# The four eras of computing

## 1960s

### Mainframe era

one computer – thousands of users

## 1980s

### PC era

one computer – one user

## 2000s

### Mobility era

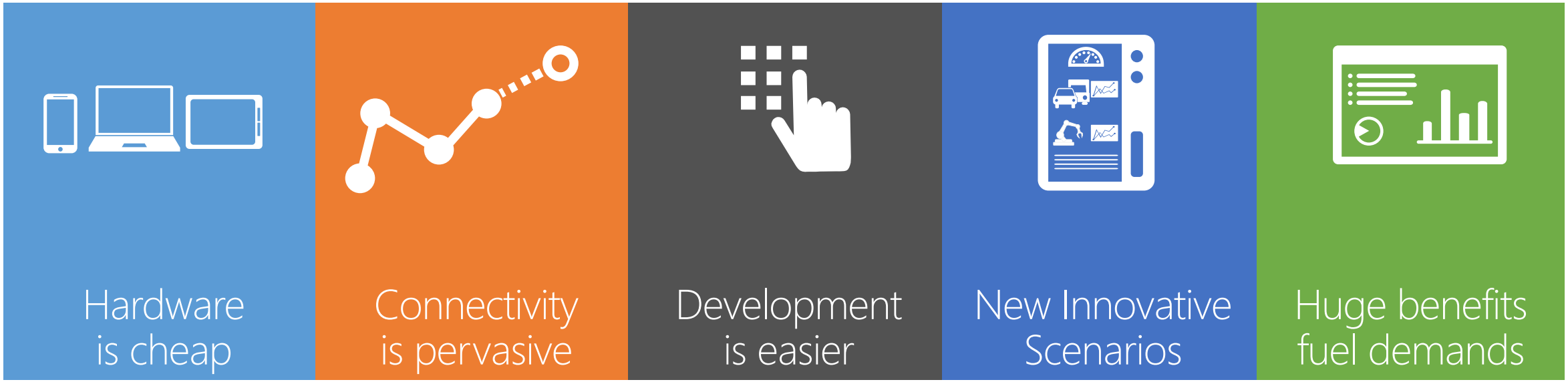
several computers – one user

## 2020s

### IoT era

many computers – one to many users

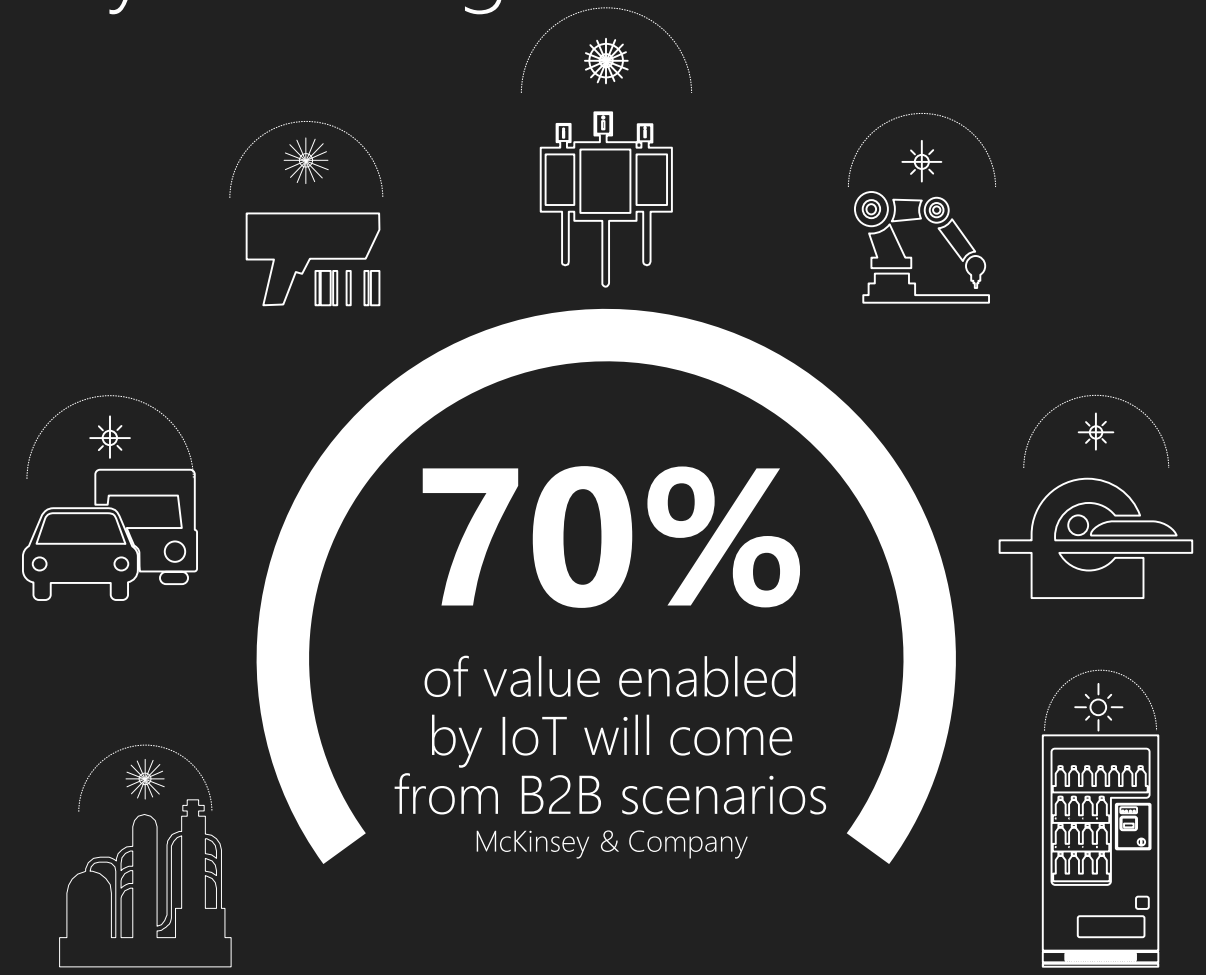
# IoT is an Inflection Point



# Microsoft's view on IoT

## The Internet of Things starts with your things

- Build on the infrastructure you already have
- Add more devices to the ones you already own
- Get more from the data that already exists



# IoT Is Gaining Momentum

Medication adherence

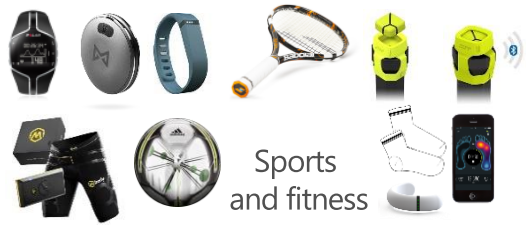
Health monitoring

Pet tracking

Behavior modification

Object tracking

Child and elder monitoring



Sports and fitness

Smart lighting

Indoor navigation

Beacons and proximity

Trip tracking and car health

**HOME** — **COMMUTE** — **WORKPLACE** — **COMMUTE** — **HOME**

Smart appliances

Food and nutrition tracking

Identity

Office equipment

Smart vending machines

Bike ride stats and protection

Sleep tracking

Air conditioning and temperature control

Environmental sensors

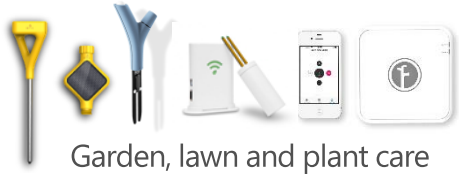
Information capture

Control

Home security

Home automation

Leak detection



Garden, lawn and plant care

New devices and sensors

Entertainment systems

# The Arduino

# The Arduino family

Uno

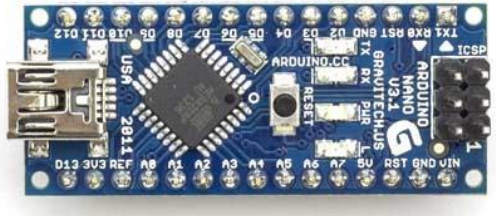
Leonardo

Yun

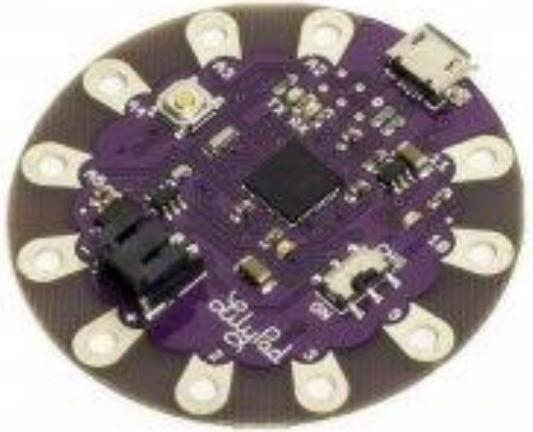
Due (Mega)

