



**FORGEROCK®**

**Identity of Things**

*Ludovic Poitou*

# ForgeRock

*The leading, next-generation,  
identity security software platform, driving digital business.*



**2010** Founded

**10** Offices worldwide with headquarters in San Francisco

**400+** Employees

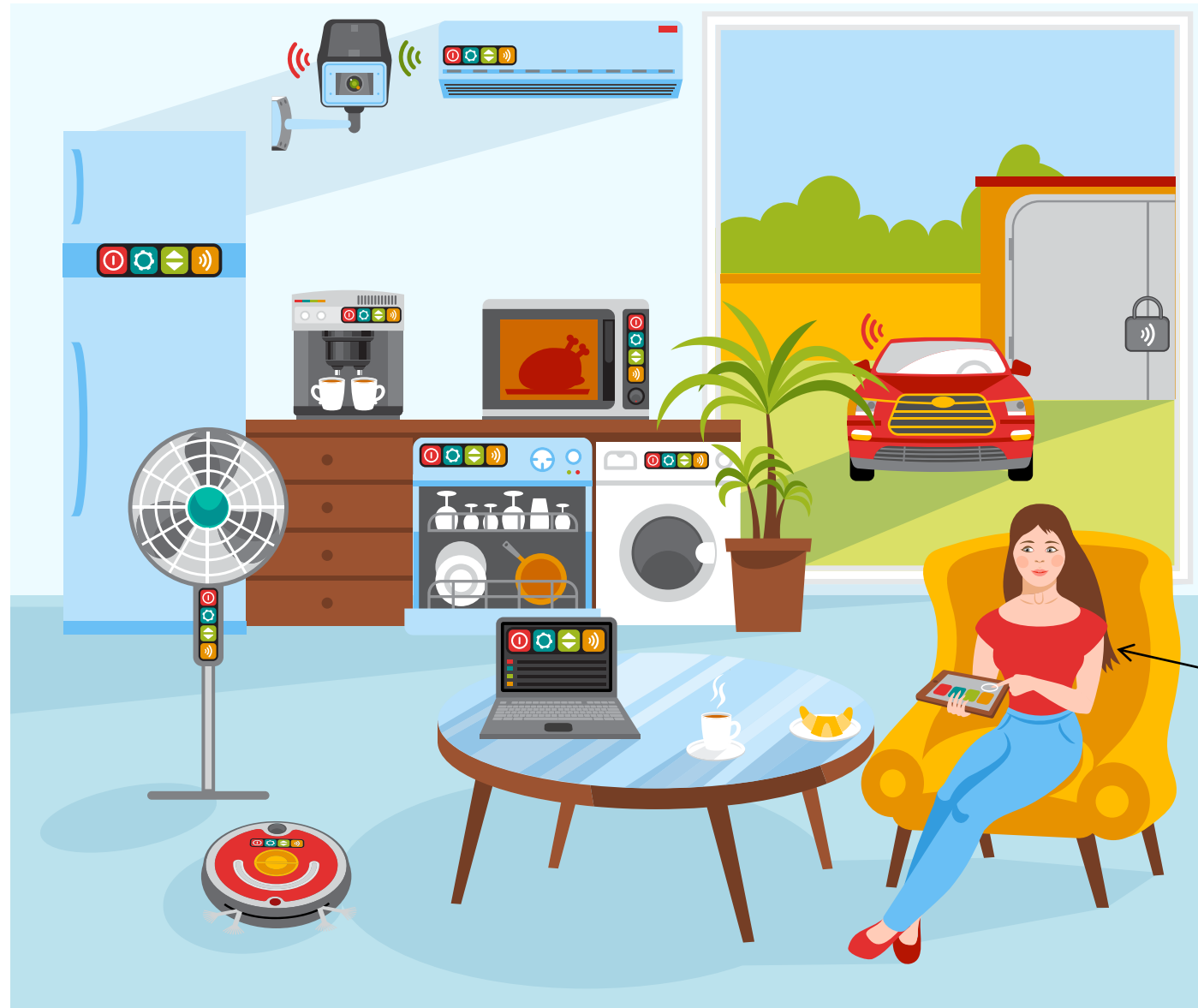
**600+** Enterprise Customers

**50%** Americas / **50%** International commercial revenues

**30+** Countries

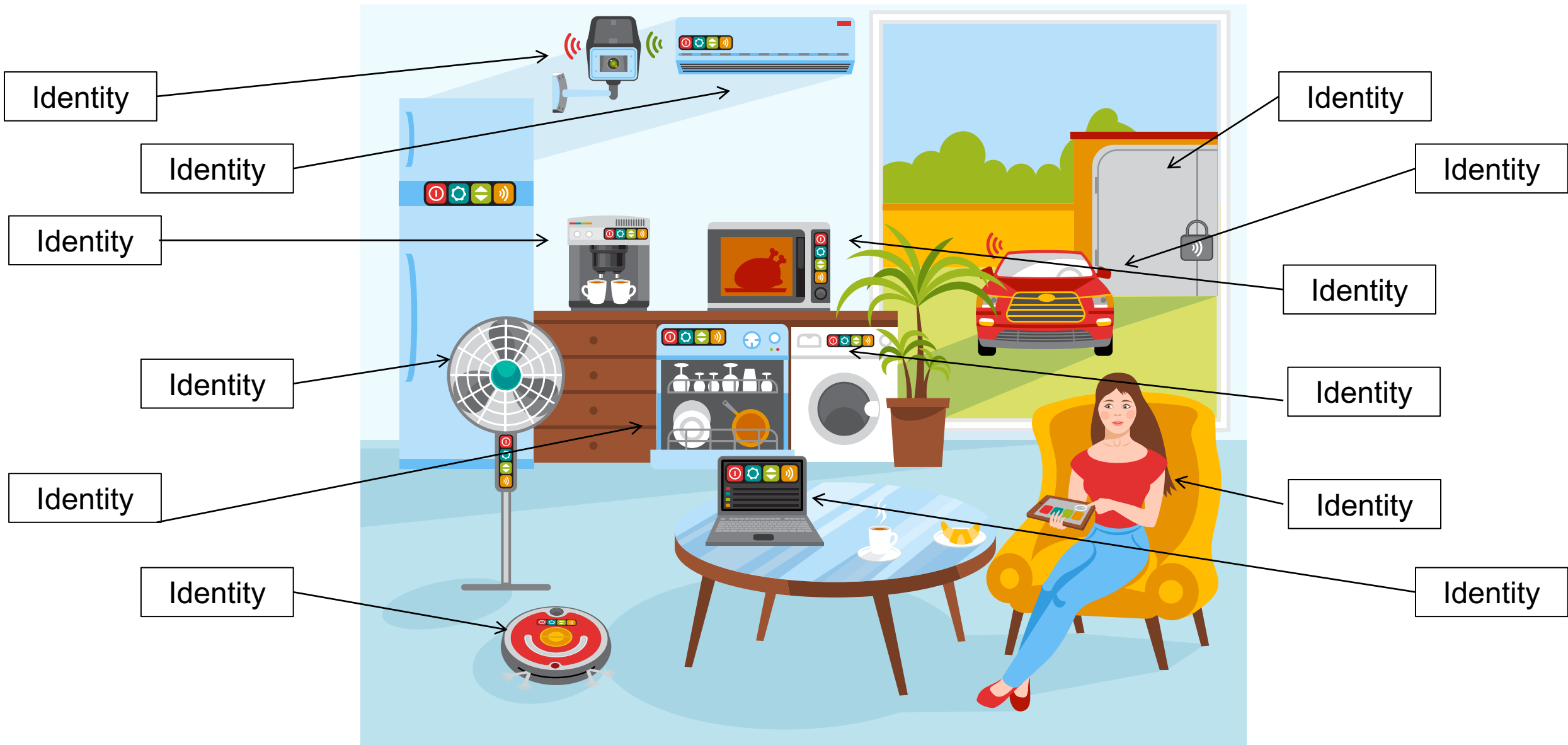


