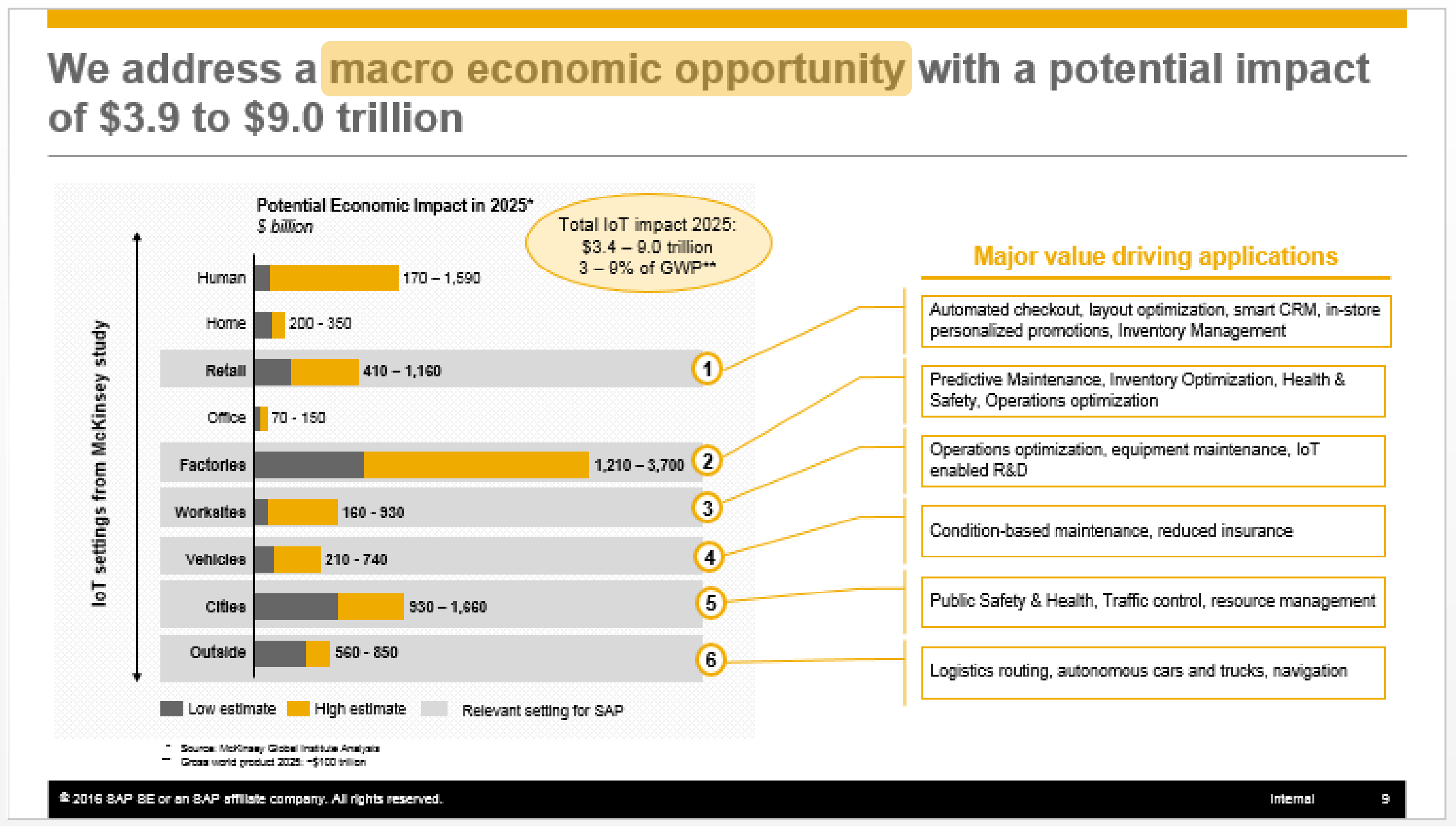
# Security for the Internet of Things: Strategy and Road Map

Dr. Laurent Gomez, SAP Product Security Research
José Márquez, IoT Central Architecture

PUBLIC

# Security for the Internet of Things

## Business case



### We address a macro economic opportunity with a potential impact of $3.9 to $9.0 trillion

**Major value driving applications**

1. Automated checkout, layout optimization, smart CRM, in-store personalized promotions, Inventory Management
2. Predictive Maintenance, Inventory Optimization, Health & Safety, Operations optimization
3. Operations optimization, equipment maintenance, IoT enabled R&D
4. Condition-based maintenance, reduced insurance
5. Public Safety & Health, Traffic control, resource management
6. Logistics routing, autonomous cars and trucks, navigation

