



# Securing Your IoT Applications and how to mitigate emerging IoT attacks

PRESENTED BY:

Nigel Ashworth

Solution Architect EMEA

WE MAKE APPS



FASTER.  
SMARTER.  
SAFER.

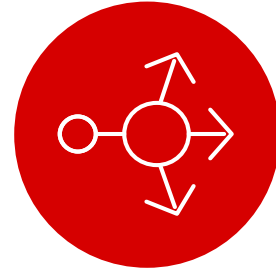
# Agenda



**IoT Threats**



**Seven Layers  
of IoT Security**



**IoT Use Cases**



**Summary**



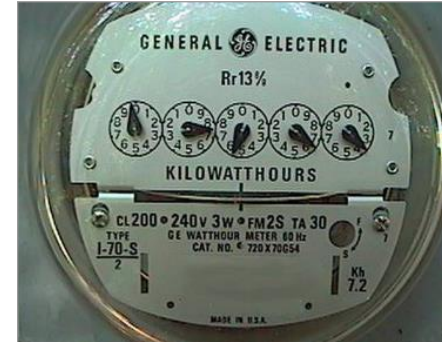
# Innovation and Technology Transformation



TRANSPORTATION



MANUFACTURING



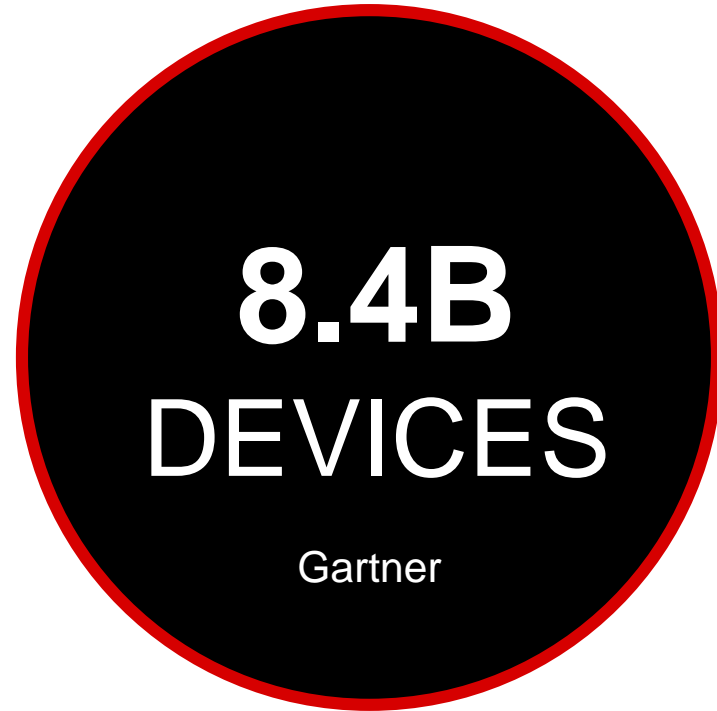
UTILITIES



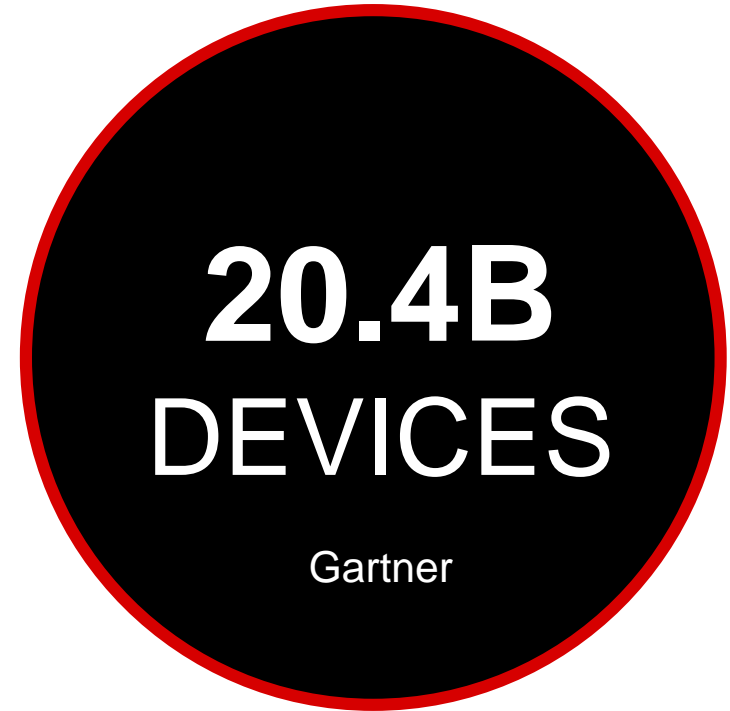
AGRICULTURE



# IoT Growth Predictions – Gartner



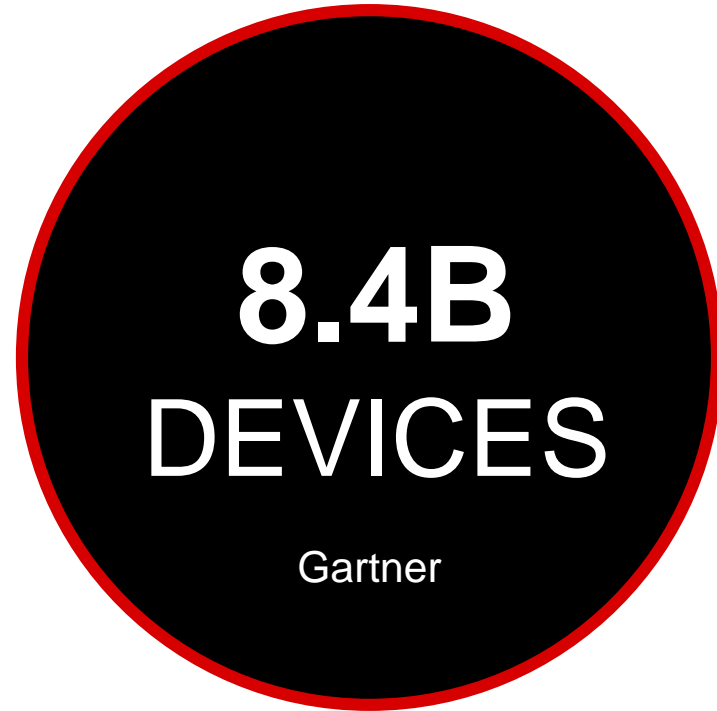
**2017**



**2020**

\*Excludes smartphones, tablets, and computers