# Users



Identity

# Users, Devices, Things, and Services



# With IoT, Identity Is Everywhere...

Identity

Identity

Identity

Identity

Identity

Identity

Identity

Identity

Identity

Identity

Identity

Identity

**Business Solutions**  
Growth Strategies For The IT Channel

Home Technology Centers Channel Top

**Channel Transitions**  
Powered By Business Solutions

2016: DALLAS  
NOVEMBER 15

By **Tim Greene** | Follow  
Network World | Nov 1, 2016 10:27 AM PT

RELATED TOPICS  
Security

COMMENTS

The DDoS attack...  
some high-...  
shout...

# Major cyber attack disrupts internet service across Europe and US

Denial of service attack from unknown culprits on domain name system company Dyn caused access to be severely restricted for users on Friday

## DDoS Attack On Dyn Cybersecurity Investment

By **Christine Kern**, contributing writer

Attack highlights the "disruptive coordinated hacking"

**Forbes** LOG IN

YOUR READING LIST

The driver was said to have used a suspended license and methamphetamine dropped out of his cap

**The Dyn DDoS Attack And The Changing Balance Of Online Cyber Power**

# The Dyn DDoS Attack And The Changing Balance Of Power

by **Kalev Leetaru**, CONTRIBUTOR  
I write about the broad intersection of data and security

Opinions expressed by Forbes Contributors are their own

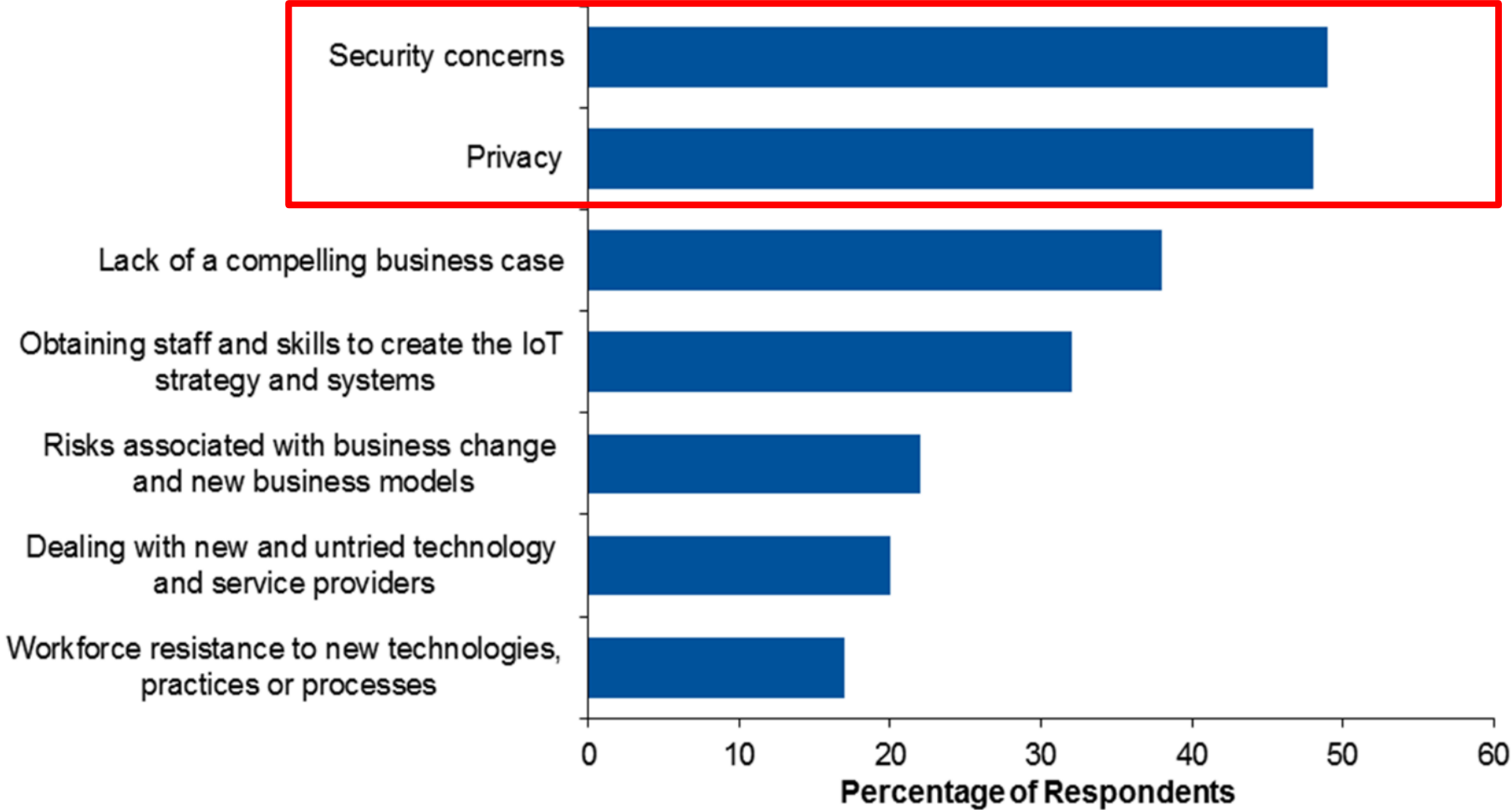
## Details emerging on Dyn DNS DDoS attack, Mirai IoT botnet

