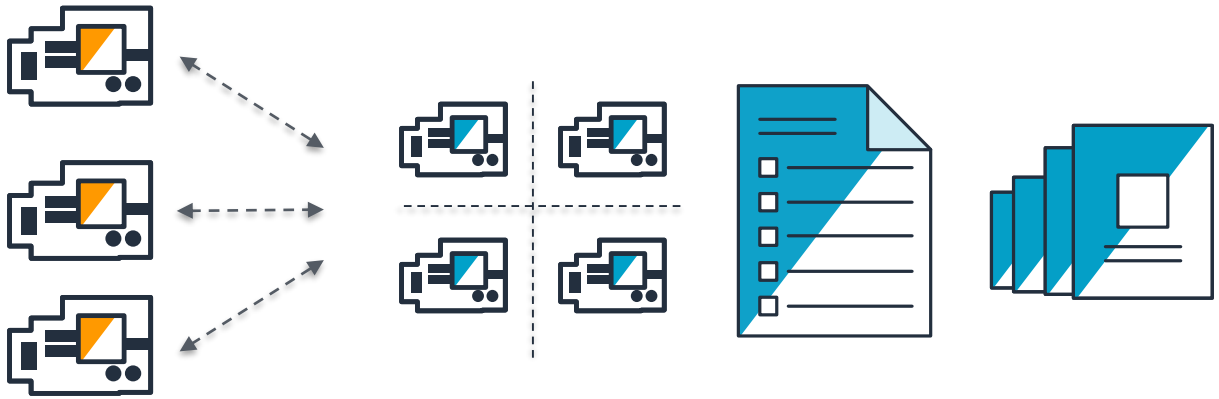


Fine Grained Device Logging & Monitoring

Over the Air Updates

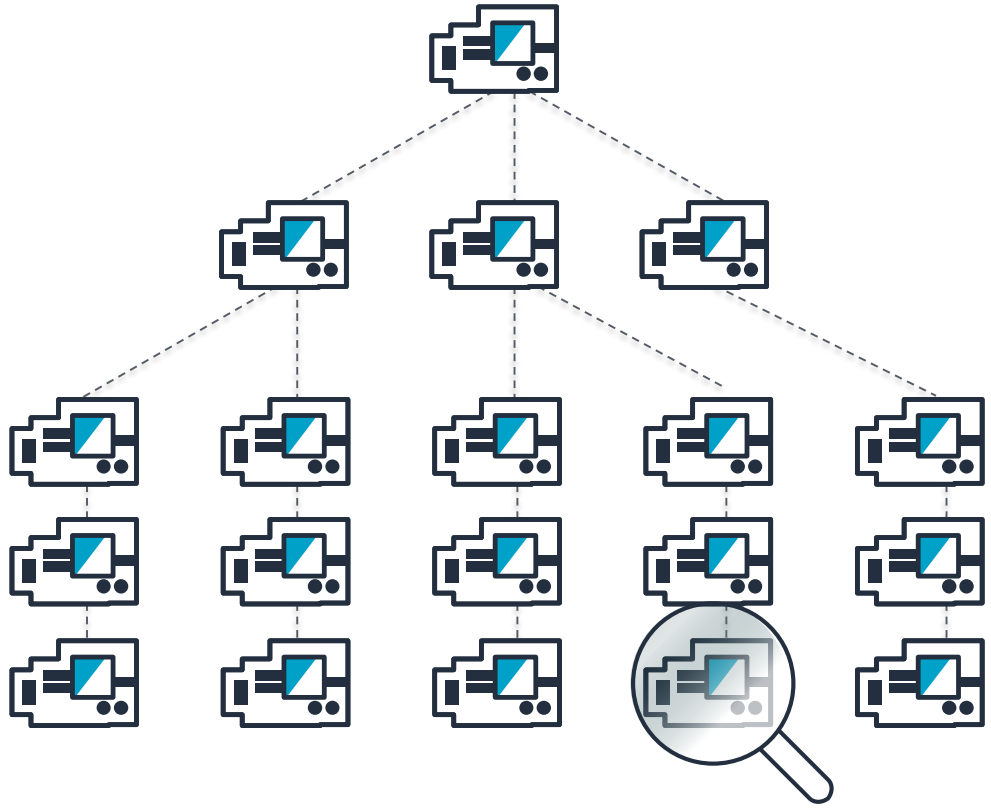
Batch Fleet Provisioning

- 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)



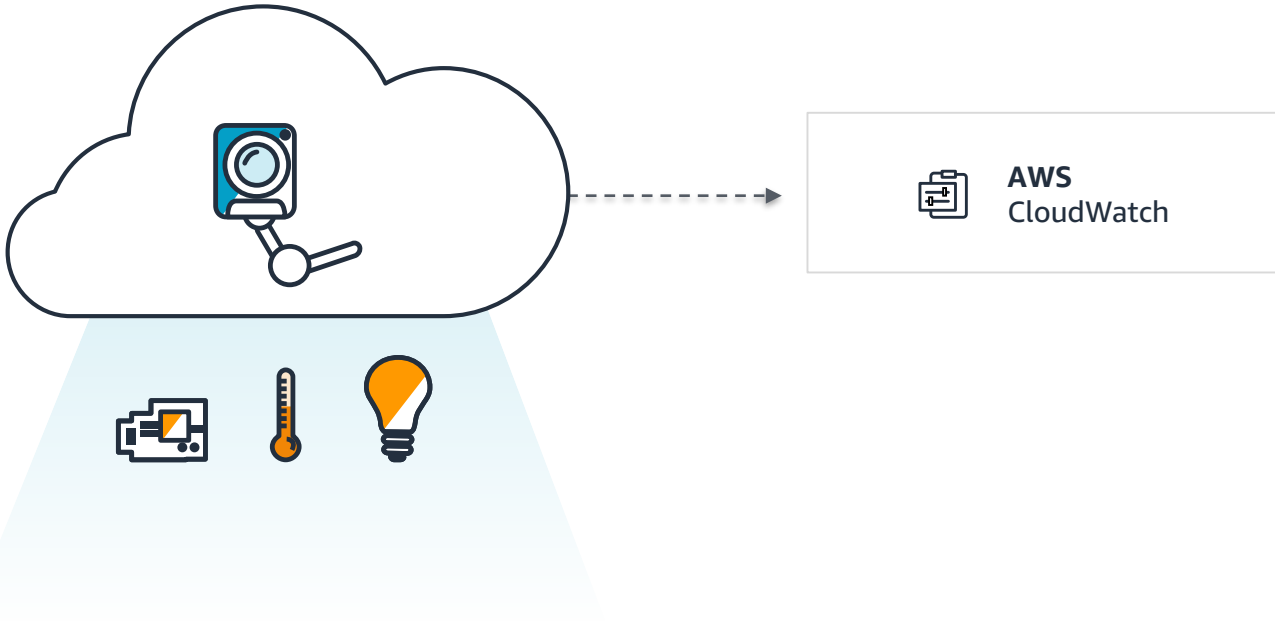
Real-time Fleet Index & Search

- 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



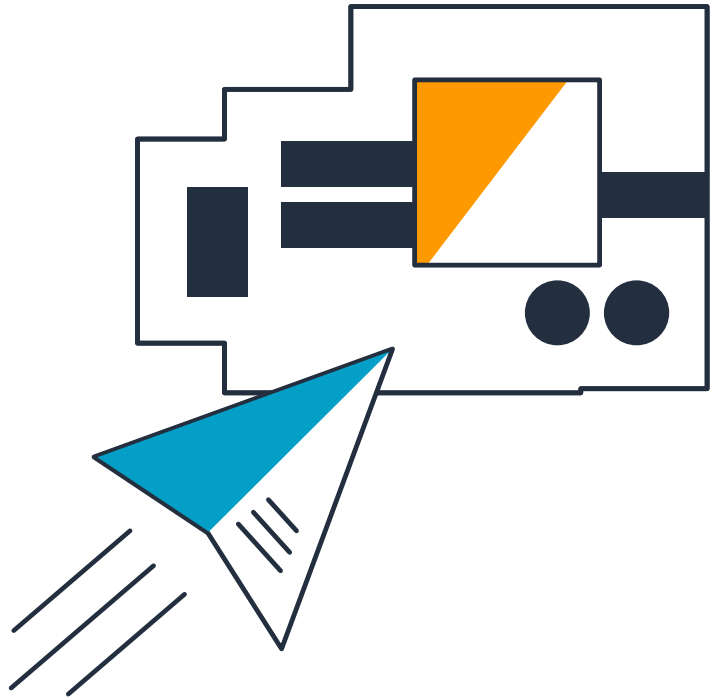
Fine Grained Device Logging & Monitoring

- Allows you to configure the logging level on a per device basis or on a group of devices
- To troubleshoot an issue, you can selectively increase their diagnostic levels across a subset of devices that are malfunctioning
- Logs are uploaded to CloudWatch



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



Problem

Trimble integrates a wide range of positioning technologies including GPS, laser, optical, and inertial technologies to provide complete commercial solutions across 150 countries. For these solutions, Trimble needs to provision and manage a diverse range of connected devices.