# IoT Growth Predictions – IDC



**2017**



**2020**

\*Excludes smartphones, tablets, and computers

# IoT Growth Predictions – SoftBank



**2017**

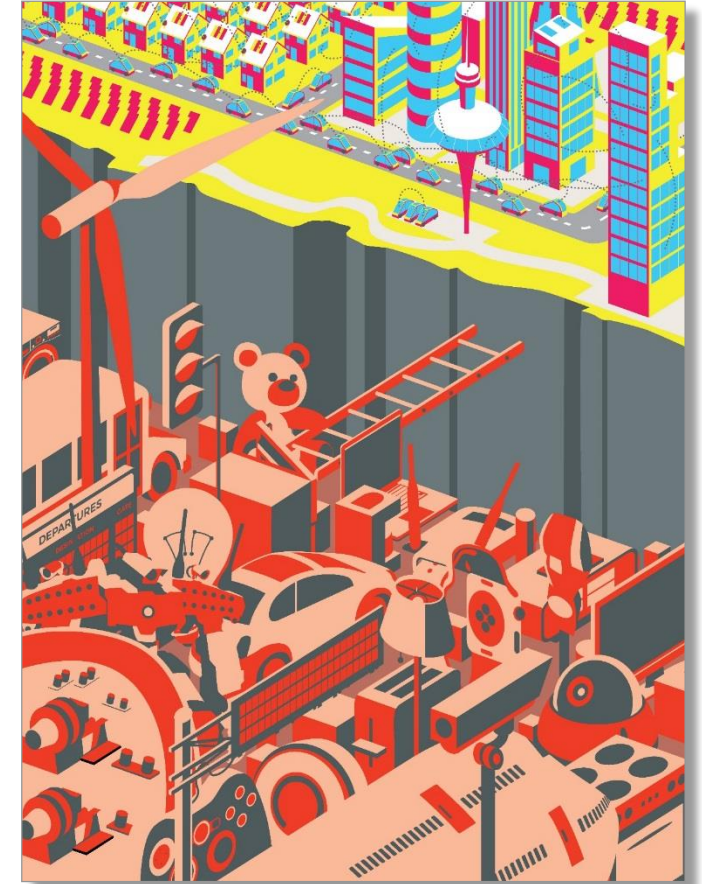
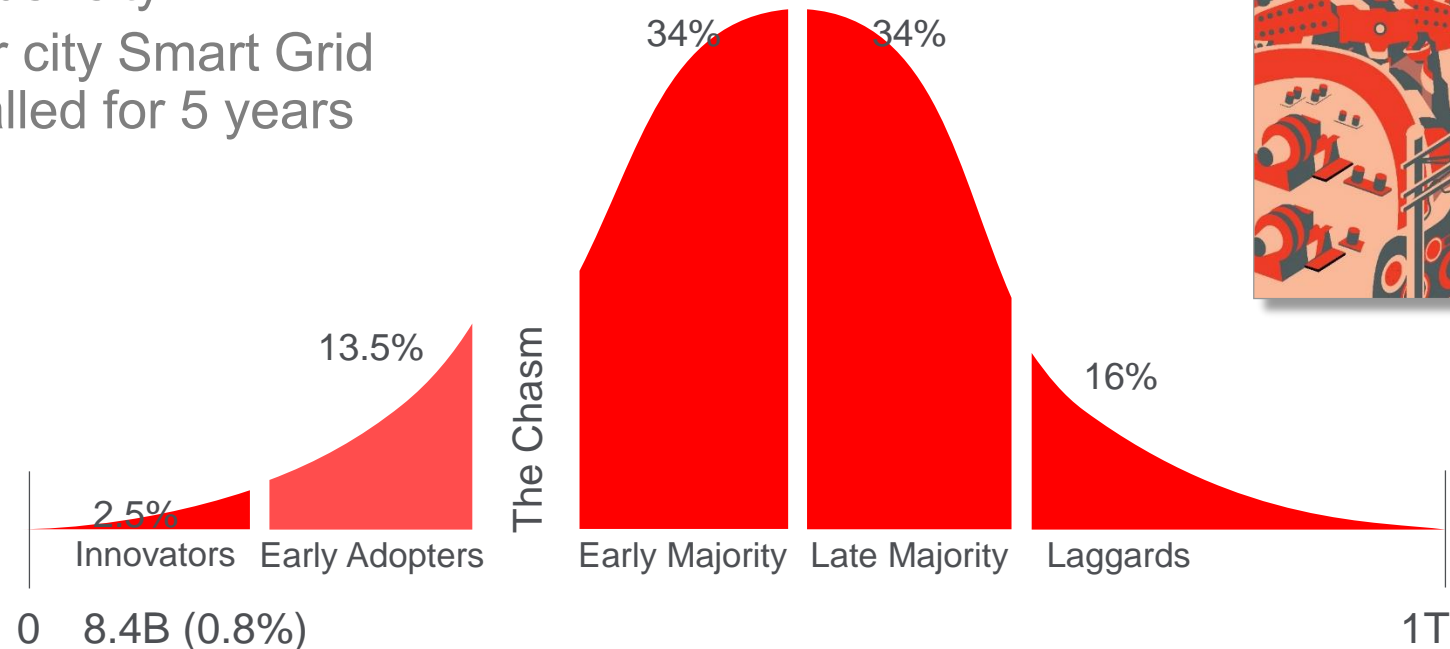


**2035**

\*Excludes smartphones, tablets, and computers

# Market Adoption?

- **50% of global population is online**
  - Home IoT still early adoption
- **Smart cities still early adoption**
  - One or two sub-systems deployed per city
  - One major city Smart Grid project stalled for 5 years





# IOT THREATS

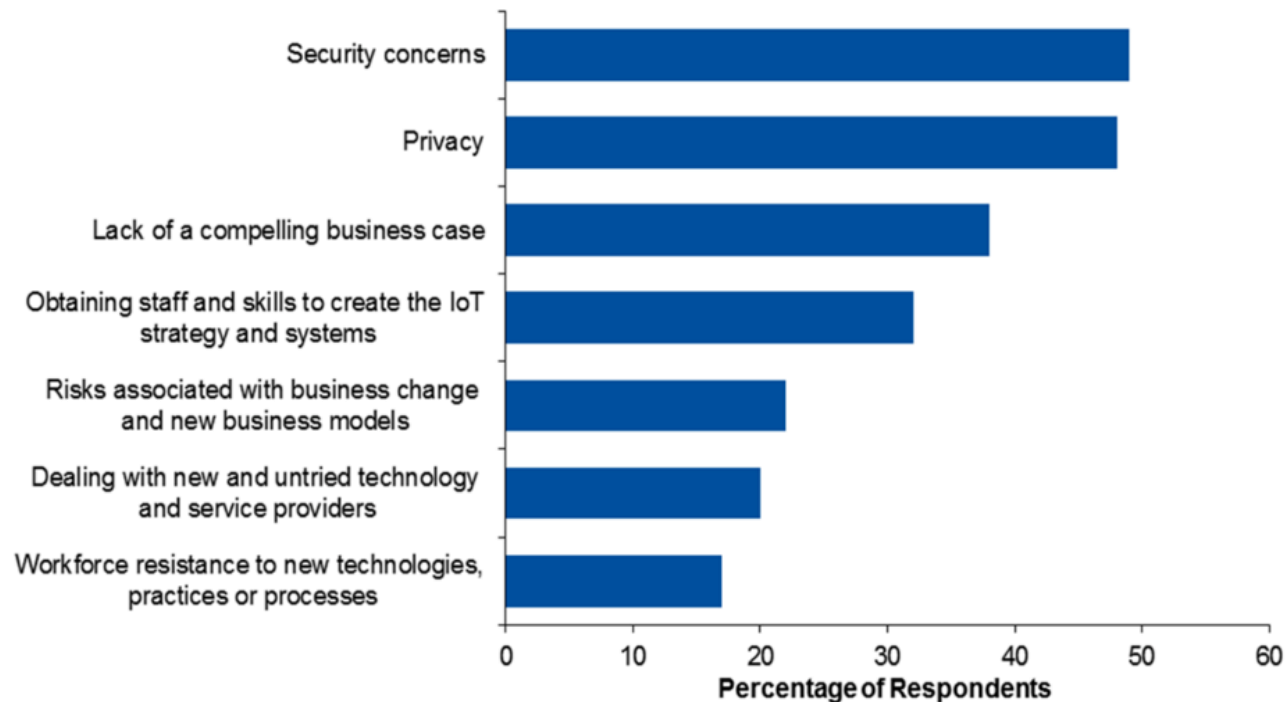




# IoT Adoption – Importance of Security

Enterprises:

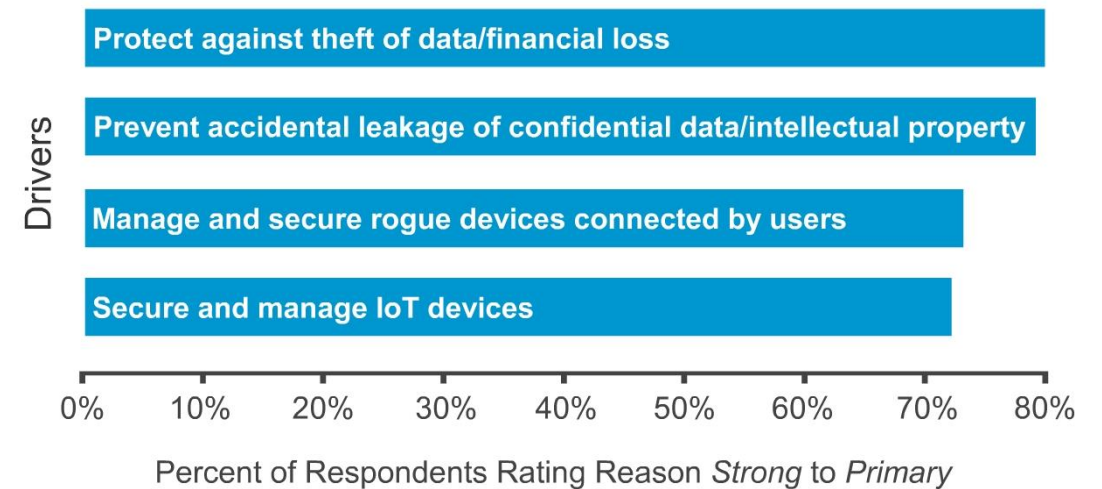
What are the key inhibitors to IoT adoption?