by **Peter Loshin**  
Site Editor  
Published 28 Oct 2016

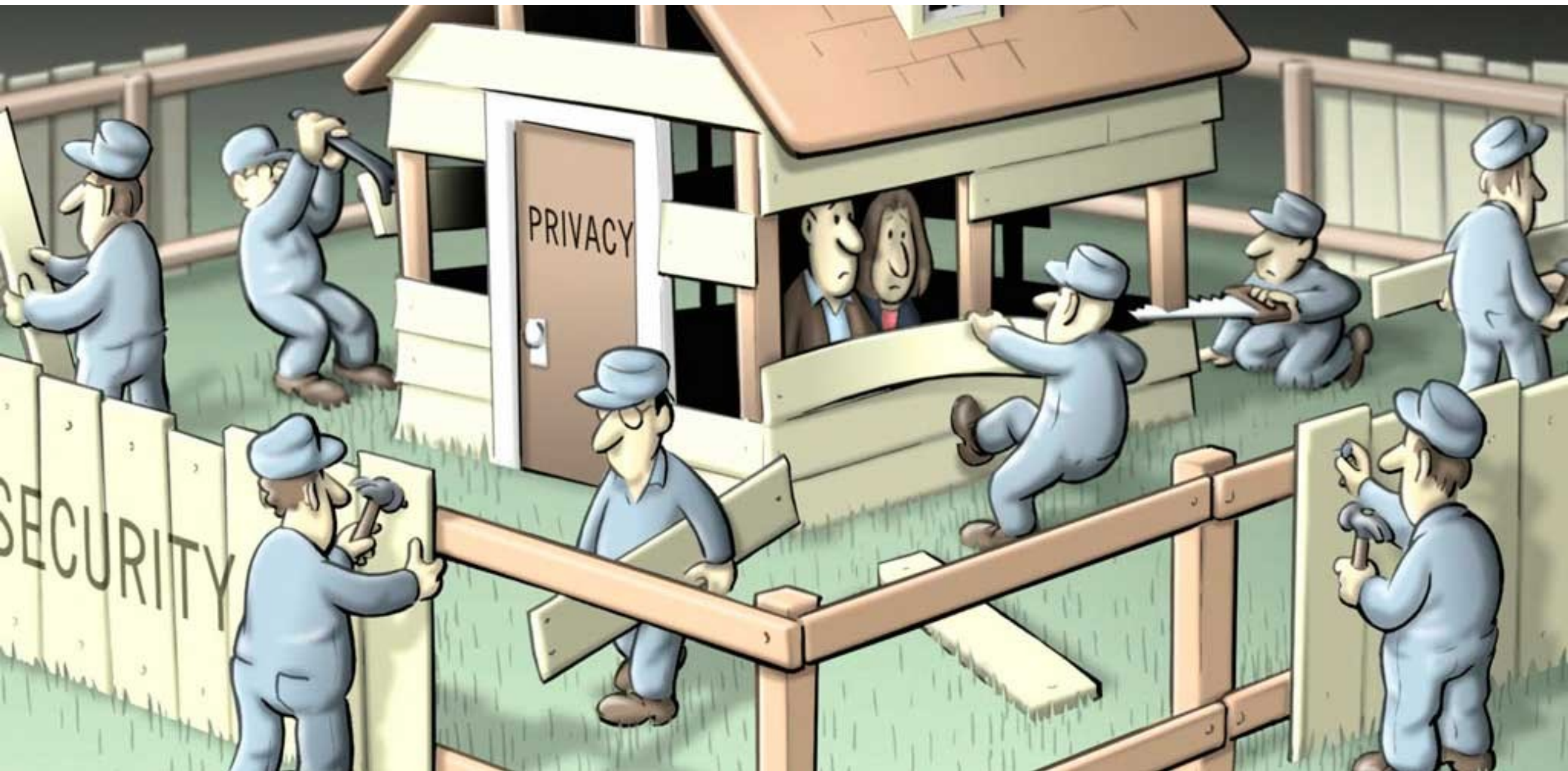
As more details emerge on last week's massive Dyn DNS DDoS, new analysis indicated as few as 100,000 Mirai IoT botnet nodes were enlisted in the incident and reported attack rates up to 1.2 Tbps.