Micro

Mini

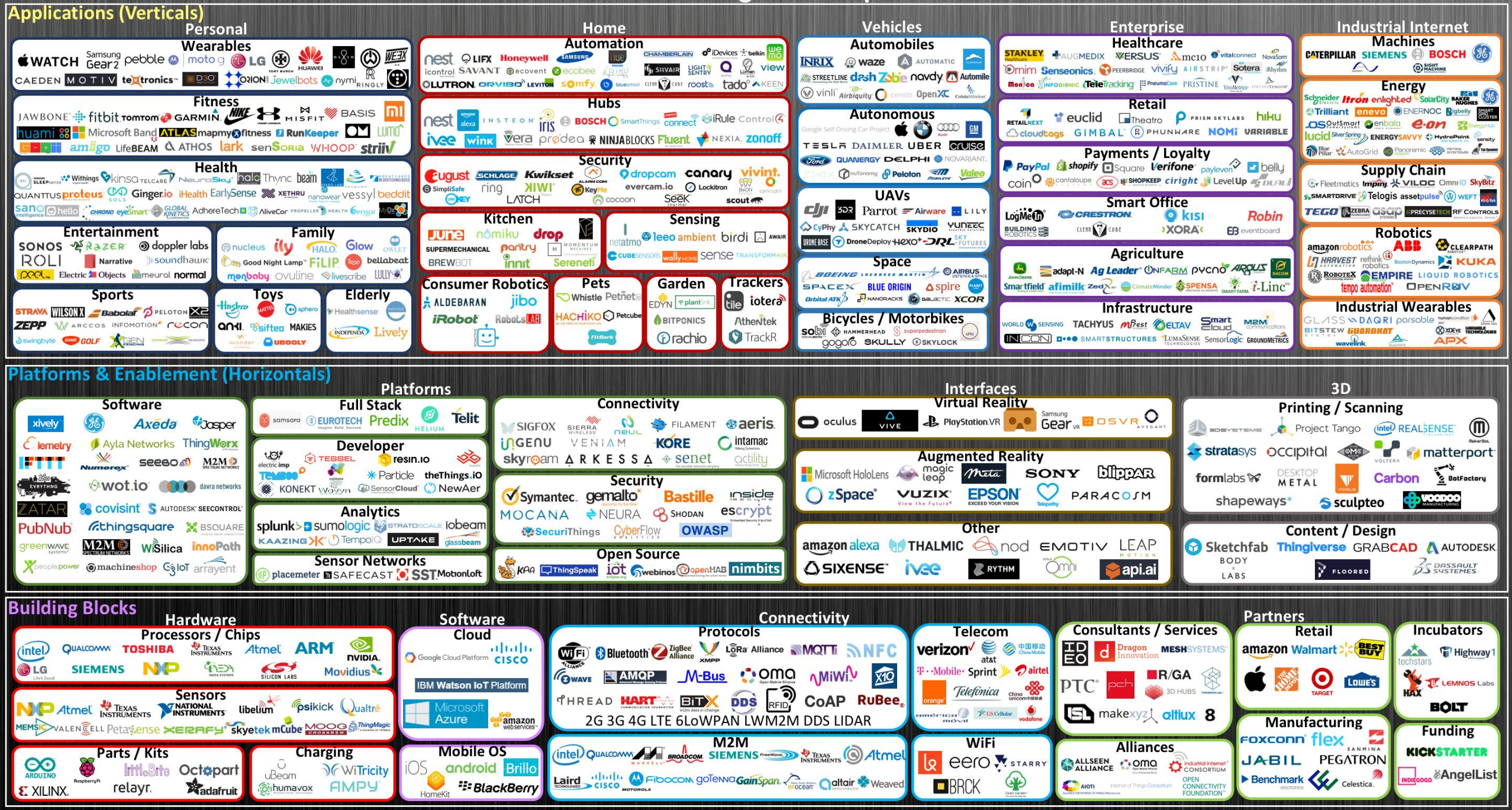


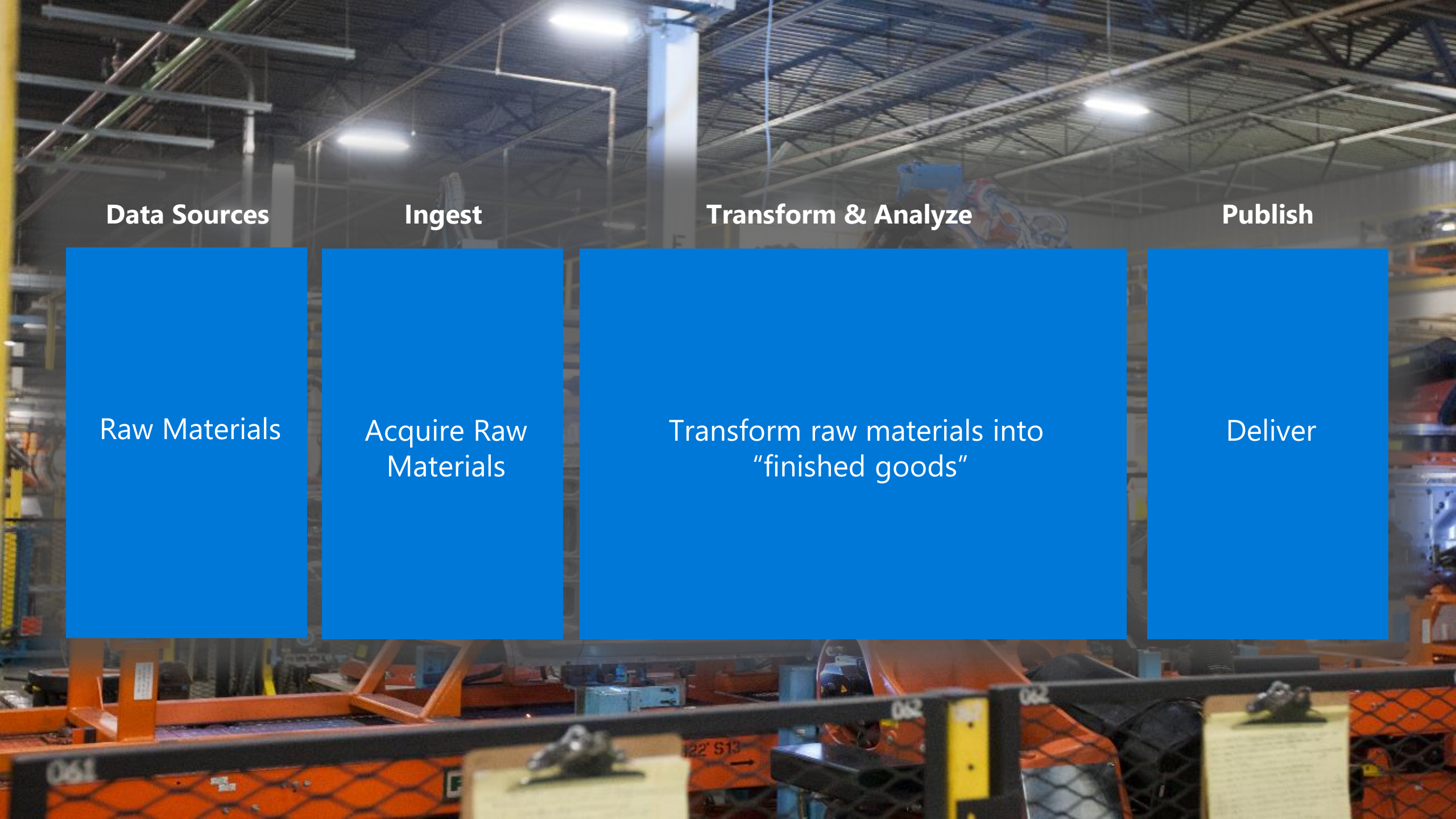
Nano



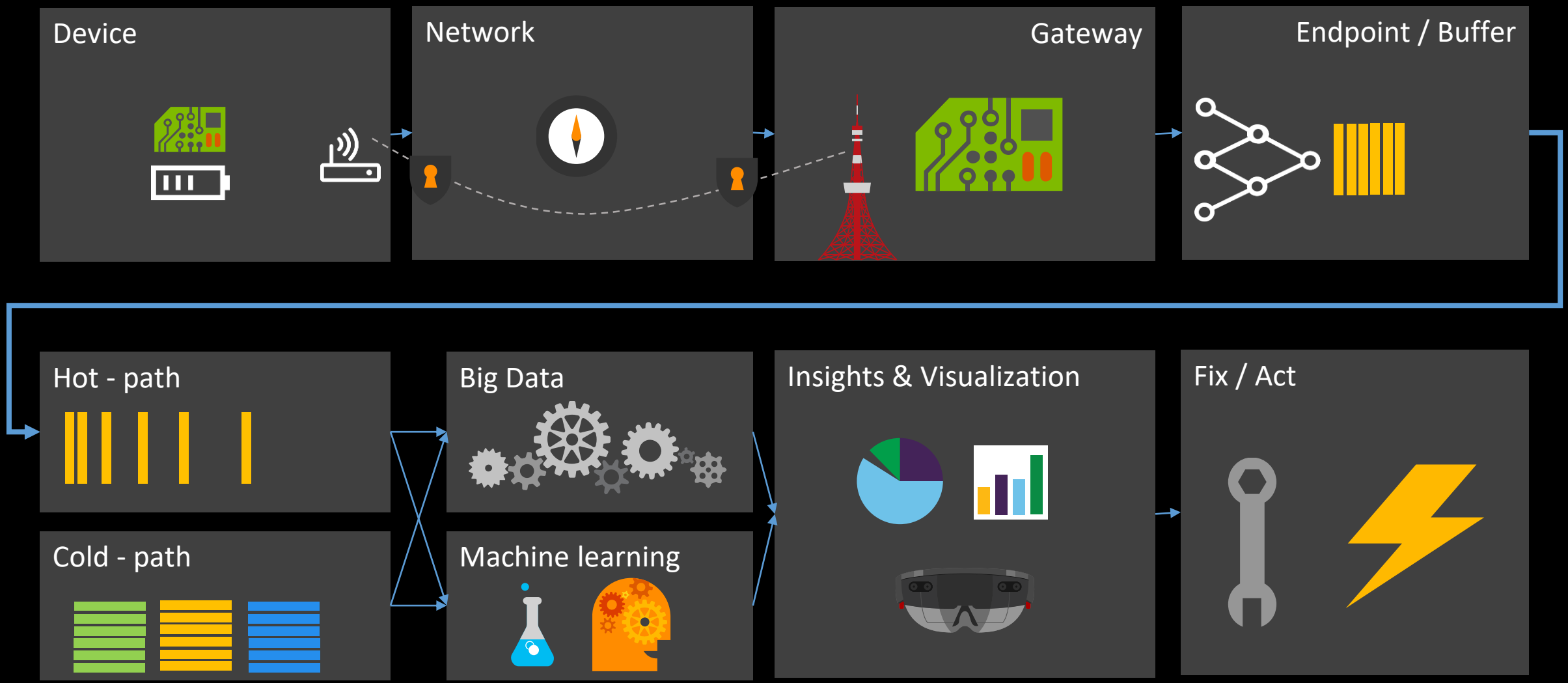
Lilypad

# Internet of Things Landscape 2016




Data Sources
Ingest
Transform & Analyze
Publish
Raw Materials
Acquire Raw Materials
Transform raw materials into “finished goods”
Deliver

# Message journey



# IOT SECURITY

2000 Sewage treatment plant release ¼ million gallons of raw sewage

2003 Slammer Worm disables Nuclear power plant

Sobig virus shuts down train signaling in the US

Alarm failure causes power loss, impacting 50M people

2005 13 DaimlerChrysler plants shutdown due to Zotob Worm

2008 14-year old hacks tram system – 12 injuries

2009 Faulty sensor causes Metro collision – fatal

2010 Stuxnet disrupts 14 plants including uranium enrichment facility

2010 – 2014 150 Attacks on energy grids

2014 Hackers attack German steel mill – melt down

2015 Consumers get both baked and frozen due to faulty thermostats

2016 …more to come…

# IOT SECURITY

Insecure Web Interface

Lack of Transport Encryption

Insufficient Security Configurability

Poor Physical Security

Insufficient Authentication

Insecure Cloud Interface

Insecure Software/Firmware

Privacy Concerns

Insecure Mobile Interface

Insecure Network Services

know the trade

## IOT TESTING GUIDANCE

### Insecure Web Interface

- Assess any web interface to determine if weak passwords are allowed
- Assess the account lockout mechanism
- Assess the web interface for XSS, SQLi and CSRF vulnerabilities and other web application vulnerabilities
- Assess the use of HTTPS to protect transmitted information

### Lack of Transport Encryption

- Assess the solution to determine the use of encrypted communication between devices and between devices & internet
- Assess the solution to determine if accepted encryption practices are used and if proprietary protocols are avoided
- Assess the solution to determine if a firewall option available is available

### Insufficient Security Configurability

- Assess the solution to determine if password security options are available
- Assess the solution to determine if encryption options (e.g. Enabling AES-256 where AES-128 is the default setting)are available
- Assess the solution to determine if logging for security events

### Poor Physical Security

- Assess the device to ensure it utilizes a minimal number of physical external ports (e.g. USB ports) on the device
- Assess the device to determine if it can be accessed via unintended methods such as through an unnecessary USB port