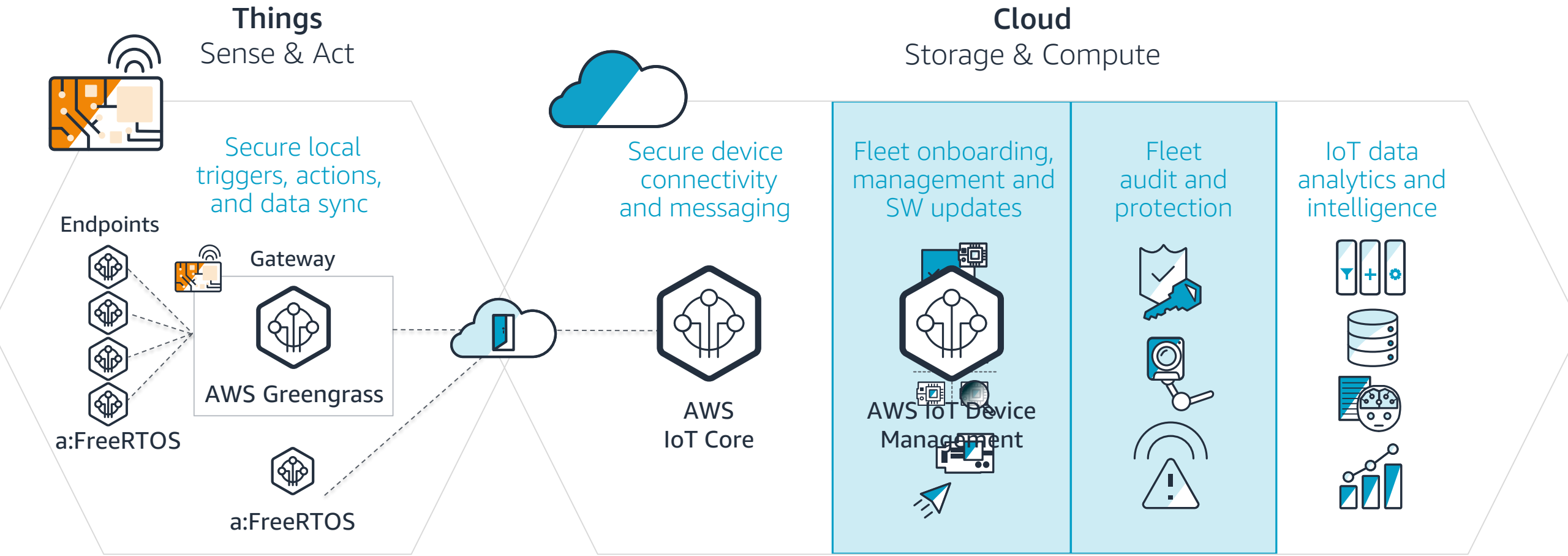
Solution

Trimble aggregates all of Trimble sub-services (IoT, Ingress, Egress, ETL, and Analytics) into an internal product called TPAAS. The TPAAS product, which leverages AWS IoT Core and IoT Device Management, will be the IoT Platform of choice for all future Trimble workloads, including migrating legacy data to the cloud.

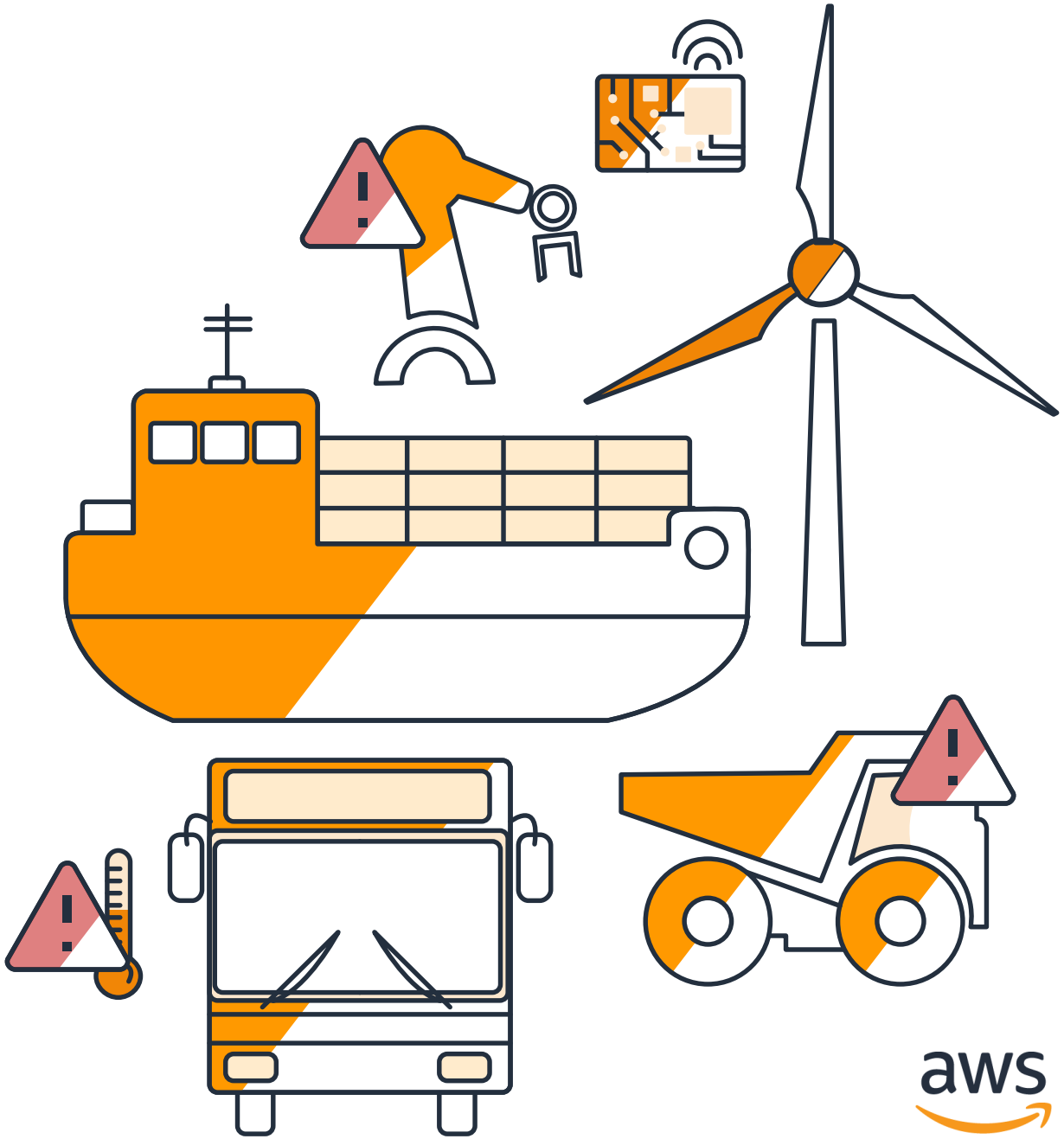
Impact

AWS IoT Device Management helped Trimble increase their device provisioning throughput by 400%, which allowed them to meet their planned production throughput for connected devices.

AWS IoT Architecture



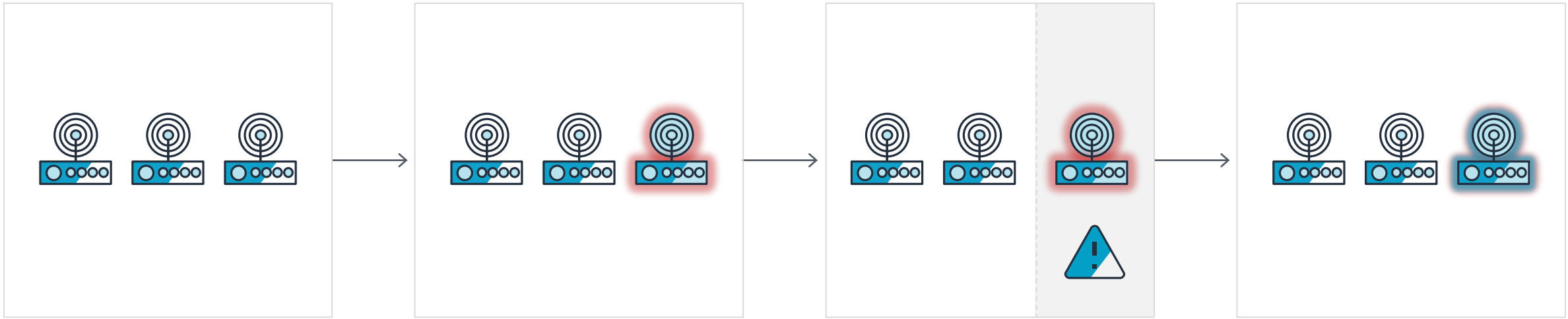
How do I ensure my connected devices stay secure?



AWS IoT Device Defender

Keep Your Fleet Secure

AWS IoT Device Defender is a fully managed IoT security service that enables you to secure your fleet of connected devices on an ongoing basis



Audit device configurations, define and monitor device behavior

Identify drifts in security settings and detect device anomalies

Generate alerts

Patch security vulnerabilities

AWS IoT Device Defender

Keep Your Fleet Secure

Audit Device Configurations

Monitor Device Behavior

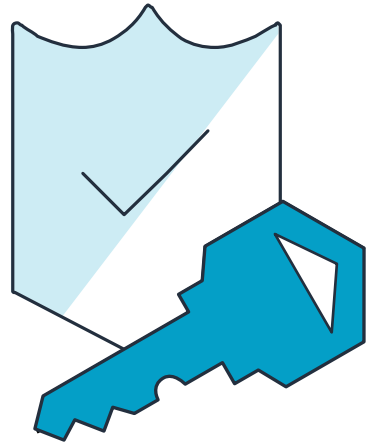
Identify Anomalies

Generate Alerts

Patch Security Vulnerabilities

Audit Device Configurations

- Audit device security policies against a set of built-in IoT security best practices
- Schedule audits (daily, weekly) or run ad-hoc audits during vulnerable periods such as device deployments
- Run audits to spot security gaps
  - Devices using the same certificate
  - One device subscribing to data from all other devices
  - Expiring certificates