# But So Is Risk.

# IoT Challenges





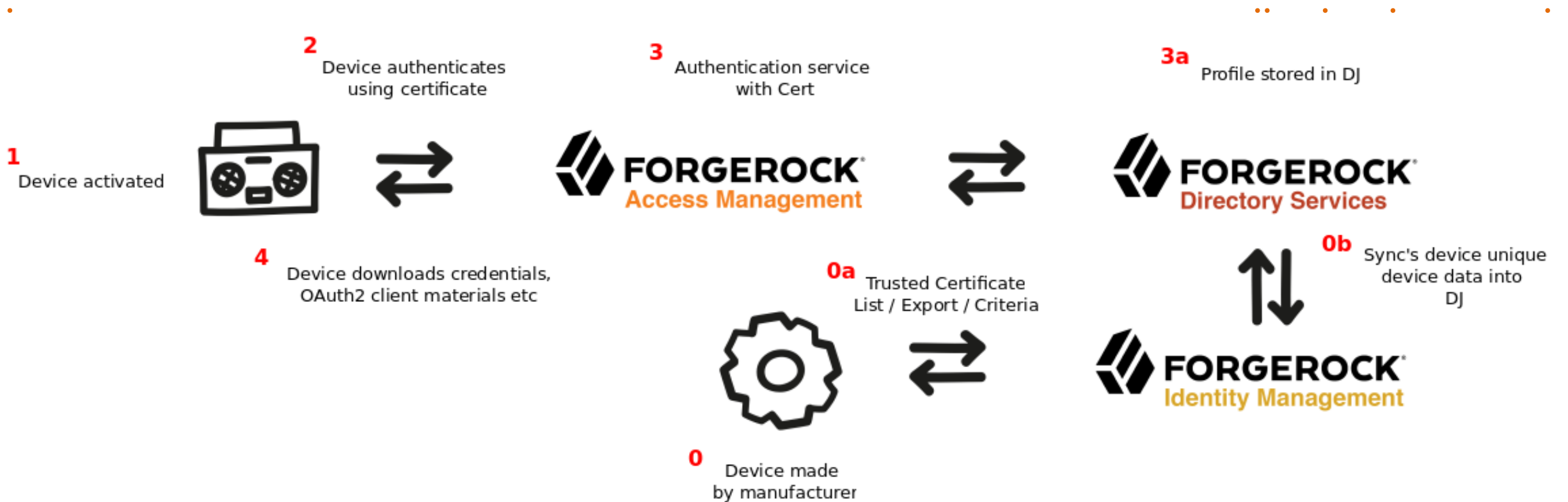




Device created with some unique, immutable identifier – MAC, certificate

Synchronized and activated in central store

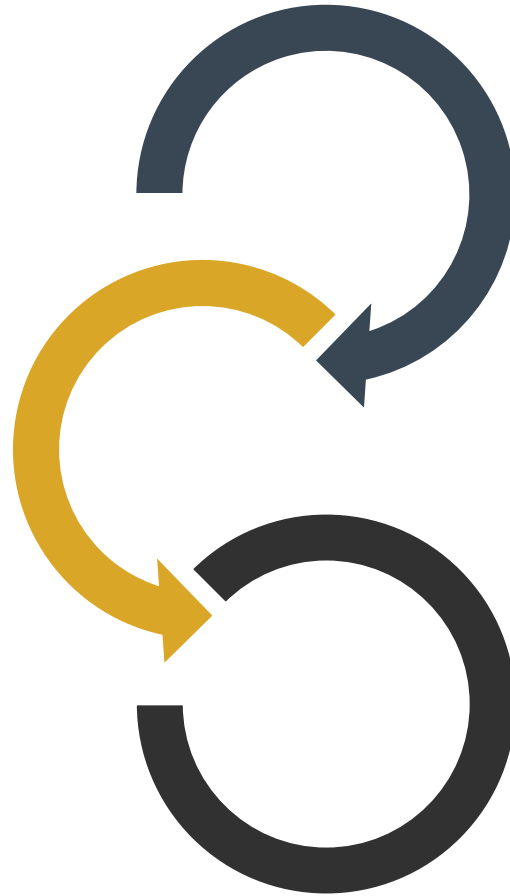
Device authenticates - to download API details, client credentials



# Device Pairing Requirements

Revoke device access when device is lost, stolen or sold

Bind a token to a device – reduce impact of token theft from MITM



Device should have scoped permissions

Device needs to represent user to APIs & services

Need to pair a device to a person

Device often has limited input capability and UI

“Pin & Pair” - user enters a unique device code out of band on their laptop/tablet

Device receives scoped access, with simple revocation

Simple out of band pairing



Device accesses services on users behalf





# OAuth2 Device Pairing Flow - “Demo”

- 1 - Start registration
- 2 – Device gets code
- 3 – User enters code out of band on web page
- 4 - Device polls AS then pairs
- 5 - Device gets access token
- 6 - Device uses token against service
- 7 - Device can be revoked via end user dashboard



Images courtesy of Jon Knight, UK Customer Engineering

Smart Guitar demo at the London Identity Summit Oct 2016 2016 - <https://youtu.be/MUoicwT9s34>