### Insufficient Authentication /Authorization

- Assess the solution for the use of strong passwords where authentication is needed
- Assess the solution for Implementation two-factor authentication where possible
- Assess password recovery mechanisms
- Assess the solution for the option to require strong passwords
- Assess the solution for the option to force password expiration after a specific period
- Assess the solution for the option to change the default username and password

### Insecure Cloud Interface

- Assess the cloud interfaces for security vulnerabilities
- Assess the cloud-based web interface to ensure it disallows weak passwords
- Assess the cloud-based web interface to ensure it includes an account lockout mechanism
- Assess the cloud-based web interface to determine if two-factor authentication is used
- Assess any cloud interfaces for XSS, SQLi and CSRF vulnerabilities and other vulnerabilities
- Assess all cloud interfaces to ensure transport encryption is used
- Assess the cloud interfaces to determine if the option to require strong passwords is available

### Insecure Software/Firmware

- Assess the device to ensure it includes update capability & can be updated quickly when vulnerabilities are discovered
- Assess the device to ensure it uses encrypted update files and that the files are transmitted using encryption
- Assess the device to ensure is uses signed files and thenvalidates that file before installation

### Privacy Concerns

- Assess the solution to determine the amount of personal information collected
- Assess the solution to determine if collected personal data is properly protected using encryption at rest and in transit
- Assess the solution to determine if Ensuring data is de-identified or anonymized

### Insecure Mobile Interface

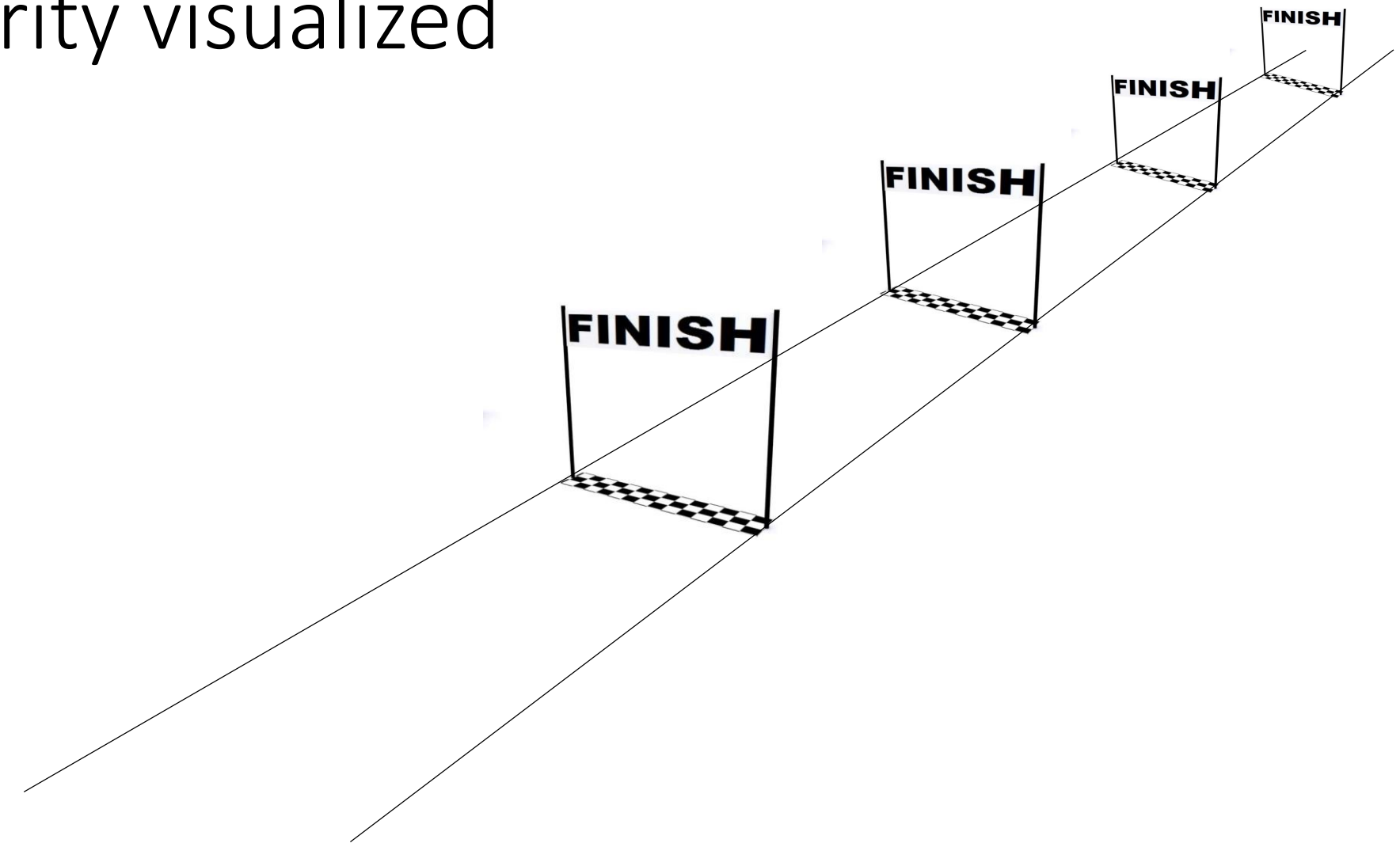
- Assess the mobile interface to ensure it disallows weak passwords
- Assess the mobile interface to ensure it includes an account lockout mechanism
- Assess the mobile interface to determine if it implements two-factor authentication
- Assess the mobile interface to determine if it uses transport encryption
- Assess the mobile interface to determine if the option to require strong passwords is available
- Assess the mobile interface to determine if the option to force password expiration after a specific period is available
- Assess the mobile interface to determine if the option to change the default username and password is available
- Assess the mobile interface to determine the amount of personal information collected

### Insecure Network Services

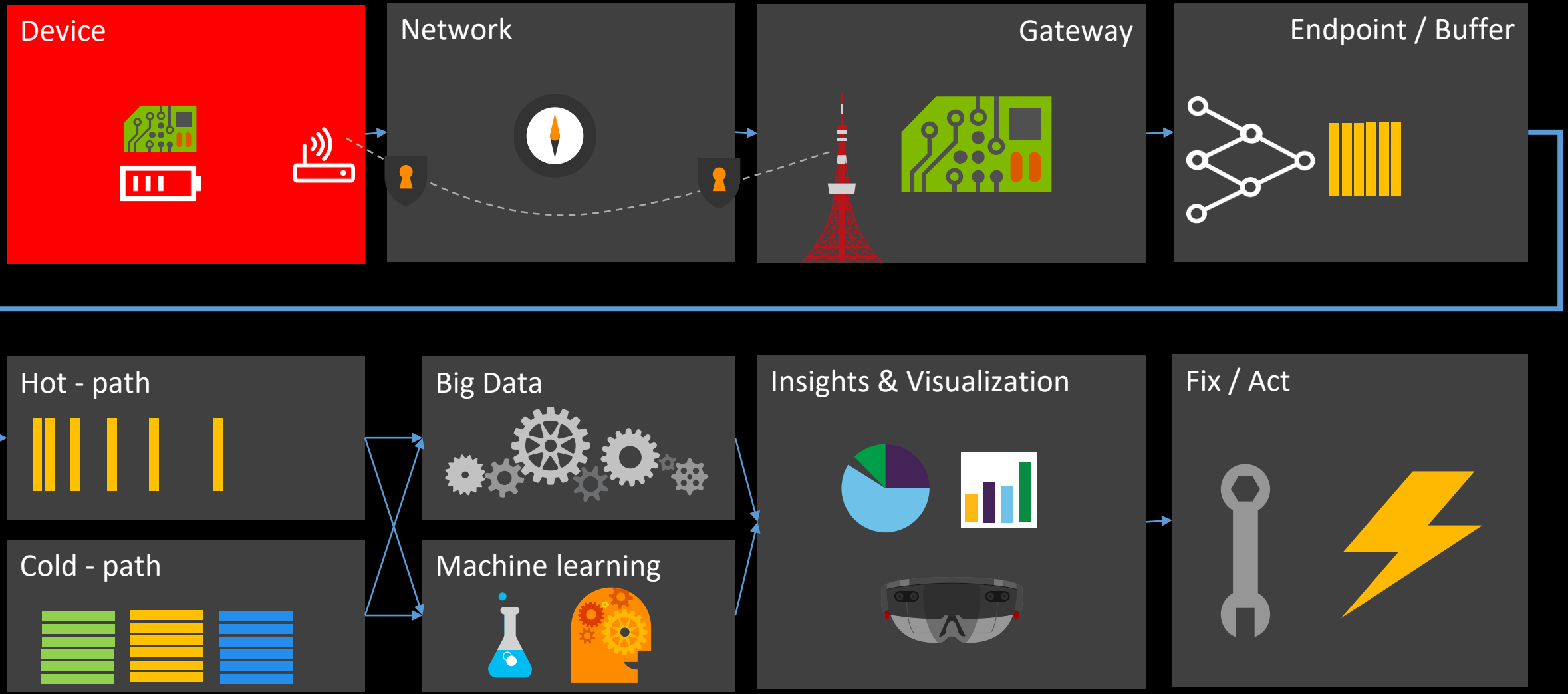
- Assess the solution to ensure network services don't respond poorly to buffer overflow, fuzzing or denial of service attacks
- Assess the solution to ensure test ports are not present