* Source: McKinsey Global Institute Analysis

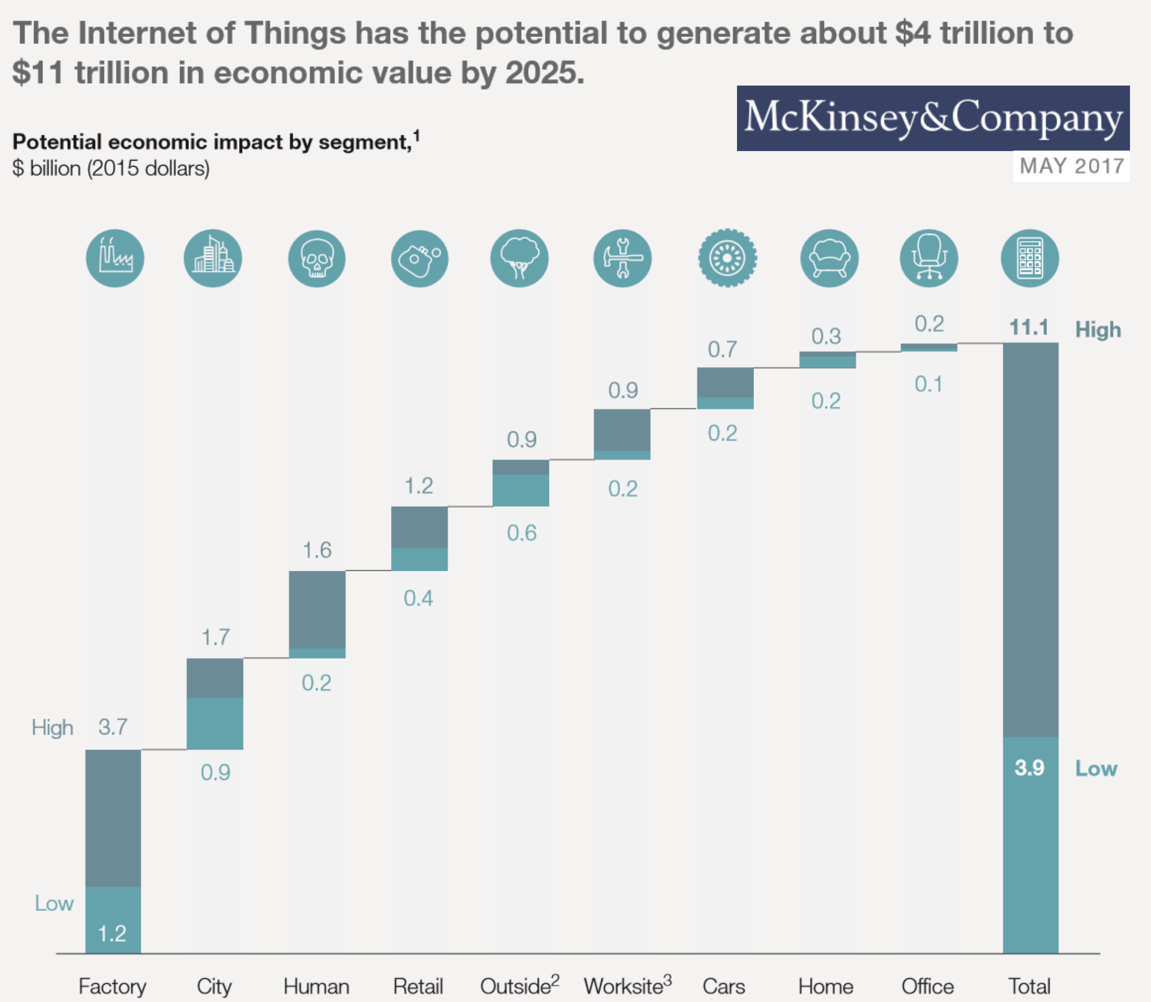
** Gross world product 2025: ~$100 trillion

