How to Easily and Securely Connect Devices to AWS IoT

Mark Buster, Director, Cloud Services at Leviton
Olawale Oladehin, Sr. Solutions Architect, AWS IoT

April 2018

What You’ll Learn Today

AWS IoT Core, Device Management, and Device Defender

Use Cases and Solutions

Leviton Use Case

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

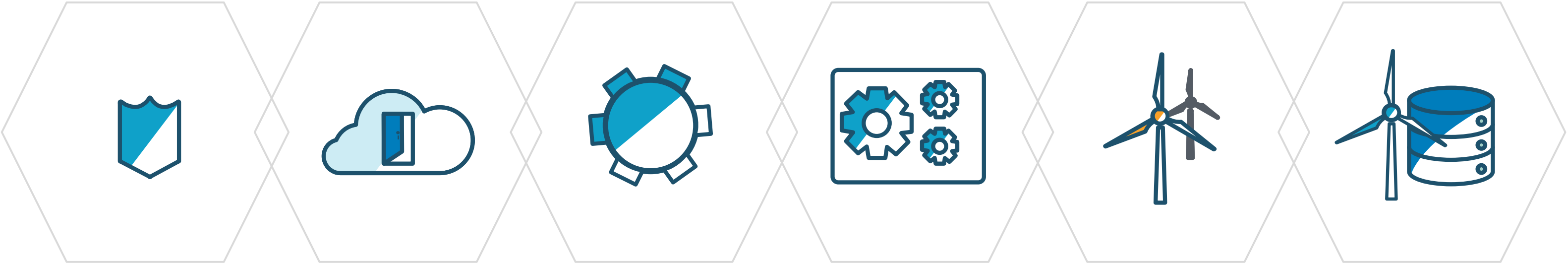
IoT payment &
connected commerce

Safeguard manufacturing
facilities

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.



Identity Service

Device Gateway

Message Broker

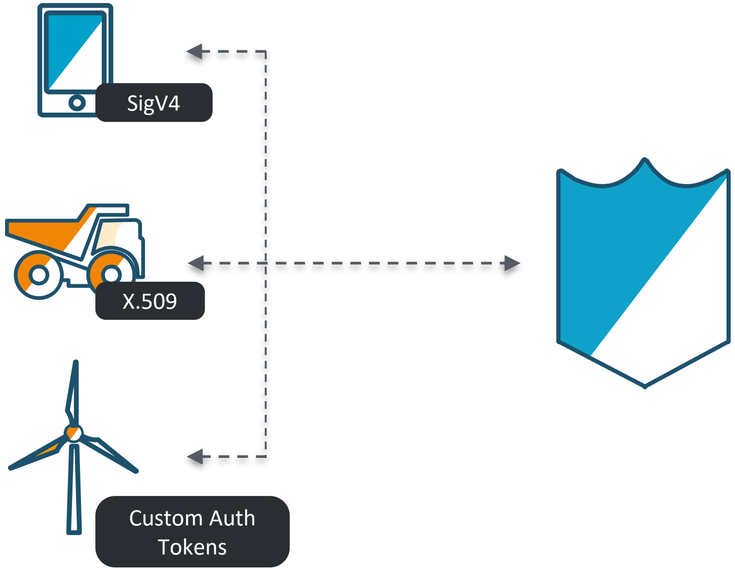
Rules Engine

Device Shadow

Registry

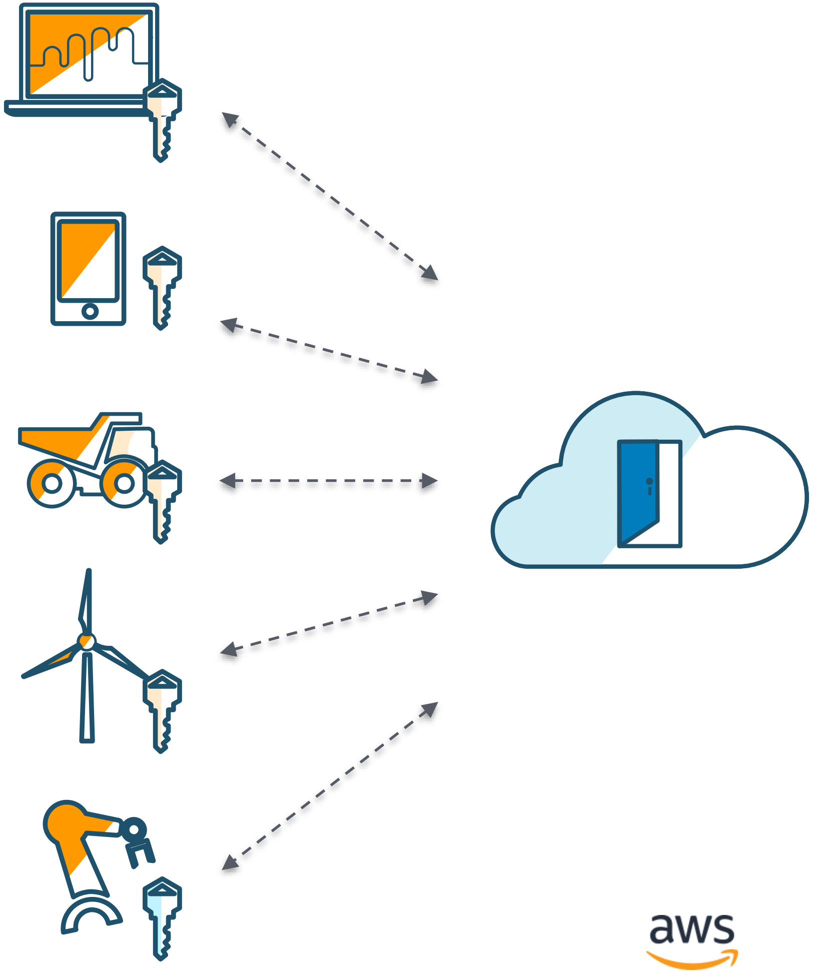
Identity Service

- 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

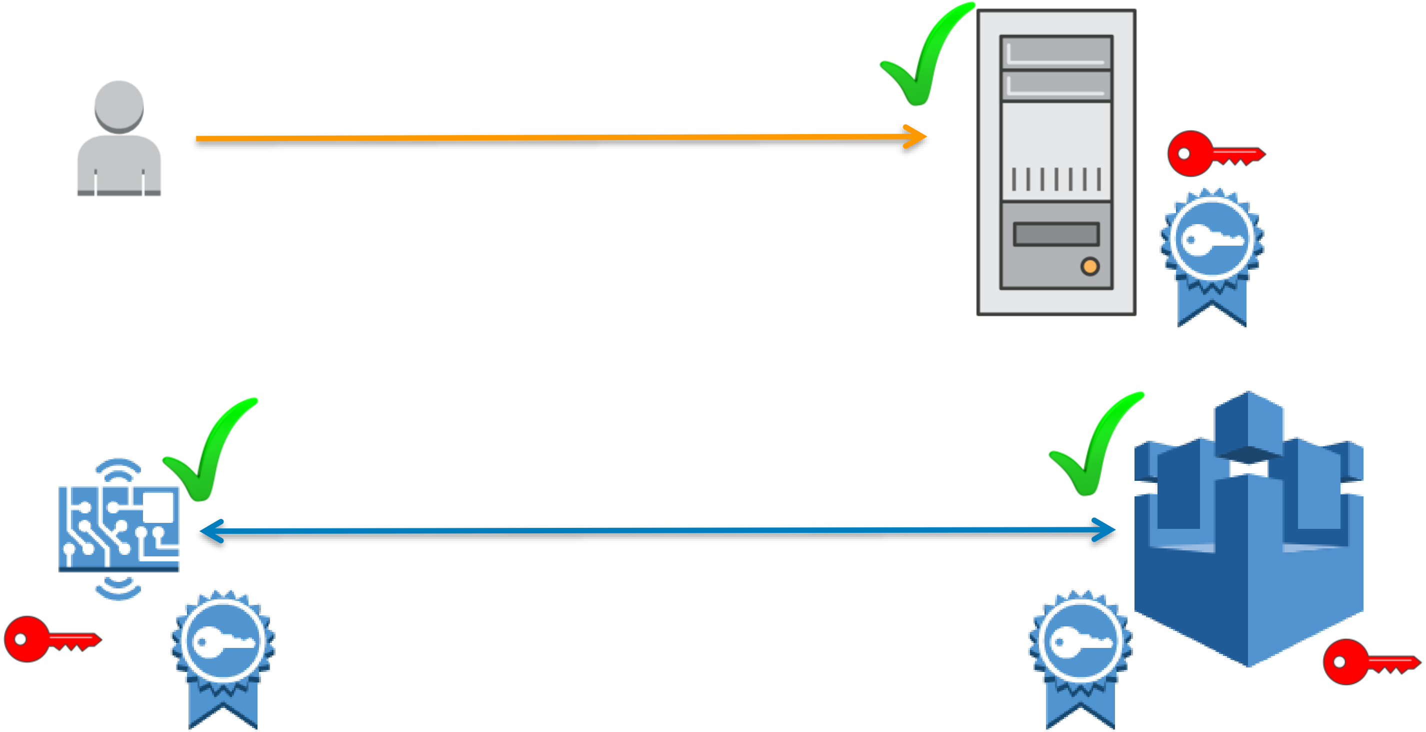


Device Gateway

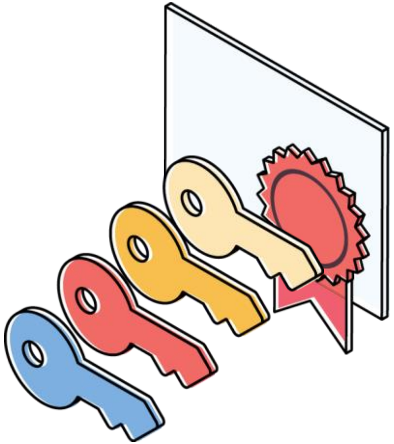
- Entry point into the cloud for IoT devices
- Long-lived connections for bidirectional communication
- Support for multiple protocols including MQTT, WebSockets, HTTP
- Supports SigV4, X.509 and token based authentication (via Custom Authorizors)
- Secure communications over TLS 1.2
    - Support for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