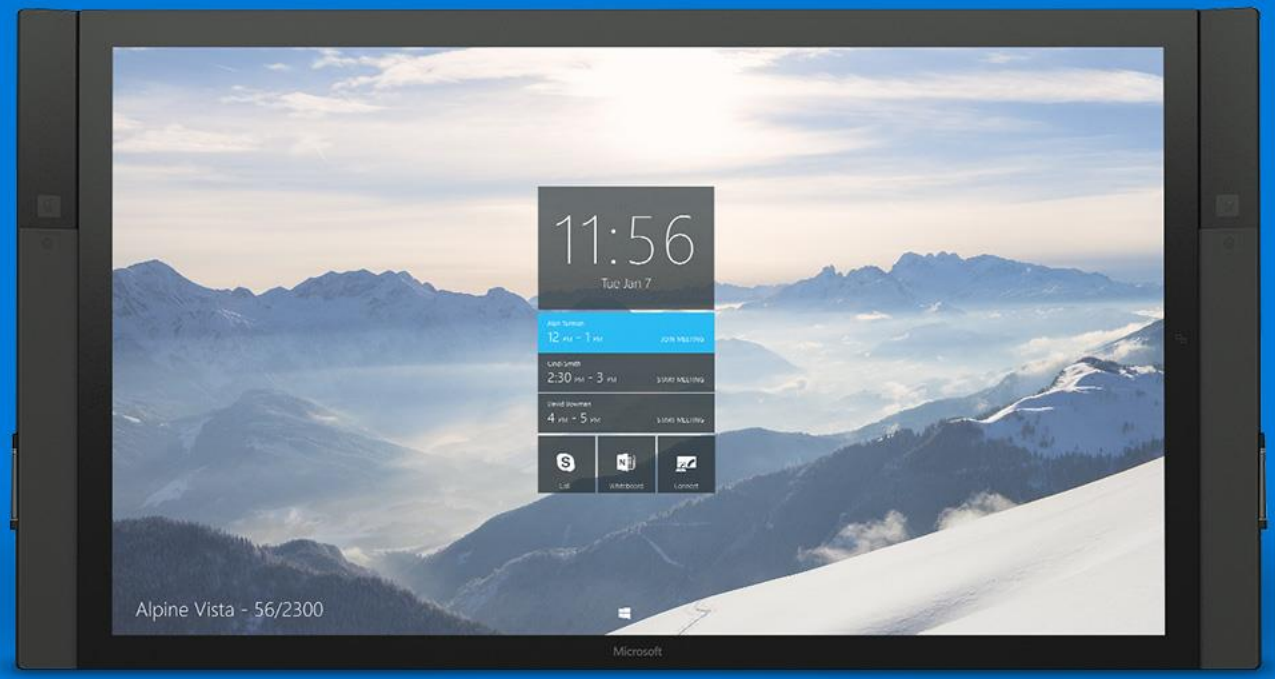
OWASP Internet of Things Top 10

# IoT Security visualized



# Message journey




11:56
Tue Jan 7
Alpine Vista - 56/2300
Microsoft

# Windows 10


Pins
NETFLIX
FORZA
Live TV
Xbox Music

## Windows 10 IoT Enterprise

UWP + Classic desktop apps + Protection + Manageability

## Window 10 IoT Mobile

Mobile devices + Peripherals + Multi-user profiles

## Windows 10 IoT Core

UWP + Headless + I/O

## Windows 10 IoT Enterprise

Rich apps, performance

## Window 10 IoT Mobile

Mobile scenario’s

## Windows 10 IoT Core

Low cost, low power

Free when using online auto updates from Microsoft

## Windows 10 IoT Enterprise

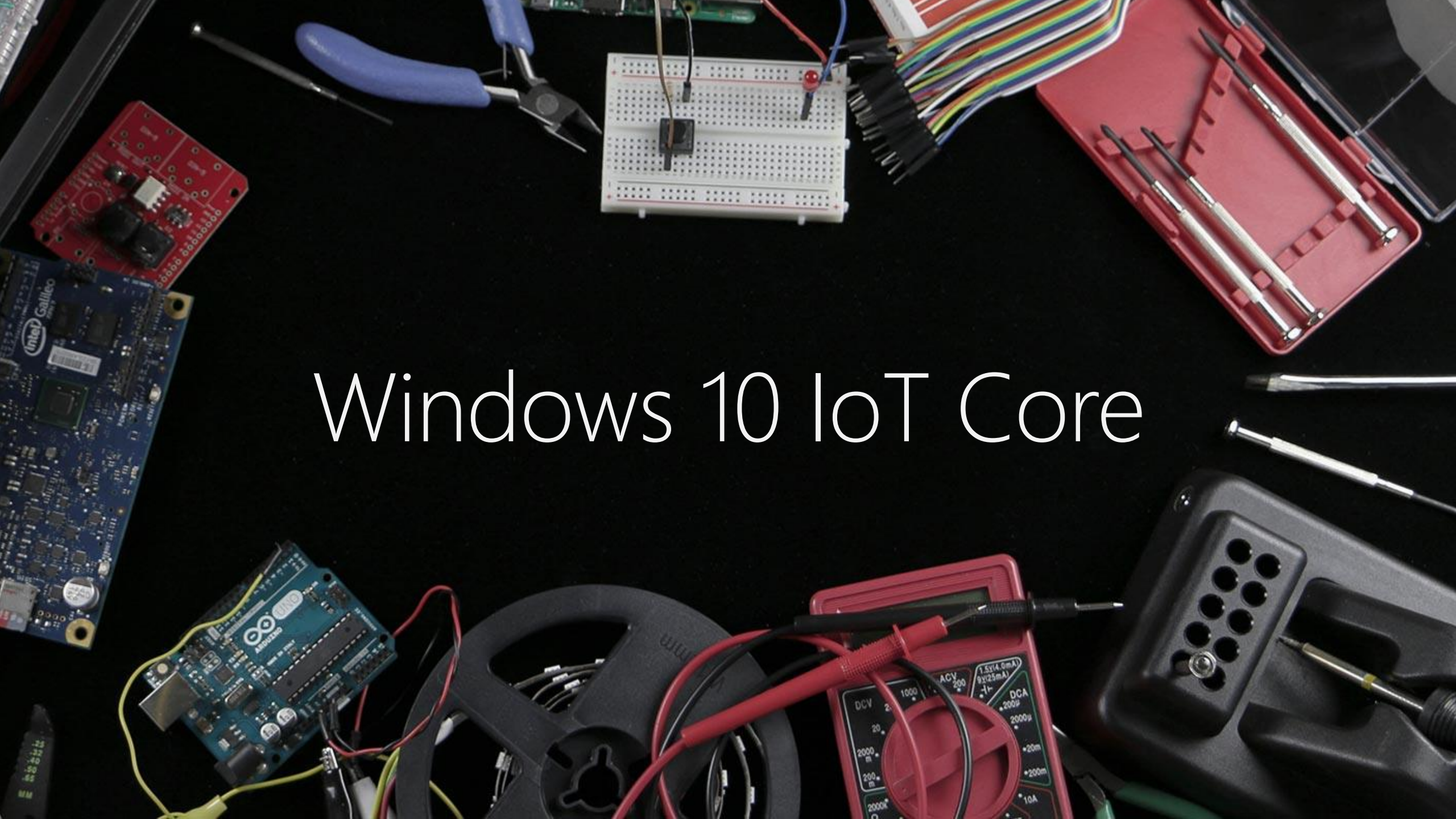
Rich apps, performance

## Window 10 IoT Mobile

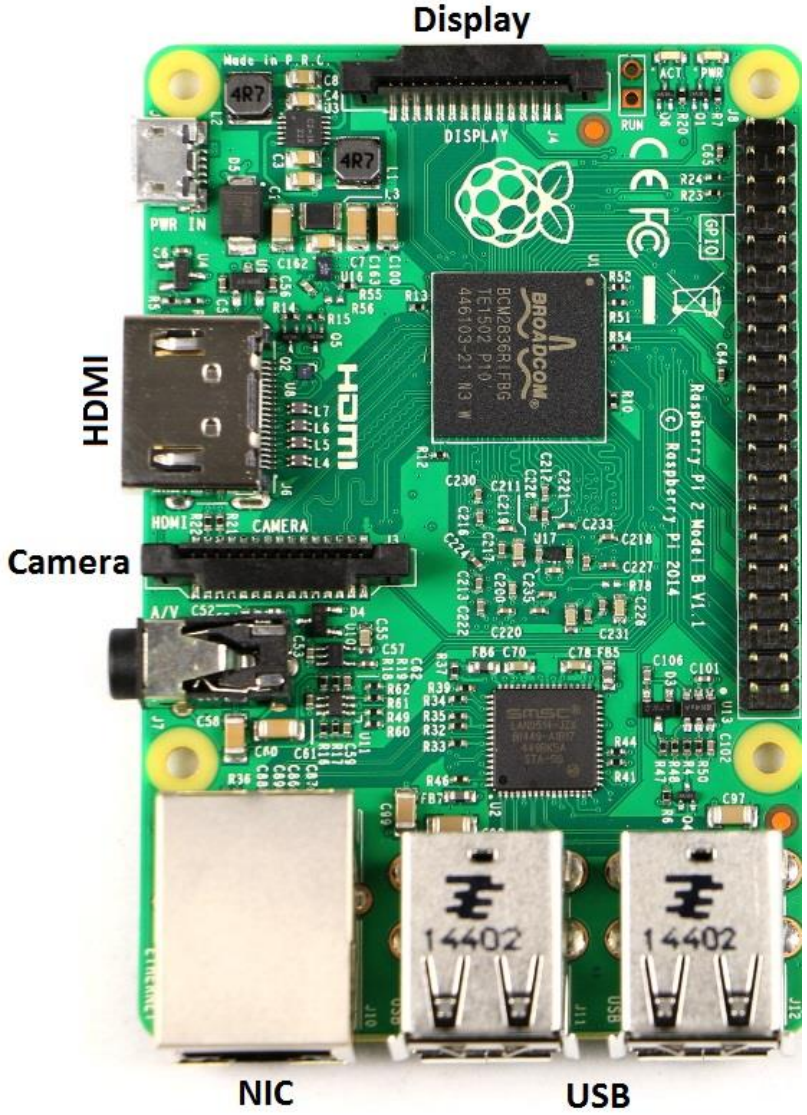
Mobile scenario’s

## Windows 10 IoT Core Pro

OEM Exclusive SKU, deferred or custom updates


Windows 10 IoT Core

# Raspberry Pi 2




35$

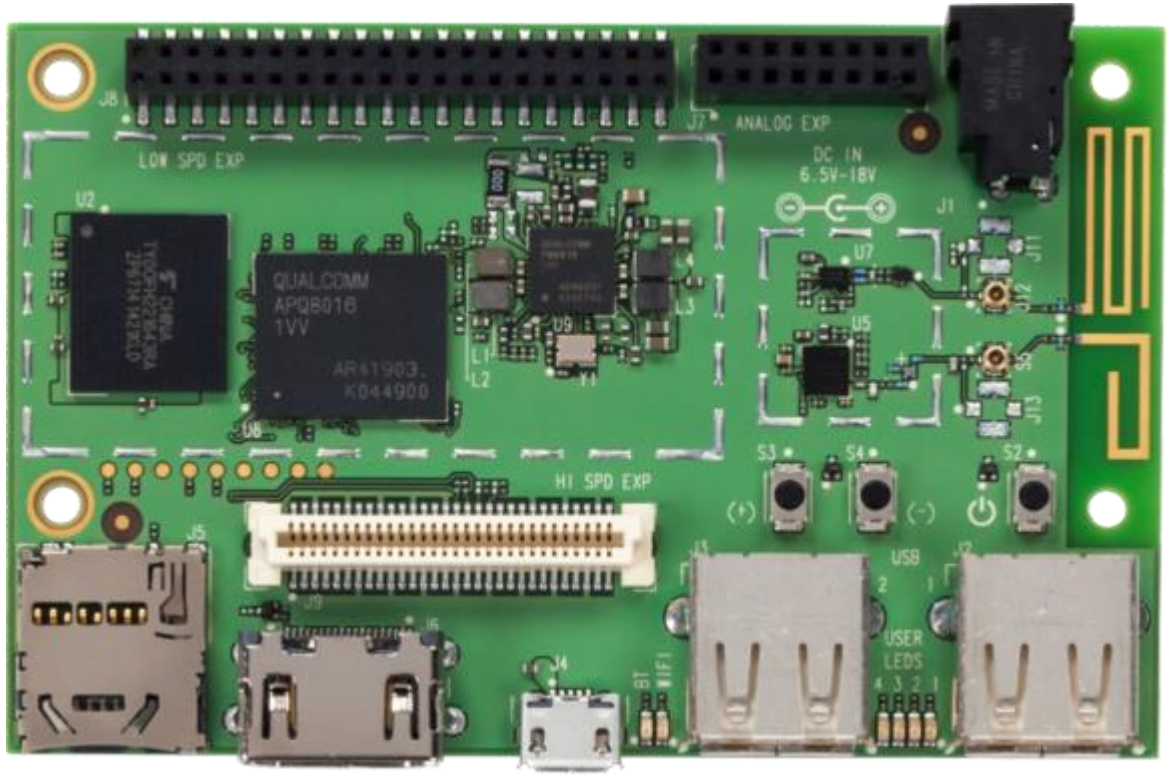
Ethernet

Linux, Windows 10 IoT Core

1GB Mem.