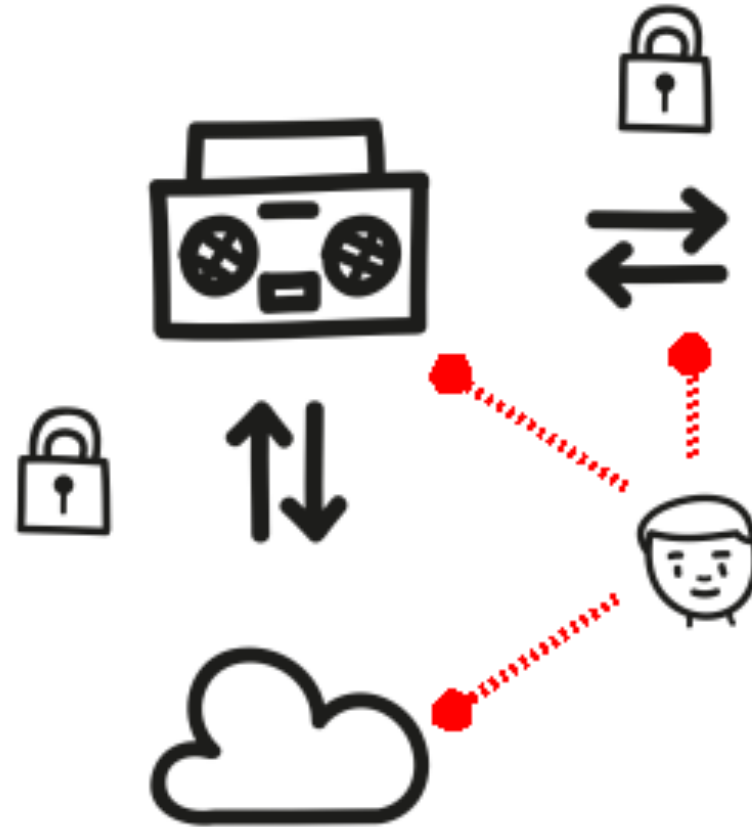
# OAuth2 Proof-of-Possession Token Safety

Protect access\_token through device binding

Device may not use HTTPS or a secure token storage area – need a method to protect hijacking or MITM

Use proof-of-possession with public key being baked into the access\_token

Provides the RS an ability to initiate challenge-response to prove correct owner



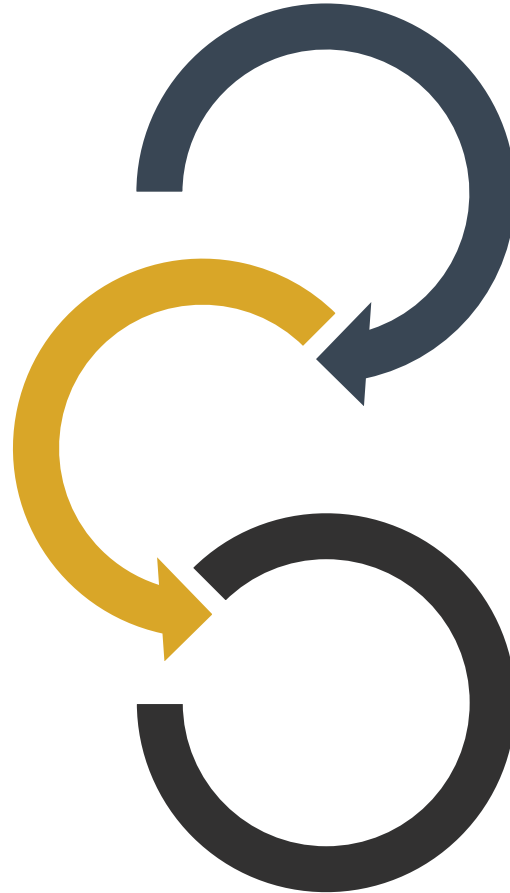
Token request with pub key

Resource server uses key for challenge response

# IoT Data Sharing Requirements

Ability to share arbitrary data from a device to other users or services

Ability for authorization policies to be created by **end user** not an admin



Leverage simple standards for fast integration





Ability for end user to perform simple approval


Ability to perform simple revocation



# User-Managed Access

My devices

 eHealthKit	 SmarteeBody Protected
Smartee Ehealth 1	Smartee Body 1
e-Health Sensor Platform V2.0 for Raspberry Pi	Smartee Body
 CardioTrack	 GlucoseMeter
Smartee Cardiotrack 1	Smartee Glucose Meter 1
Smartee CardioTrack cardio health device	Smartee Connected Glucose Meter

 HealthWatch  
Protected

Smartee Health Watch 1

Heart Rate	Steps
80	4812
<a href="#">READ</a>	<a href="#">READ</a>

Devices registered & managed

Devices make data!  
Needs protecting...