AWS IoT: Secure Communication over TLS



Certificates and keys



- Private **key** (authenticate the device)
- **Certificate** (register the device with IoT)
- Root **certificate authority** (authenticate IoT)

AWS IoT Permissions

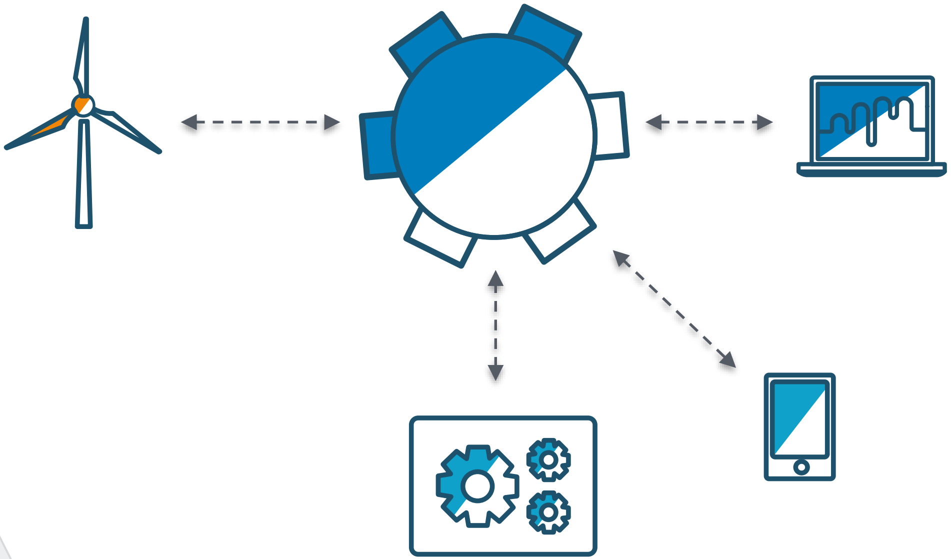
- Control what a thing is **allowed** to do
  - Connect, publish, subscribe, receive
- Attach **policy** to **certificates**

AWS IoT Policies

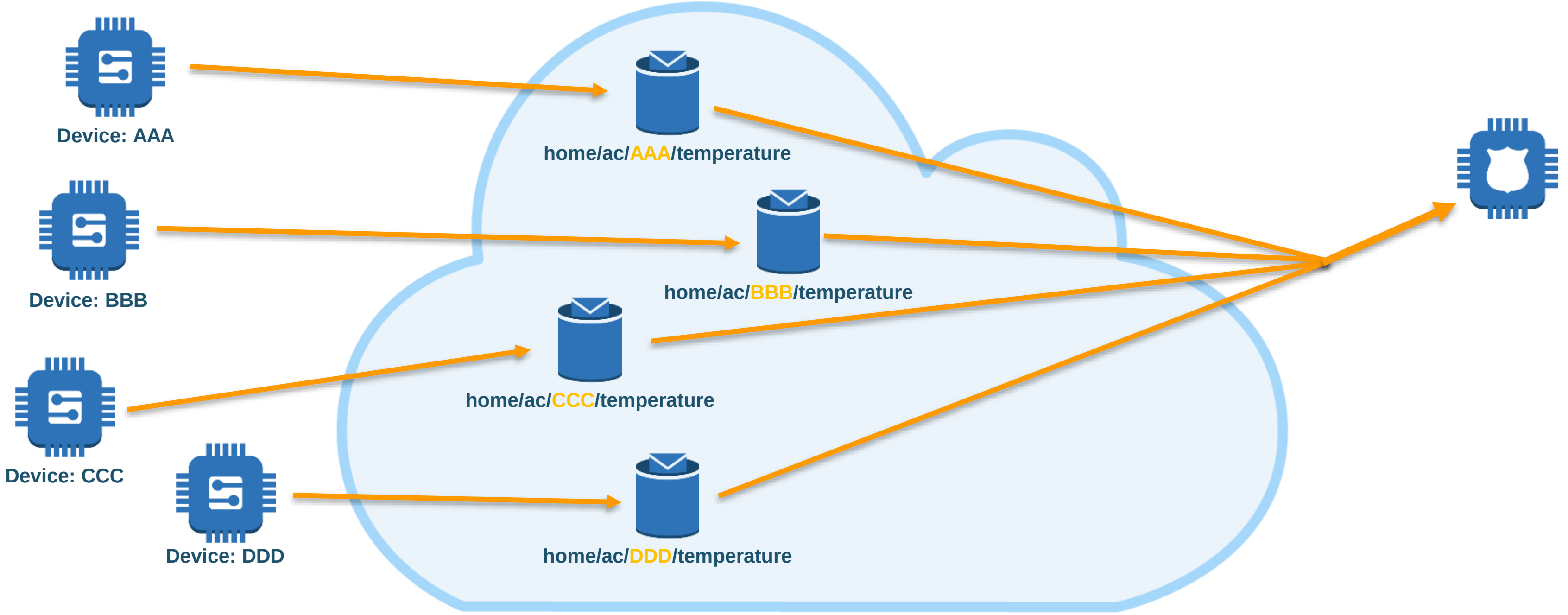
```
{
  "Effect": "Allow",
  "Action": "iot:Publish",
  "Resource": [
     "arn:*:topic/private-topic/${iot:ClientId}",
     "arn:*:topic/open-topic-space/*"
  ]
},
{
  "Effect": "Allow",
  "Action": "iot:Subscribe",
  "Resource": "arn:*:topicfilter/private-topic/${iot:ClientId}/*"
}
```

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



Publishing and Subscribing with MQTT Topics

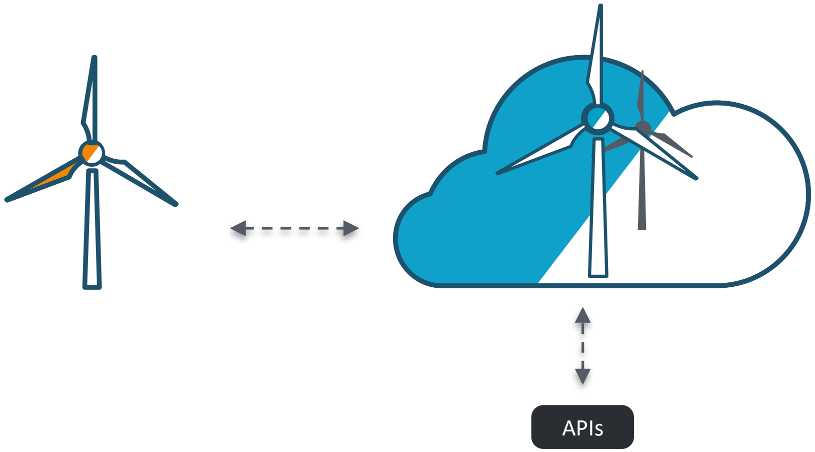


PUB: home/ac/${clientId}/temperature

SUB: home/ac/+/temperature

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
- REST APIs for applications to discover and interact with devices
- Device SDK integration for easy integration with devices



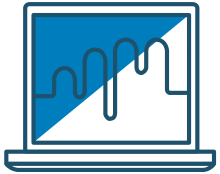
AWS IoT Core Device Shadow

Device

Report its current state to one or multiple shadows
Retrieve its desired state from shadow

Shadow

Shadow reports delta, desired and reported states along with metadata and version