Internal 9

- Enable this opportunity by discarding security as a showstopper for adoption

# Security for the Internet of Things

## Industries with the highest IoT spent potential



**The Internet of Things has the potential to generate about $4 trillion to $11 trillion in economic value by 2025.**

McKinsey&Company

MAY 2017

**Potential economic impact by segment,**[1]

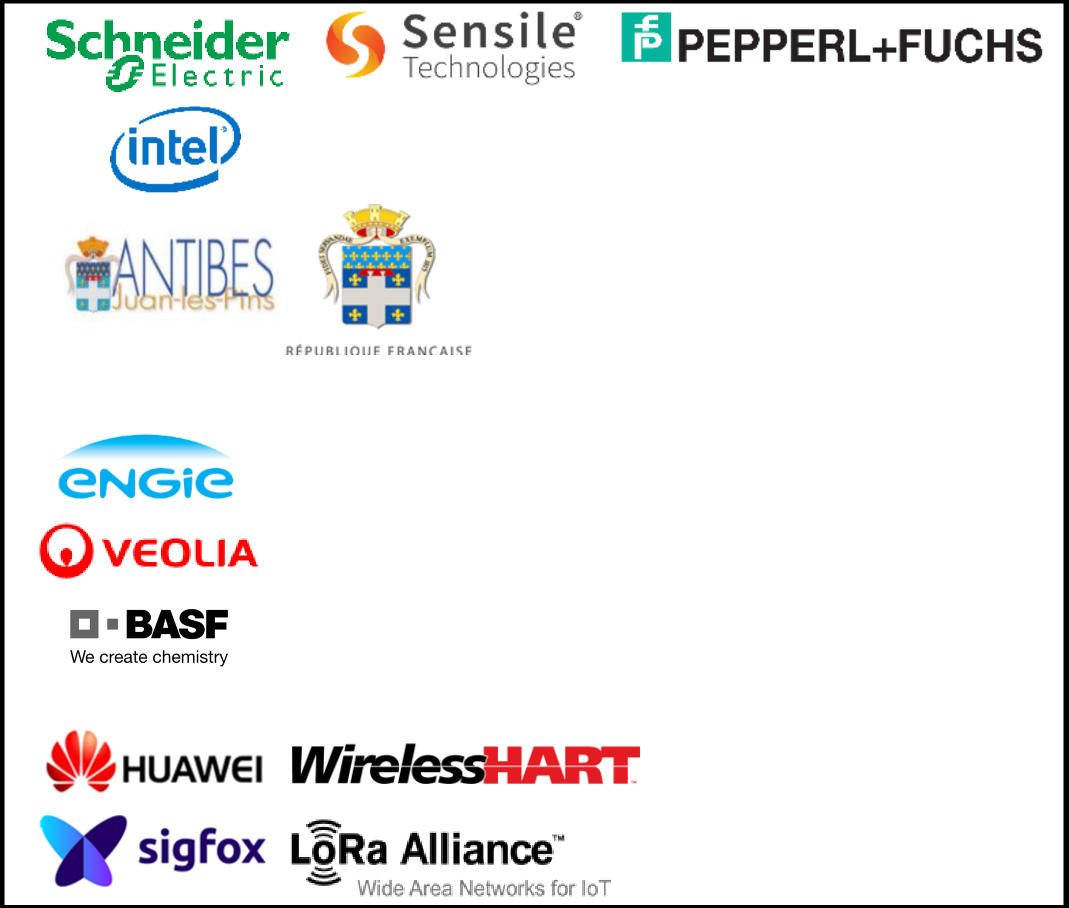
$ billion (2015 dollars)

# Security for the Internet of Things

## Focus industries

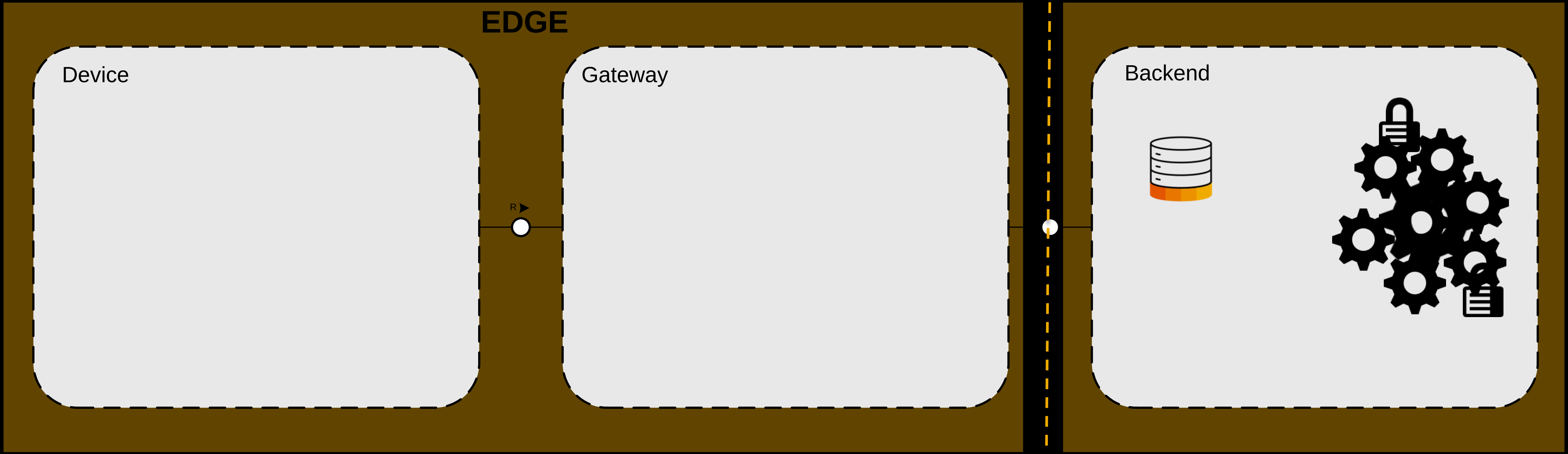
Penetrate the industries with the highest IoT spent potential