Source: Gartner

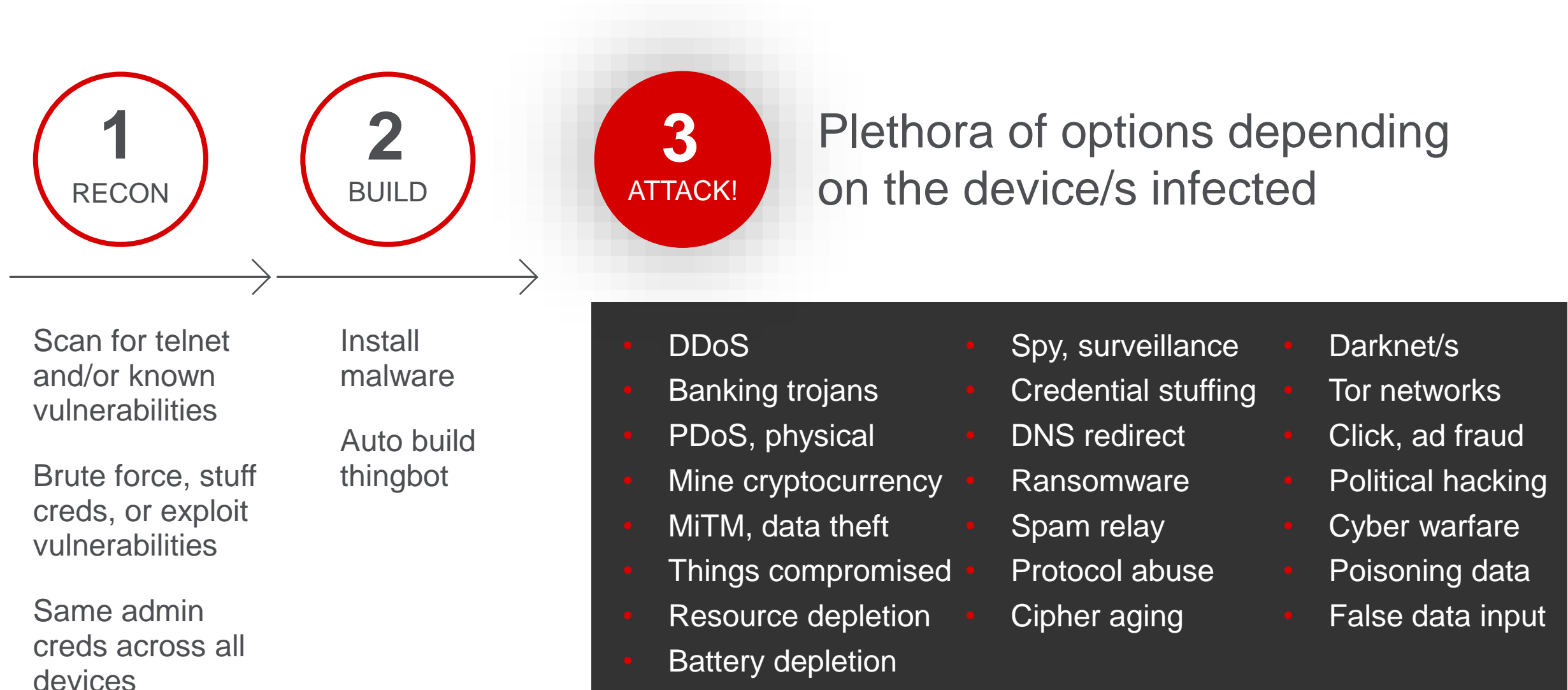
Enterprises:

Which factors drive your decision to purchase security solutions for mobile and IoT devices?

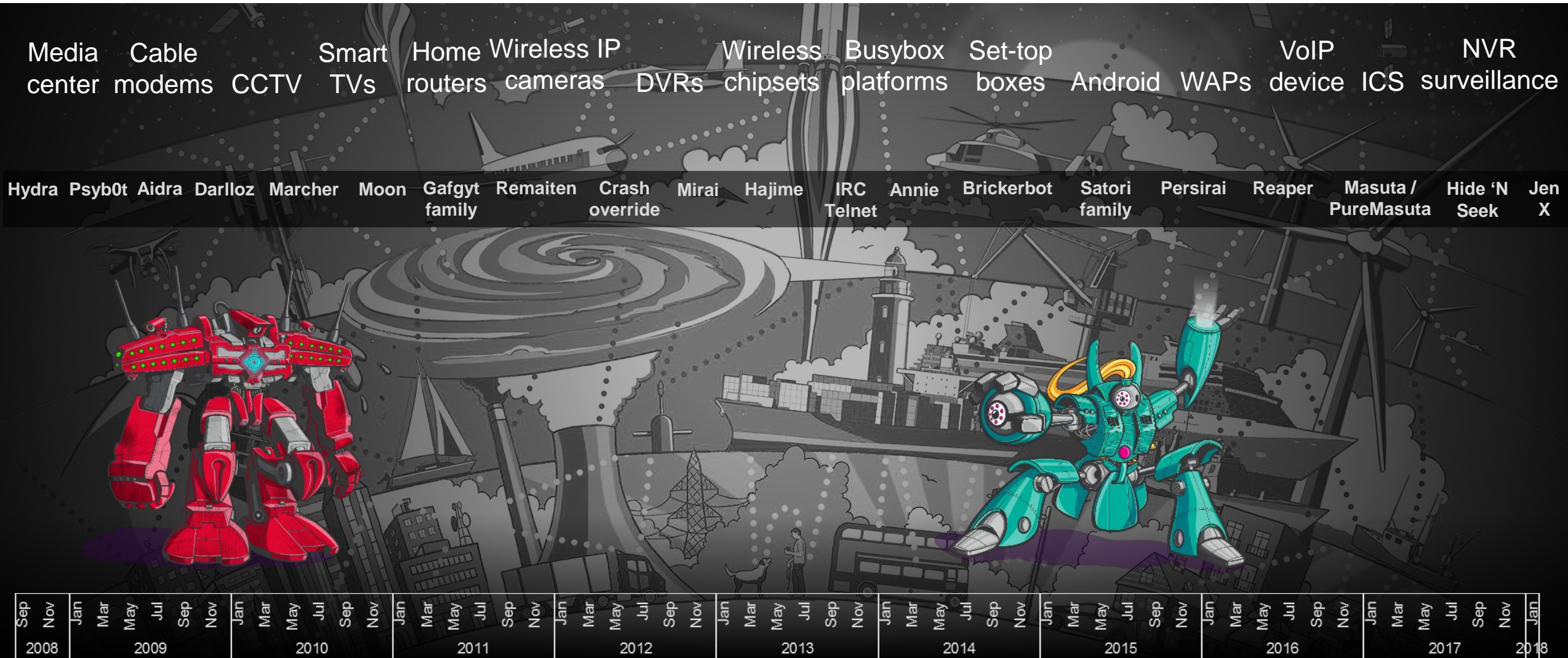


Source: Infonetics Research

# Typical IoT Attack Path

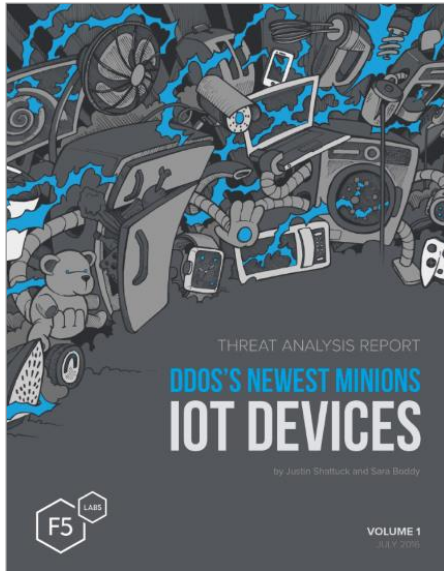


# Thingbots Have Been Hiding In Plain Sight





# The Hunt for IoT Research Evolution



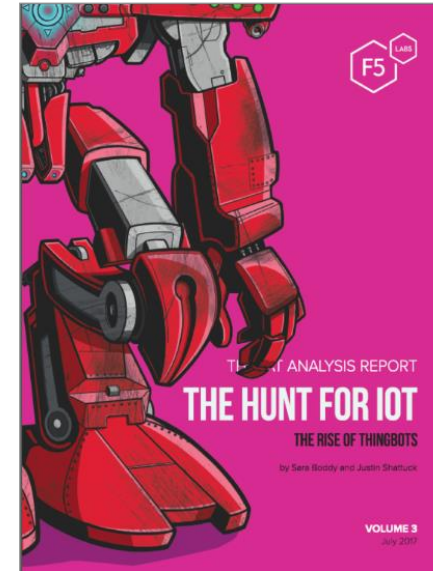
*DDoS's Newest Minions:  
IoT Devices*

- Telnet brute force attacks compromise “things” that launch damaging DDoS attacks



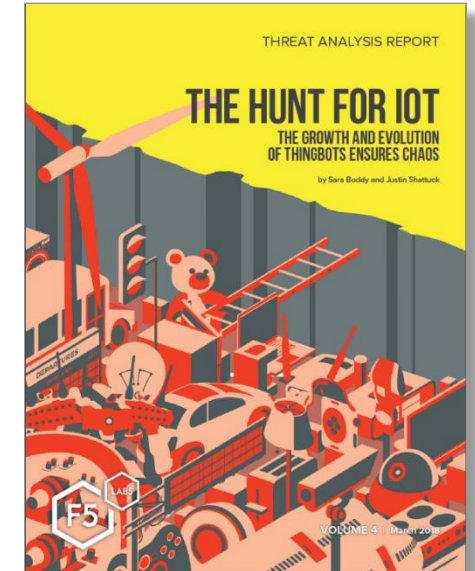
*Building Death Star-sized  
Botnets from IoT Minions*

- Hunt for IoT is exponentially increasing
- Published networks behind the attacks



*The Rise of Thingbots*

- Profiling thingbots, the attacker infrastructure of the future
- New thingbots being developed based on source traffic industry