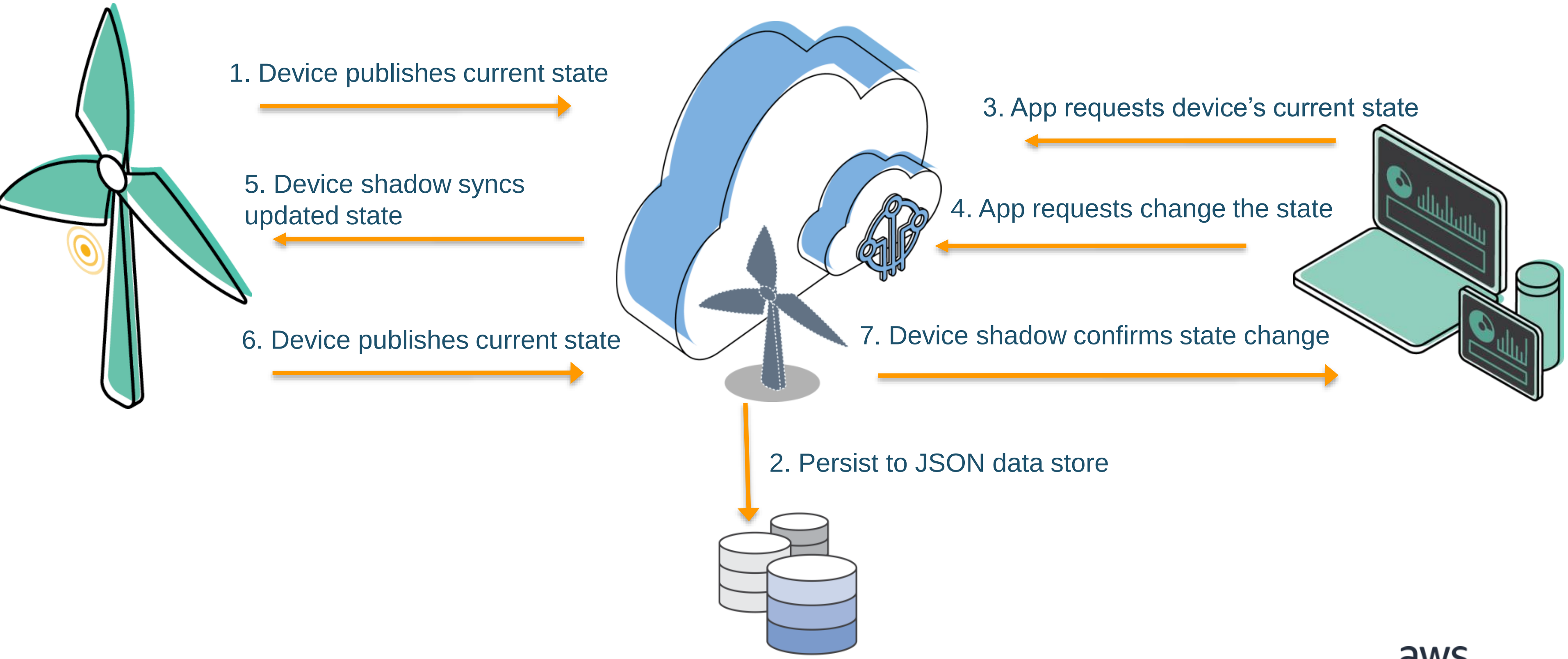
Application

Set the desired state of a device
Get the last reported state of the device
Delete the shadow

```
{
"state" : {
          "desired" : {
               "lights": { "color": "RED" },
               "engine" : "ON"
          },
          "reported" : {
               "lights" : { "color": "GREEN"  },
          "engine" : "ON"
          },
          "delta" : {
               "lights" : { "color": "RED"  }
           }
  },
  "version" : 10,
  "timestamp" : 28034023492,
  "clientToken": "UniqueClientToken"

}
```

AWS IoT Core Device Shadow Flow



1. Device publishes current state

5. Device shadow syncs updated state

6. Device publishes current state

3. App requests device’s current state

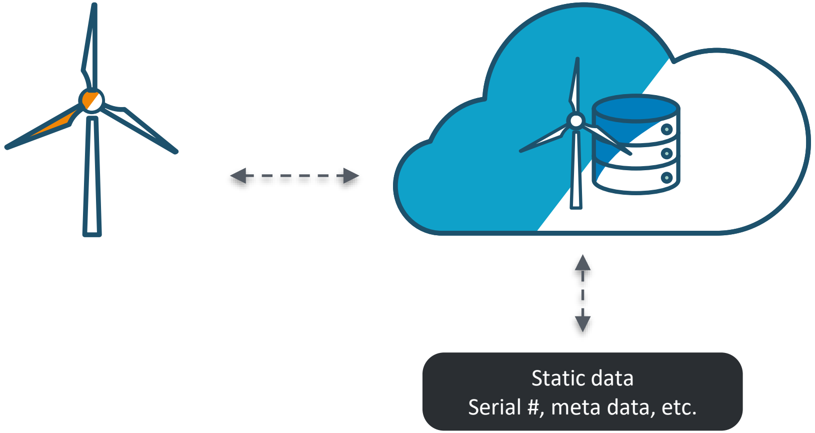
4. App requests change the state

7. Device shadow confirms state change

2. Persist to JSON data store

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

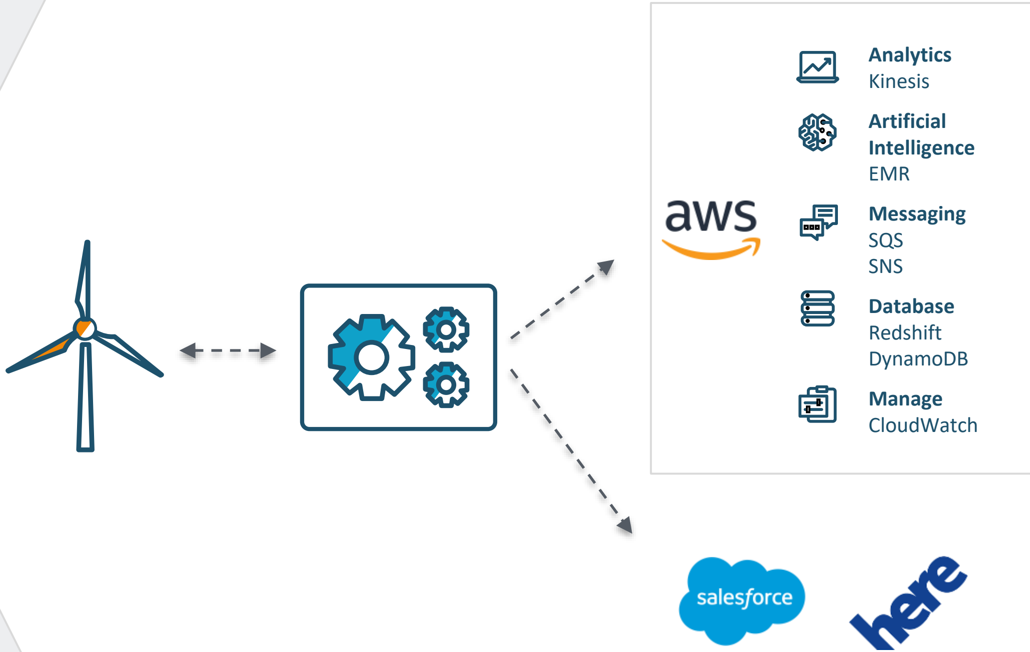


Static data
Serial #, meta data, etc.

Rules Engine

Data transformation and actions

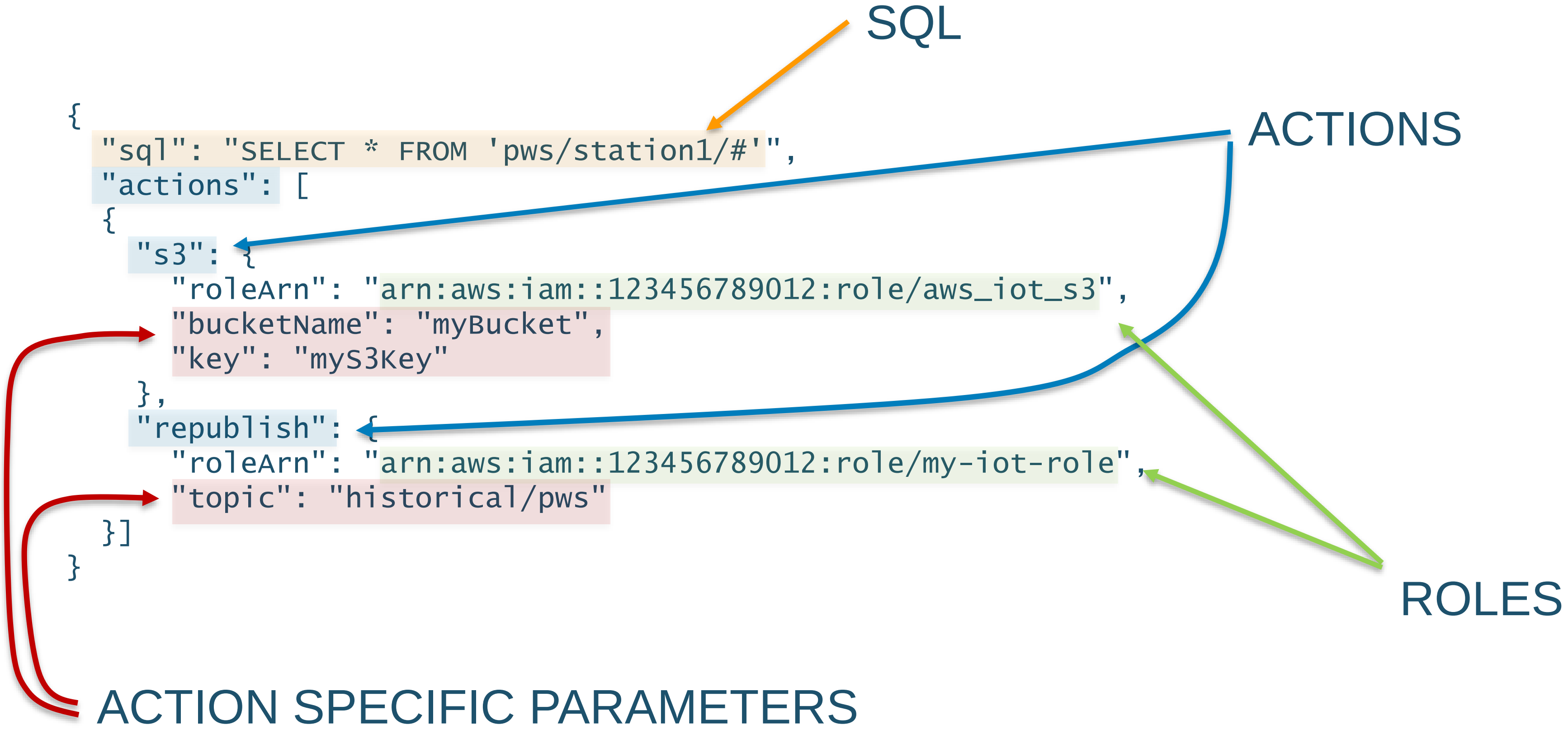
- Easy to use SQL-like language for transforming, filtering and enriching your data
- Transform—built in functions for math, string manipulation, dates, etc.
- Filter—use the WHERE clause to capture only the data you want
- Enrich—bring in context from the Device Shadow and Amazon Machine Learning or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