- Discrete industries
  - – Industrial machinery and components
  - – High tech
- Public services
  - – Future cities
  - – Defense and security
- Energy and natural resources
  - – Oil and gas
  - – Utilities
  - – Chemicals
- Service industries
  - – Telecommunications



# Decentralization and distribution of enterprise systems

## Edge computing from SAP (as part of SAP Leonardo)

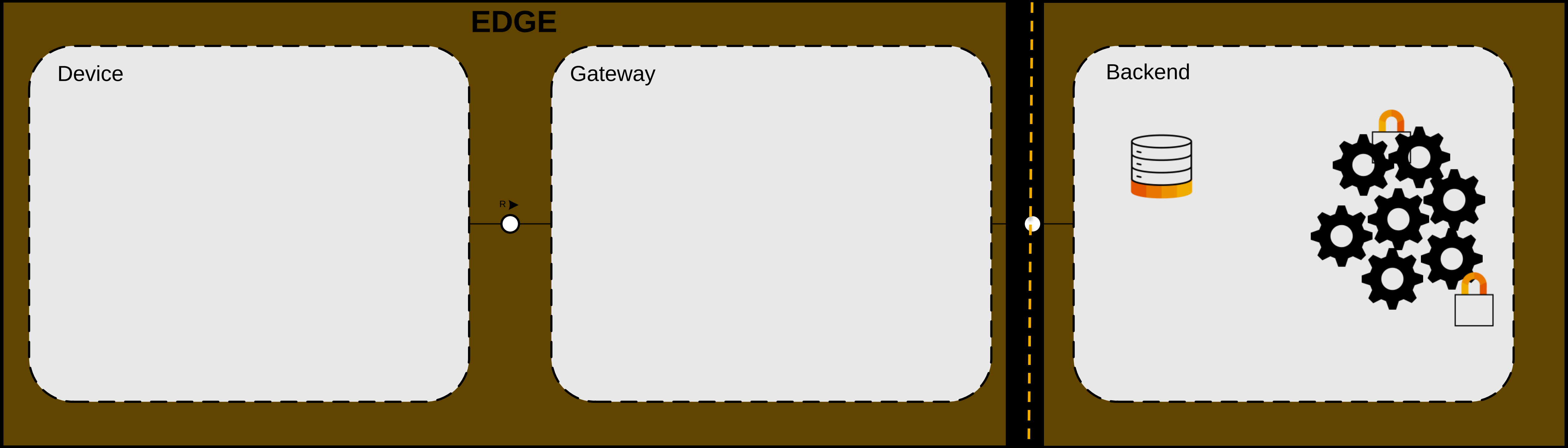


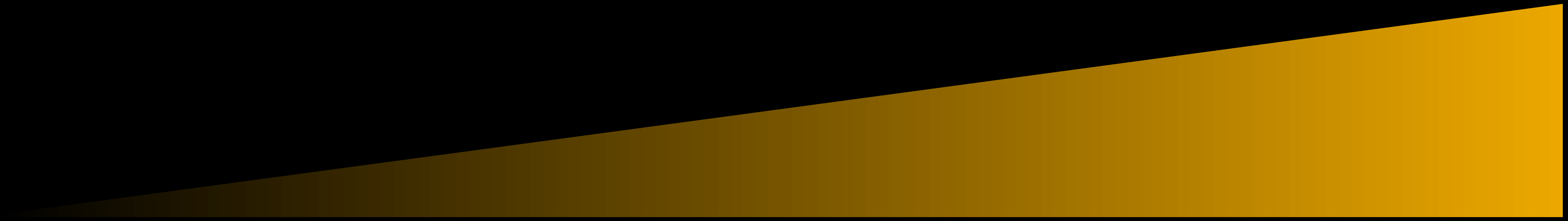
**Highest level of**

- Business visibility
- Application centralization
- Data consolidation
- Technology abstraction