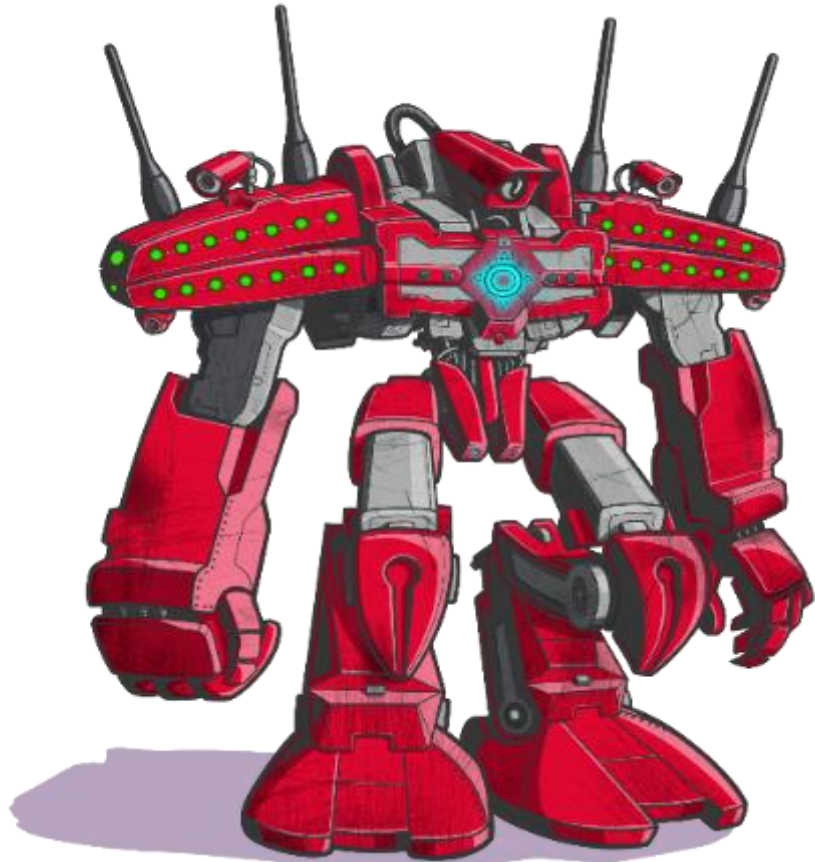


*The Growth and Evolution of  
Thingbots Ensures Chaos*

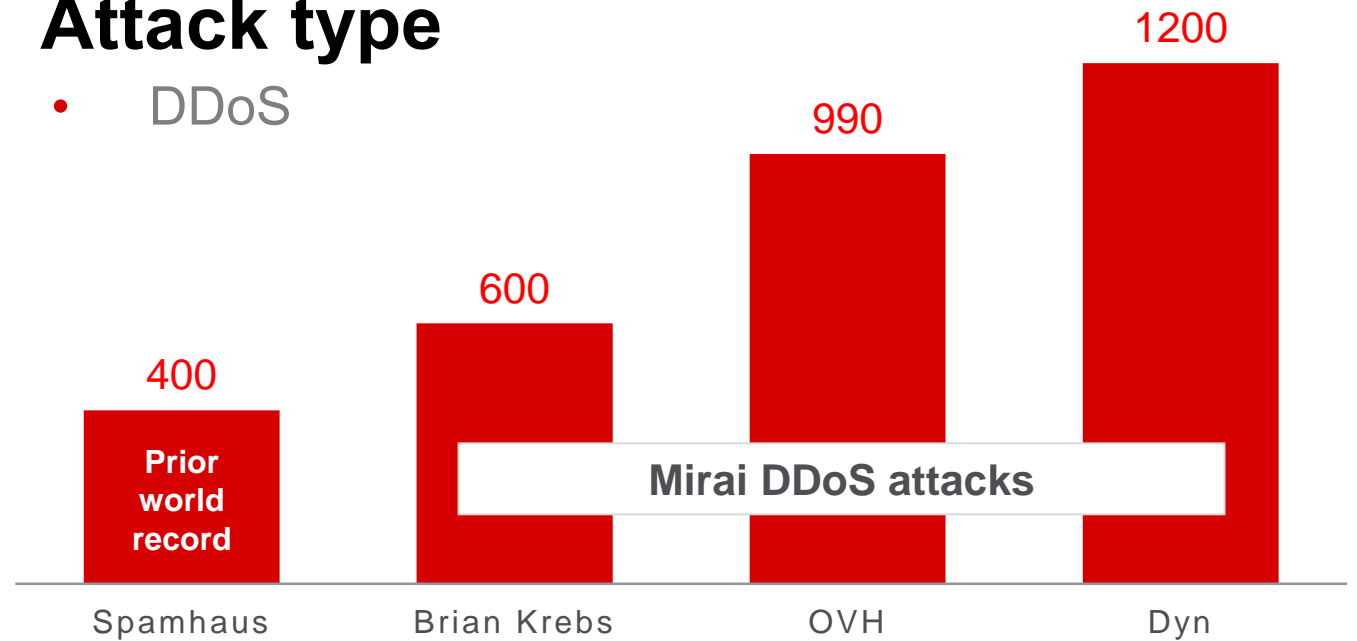
- Attackers evolving methods
- No slowing down thingbots
- Published attacking IPs



# IoT Compromises Are Common



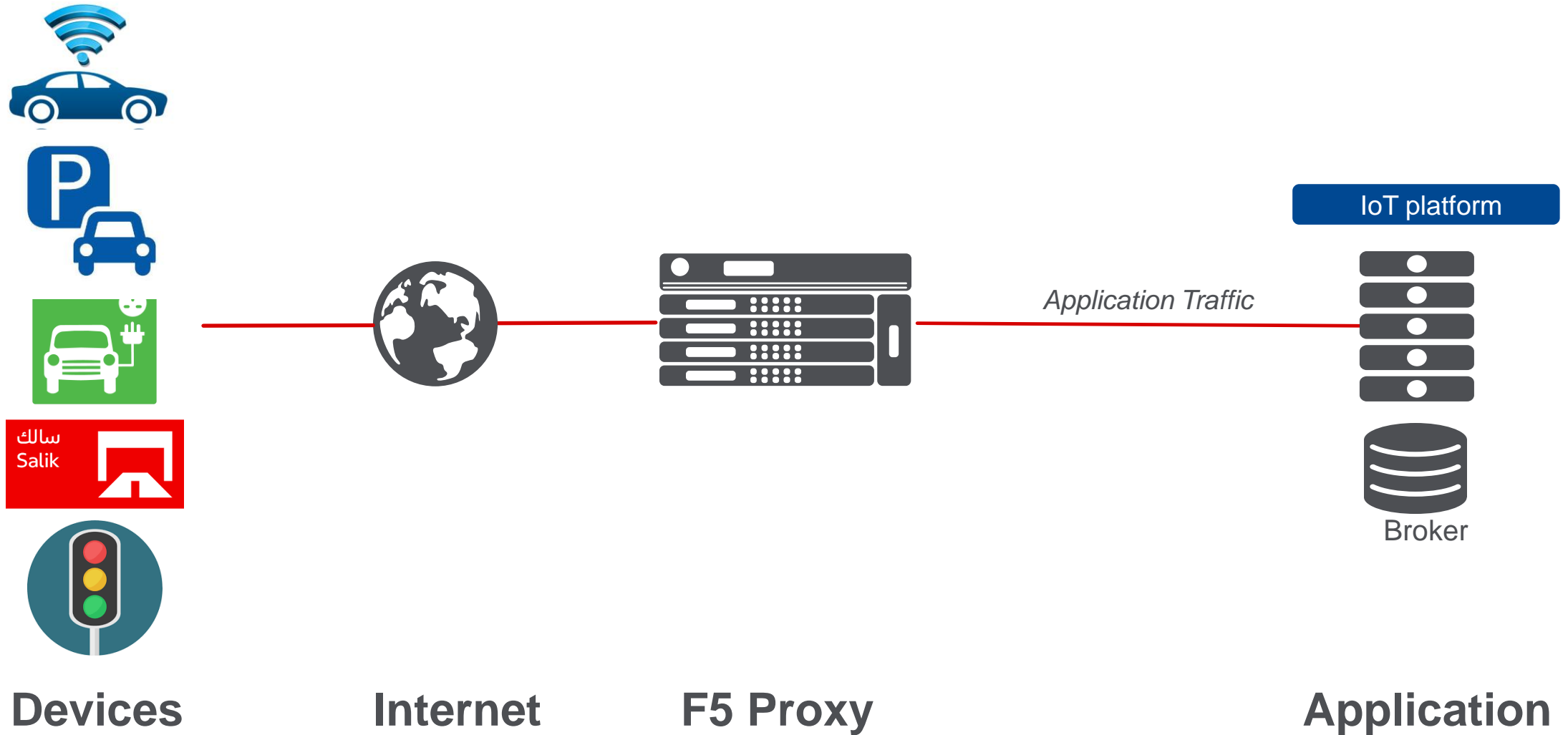
- **Mirai**
- **IoT devices**
  - DVR, IP cameras, and wireless routers
- **Attack type**
  - DDoS