Breakdown of a Rule (JSON)

```
{
  "sql": "SELECT * FROM 'pws/station1/#'",
  "actions": [
  {
    "s3": {
      "roleArn": "arn:aws:iam::123456789012:role/aws_iot_s3",
      "bucketName": "myBucket",
      "key": "myS3Key"
    },
    "republish": {
      "roleArn": "arn:aws:iam::123456789012:role/my-iot-role",
      "topic": "historical/pws"
  }]
}
```

Breakdown of a Rule (JSON)



```
{
  "sql": "SELECT * FROM 'pws/station1/#'",
  "actions": [
  {
    "s3": {
      "roleArn": "arn:aws:iam::123456789012:role/aws_iot_s3",
      "bucketName": "myBucket",
      "key": "myS3Key"
    },
    "republish": {
      "roleArn": "arn:aws:iam::123456789012:role/my-iot-role",
      "topic": "historical/pws"
  }]
}
```

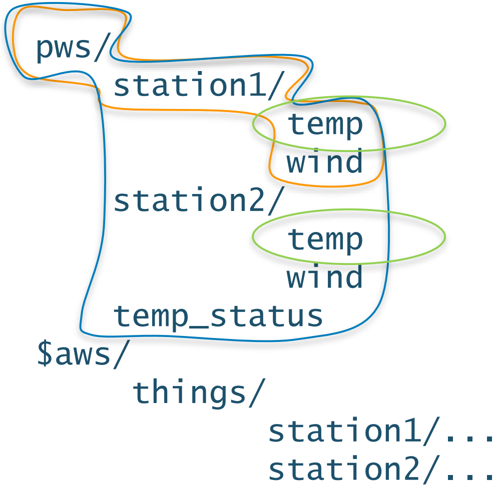
SQL

ACTIONS

ROLES

ACTION SPECIFIC PARAMETERS

Topics



```
pws/
    station1/
            temp
            wind
    station2/
            temp
            wind
    temp_status
$aws/
    things/
            station1/...
            station2/...
```

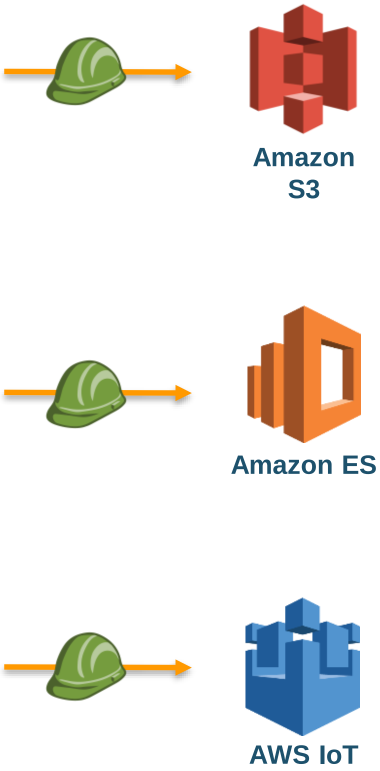
Rules

```
{
  "sql": "SELECT * FROM 'pws/station1/#'",
  "actions": [
  {
    "s3": {
      "bucketName": "myBucket",
      "key": "myS3Key"
    }
  }]
}
```

```
{
  "sql": "SELECT * FROM 'pws/#'",
  "actions": [
  {
    "elasticsearch": {
      "endpoint": "http://my-endpoint",
      "index": "my-index",
      "id": "${newuuid()}"
    }
  }]
}
```

```
{
  "sql": "SELECT * FROM 'pws/+/temp'",
  "actions": [
  {
    "republish": {
      "topic": "pws/temp_status"
    }
  }]
}
```

Actions



Leviton

Leviton at a Glance

110+ years only 4 Presidents

5 business units

7,000+ employees

2.5 million units manufactured daily

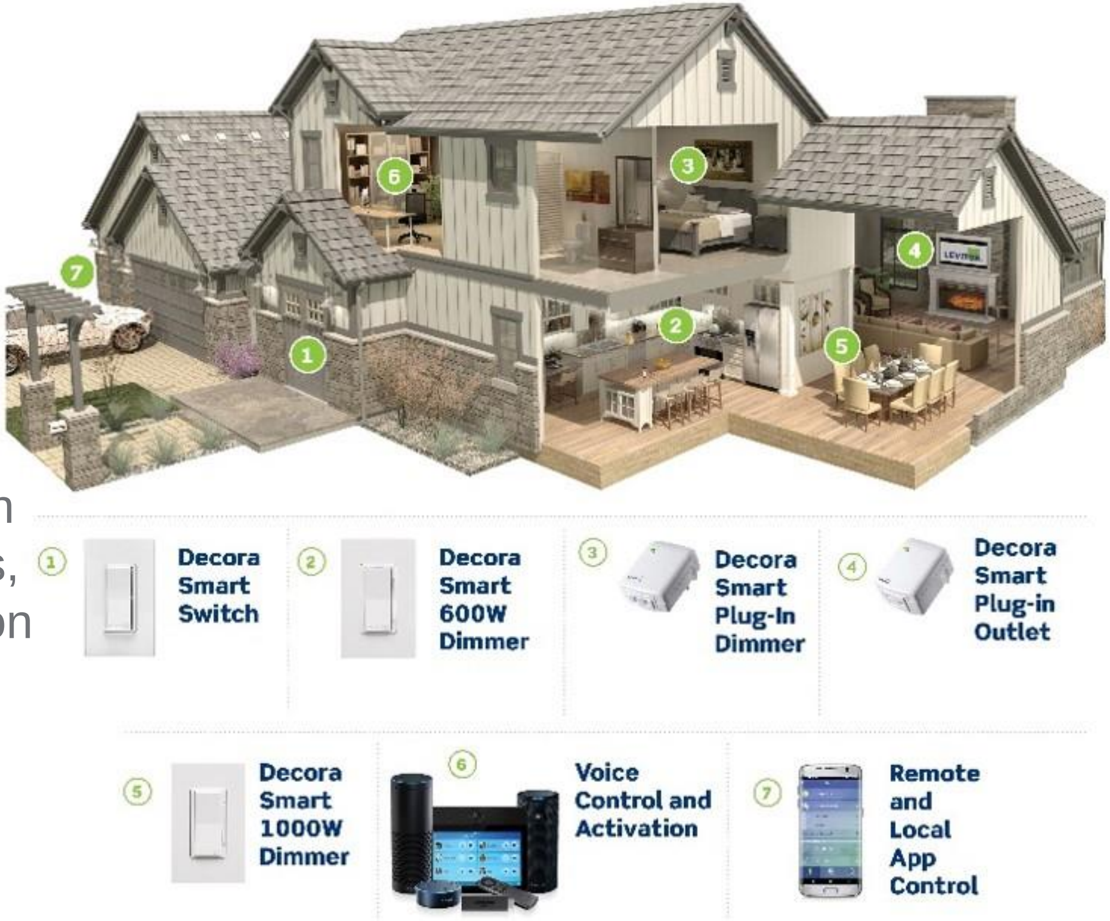
25,000+ products

65% of homes in the U.S. contain a Leviton device

Products available in **100+** countries

The Decora Smart Whole House Experience

- Dimmers & Switches
  - In-Wall and Plug-In
- The next generation of Leviton home automation – schedules, remote access, voice activation and easy-to-install familiar devices
- Multiple high-profile awards in 2018