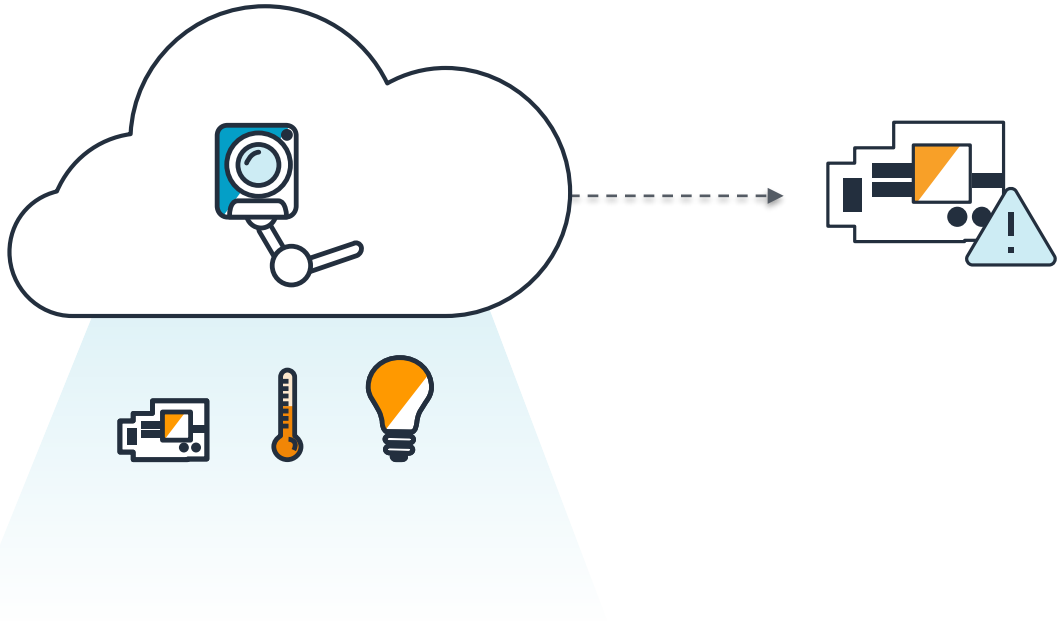


scheduled

Ad-hoc

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



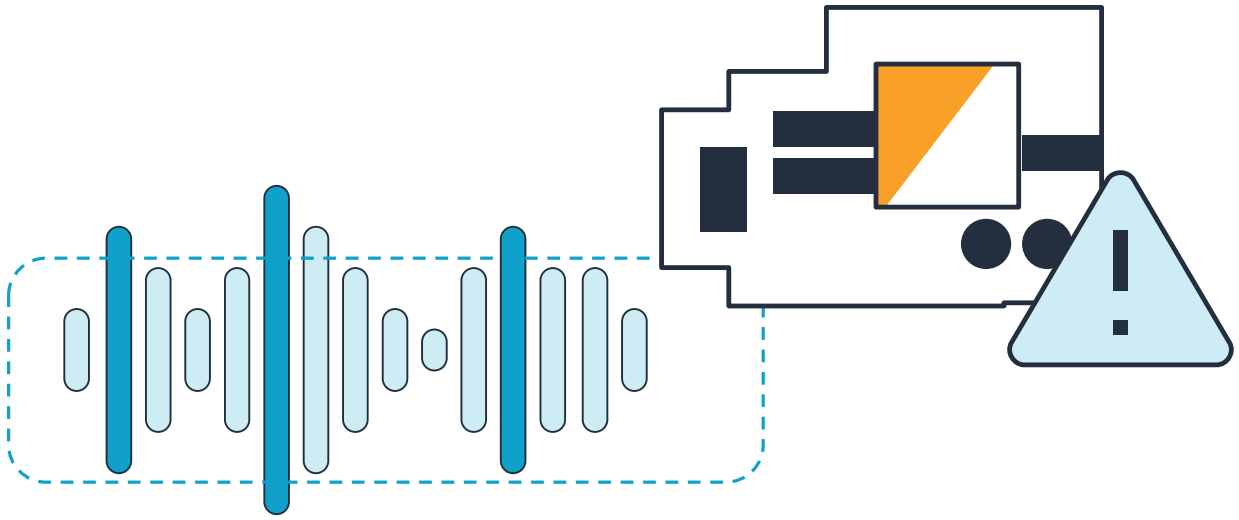
Identify Anomalies

Blacklist/Whitelist behaviors for:

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

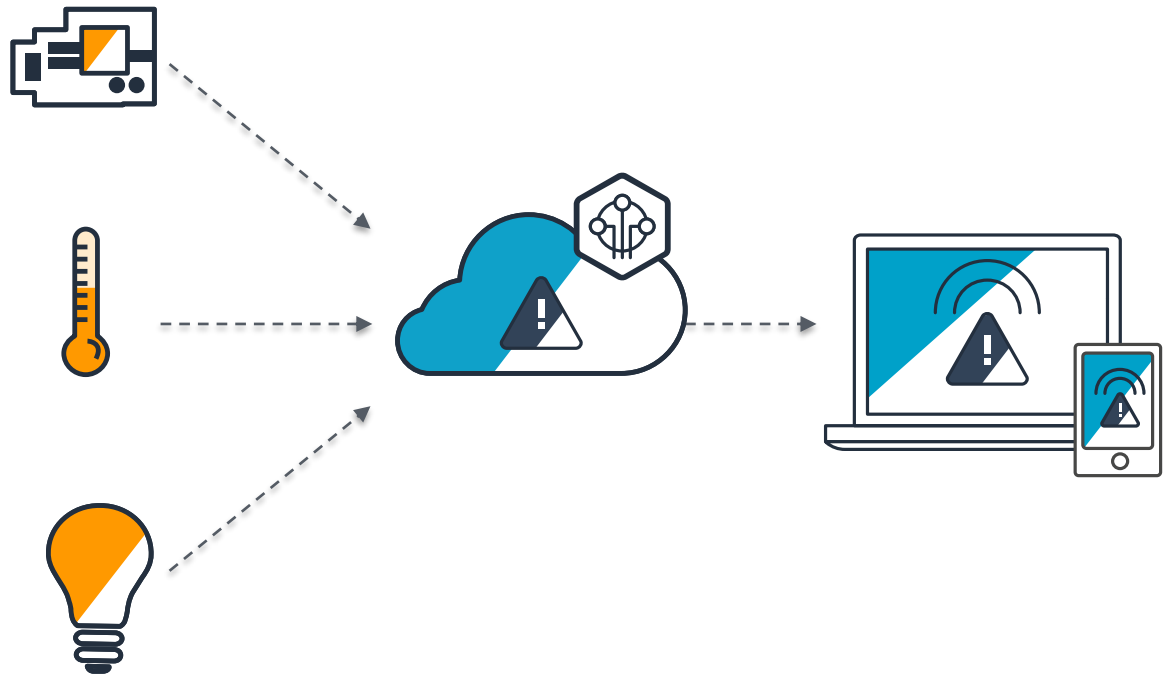
Define thresholds behavior for:

