100+ Billion Devices
IoT Challenges and Considerations

Roger N. Mahler

Sr. Spec Systems Design Engineer

Atlanta, GA

Growth of IoT

The growth of the Internet of Things, or more specifically connecting everything to the internet has been a aspiration almost since the invention of the internet. It wasn't until recently that this vision has grown into a reality.

This has been fueled by five key drivers by two differet types of developers:

- Cheap Hardware
- Open Source Technologies (Tools and Platforms)
- Proliferation of Inexpensive and Free Wireless Connectivity
- New computing models (Local, Fog & Edge Computing)
- Extremely long lifespan (10+ years)

The Wild West wasn't this wild!!!

Sheer Scale of the problem

It is estimated that by 2025 there will be between 74.5 Billion and 100 Billion IoT devices worldwide:

100,000,000,000 Devices

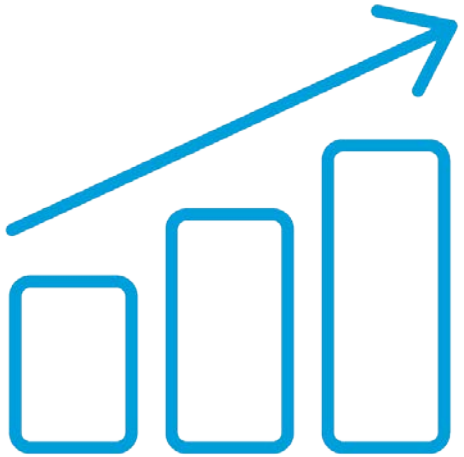
333 devices a second until 2025

The current methods used in deploying both the devices, and the services that run on the devices are inadequate for this scale. This presentation will look at potential concepts around:

1. Rolling out at scale
2. Security at Scale
3. Lifecycle Management
4. Data Management

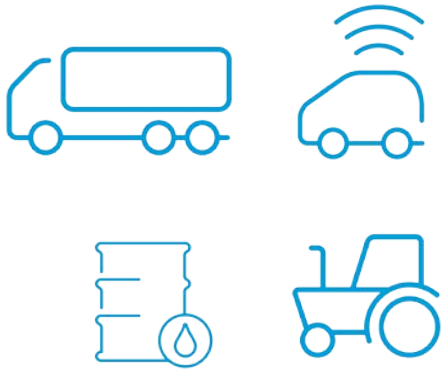
IoT Momentum at AT&T

AT&T Business



~36M

Total Connected Devices*



1.7M

Connected asset management devices*

2.5M

Connected fleet vehicles*

14.6M

Connected Cars in the US and abroad*

*As of Q3 2017

New and Emerging IoT Verticals

AT&T Business

Manufacturing

Logistics

UBI

Fleet OEM

Value Added Reseller

Retail

Security

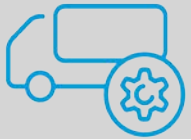
Drones

Agri-Tech

Oil / Gas

Connected Car

Fleet Mgmt



Wearables

Automation

mHealth

Smart Cities

IoT Considerations

AT&T Business

1) Initial Deployment

- Current methods of configuring and securing are inadequate
- Security and security management will be key, and may be the last consideration

2) Runtime Security (Anomaly Detection)

- AI, Deep Learning and Cognative Computing will be critical

3) Long Term Lifecycle Considerations

4) Data Management and Filtering

The IoT threat landscape requires a multi-layered approach

AT&T Business

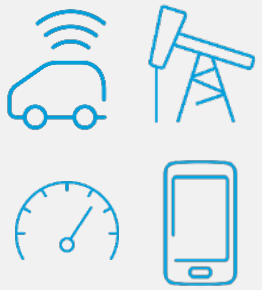
Top IoT security concerns:

- Device security
- Convergence of OT and IT
- Secure data in transit
- Secure data at rest
- Integrity of the data
- Reliability of the data
- Sustaining operations
- Physical safety
- Operational efficiency
- Access & authentication (devices & users)
- Software/Firmware updates

AT&T recommends a multi-layered approach to security to help protect the IoT ecosystem end-to-end.