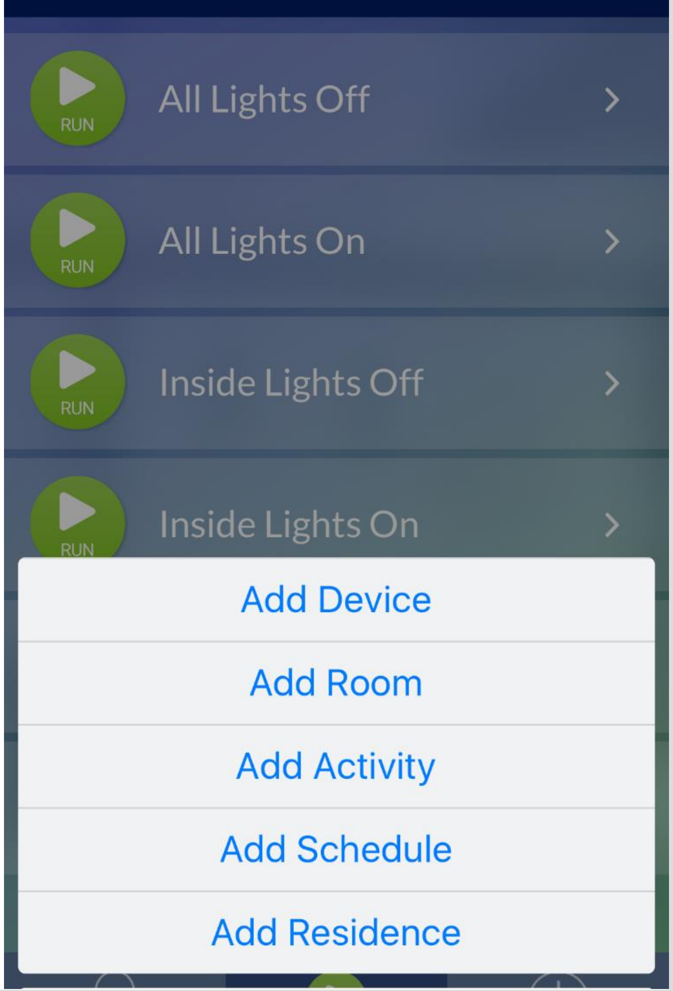

1
2
3
4
5
6
7
1 Decora Smart Switch
2 Decora Smart 600W Dimmer
3 Decora Smart Plug-In Dimmer
4 Decora Smart Plug-in Outlet
5 Decora Smart 1000W Dimmer
6 Voice Control and Activation
7 Remote and Local App Control

Decora Smart™ with Wi-Fi

- Local and remote control
  - All you need is a dimmer, Wi-Fi, internet access and iOS and/or Android mobile device
    - No on-site gateway/bridge/hub required

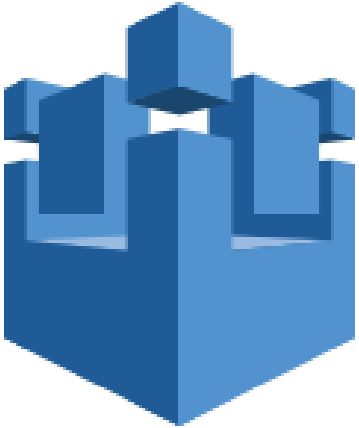
- Devices are truly smart – schedules and clocks live in each device as well as the cloud

- A platform for the future allowing apps and the cloud to join together systems in the home



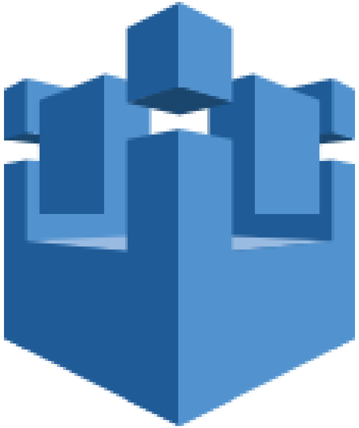
Decora Smart™ with Wi-Fi

- Why AWS IoT?



Decora Smart™ with Wi-Fi

- **Project Requirements**
    - VOICE
    - HUBLESS
    - Fast Prototyping – Small Team
    - Standards Compliance
    - Security
    - Managed Service

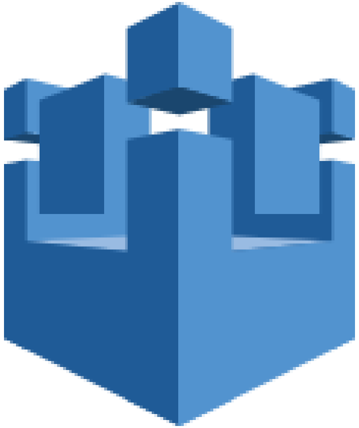


Decora Smart™ with Wi-Fi

- **When The Dust Settled**
  - AWS IoT Core
  - Already Using AWS
  - Super Fast Development
  - Tight Integration With Services

Decora Smart™ with Wi-Fi

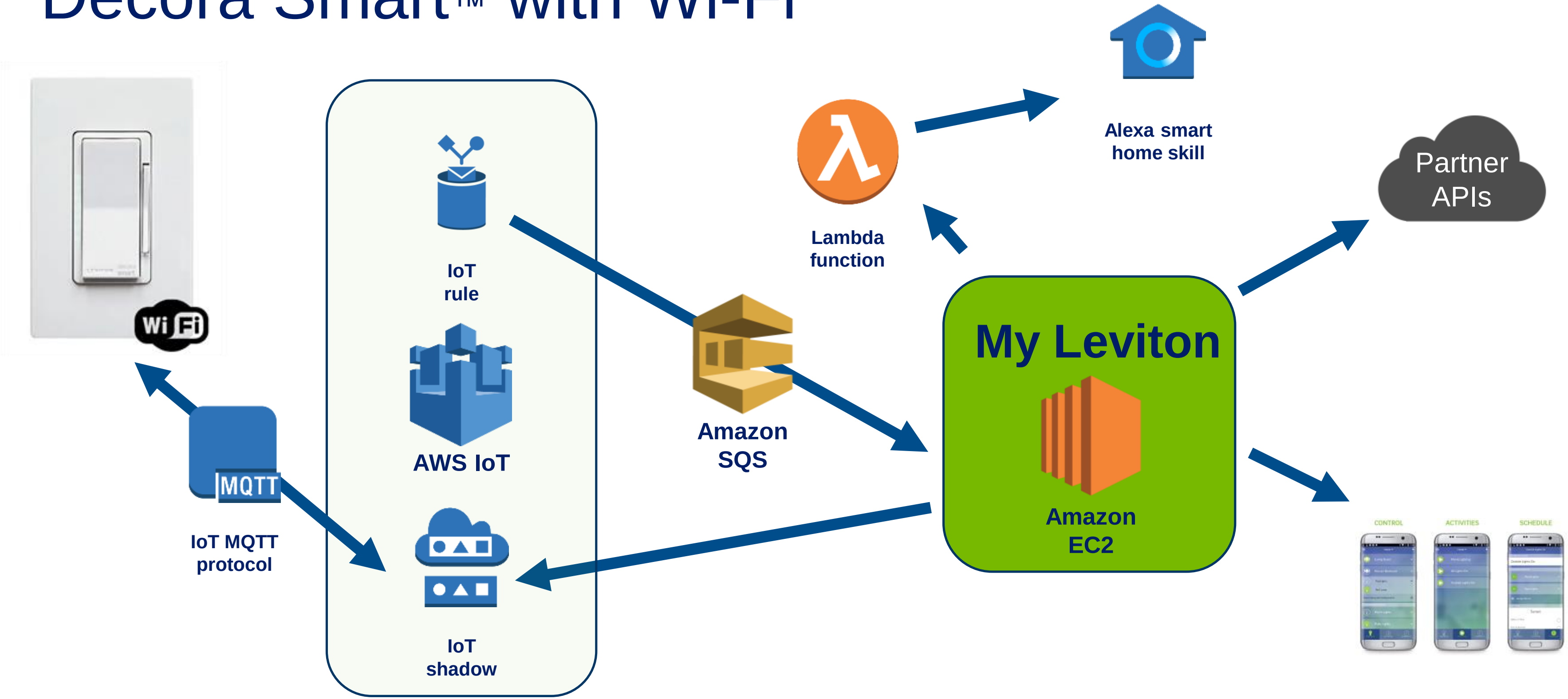
- **IoT Rules Engine**
  - Manages Communication to My Leviton services
  - Monitors and Reacts to Connectivity Changes



Decora Smart™ with Wi-Fi

- **Rules Engine Integration**
  - My Leviton Cloud Service
  - Mobile apps
  - Voice
  - Partners