- 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



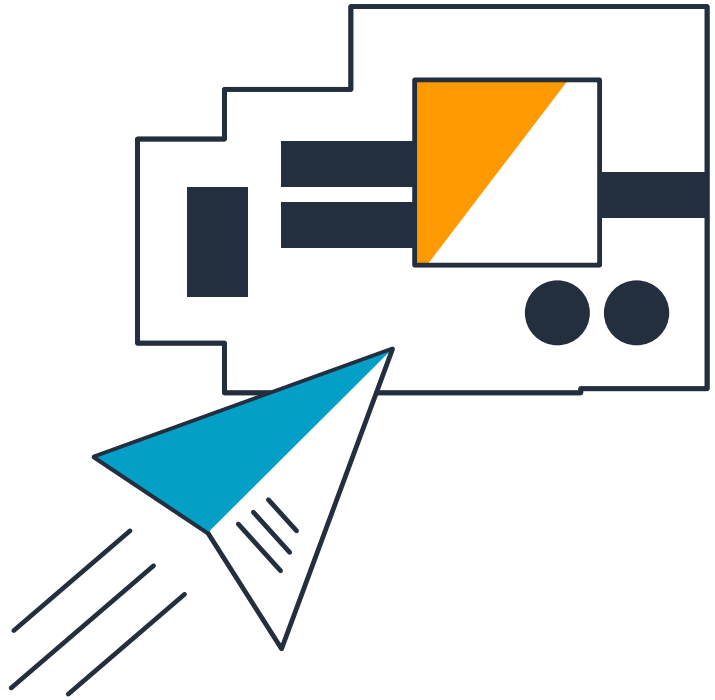
Generate Alerts

- 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

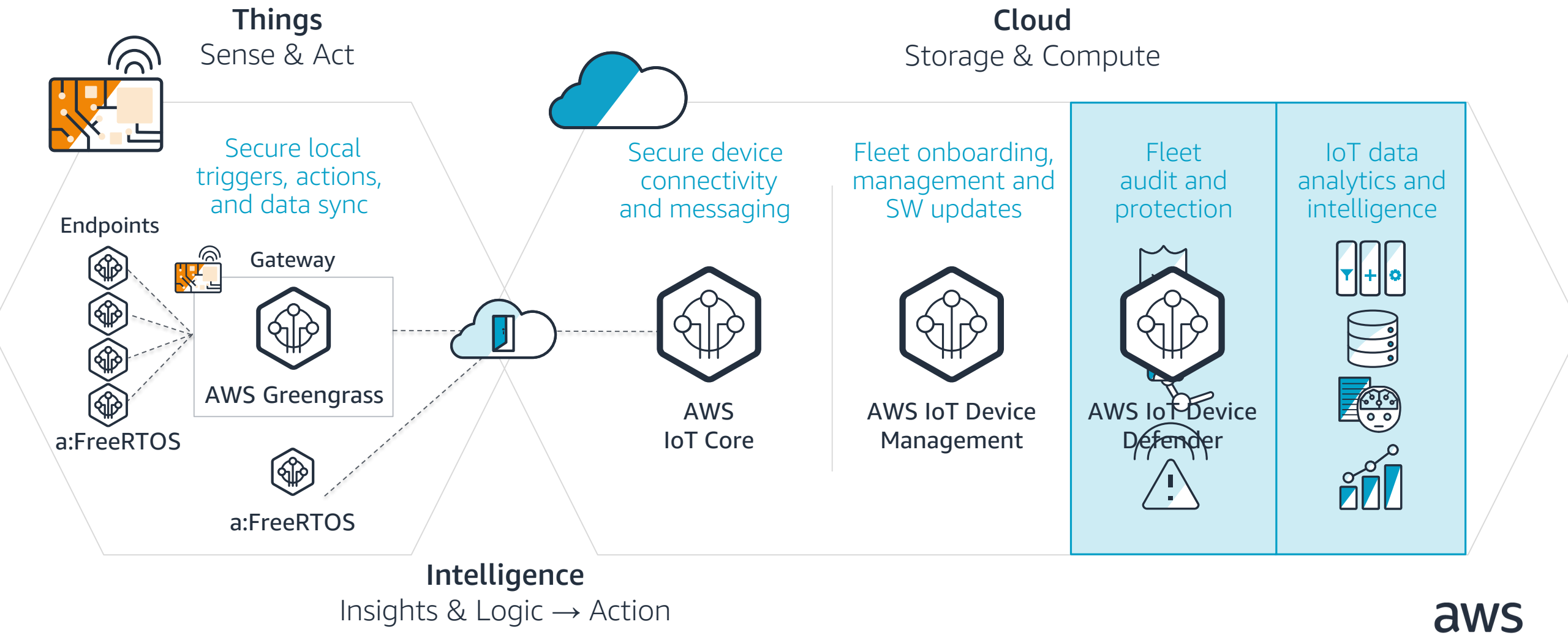


Patch Security Vulnerabilities

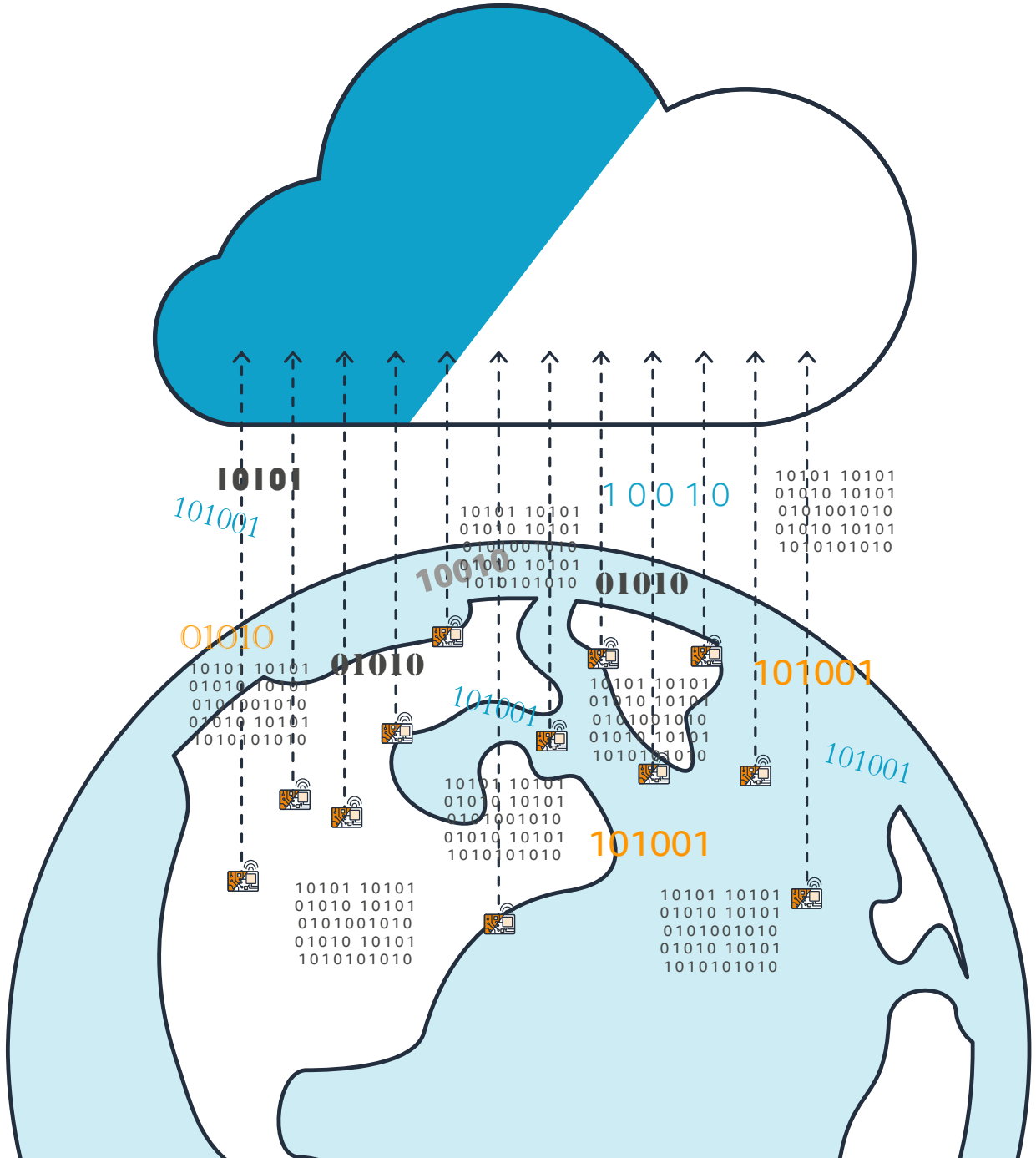
- Take actions that makes sense for your devices and use cases
- Revoke permissions
- Reboot a device
- Reset factory defaults
- Push security fixes



AWS IoT Architecture



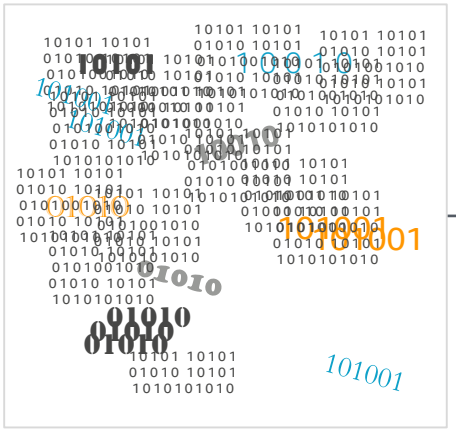
How do I generate value from my device data?



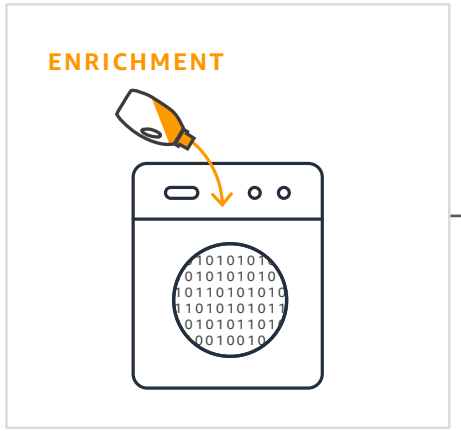
AWS IoT Analytics

Analytics for IoT Devices

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



IoT data is noisy and contains gaps and false readings



Filter, process, transform, and enrich your data

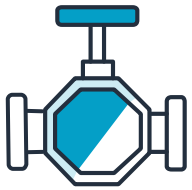
Store raw data and processed data

Ad-hoc queries or sophisticated IoT analytics and visualization

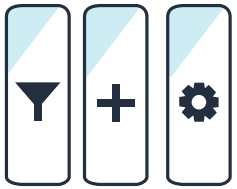
AWS IoT Analytics

Easily analyze IoT data

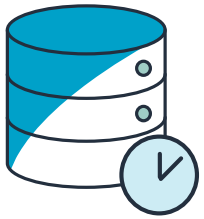
AWS IoT Analytics is a service that processes, enriches, stores, analyzes, and visualizes IoT data for manufacturers and enterprises