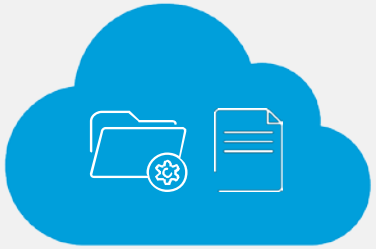
Strategy & Governance
Consulting

Endpoint
Mobile, IoT, Office/Fixed



Connectivity
Securing the network

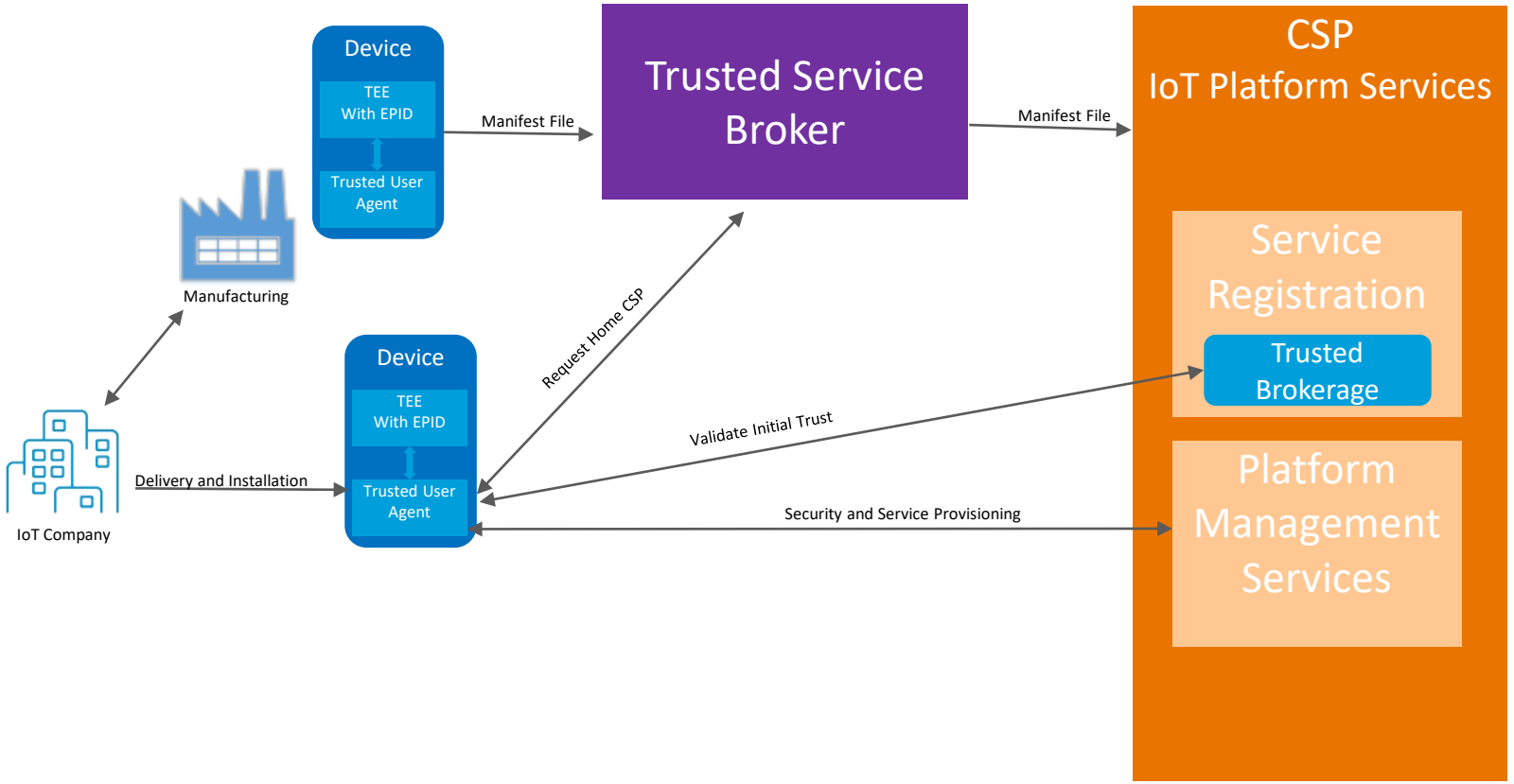
Data/Application
Securing workloads/applications