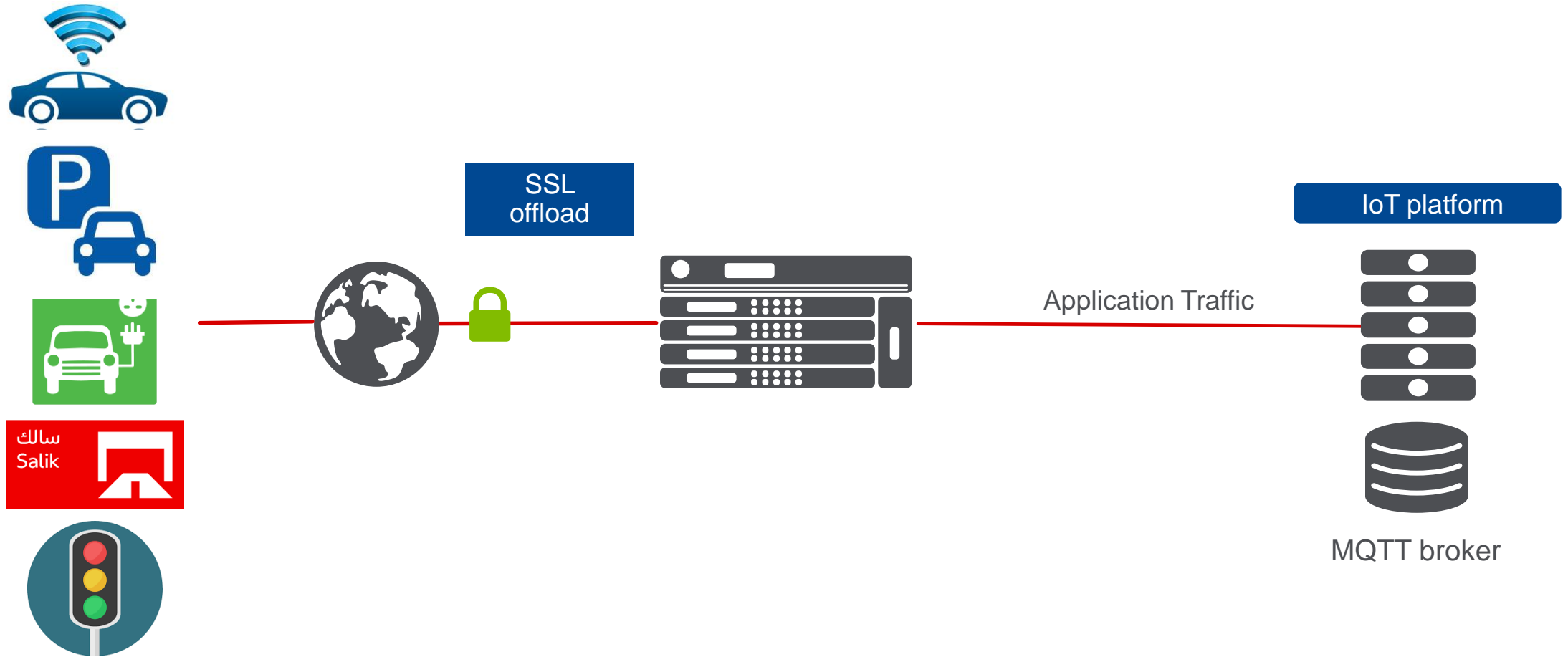
# SEVEN LAYERS OF IOT SECURITY



# Seven Layers of IoT Security



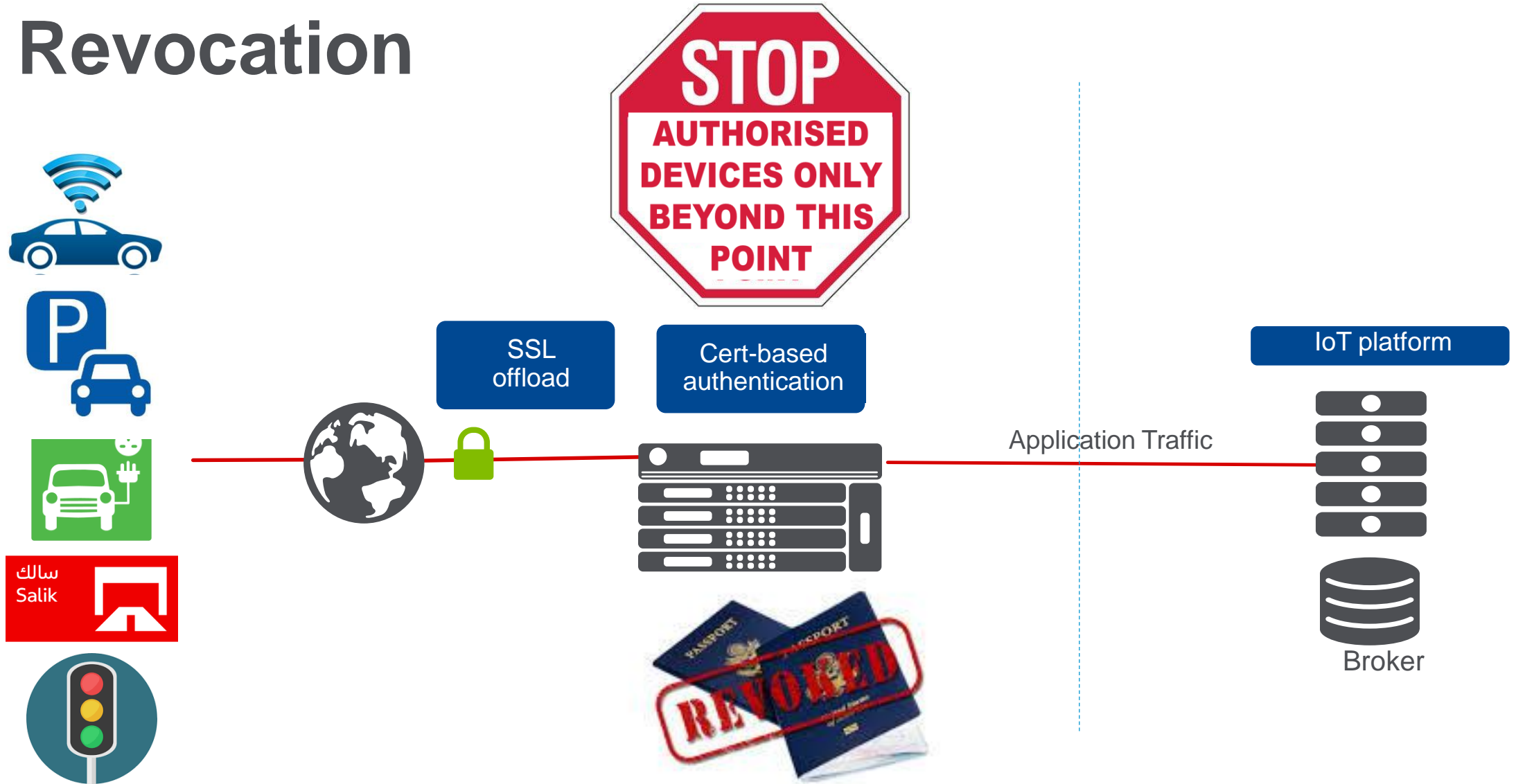
# 1. Transport



SSL everywhere, avoid man in the middle



## 2. Revocation



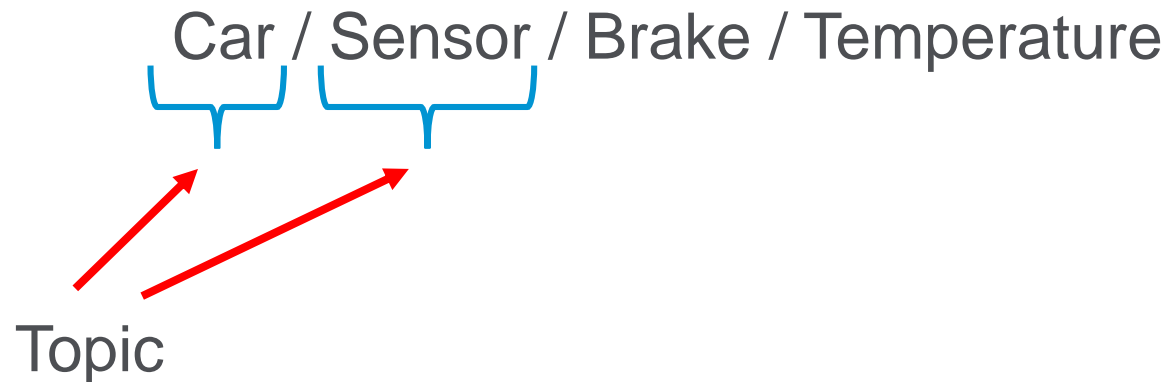
Manage devices – Good / bad / expired / compromised devices

# 3. Inspection

Field Name	Value Selection
Type	Standard
Service port	Either type or select MQTT service port
Configuration	Advanced
Protocol	TCP
MQTT	Click to enable MQTT