# Decentralization and distribution of enterprise systems

## Edge computing from SAP (as part of SAP Leonardo)



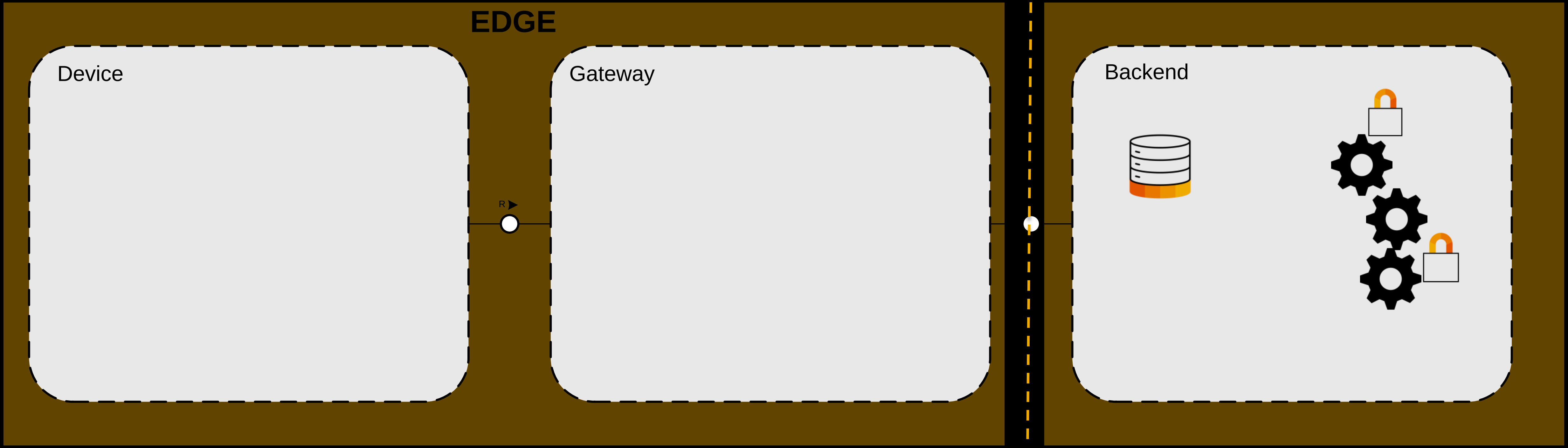


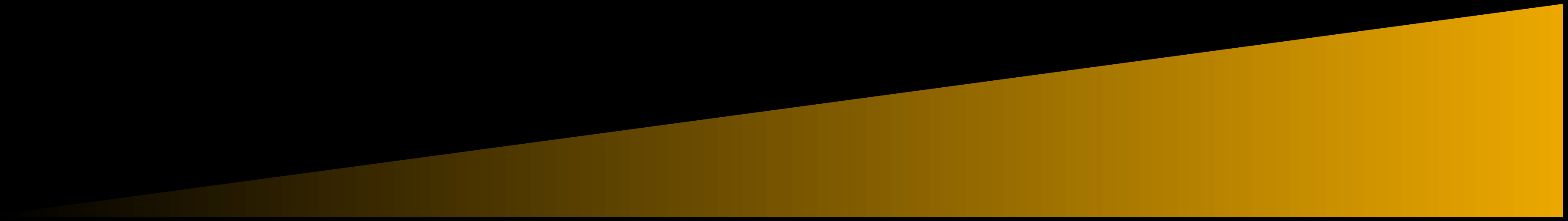
**Highest level of**

- Business visibility
- Application centralization
- Data consolidation
- Technology abstraction