Decora Smart™ with Wi-Fi



Wi Fi

IoT MQTT protocol

MQTT

IoT rule

AWS IoT

IoT shadow

Amazon SQS

Lambda function

Alexa smart home skill

Partner APIs

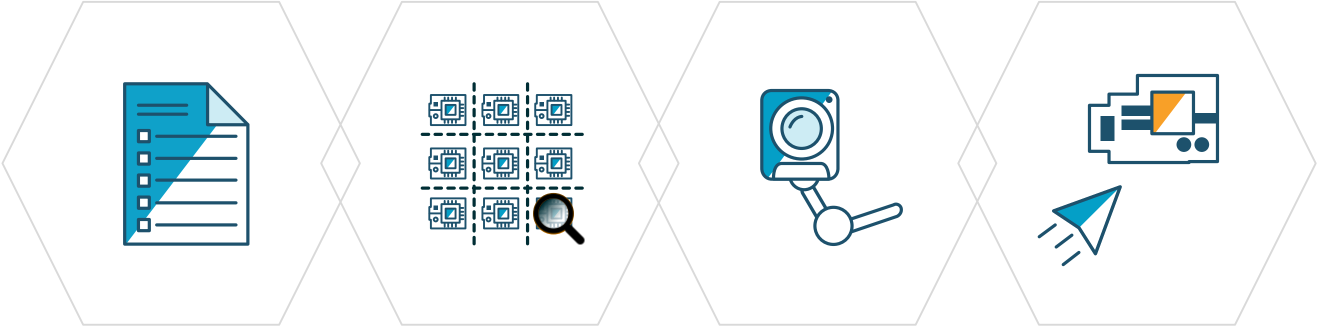
My Leviton

Amazon EC2

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.



Batch Fleet Provisioning

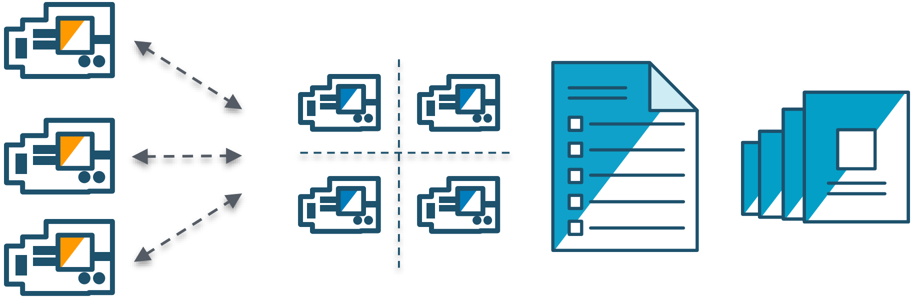
Real-time Fleet Index & Search

Fine Grained Device Logging & Monitoring

Over the Air Updates

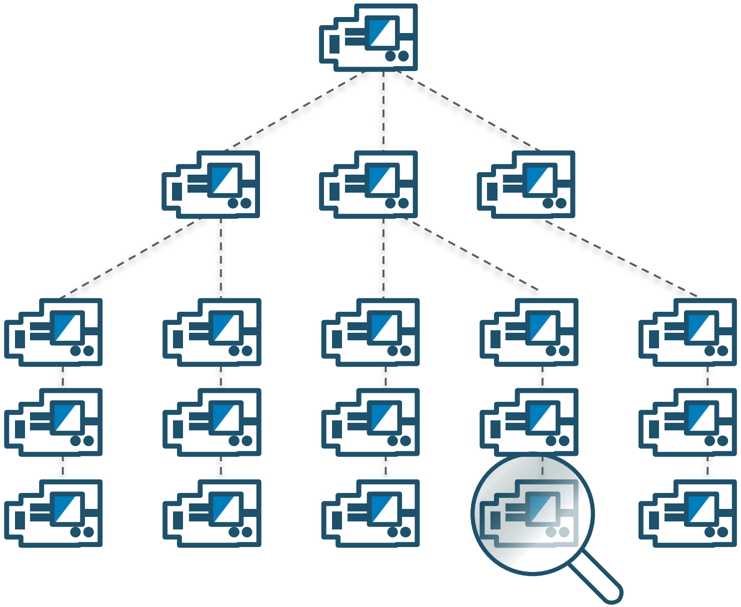
Batch Fleet Provisioning

- 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)



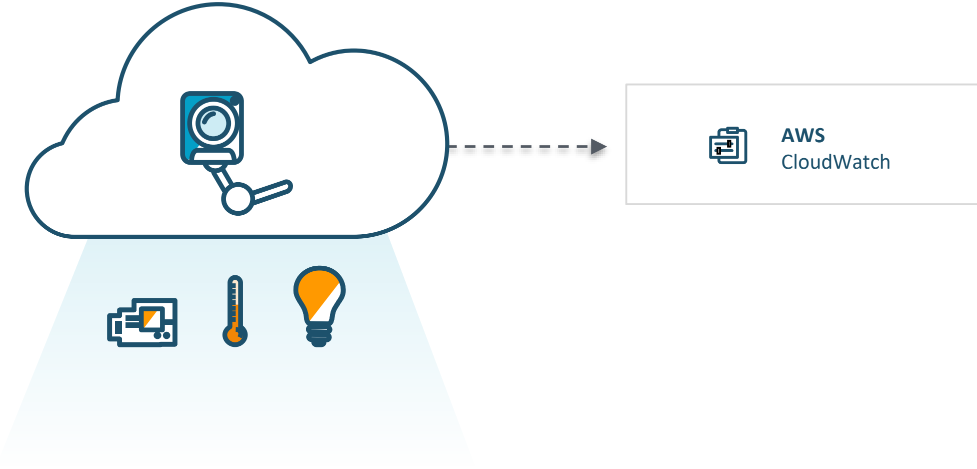
Real-time Fleet Index & Search

- 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.



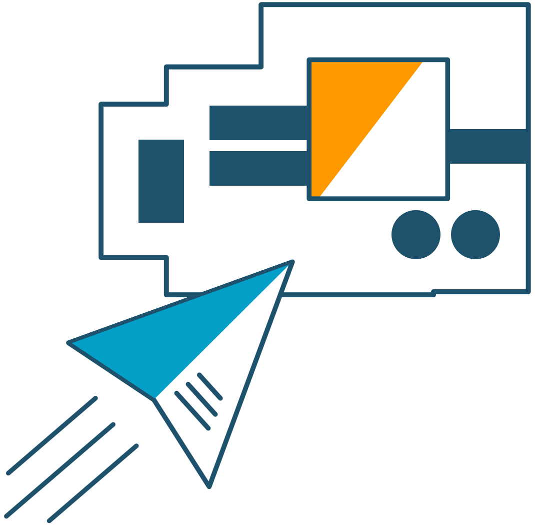
Fine Grained Device Logging & Monitoring