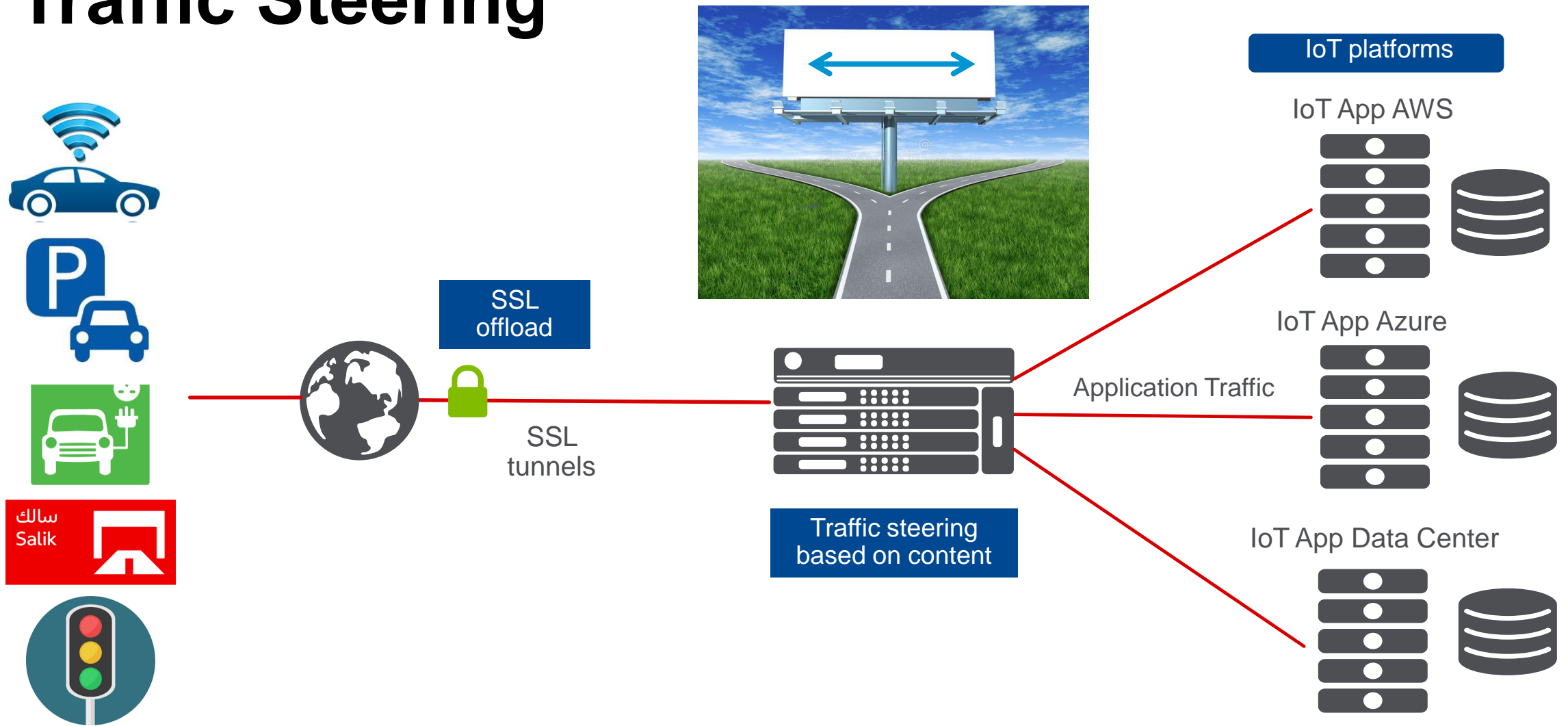
Car / Sensor / Brake / Temperature

Topic

A diagram illustrating the MQTT topic structure. The text 'Car / Sensor / Brake / Temperature' is shown. Below it, blue brackets group 'Car' and 'Sensor' together, and 'Brake' and 'Temperature' together. Two red arrows point from the word 'Topic' to the first bracket (under 'Car') and the second bracket (under 'Sensor').

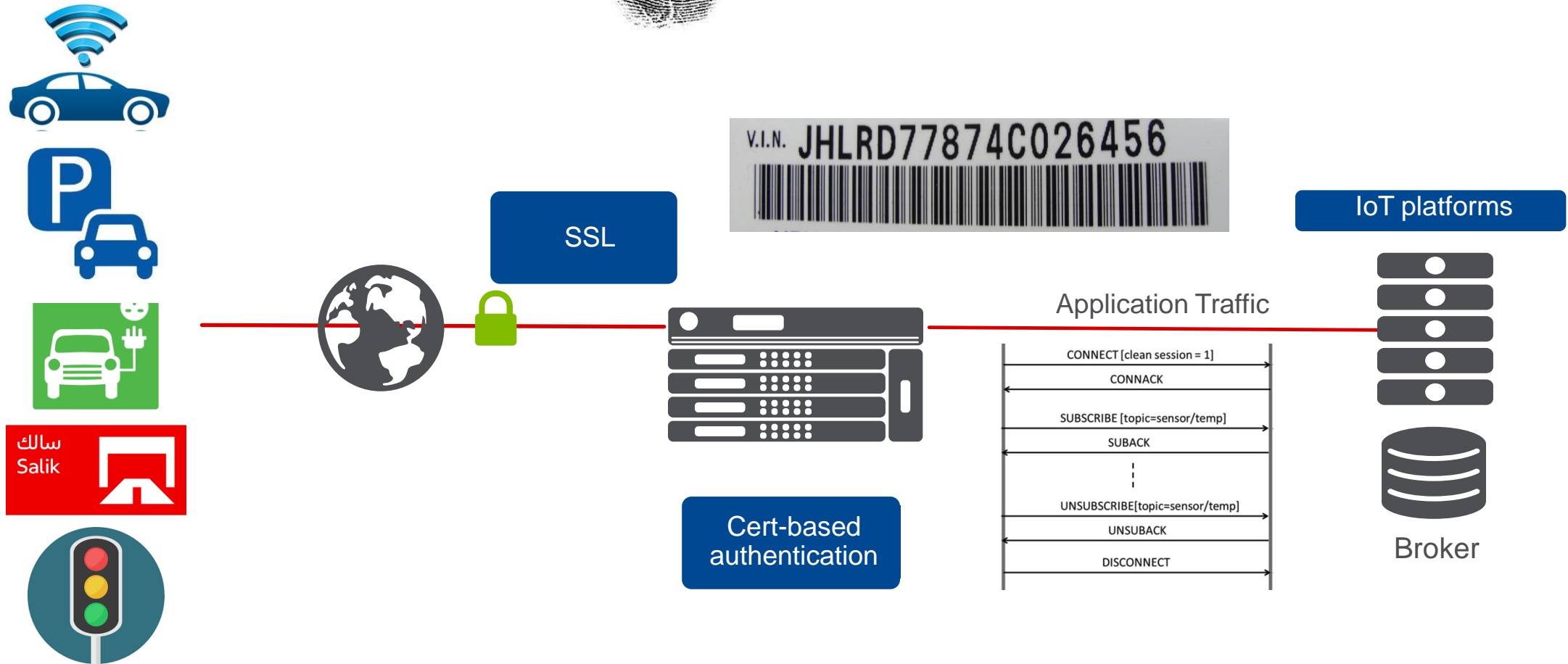
Inspect and Enforce – Device topics – what do you allowed to see