Channels



Pipelines



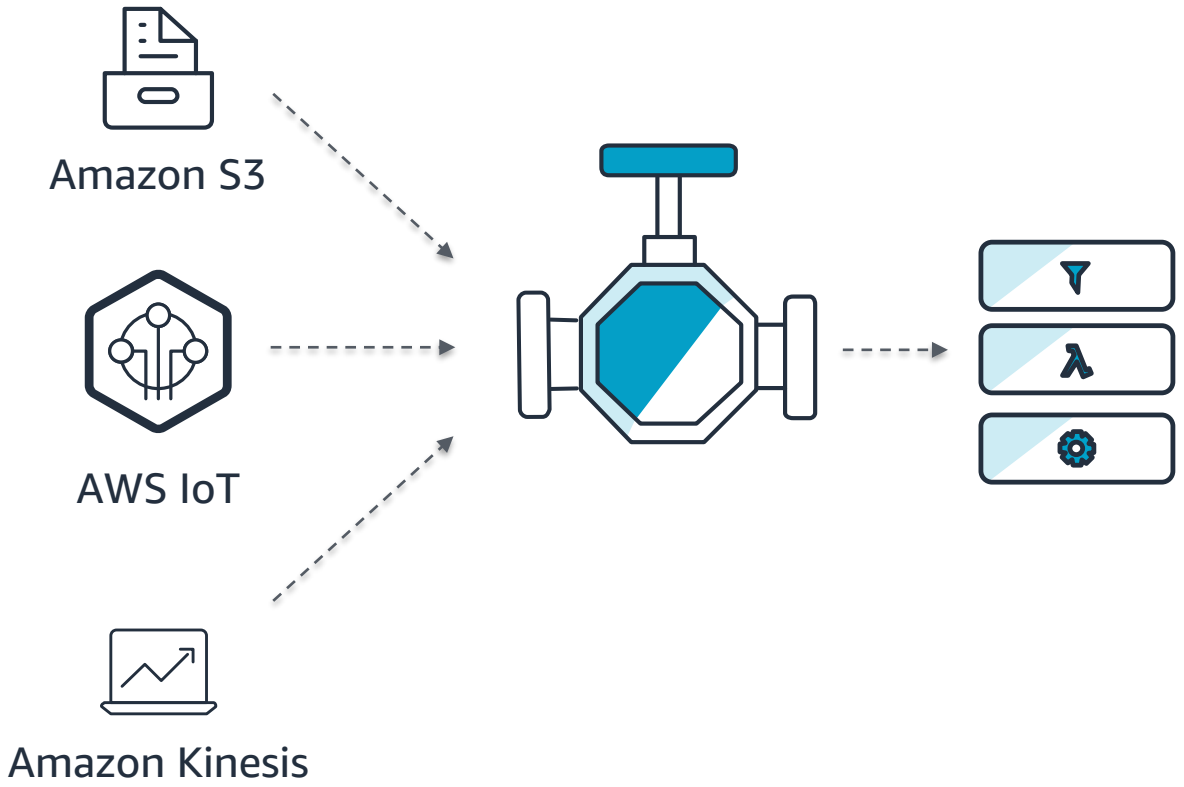
Data Stores

Datasets

Jupyter Notebooks & Templates

Channels

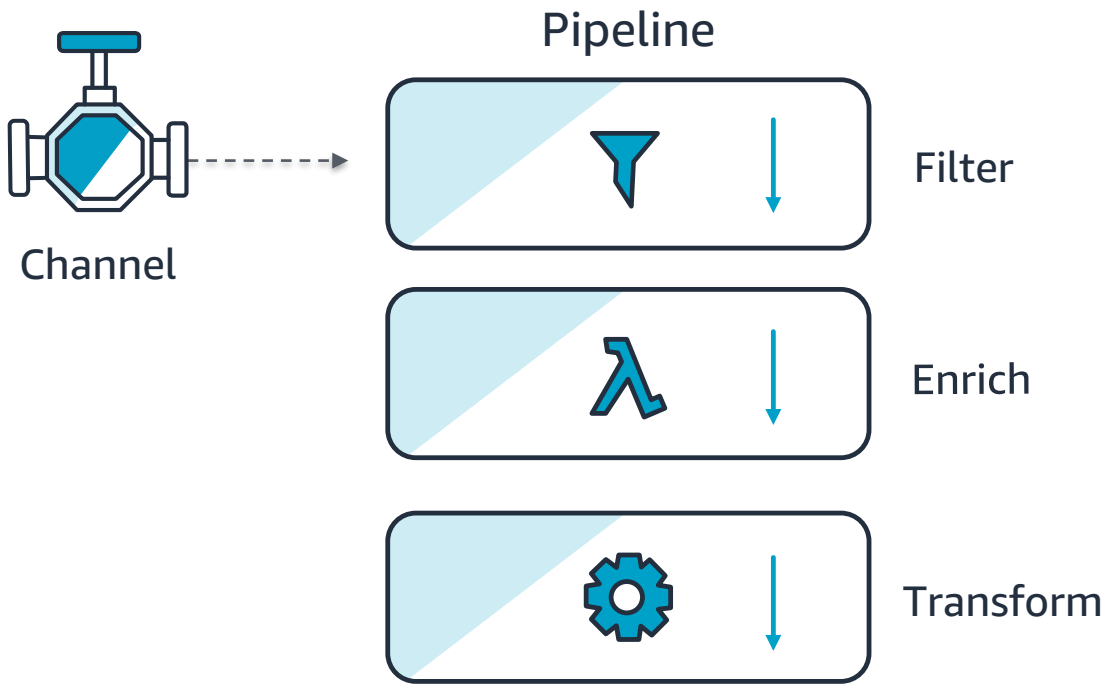
- Entry point to AWS IoT Analytics
- IoT Data Collection from Multiple Sources: IoT Core, Amazon Kinesis, S3, or custom source through APIs
- Data format agnostic
  Binary, JSON
- Elastically scalable



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

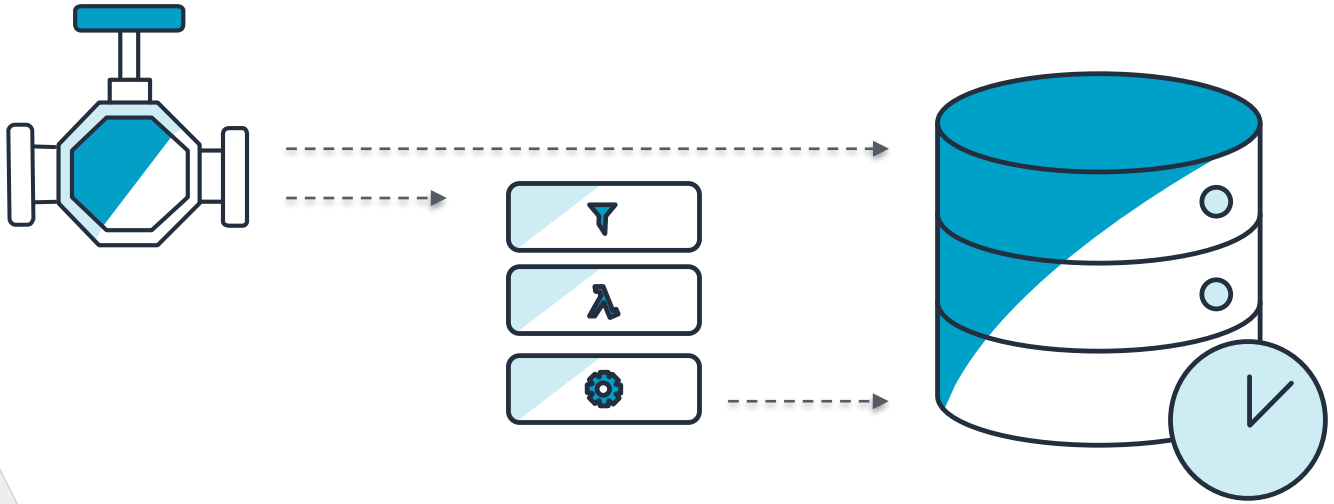
Raw and Processed Data Storage

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

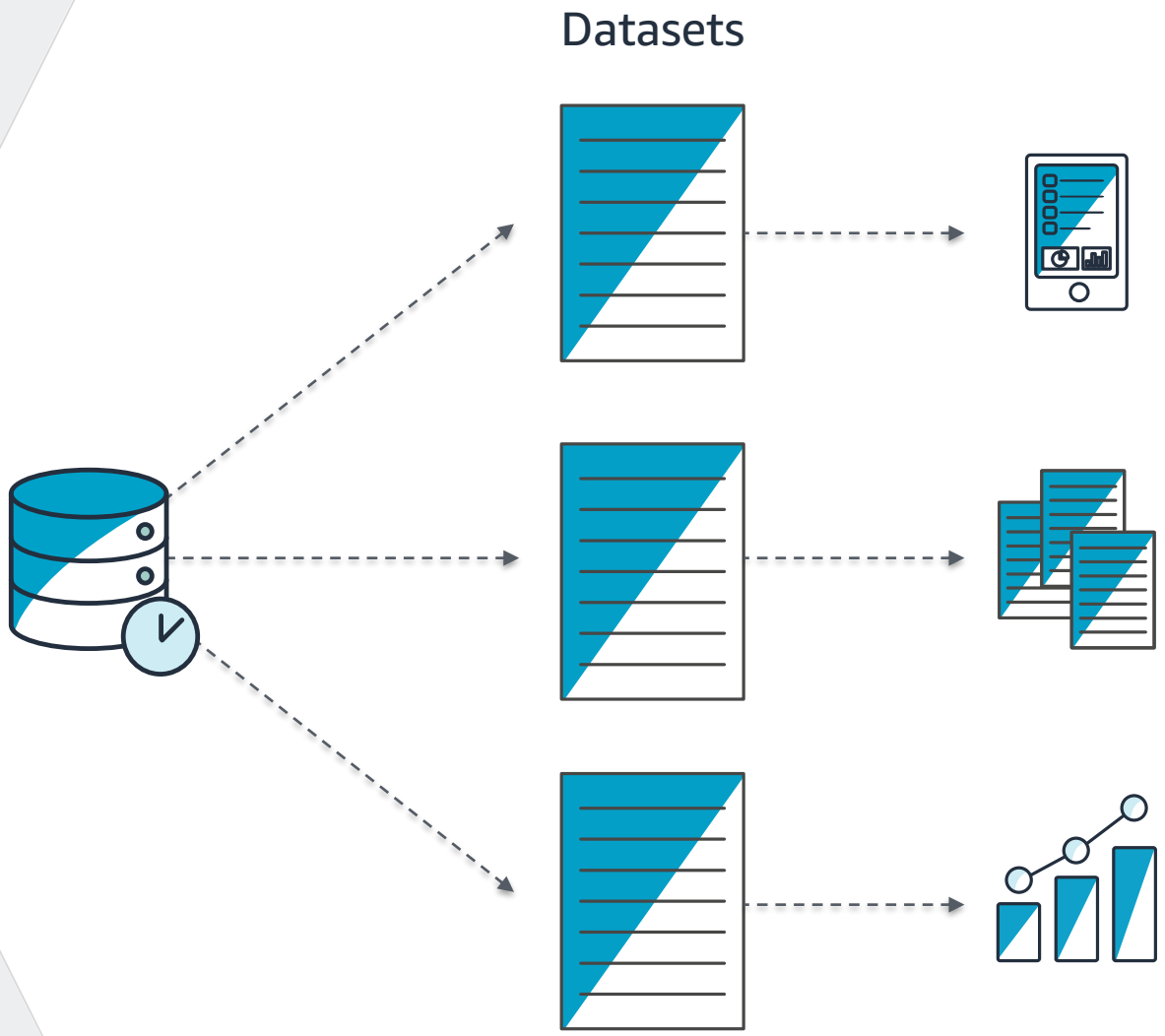
- Partitioned by time
  Supports faster query response on time series data
- More than a single database
  Abstraction on top of several database technologies in a single interface
- Manageable data retention policies