Threat Management
Detection & response

Potential Approach – Zero Touch Deployment

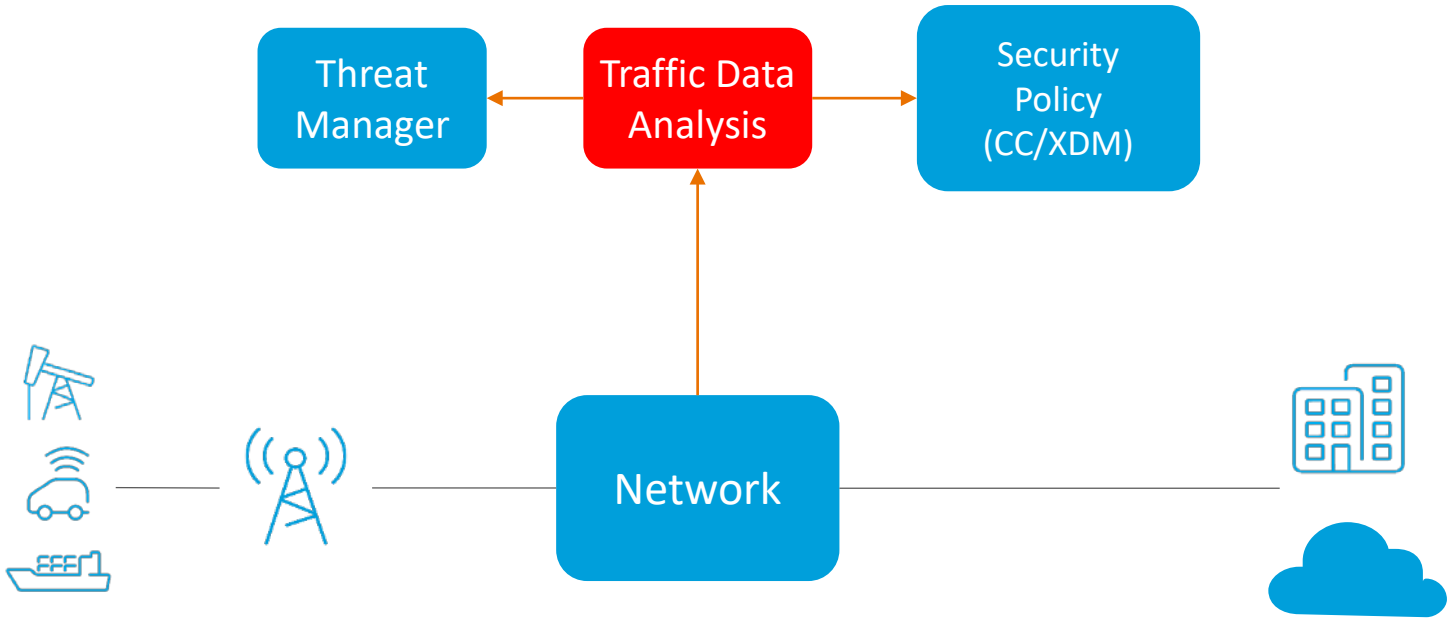
Zero touch concept can potentially automate the entire provisioning process including Software and Certificate Management.



Key Technologies

- Trusted Execution Environment
- Trusted Service Broker
- Certificate Management
- IoT Platform Service/Device Management (Internal or Hosted)

Anomaly Detection & Deep Learning



- Device traffic data is used to create a known-good profile
- This profile will use information like source and destination IP address, port, number of sessions per day, data transfer per session, and other traffic related information
- Device behavior on the network will be compared to the profile
- Abnormal behavior will be detected and security policy will be initiated
  - What is the severity (is the payload larger or more frequent or, is the data being redirected.)
  - Should the Data Quarantined or monitored (may just be a software or configuration update)

Life Cycle Management

IoT by default are long lived devices potentially being left untouched for up to 10 years.

Device Management will become a critical feature for IoT Devices

Device Management Considerations

- Software Fixes
- Feature Enhancements
- Configuration Changes
- Security Updates
- More…

Q&A


AT&T Business