# Decentralization and distribution of enterprise systems

## Edge computing from SAP (as part of SAP Leonardo)



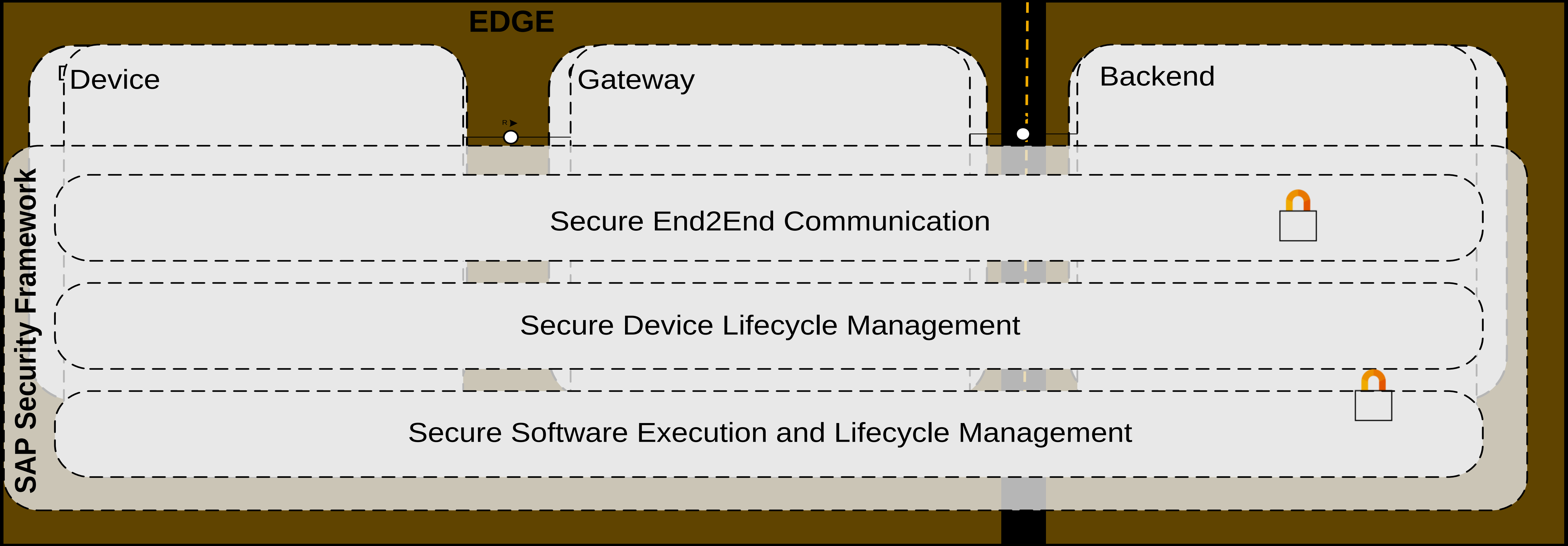


**Highest level of**

- Business visibility
- Application centralization
- Data consolidation
- Technology abstraction

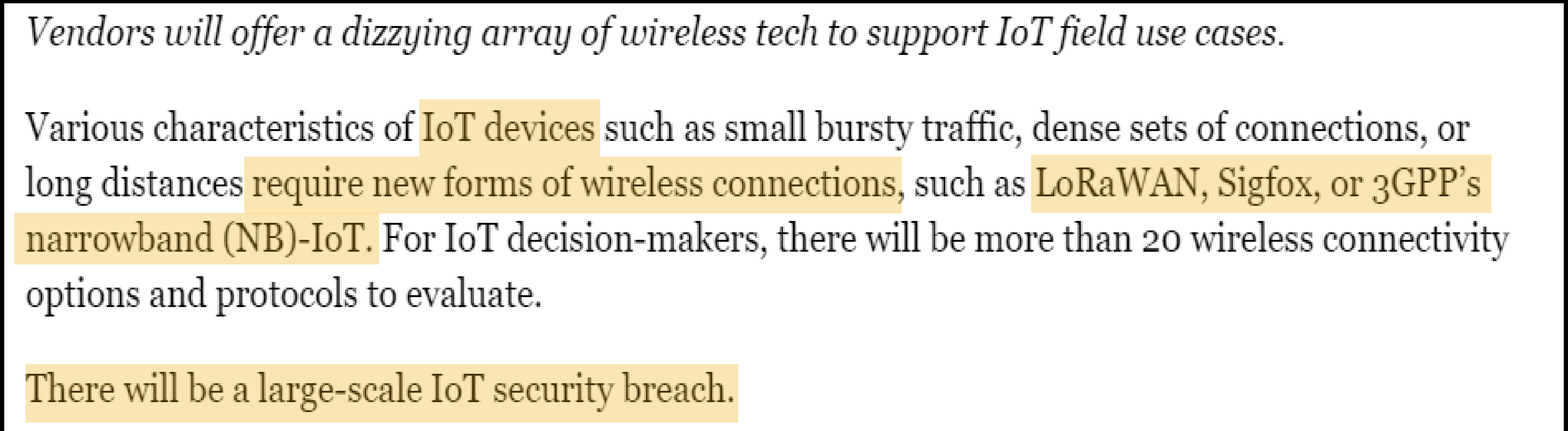
# Decentralization and distribution of enterprise systems

## Edge computing from SAP (as part of SAP Leonardo)


EDGE
Device
Gateway
Backend
SAP Security Framework
Secure End2End Communication
Secure Device Lifecycle Management
Secure Software Execution and Lifecycle Management

# Connectivity stands first

“We cannot capitalize on the data at our solutions if we do not **assure** and broaden our **connectivity capabilities** to ingest all data from all type of devices & networks.”