# 4. Traffic Steering



Traffic steering to cloud, on-premises, hybrid, multi-cloud

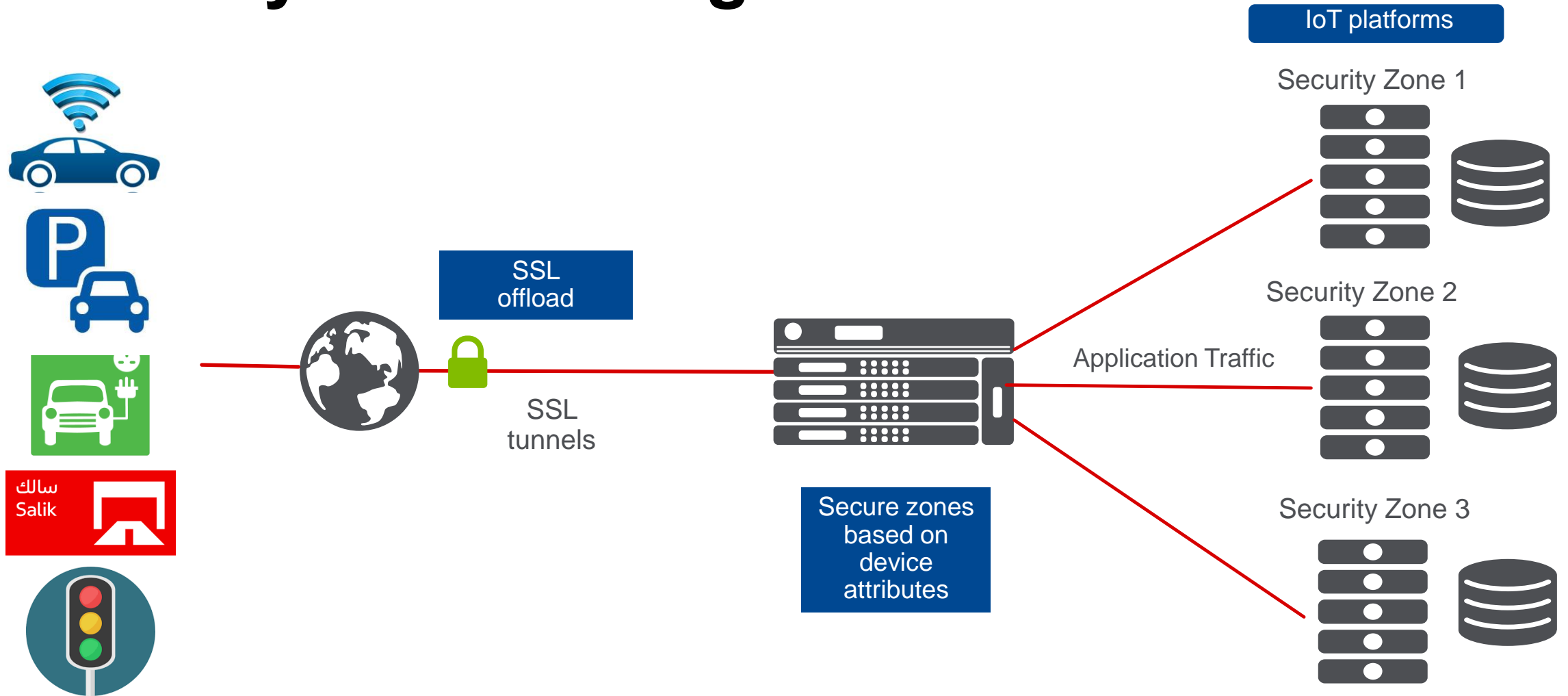
# 5. Authentication



**Do not rely on passwords: Use common name from the certificate in the headers to authenticate to the backend IoT application**



# 6. Security Zone Management



Agility to create different security zones, per group of devices or types of devices

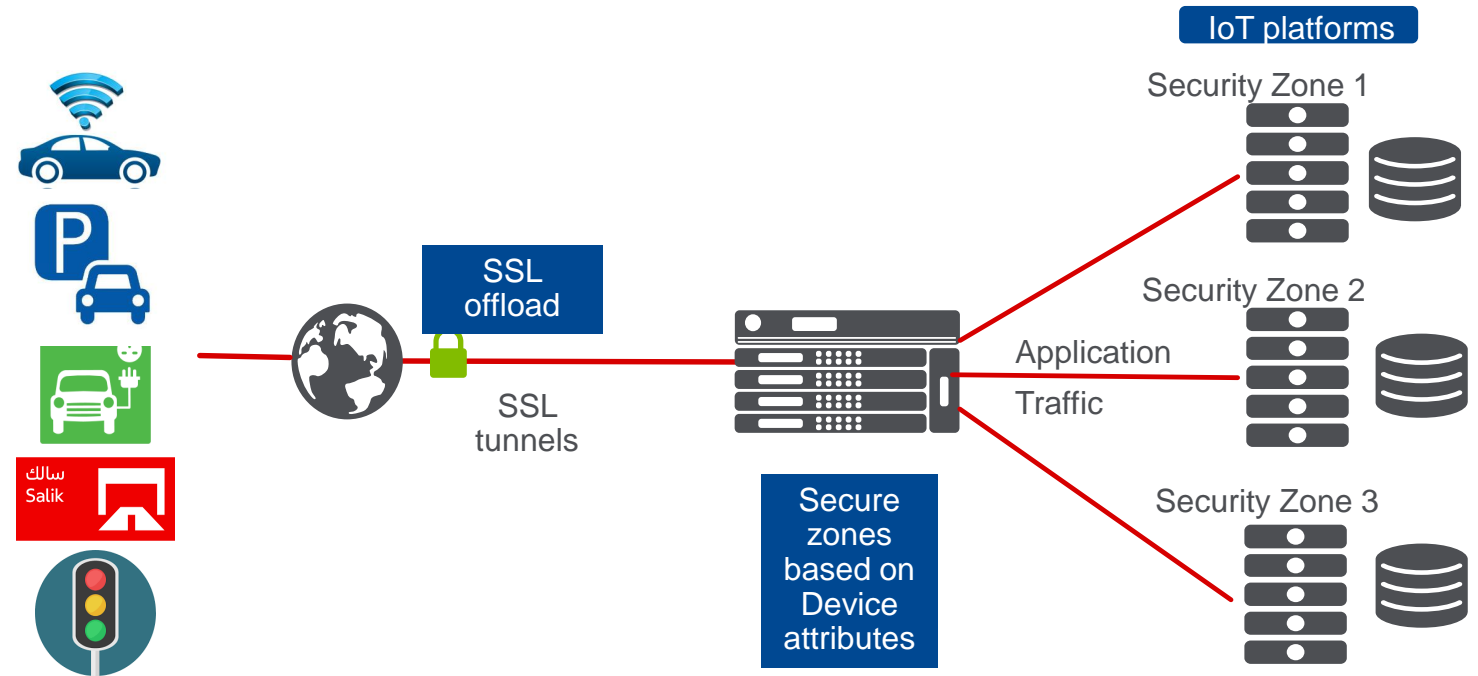
# 7. IoT Language (Protocols)

Verticals	MQTT	CoAP	AMQP	XMPP	HTTP	HTTP 2.0	WebSkt	LWM2M
<b>Manufacturing</b> Factories, Mining	●	●			●	●		●
<b>Utilities</b> Energy	●	●			●			●
<b>Smart Spaces</b> Home, Building, City	●	●		●			●	
<b>Transportation</b> Cars, Public Transit	●				●	●	●	●
<b>Platform Providers</b> Cloud, Service, Integration	●	●	●	●	●	●		

MQTT – Message Queuing Telemetry Transport  
CoAP – Constrained Application Protocol  
XMPP – Extensible Messaging and Presence Protocol  
AMQP – Advanced Message Queuing Protocol

# Seven Layers of IoT security

- Transport
- Revocation
- Inspection
- Traffic steering
- Authentication
- Zone Management
- Protocol



*... all of this makes up an IoT Firewall for your IoT applications and services*