Datasets

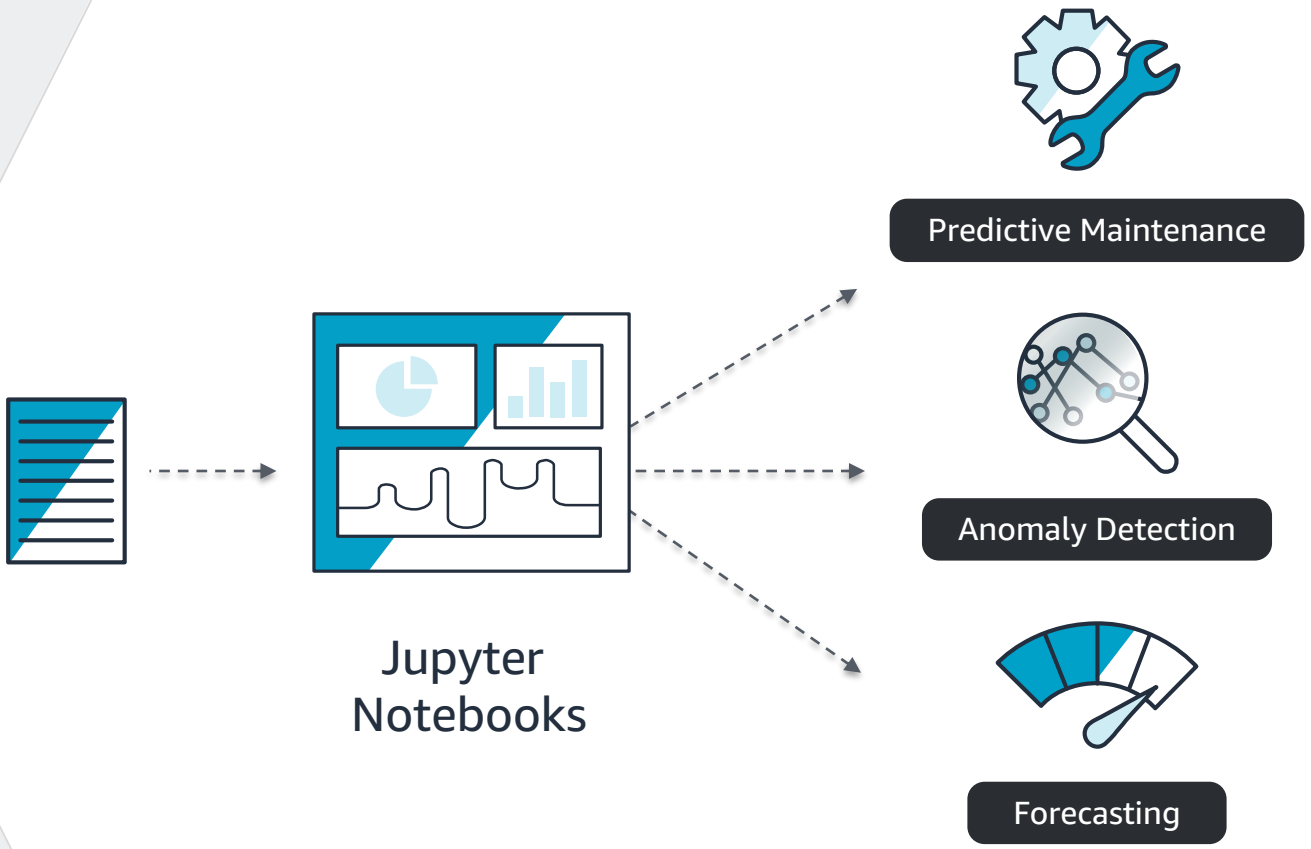
Queries on Data Store

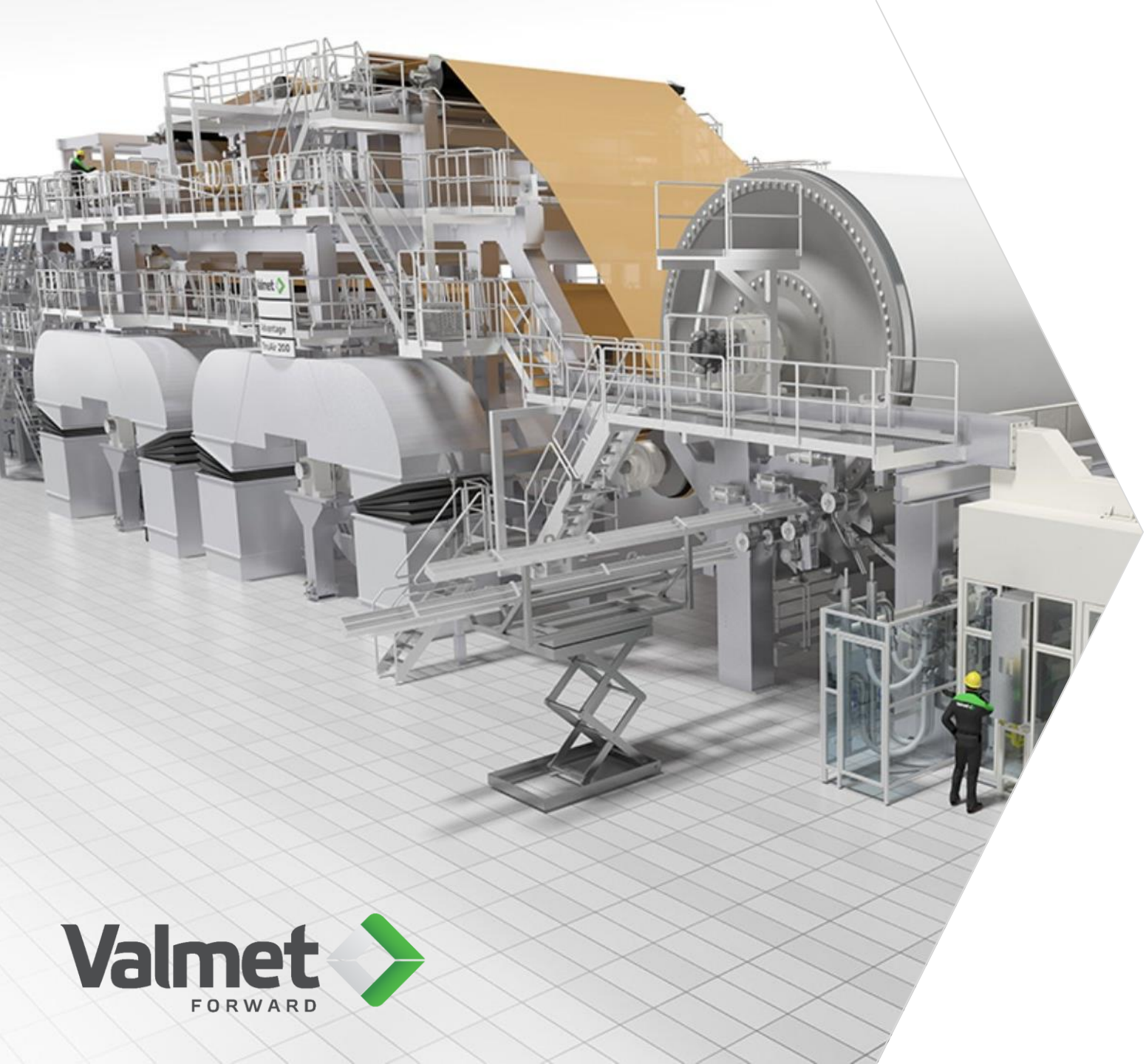
- Query IoT Analytics Data Stores using standard SQL
- Queries can be run ad hoc, or scheduled
- Popular tabular format
- Visualize in QuickSight dashboards
  Native QuickSight Connector to easily build metrics or inspect datasets
- Available via API, console download, or within Jupyter Notebooks
- Console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





Valmet FORWARD

Problem

Valmet produces complex equipment with multiple dependent processes running in parallel. Valmet customers need visibility into the state of these processes to control quality and avoid downtime.

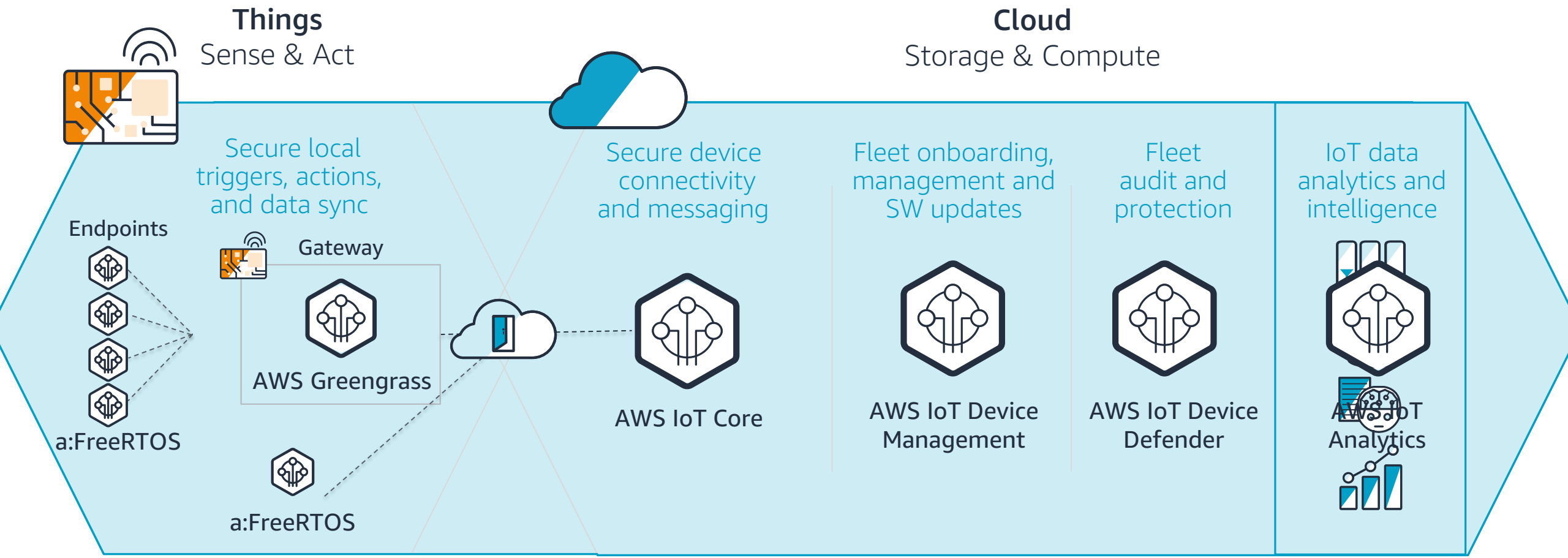
Solution

Valmet is building a new digital twin capability to allow paper mill operators to view equipment and process data during production runs. AWS IoT Analytics is at the core of this solution training ML models for paper quality forecasting and scheduling metrics generation for digital twin view-generation.