- 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

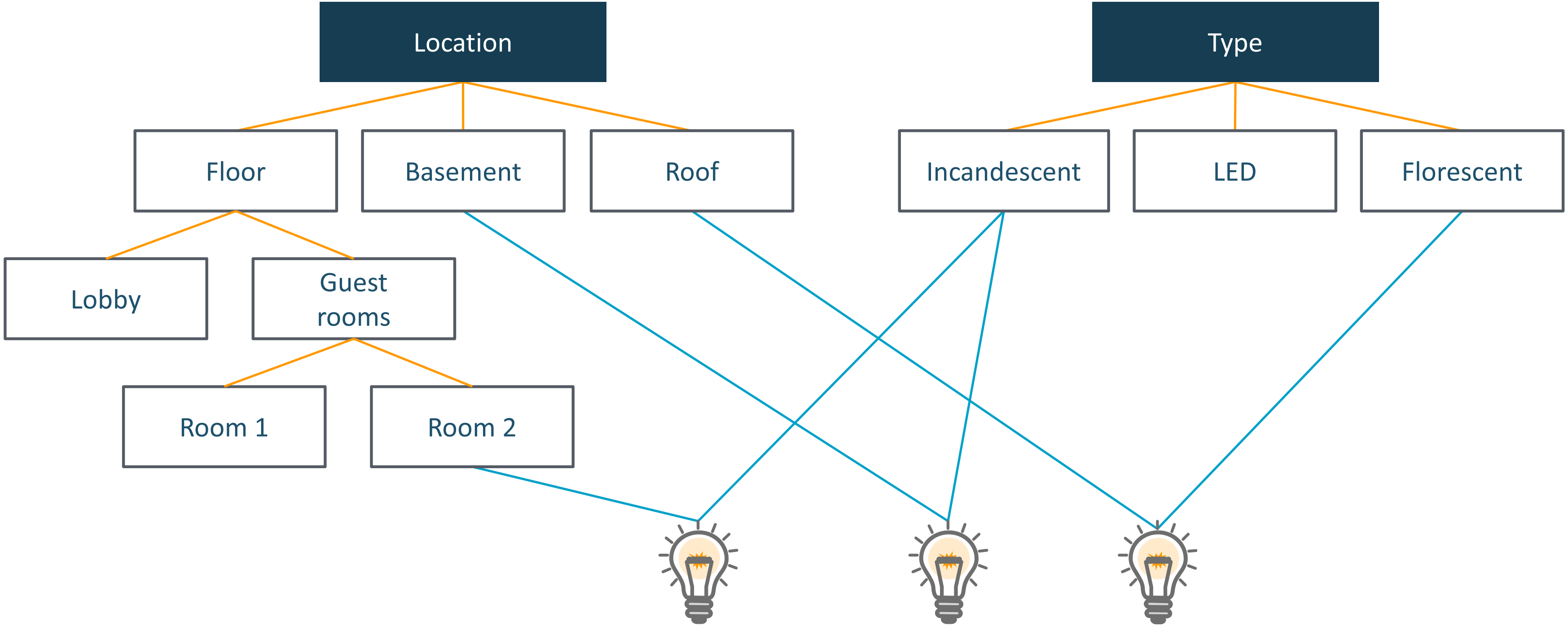


Over the Air Updates

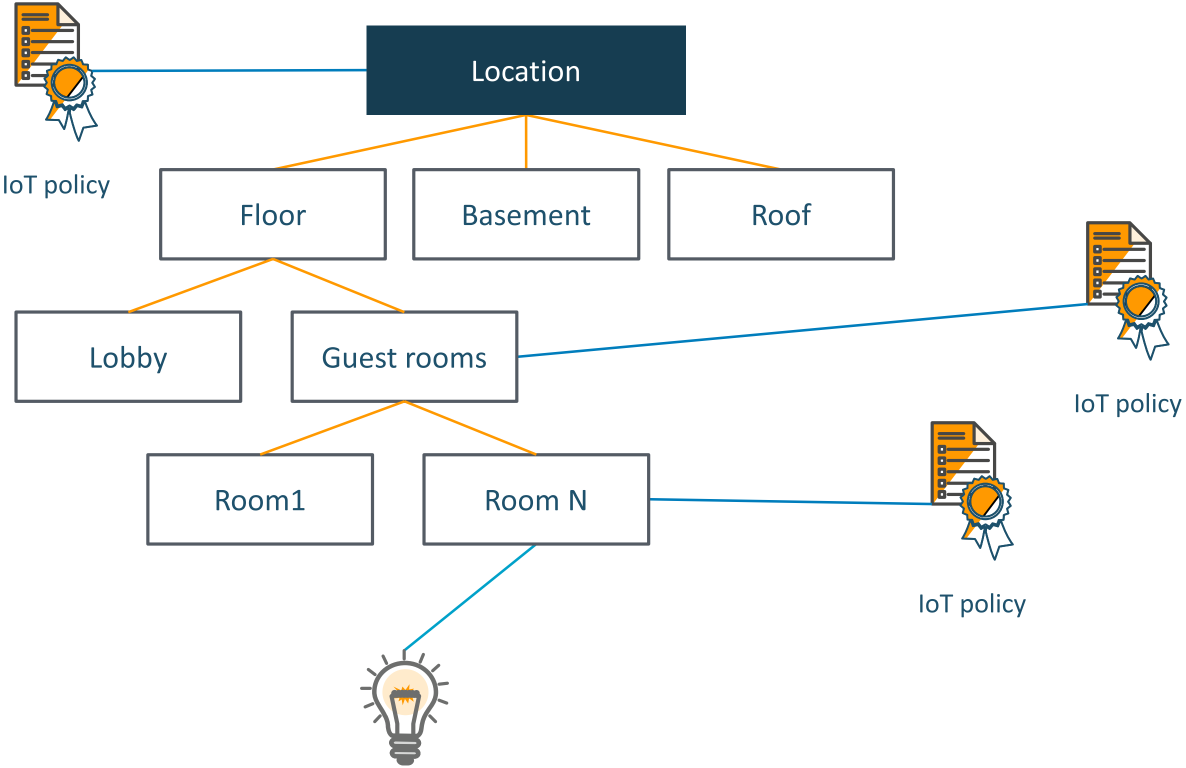
- Push over the air updates to your devices after they're deployed to the field to improve device functionality
- Receive notifications on the status of each device update to monitor your updates as they execute
- Target groups of devices to update in bulk, or pinpoint single devices to update
- Control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



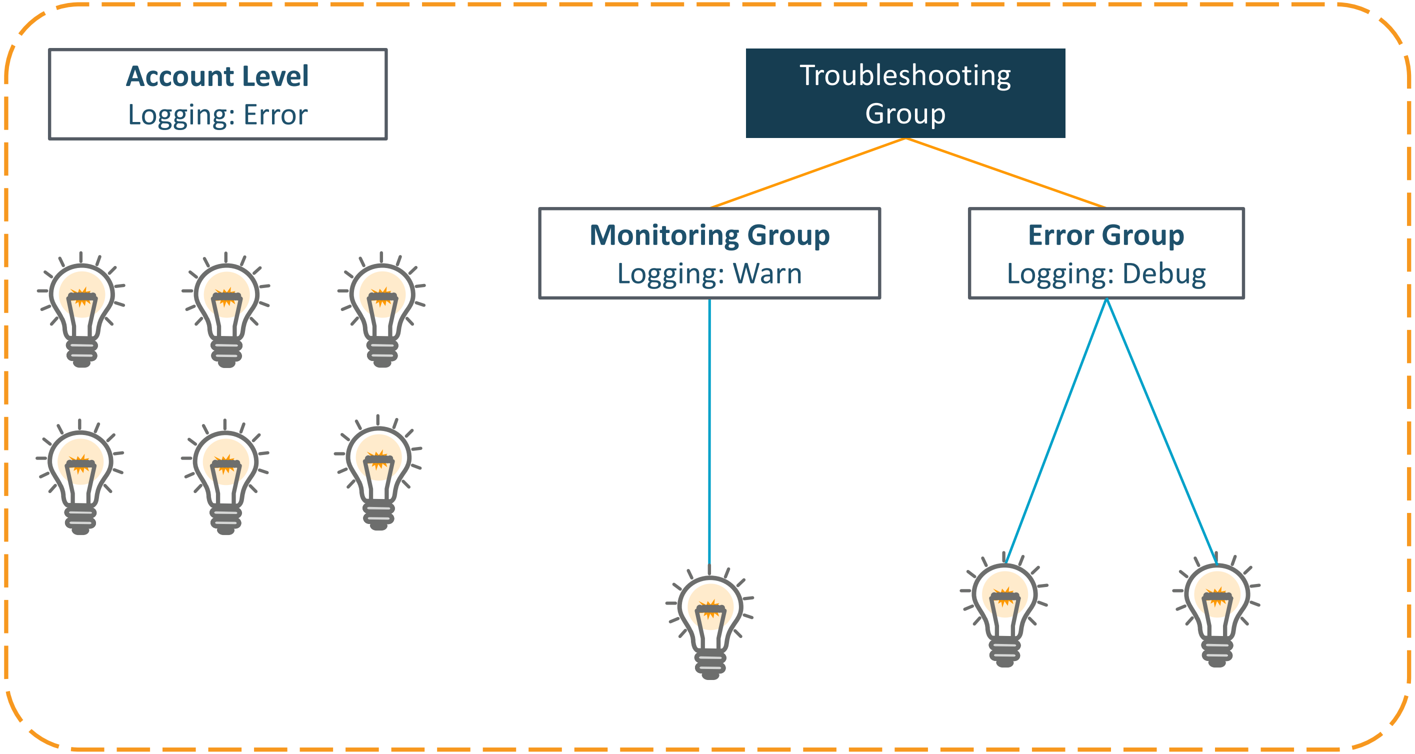
Thing Groups



Thing Group Policies



Thing Group Log Levels



Account Level
Logging: Error

Troubleshooting Group

Monitoring Group
Logging: Warn

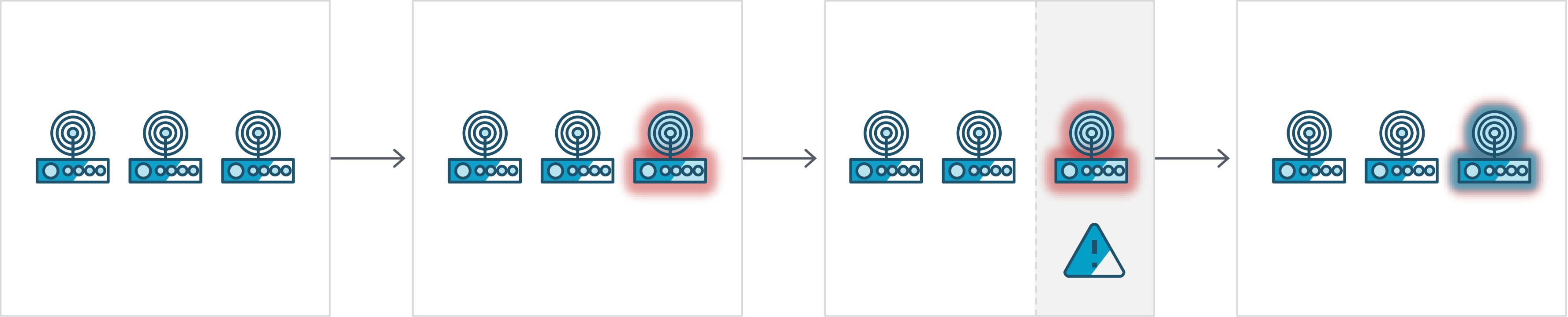
Error Group
Logging: Debug

AWS IoT Device Defender

COMING IN 2018

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

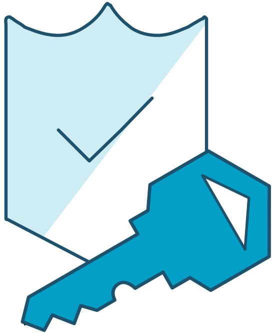
COMING IN 2018

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 specific 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