*Vendors will offer a dizzying array of wireless tech to support IoT field use cases.*

Various characteristics of IoT devices such as small bursty traffic, dense sets of connections, or long distances require new forms of wireless connections, such as LoRaWAN, Sigfox, or 3GPP’s narrowband (NB)-IoT. For IoT decision-makers, there will be more than 20 wireless connectivity options and protocols to evaluate.

There will be a large-scale IoT security breach.

Source: www.forbes.com/sites/gilpress/2016/11/01/internet-of-things-iot-2017-predictions-from-forrester/#47c14f436bb6

# Retrofit on physical assets with sensors

## Low-powered devices and networks

### Reliable and cost effective, meeting industrial needs

Low-powered devices

- Do not consume much power to work and communicate
- Do not require a continuous communication link

Low-powered wide area networks (LPWAN)

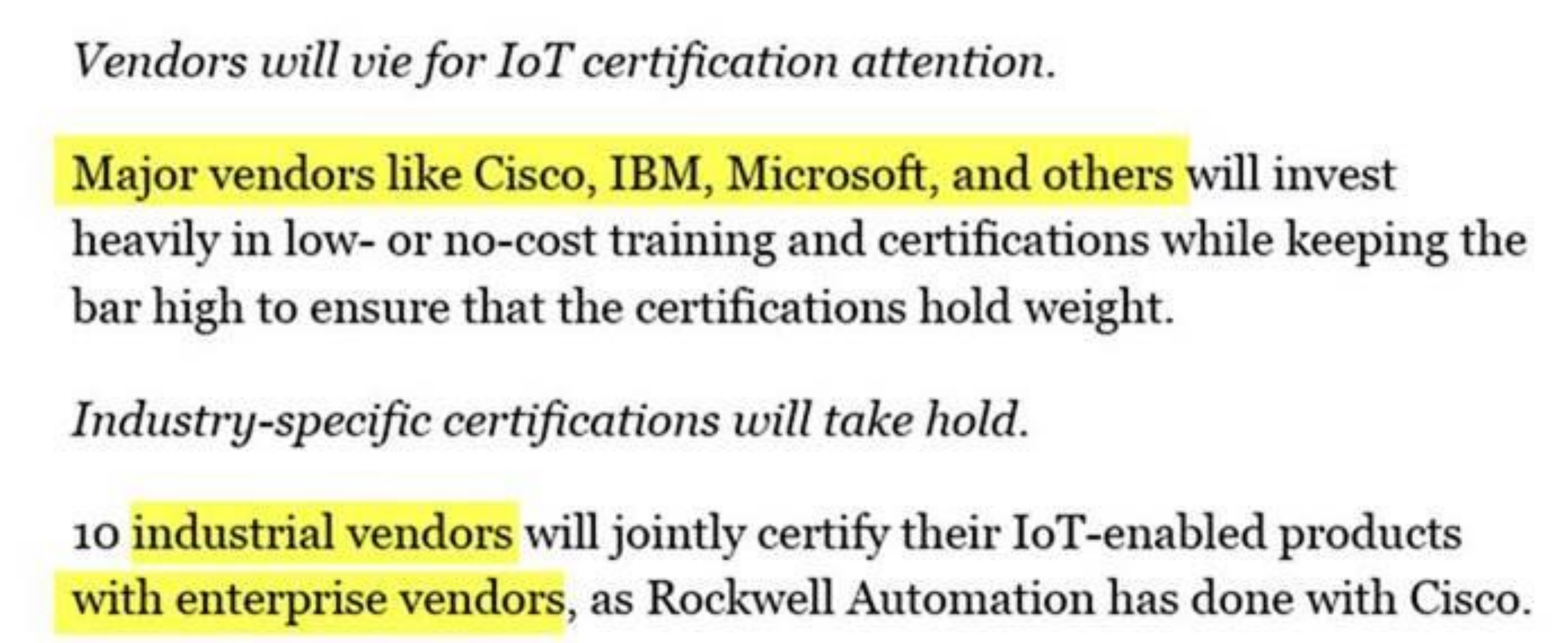
- Reduced packet size
- High latency
- Low throughput

Lte
LoRa Alliance™
Wide Area Networks for IoT
HUAWEI
WirelessHART
sigfox
ZigBee

**Current market leaders**

# Internet of Things (IoT): 2018 Predictions from Forrester

## Device certification



*Vendors will vie for IoT certification attention.*

Major vendors like Cisco, IBM, Microsoft, and others will invest heavily in low- or no-cost training and certifications while keeping the bar high to ensure that the certifications hold weight.

*Industry-specific certifications will take hold.*

10 industrial vendors will jointly certify their IoT-enabled products with enterprise vendors, as Rockwell Automation has done with Cisco.