# User-Managed Access

Ability for data owner to make easy access revocation decisions across

Share the resource



Not shared

Add or select people to share your resource with

Select Permission

Please Select

- Heartrate
- Steps
- Bodyfat
- Sleep

Ability for data owner to make well informed and consent driven decisions

RESOURCE

## Smartee Health Watch 1

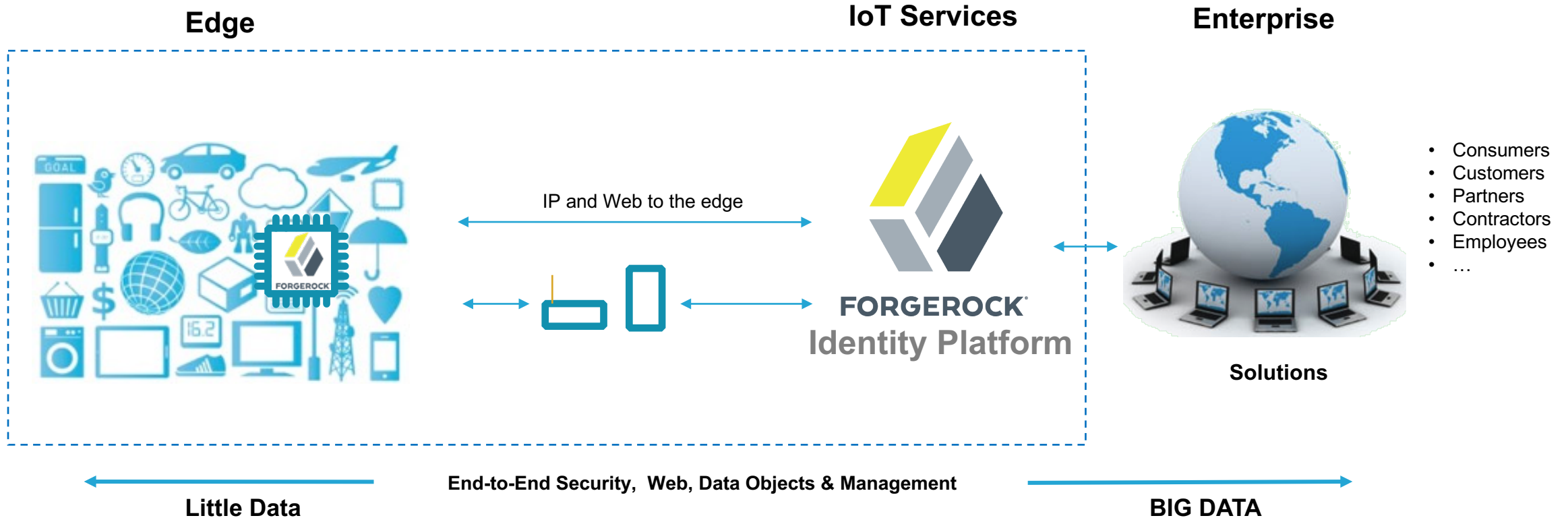
Users allowed to access this resource and their permissions

[EDIT LABELS](#)

User	Permissions
drmccoy@enterprisehealth.org	<a href="#">Heartrate</a> <a href="#">Steps</a> <a href="#">Bodyfat</a> <a href="#">Sleep</a>
alfredp@gotham.net	<a href="#">Heartrate</a> <a href="#">Steps</a> <a href="#">Bodyfat</a>
catwoman@hotmail.com	<a href="#">Heartrate</a> <a href="#">Steps</a>

# End-to-end IoT Identity Platform

FROM DEVICE TO CLOUD





# Thank You

Ludovic Poitou

Director Product Management, General Manager France,  
ForgeRock

Ludovic.Poitou@ForgeRock.com  
@ludomp