# IOT USE CASES

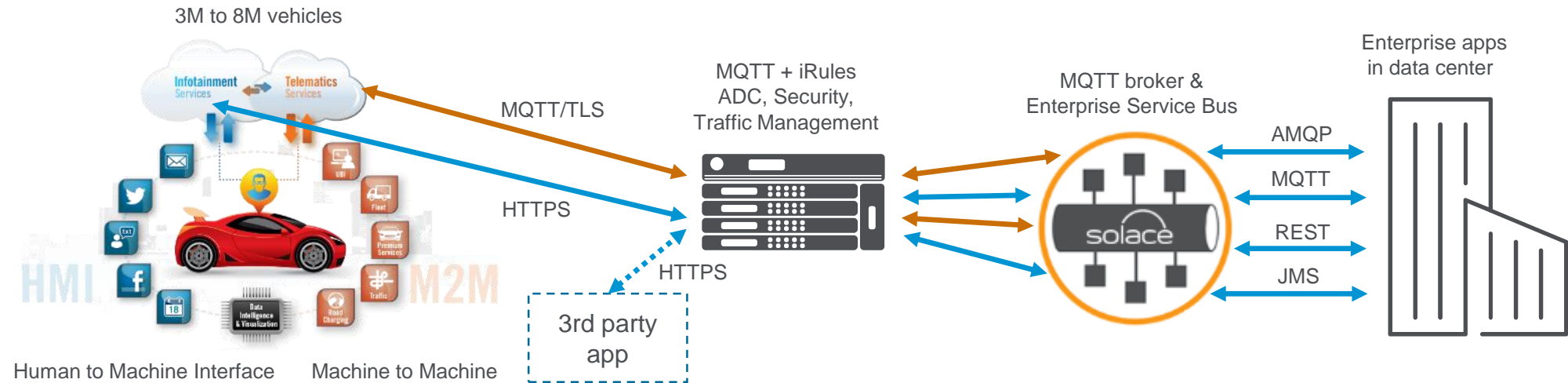




# Transportation

## Connected cars

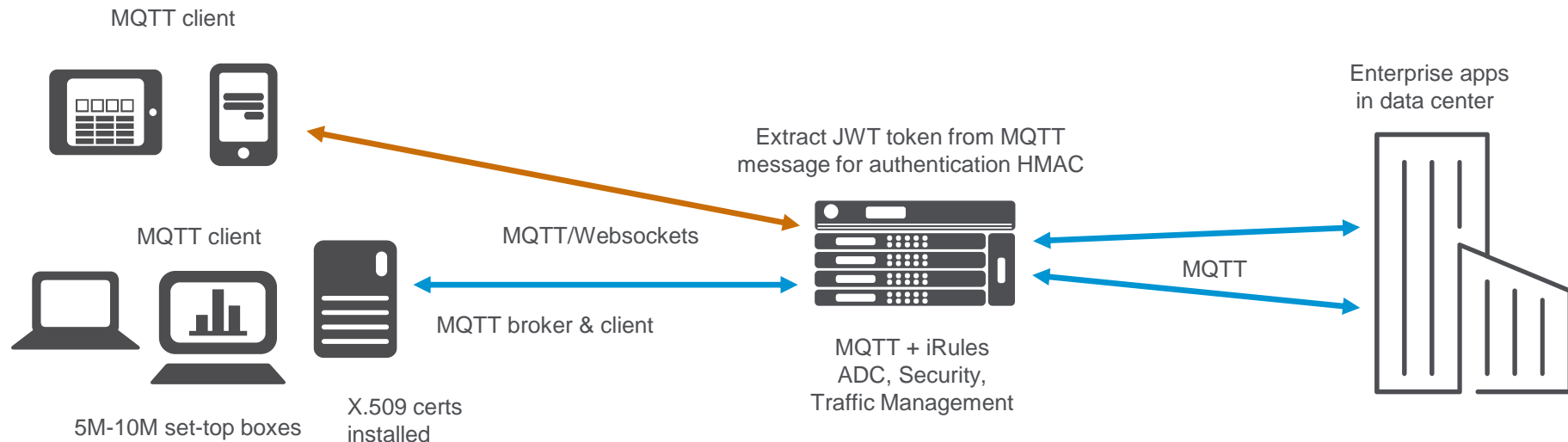
- Secure data transport to car
- Revocation of car
- Long term cipher management
- Car segmentation (class, models)
- Scaling brokers
- Broker protection
- Availability, failover, recovery



# Smart Entertainment

## Connected box

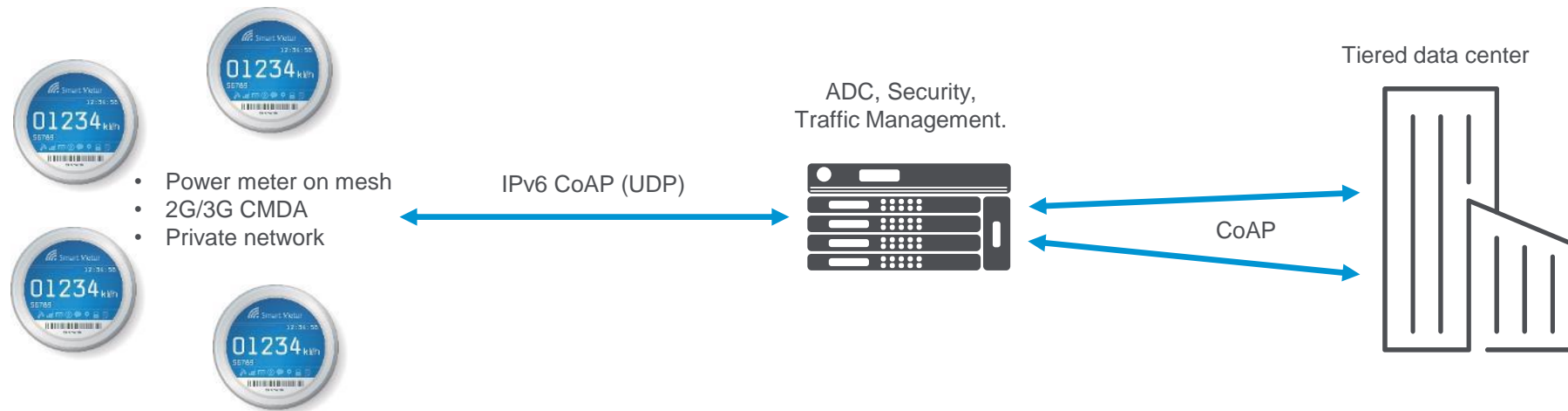
- Certificate management OCSP / HMAC
- MQTT traffic steering
- Management of set top boxes and client devices
- MQTT for maximum efficiency
- New and existing set top boxes
- Quality of service for customers
- Scale globally
- MQTT over Websockets



# Utilities

## Power meters

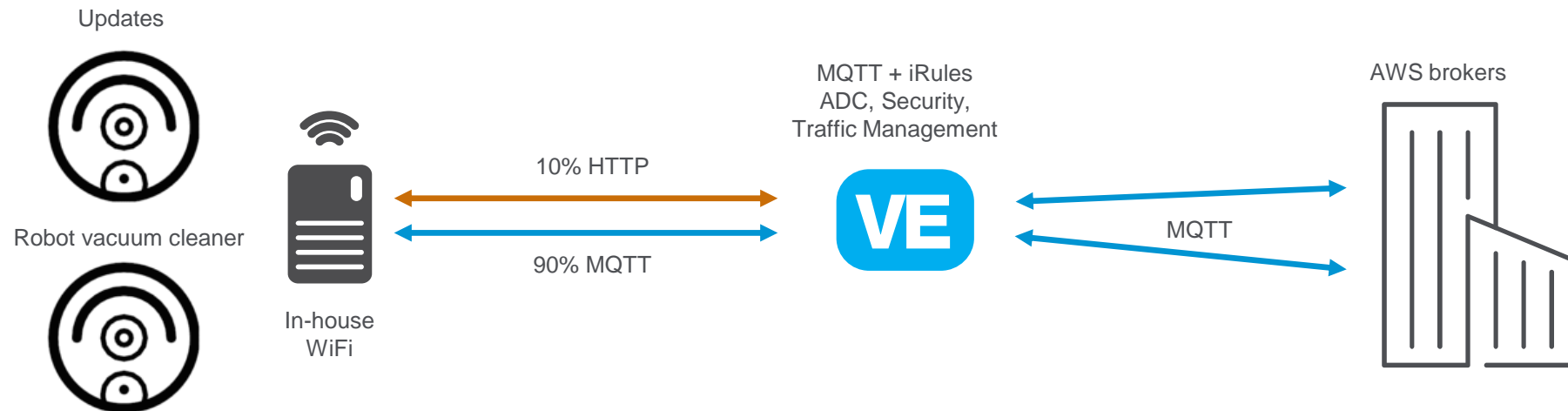
- Millions of smart meters
- Energy efficiency the key driver
- Gas, electricity, and water meters
- Software, hub, and meter provider



# Manufacturing

## Vacuum cleaners

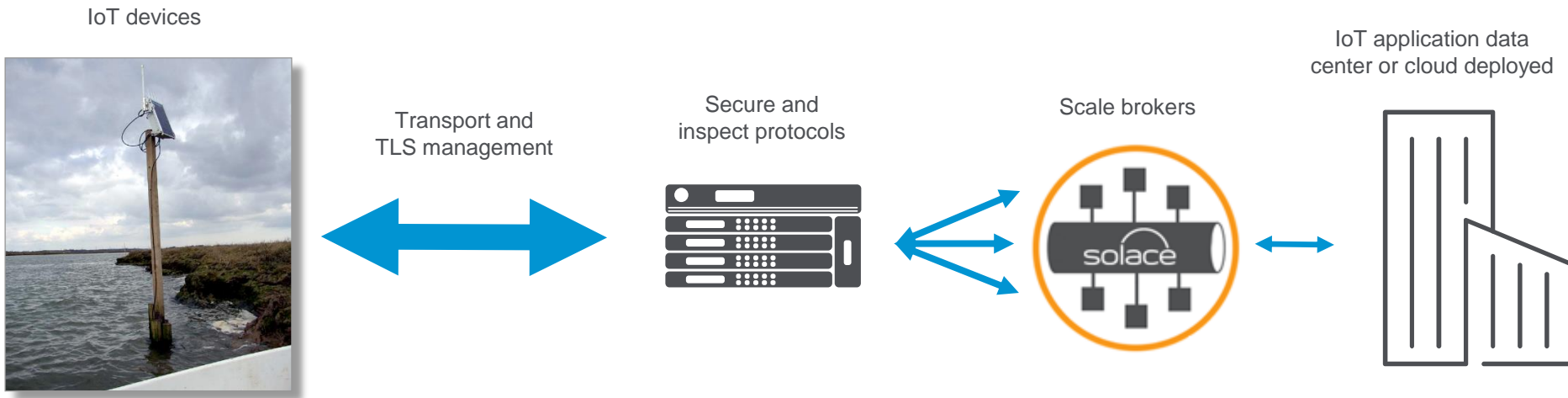
- **Scale – How many**
- **Secure transport and broker authentication**
- **Broker security**
- **HTTP and MQTT**
- **Maintenance, servicing, lifespan**



# Environmental

## Secured IoT

- **Certificate or token checking / revocation**
- **Water temperature limits**
- **Cyclic learning day and night**
- **Sensor reputation**
- **Logging on lost sensors**





# SUMMARY



# How to Secure Your IoT Applications

- **Your project, Your application, Your business**
- **Plan ahead – Architect in or architect after**
- **Best practice – Seven layers of IoT security**



WE MAKE APPS



FASTER. SMARTER. SAFER.