Impact

AWS IoT Analytics allows Valmet to combine historical models of equipment performance with live data from current operations to glean insights that help them learn how to make their paper better and stronger.

AWS IoT Architecture



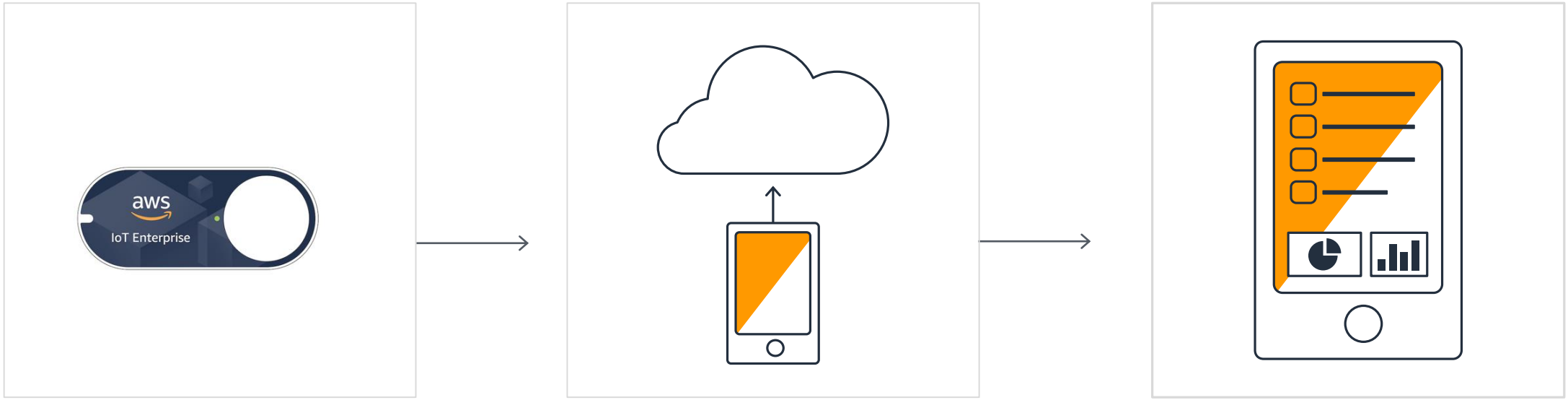
Intelligence
Insights & Logic → Action

Can you start working with IoT even faster?

AWS IoT 1-Click

Easily Trigger Actions in the Cloud

AWS IoT 1-Click makes it easy for simple devices to trigger actions such as Lambda functions with one click



Acquire device

Configure & deploy

Extract reports

AWS IoT 1-Click

Easily Trigger Actions in the Cloud

Ready to Use Devices Out-of-the-Box

Securely Connect to the Cloud

Associate Devices to Lambda Functions with One Click

Fleet Identification and Reporting

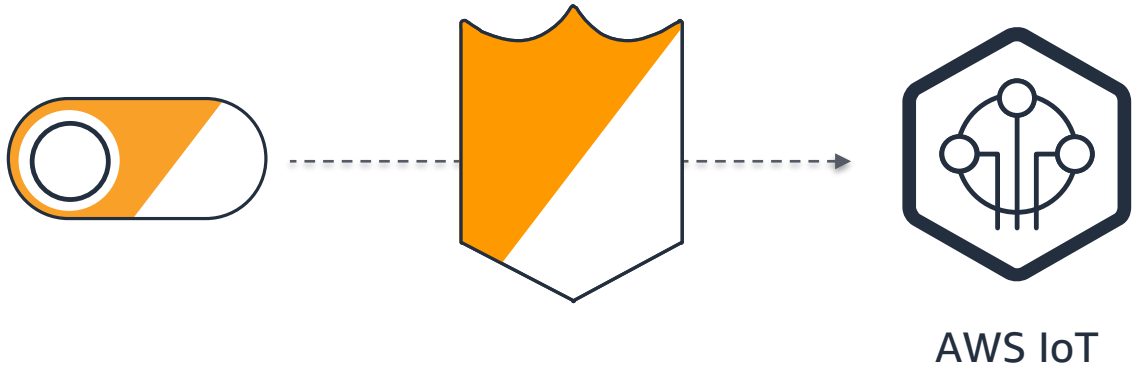
Mobile Application

Ready to Use Devices Out-of-the-Box

- AWS IoT 1-Click devices are ready to be deployed right away
- Devices supported during preview:
  - AWS IoT Enterprise Button
  - AT&T LTE-M Button
- Future support for different device types including asset trackers, sensors, card readers, etc.
- Easy claim-process for AWS IoT Enterprise Button for immediate use
- AT&T LTE-M button appears on your AWS account immediately after log-in

Securely Connect to the Cloud

- Secure connectivity to AWS IoT right Out-of-the-Box
- All AWS IoT 1-Click devices are pre-provisioned with security credentials at the time of manufacture
- This will ensure that the devices can connect securely to AWS IoT once acquired
- The certificates are locked and cannot be replaced

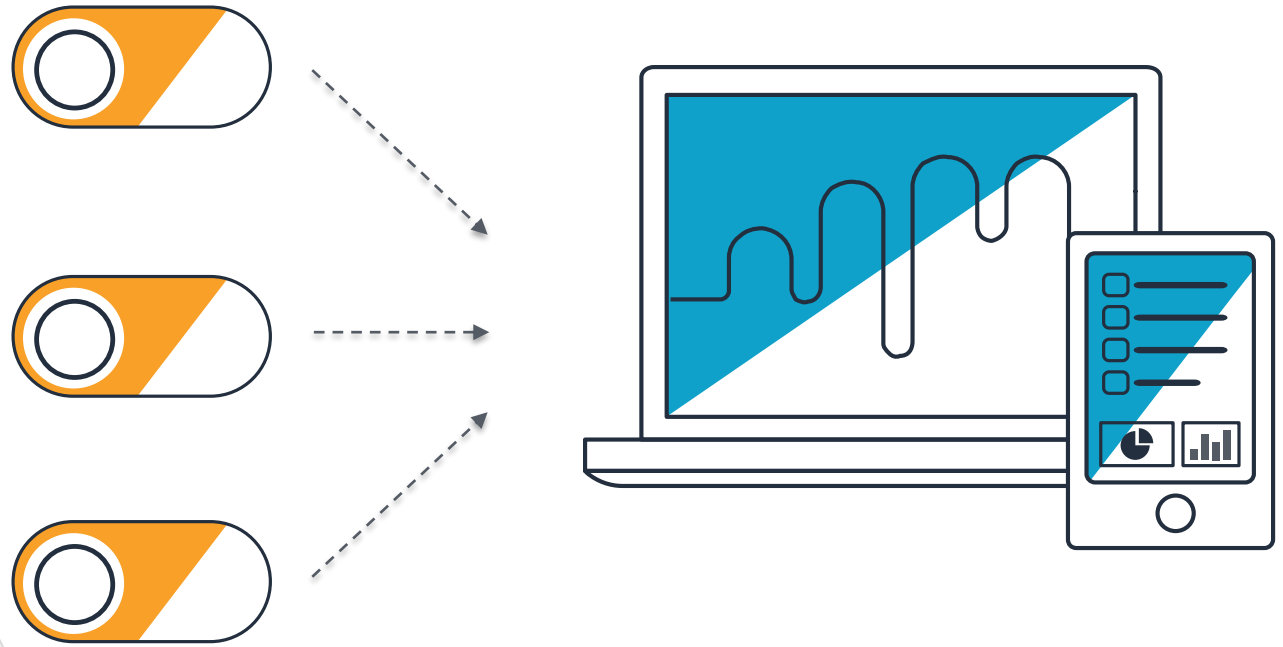


Associate devices to Lambda functions

- Associate devices to Lambda functions for dedicated actions
- Choose from ready-made templates such as email and SMS
- Associate custom lambda functions from your AWS account to devices, all with a single click