Quad Core ARM Cortex

# DragonBoard 410c




< 75$

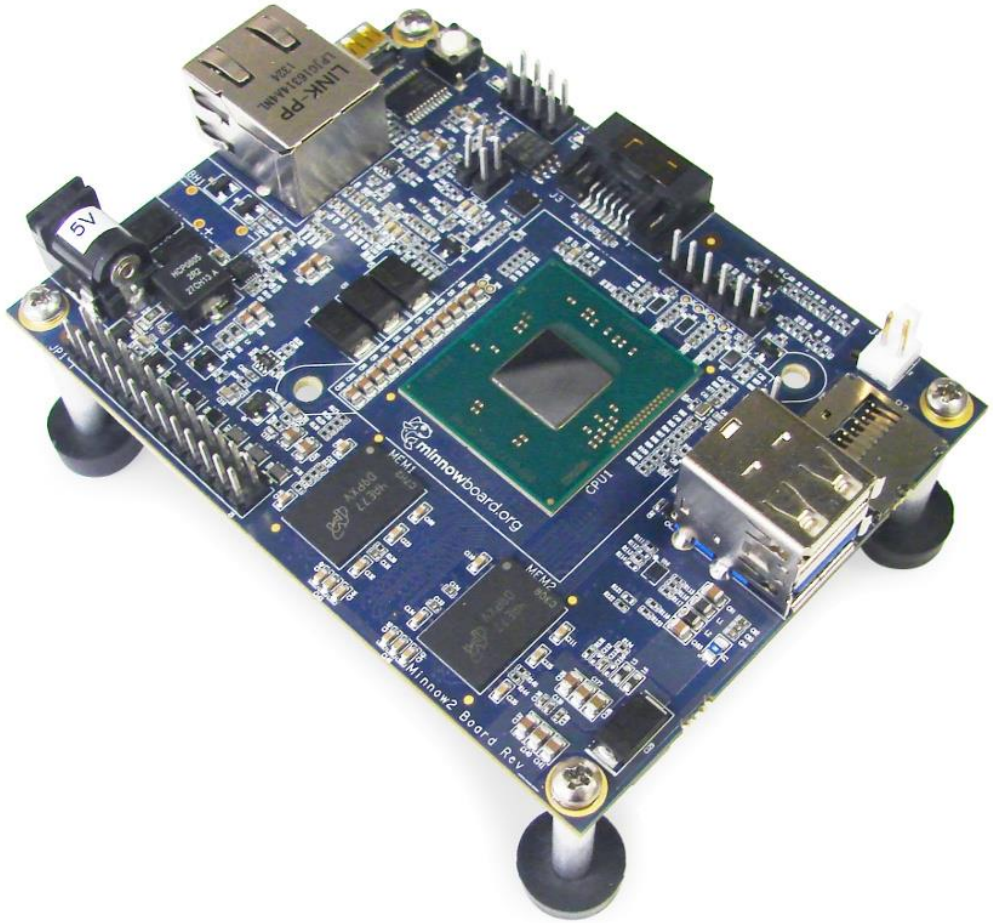
WIFI, BT, GPS

Android, Linux,
Windows 10 IoT Core

1GB Mem.

Quad Core ARM Cortex

# MinnowBoard Max




99-140$

Ethernet

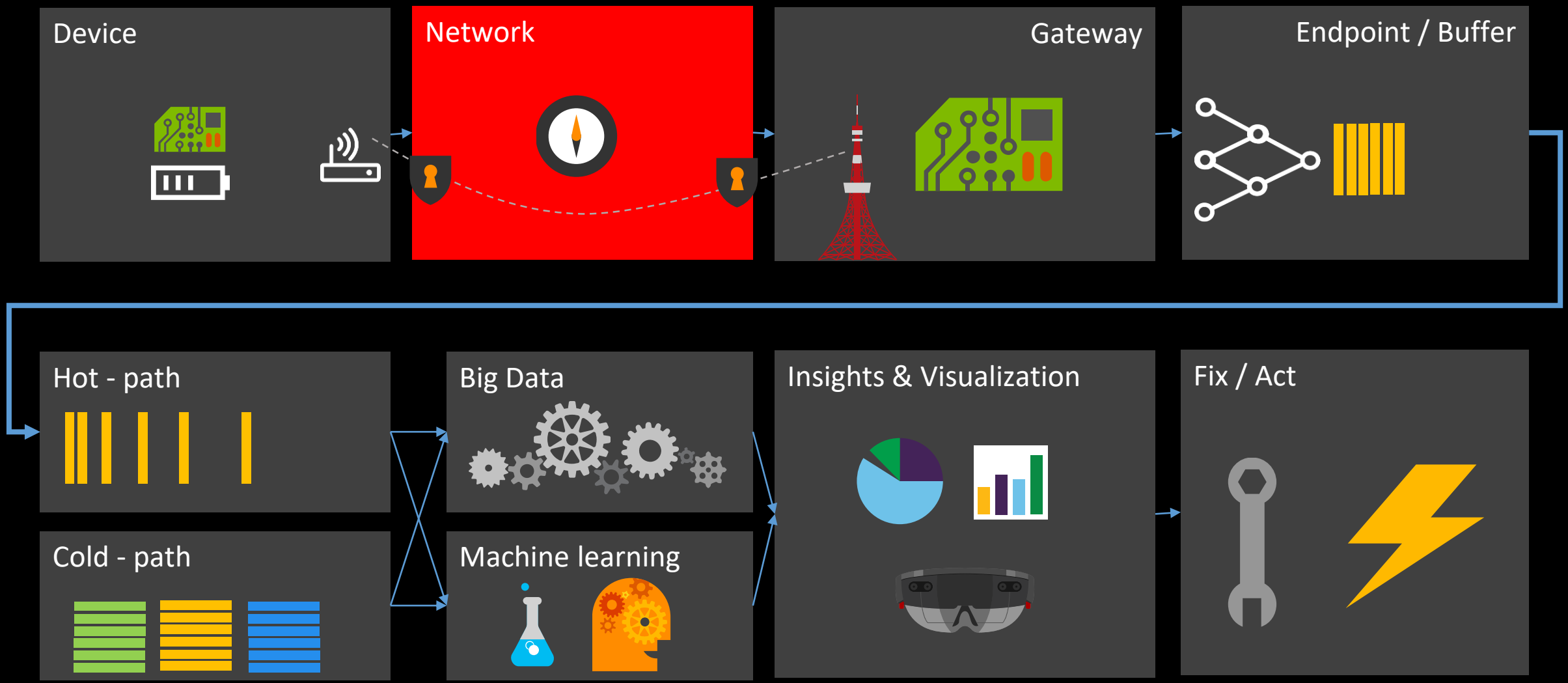
Linux, Windows 8.1/10 IoT Core

1-2GB Mem.

64-bit dual core Intel Atom CPU

# Toradex Colibi T30


# Message journey

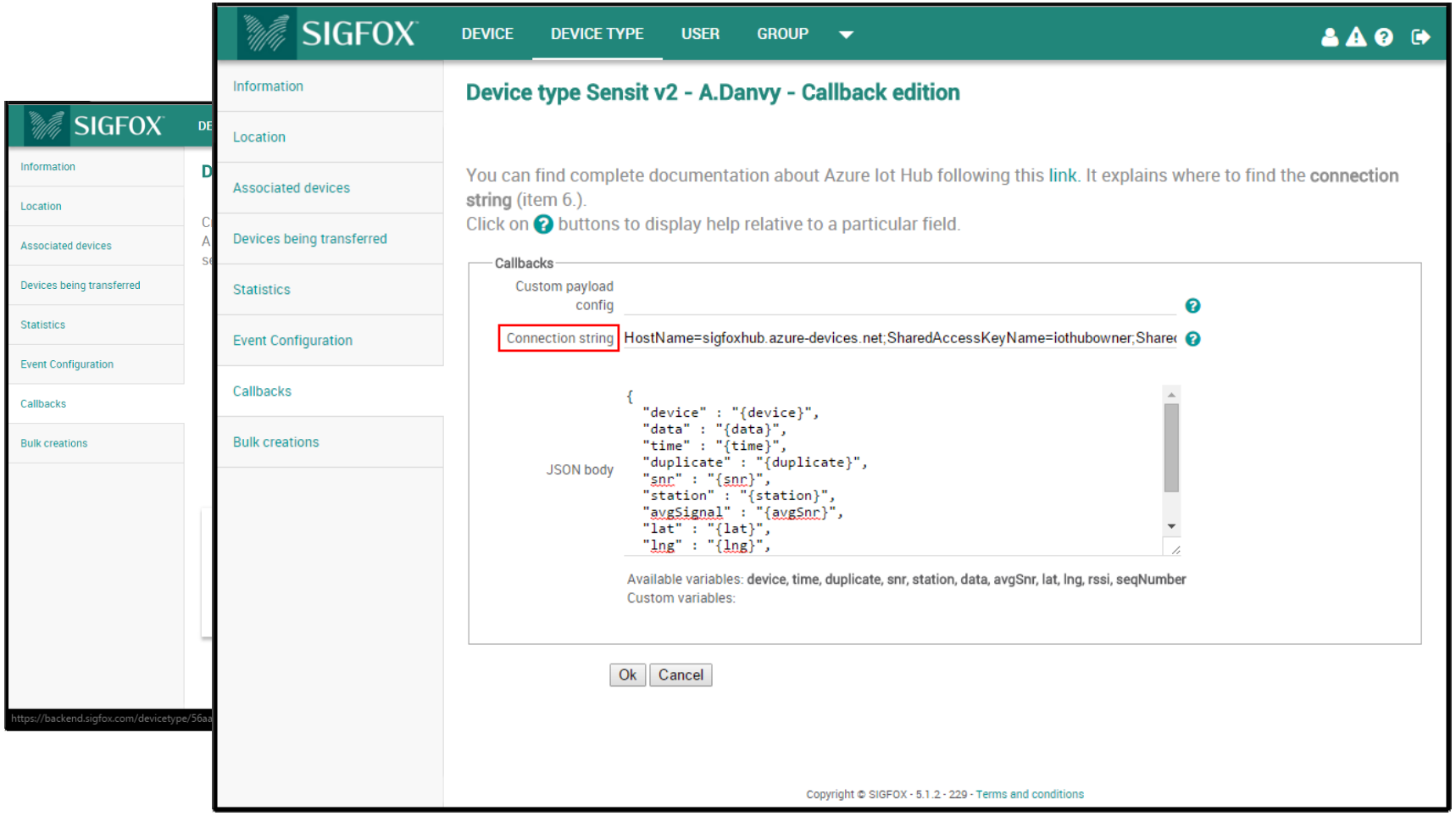


# Comparison

| | Transport | Network Footprint | Memory | Flow Control | Security | Messaging patterns | Other Notes | Delivery guarantees | IoT Applicability |
|---|---|---|---|---|---|---|---|---|---|
| CoAP | UDP | X Bytes Min<br>But typical overhead<br>Depends on options and URI lengths | • ~64K bytes client.<br>• Lower state retention requirements than most | By convention only. | DTLS + 8-byte token to impede response spoofing | Request/Reply, Fire &Forget, Subscribe (Observe) | Multicast Discovery<br>Extensibility | At most once<br>At least once (always ignore duplicates if you can) | 1. D2D<br>2. D2C |
| MQTT | TCP | X bytes Min. But Typical overhead depends on Topic names | • ~? bytes client<br>• State retention varies with QOS | Minimal | TLS+user id and password only | Pub/Sub | Last Will & Testament, Retain<br>Not extensible<br>Must implement full specification | At most once<br>At least once<br>Exactly once | D2C |
| AMQP | TCP | ~70 bytes Min | • ~95K bytes client<br>• State retention varies with QOS | Rich, dynamic | TLS+SASL authentication | Pub/Sub<br>Fire&Forget<br>Request/Reply | Transactions<br>Queueing/Persistence<br>Extensibility | At most once<br>At least once<br>Exactly once | 1. D2C,<br>2. D2D |