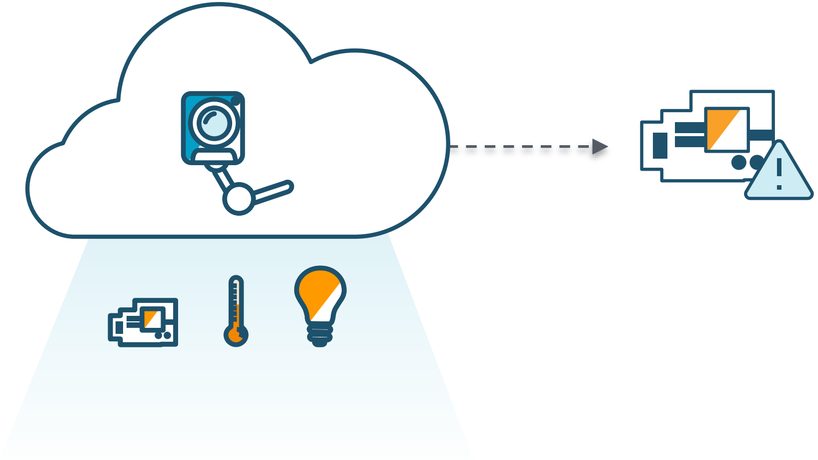


scheduled

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



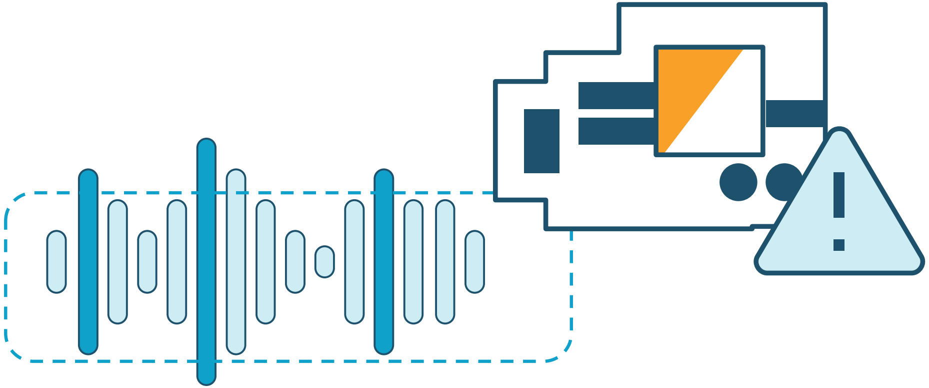
Identify Anomalies

Blacklist/Whitelist behaviors for:

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

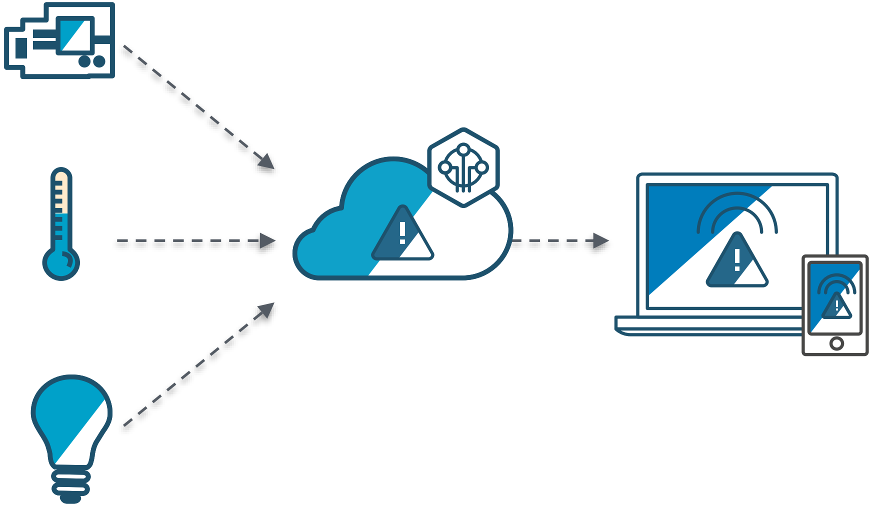
Define thresholds behavior for:

- 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



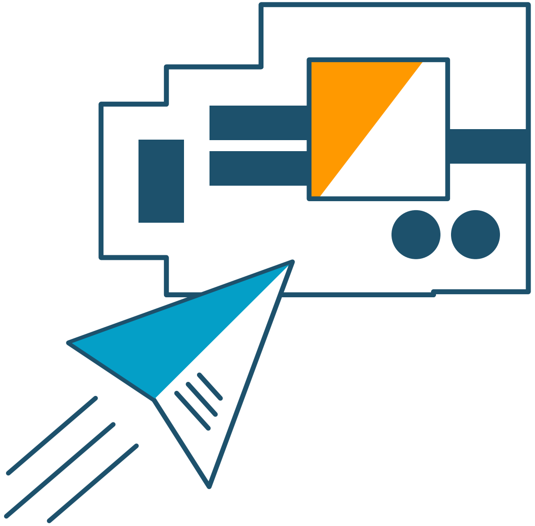
Generate Alerts

- 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



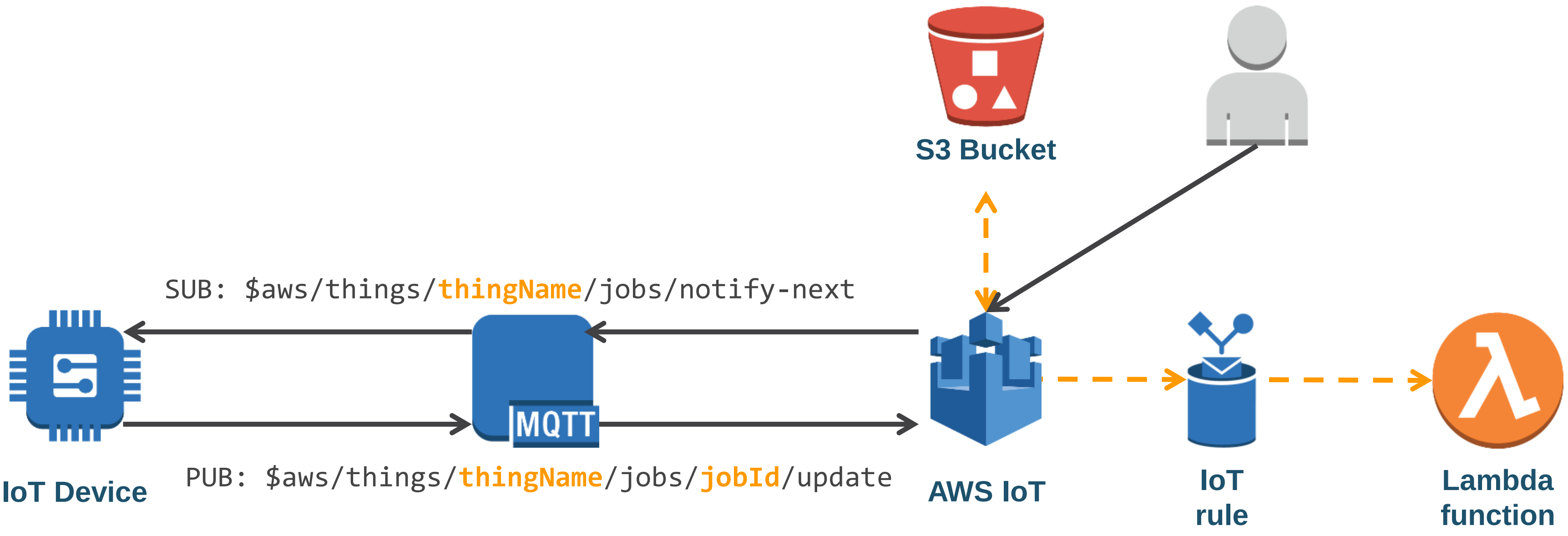
Patch Security Vulnerabilities

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



Demo – Continuous IoT Jobs

Architecture – Continuous IoT Jobs



S3 Bucket
SUB: $aws/things/thingName/jobs/notify-next
MQTT
IoT Device
PUB: $aws/things/thingName/jobs/jobId/update
AWS IoT
IoT rule
Lambda function

In Summary

- How to use AWS IoT Core to easily and securely connect devices
- How AWS IoT Device Management and Device Defender support and ease day to day IoT operations
- How AWS customers use AWS IoT Core to solve their IoT challenges

Thank you!