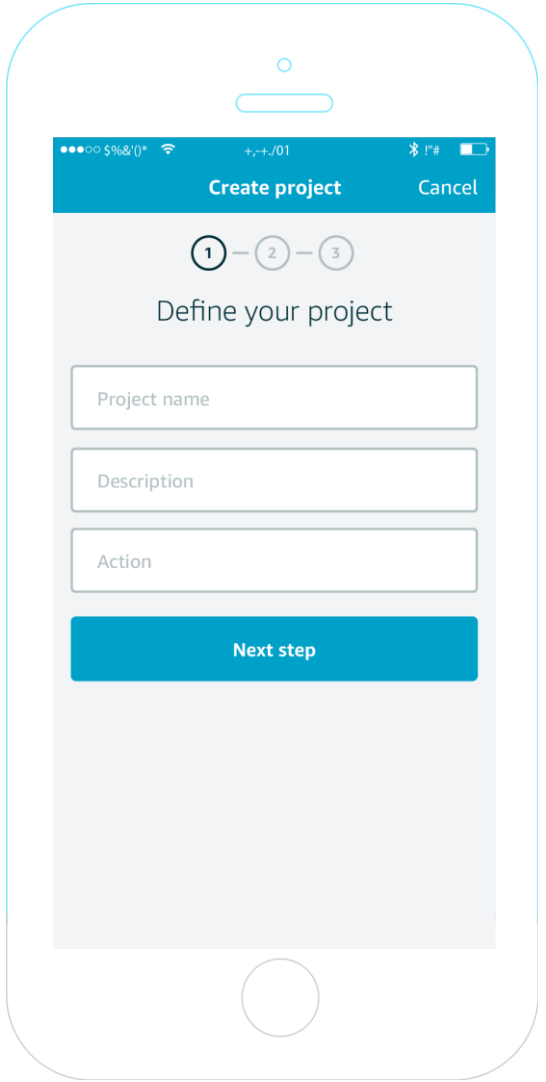
Fleet Identification & Reporting

- Add contextual data to devices to identify fleets of devices for easy identification
- Ability to add custom attributes such as location, user ID, department ID etc., for project wide tracking and usage
- Generate reports to determine usage and status
- Preconfigured and customized reports



Mobile Applications

- All features of AWS IoT 1-Click are available through the 1-Click mobile app for “anytime anywhere” use
- Mobile app available on Android and iOS platforms
- 1-Click service access through both mobile app and AWS management console at GA



Search for …

AWS IoT 1-Click

on

Download on iTunes

GET IT ON Google play

AWS IoT Services Suite

Things

Sense & Act

Secure local triggers, actions, and data sync

Endpoints

Amazon FreeRTOS

Gateway

AWS Greengrass

Cloud

Storage & Compute & Learn

Secure device connectivity and messaging

AWS IoT Core

Fleet onboarding, management and SW updates

AWS IoT Device Management

Fleet audit and protection

AWS IoT Device Defender

IoT data analytics and intelligence

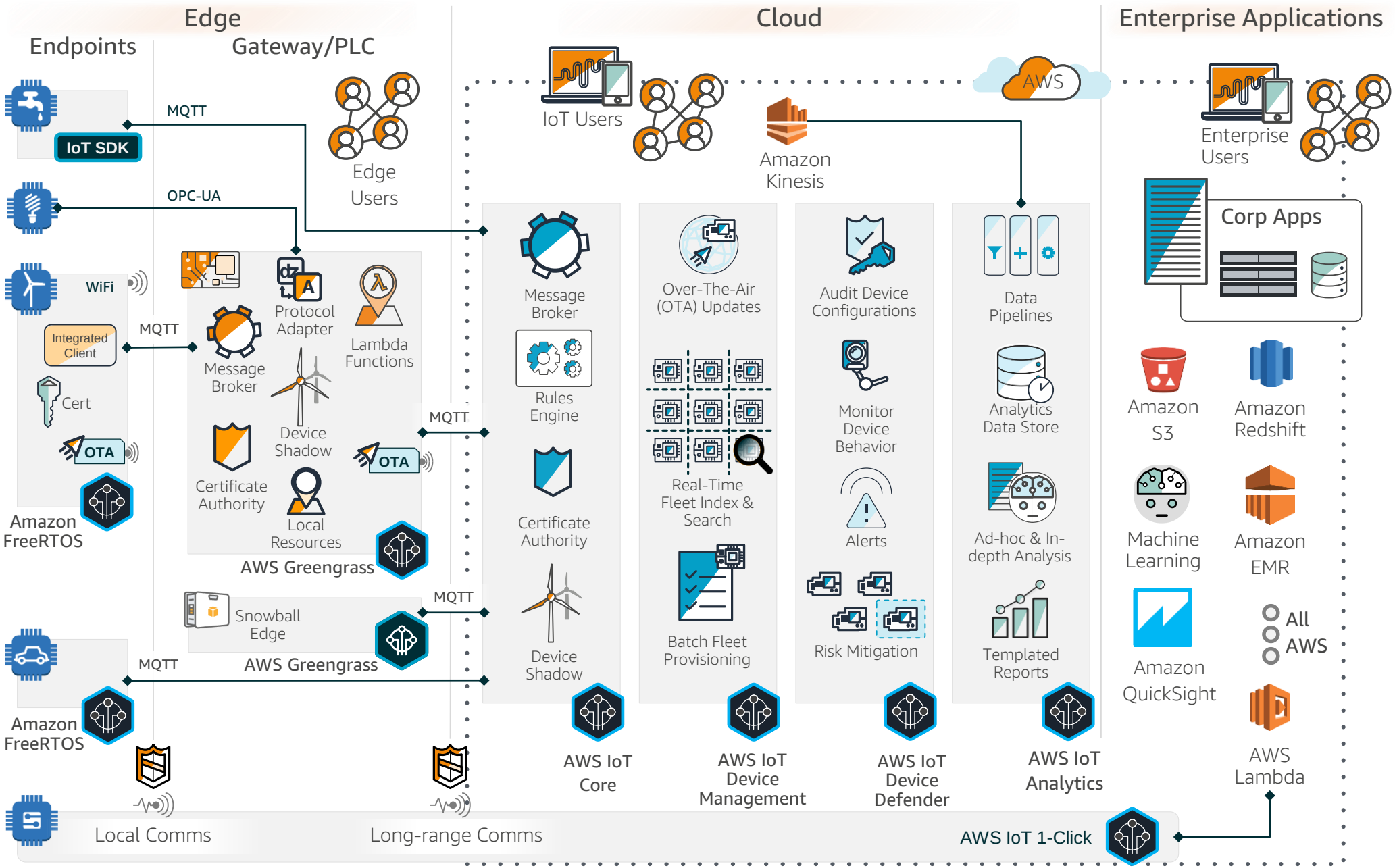
AWS IoT Analytics

AWS IoT 1-Click

Intelligence

Insights & Logic → Action

IoT with AWS



IoT Partners

Consulting / SI

Accenture, Aricent, Clearscale, CTP, Luxoft, Mobiquity, Solstice, Storm Reply, Sturdy Networks, TCS, Trek10, …

ISV (Platform)

Ayala, Bright Wolf, BSquare, C3IoT, Mnubo, Salesforce, Splunk, Thinglogix, …

Connectivity

Amdocs, Asavie, AT&T, Eseye, Soracom, TATA Communications, Telus, Verizon, …

Gateway

Adlink Technology, Advantech, MachineShop, Samsung, Technicolor, …

Edge

ARM, Broadcom, Digi, Expressif, Intel, MediaTek, Microchip, NXP, ST, TI, Qualcomm, …

We Build IoT Solutions through Our Good Friends

AWS Partner Ecosystem

Now that you **can** know the state of everything and **can** reason on top of that data…

what problems will you solve?

Thank you!

@danilop

Annex

Problem

Nokia needed an industrial IoT solution so they could analyze video streams from oil operations in the field at the edge and send the data to remote centers only when anomalies are detected.

Solution

Nokia deployed Greengrass on Nokia Multi-access Edge Computing platform and combined it with Nokia private mobile network solutions. This joint solution will make it possible for the oil industry to pair real time drilling data with production data of nearby wells.

Impact

The cost of bandwidth is expensive. AWS Greengrass allows Nokia to optimize the data sent to other wells and to the cloud based on rules and alerts set up on the locally-processed data. They save valuable data and reduce costs.

Problem

As Konecranes specializes in the manufacturing and service of cranes globally, they discovered that when they needed to make updates to their machinery it meant downtime and local presence onsite.

Solution

Using Greengrass has enabled them to deploy updates using cloud models that continually get smarter over time as they sync with the local environments.

Impact

This allows them to simplify their current crane architecture and make it possible to update calculations to the cranes in a secure way even after the installation has taken place.

Problem

Stanley Black and Decker finds it unsustainable to ingest, transmit, store, query and analyze all data generated at the edge and more specifically on construction sites or rural areas with constrained network resources.

Solution

AWS Greengrass enables Stanley Black and Decker to monitor and filter data at the edge of the network enabling applications to send asset health and predict any mechanical failures before they occur. Edge-based applications built on Greengrass will help detect and compare vibrations emitted by high value tools to historical signatures that indicate everything from normal operations to imminent failure.

Impact

Instead of trying to use all the data, Stanley Black and Decker can use Greengrass as the service allows them to choose what data is valuable so they can focus on the right data. Applications include remote troubleshooting of hydraulic assets by technicians, maintenance interval tracking, fuel savings, and alerts.

Problem

Wärtsilä needed to accurately predict, when the marine engines they manufactured needed to get serviced. Understanding and predicting the service schedule is vital for Wärtsilä to increase their service and parts revenue.

Solution

Accenture worked with AWS account SAs, AoD SAs, and Salesforce SAs to architect an IoT solution using Salesforce and AWS IoT Core to collect data and build predictive models. The solution developed is scalable and extensible beyond just this use case, as Wärtsilä has 14,000 ships with 35,000 engines installed. There are great possibilities for sensor driven IoT use cases.

Impact

The entire solution should result in an increase in parts/service sales for Wärtsilä and higher customer retention.

IoT solutions require good friends

AWS IoT Competency Program

Successful IoT implementations require services and technologies not traditionally part of the enterprise's DNA

IoT Competency guides customers through the selection of IoT partners required to integrate AWS IoT and other related AWS services with applications and physical devices

Customers are looking for skilled partners that can provide support and strategy for every piece in the complex IoT value **chain**