# SIGFOX + Azure

One network A billion dreams




12 byte messages

< 140 per day

Multi year battery life

KMs of range

<10$ per device

7 million devices deployed today


LoRa™

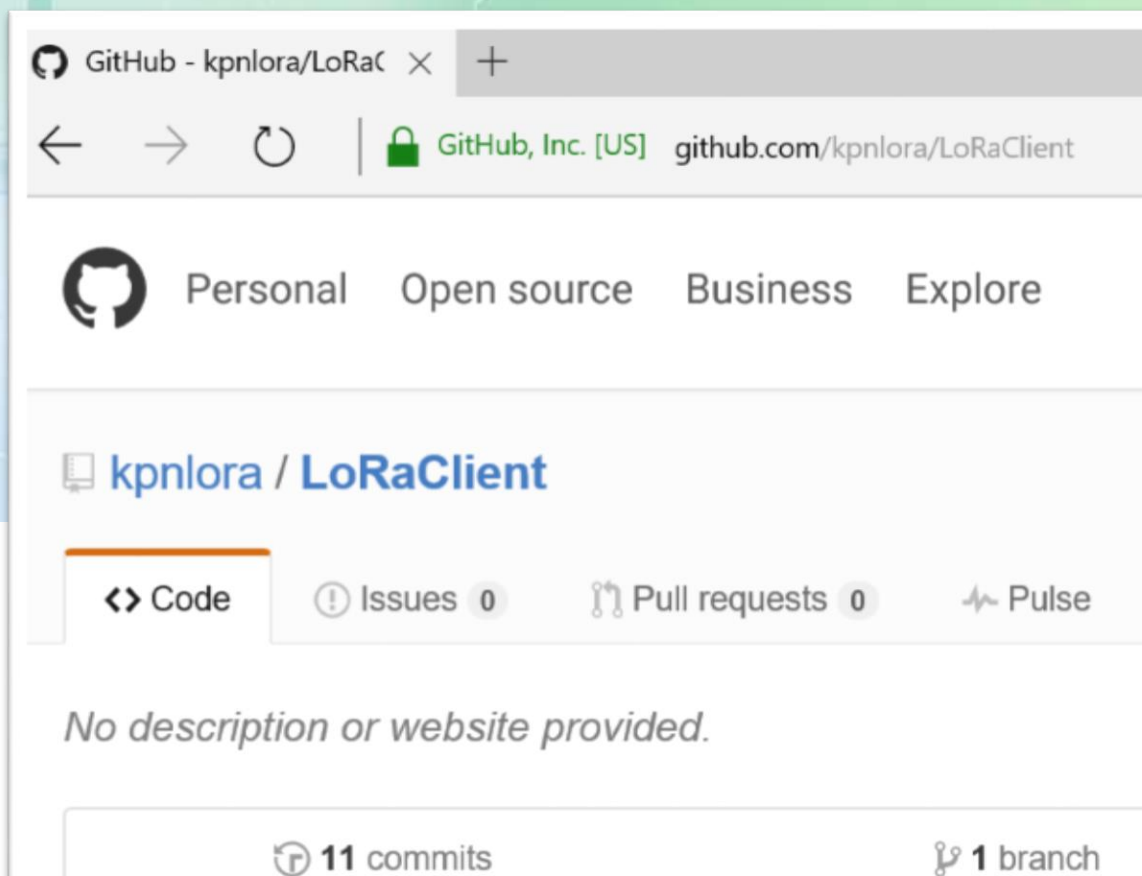

THE THINGS
NETWORK

LoRa®

kpn

# Microsoft Azure

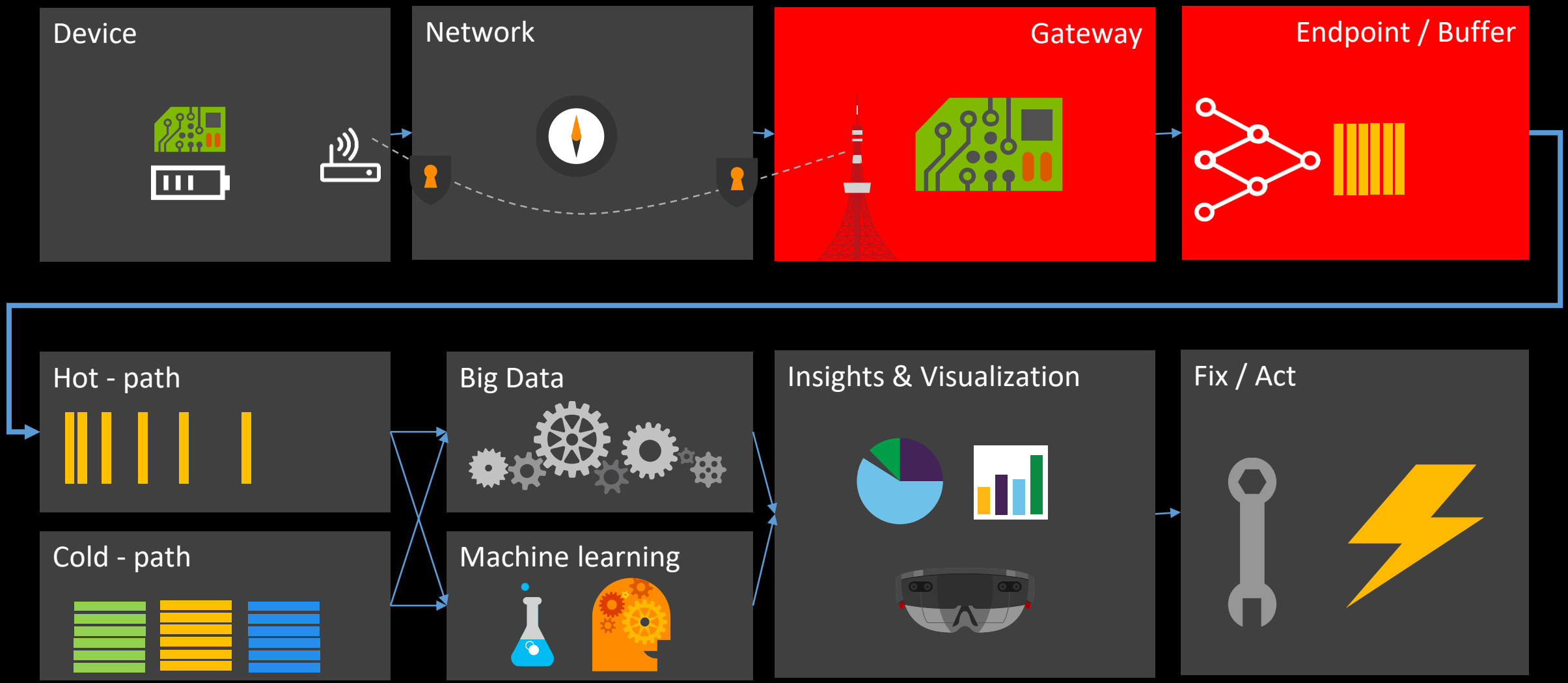
github.com/kpnlora/LoRaClient



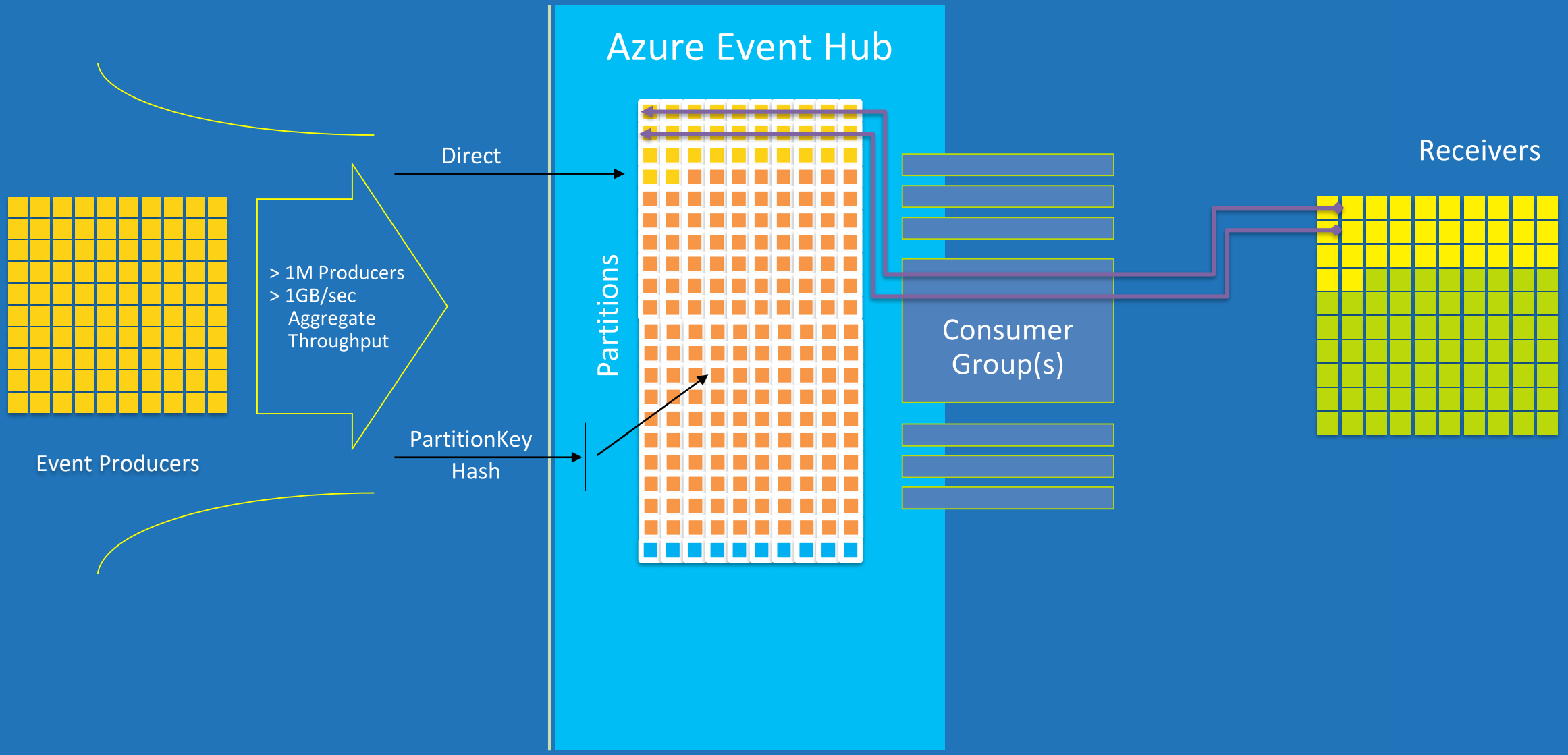

betabit {...}

bijzonder maken;

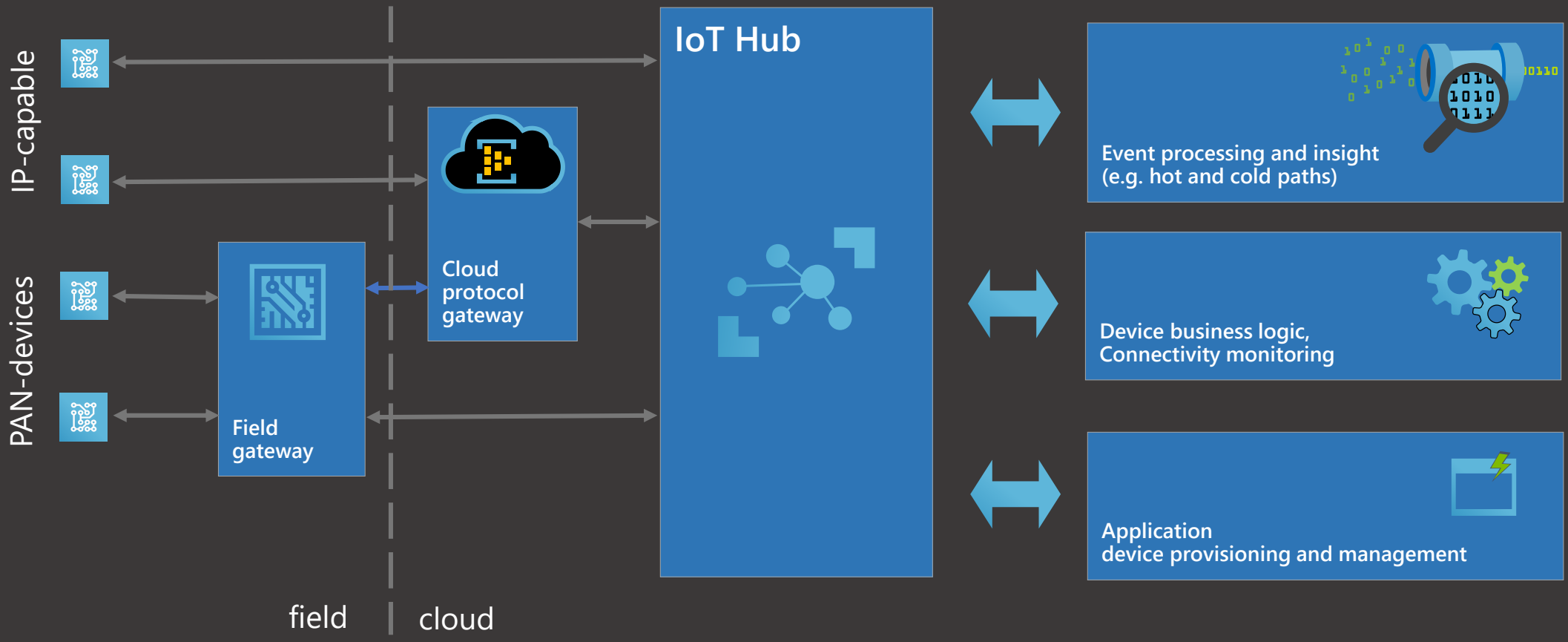
# Message journey



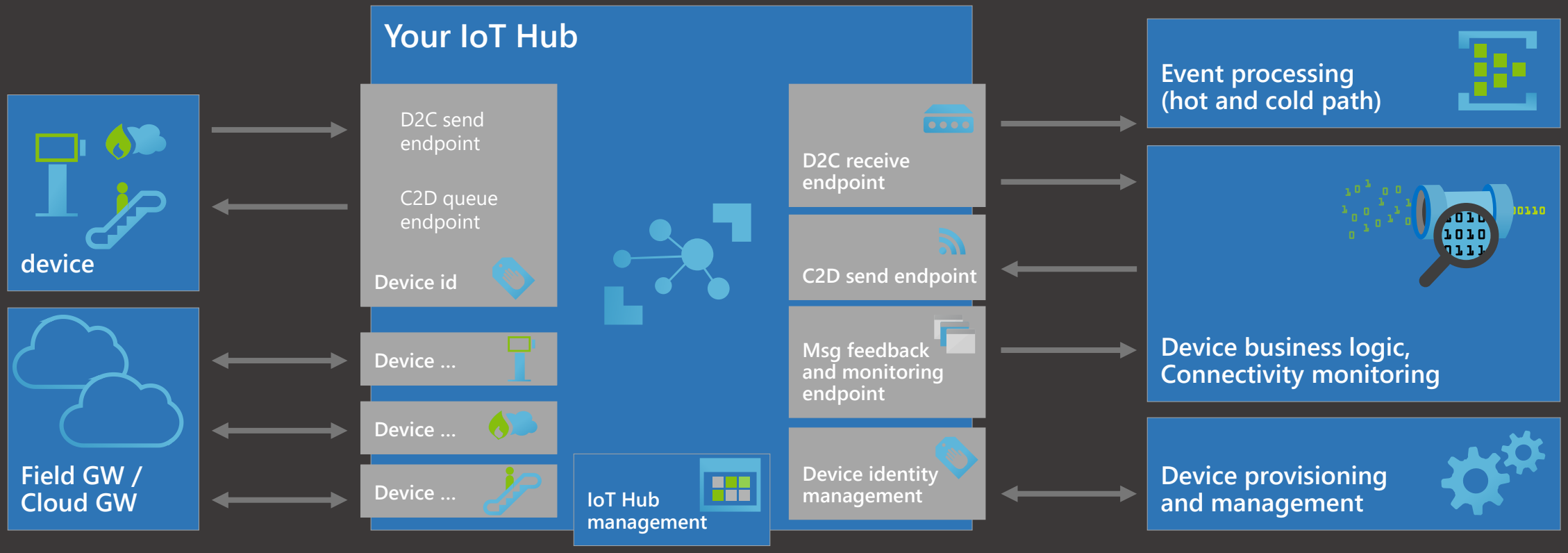
# Microsoft Azure Event Hubs



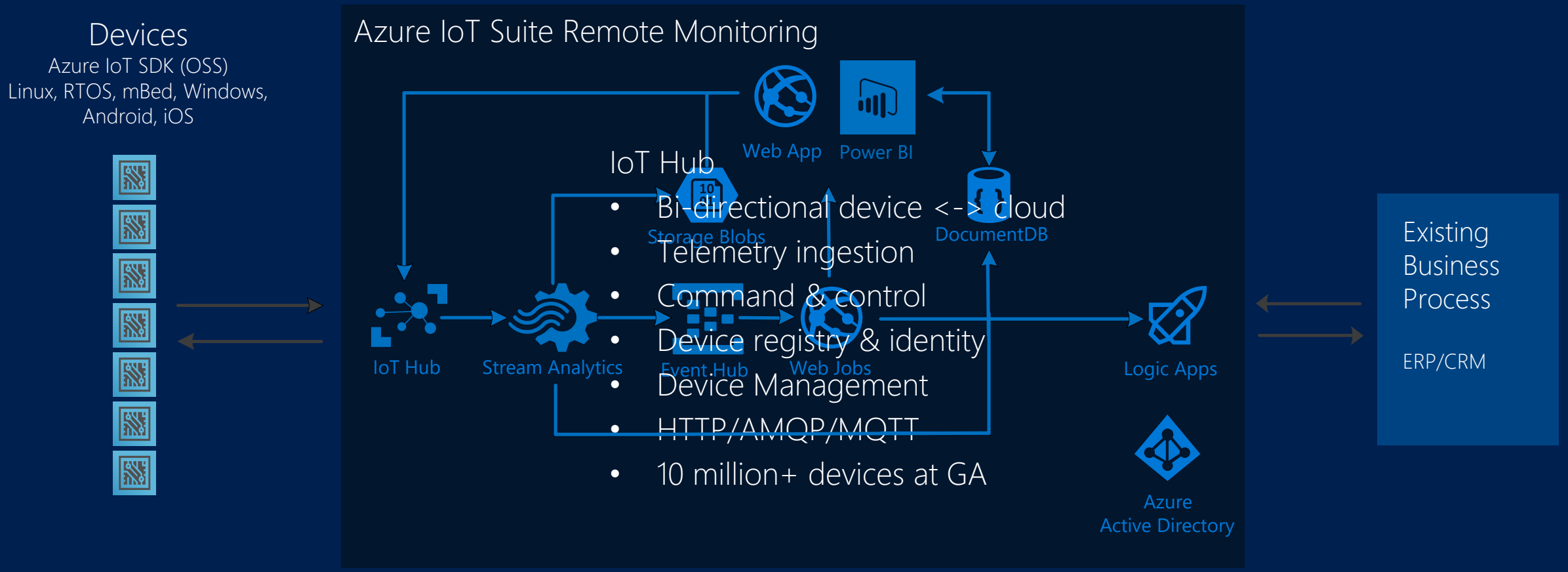
# IoT Hub


IP-capable
PAN-devices
Field gateway
Cloud protocol gateway
IoT Hub
Event processing and insight (e.g. hot and cold paths)
Device business logic, Connectivity monitoring
Application device provisioning and management
field
cloud

# IoT Hub endpoints



# Remote Monitoring Service Architecture



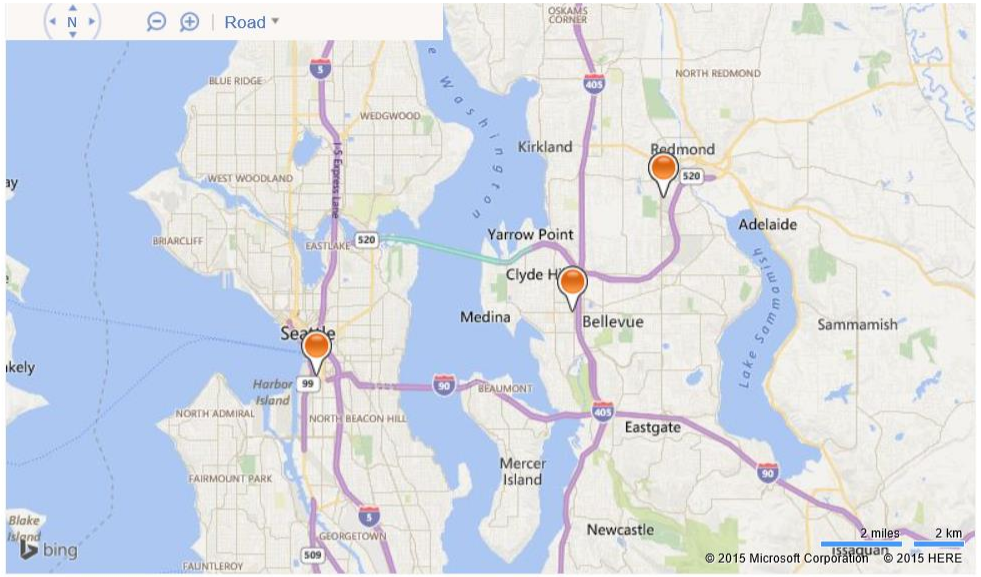
InPrivate | IoT Device Portal - Dash

stevehobiotdemo.azurewebsites.net/Dashboard/Index

Microsoft Azure IoT Suite | StevehobIoTDemo

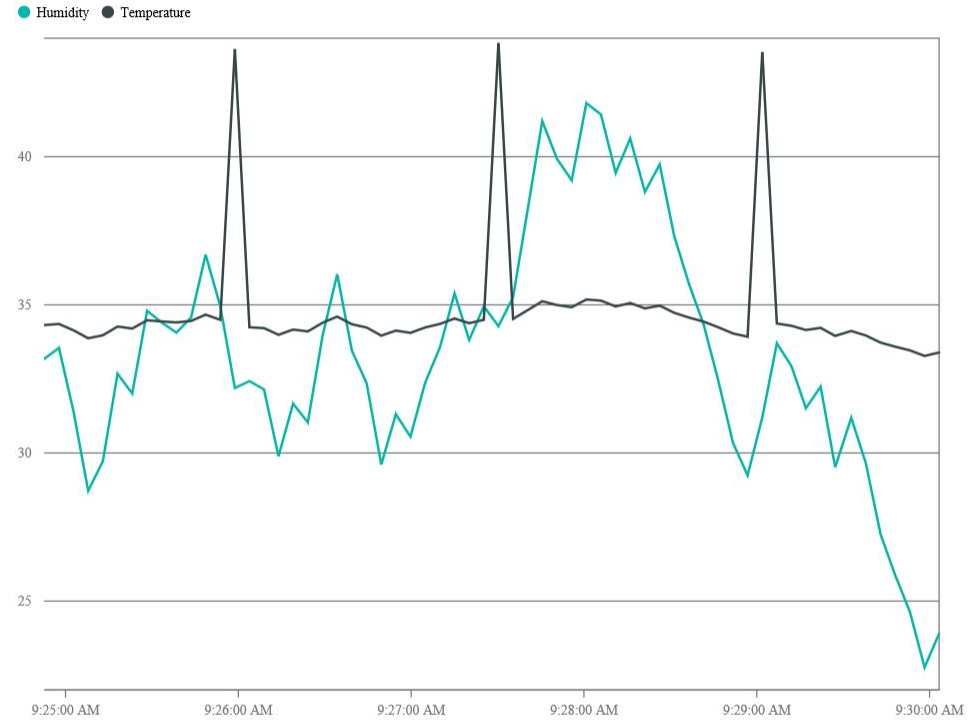
stevehob@iots01.onmicrosoft.com
ADMINISTRATOR
Sign Out

DASHBOARD
DEVICES
RULES
ACTIONS
ADD A DEVICE




Device to View: SampleDevice001_967

## Telemetry History

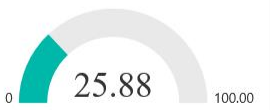



## Alarm History

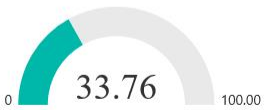
| TIME | DEVICE ID | RULE OUTPUT | VALUE |
|---|---|---|---|
| 09/26/2015 9:29:01 AM | SampleDevice001_967 | AlarmTemp | 43.540 |
| 09/26/2015 9:29:01 AM | SampleDevice001_967 | AlarmHumidity | 31.201 |
| 09/26/2015 9:27:30 AM | SampleDevice001_967 | AlarmTemp | 43.848 |
| 09/26/2015 9:27:30 AM | SampleDevice001_967 | AlarmHumidity | 34.283 |
| 09/26/2015 9:25:58 AM | SampleDevice001_967 | AlarmTemp | 43.639 |
| 09/26/2015 9:25:58 AM | SampleDevice001_967 | AlarmHumidity | 32.192 |
| 09/26/2015 9:24:26 AM | SampleDevice001_967 | AlarmTemp | 43.332 |
| 09/26/2015 9:24:26 AM | SampleDevice001_967 | AlarmHumidity | 29.125 |

Max of device humidity


Min of device humidity



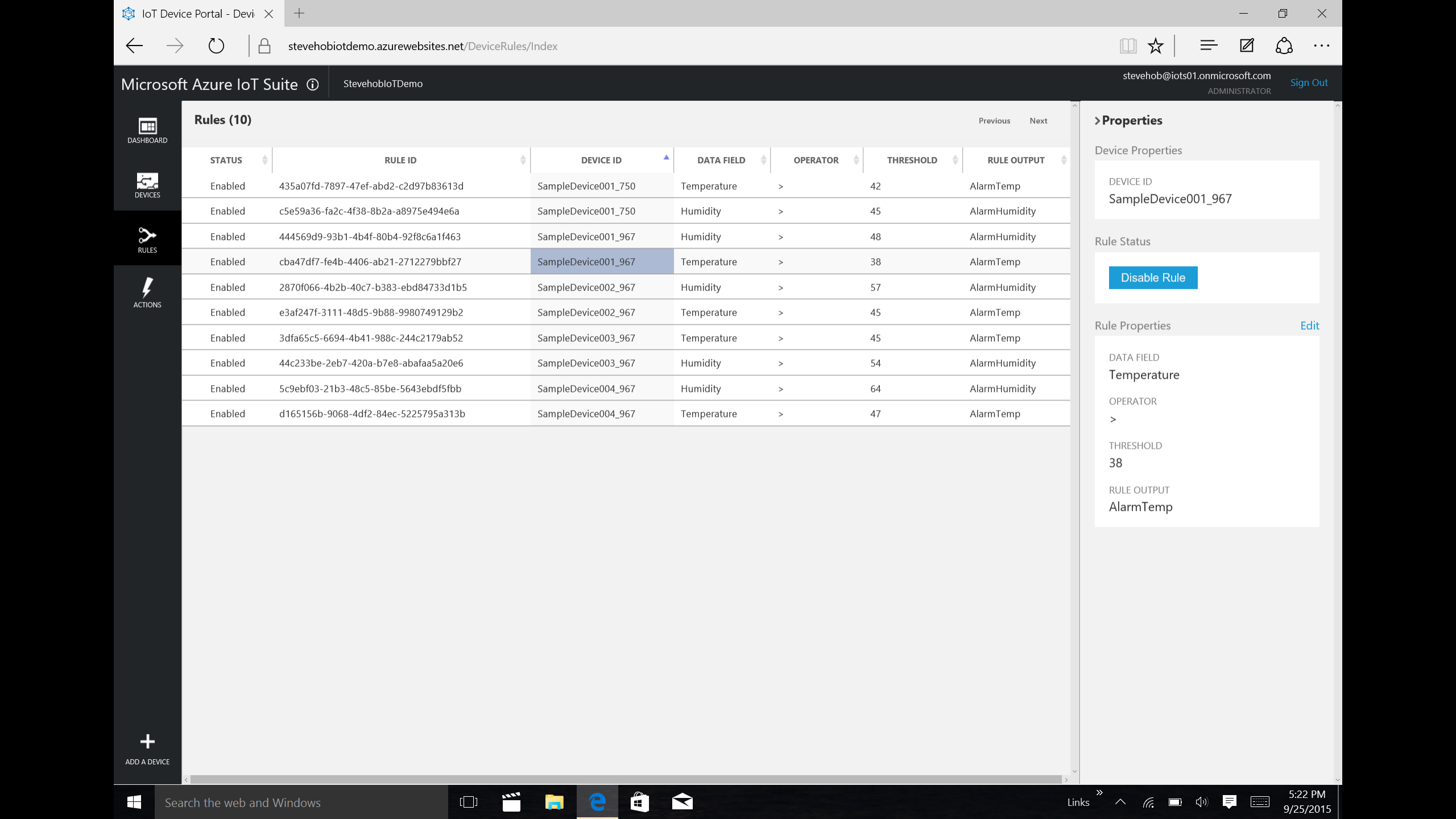

Average of device humidity




Search the web and Windows

Links

9:30 AM
9/26/2015


IoT Device Portal - Devi
stevehobiotdemo.azurewebsites.net/DeviceRules/Index
Microsoft Azure IoT Suite
StevehobIoTDemo
stevehob@iots01.onmicrosoft.com
ADMINISTRATOR
Sign Out
DASHBOARD
DEVICES
RULES
ACTIONS
ADD A DEVICE
Rules (10)
Previous
Next
STATUS
RULE ID
DEVICE ID
DATA FIELD
OPERATOR
THRESHOLD
RULE OUTPUT
Enabled 435a07fd-7897-47ef-abd2-c2d97b83613d SampleDevice001_750 Temperature > 42 AlarmTemp
Enabled c5e59a36-fa2c-4f38-8b2a-a8975e494e6a SampleDevice001_750 Humidity > 45 AlarmHumidity
Enabled 444569d9-93b1-4b4f-80b4-92f8c6a1f463 SampleDevice001_967 Humidity > 48 AlarmHumidity
Enabled cba47df7-fe4b-4406-ab21-2712279bbf27 SampleDevice001_967 Temperature > 38 AlarmTemp
Enabled 2870f066-4b2b-40c7-b383-ebd84733d1b5 SampleDevice002_967 Humidity > 57 AlarmHumidity
Enabled e3af247f-3111-48d5-9b88-9980749129b2 SampleDevice002_967 Temperature > 45 AlarmTemp
Enabled 3dfa65c5-6694-4b41-988c-244c2179ab52 SampleDevice003_967 Temperature > 45 AlarmTemp
Enabled 44c233be-2eb7-420a-b7e8-abafaa5a20e6 SampleDevice003_967 Humidity > 54 AlarmHumidity
Enabled 5c9ebf03-21b3-48c5-85be-5643ebdf5fbb SampleDevice004_967 Humidity > 64 AlarmHumidity
Enabled d165156b-9068-4df2-84ec-5225795a313b SampleDevice004_967 Temperature > 47 AlarmTemp
Properties
Device Properties
DEVICE ID
SampleDevice001_967
Rule Status
Disable Rule
Rule Properties
Edit
DATA FIELD
Temperature
OPERATOR
>
THRESHOLD
38
RULE OUTPUT
AlarmTemp
Search the web and Windows
Links
5:22 PM
9/25/2015