## Security for Internet of Things

Once IoT devices are connected to the Internet

> “Driven by the current large-scale deployment of connected objects as well as the upcoming mass-adoption of digitally charged products, cybersecurity has to keep the pace with these developments in order to embrace the new ends of the system boundaries, i.e. the physical devices.”

# SAP security reference model

## SAP security framework, version 1.2

| | | Edge | | | |
|---|---|---|---|---|---|
| | | Device | Gateway | Back end | Application |
| SAP security framework | Data access control | | | | |
| | Data transmission control | | | | |
| | Data integrity | | | | |
| | Access control | | | | |
| | System access control | | | | |
| | Availability control | | | | |
| | Data input control | | | | |
| | Job control | | | | |
| | Data separation control | | | | |

# SAP security reference model

IoT-driven enhancement

SAP security framework version 1.2

| SAP security framework | Edge<br>Device | <br>Gateway | Back end | Application |
|---|---|---|---|---|
| Data access control | | | | |
| Data transmission control | | | | |
| Data integrity | | | | |
| Access control | | | | |
| System access control | | | | |
| Availability control | | | | |
| Data input control | | | | |
| Job control | | | | |
| Data separation control | | | | |

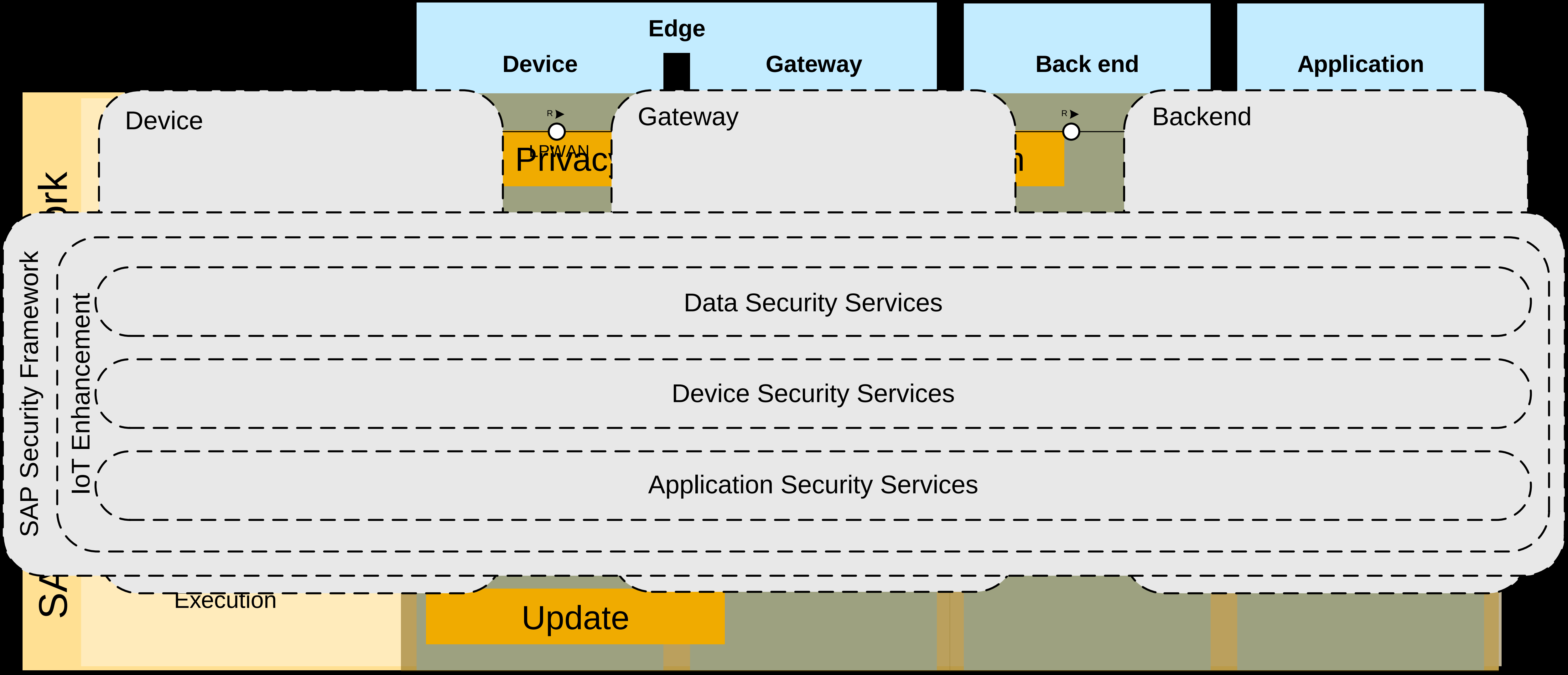
# SAP security reference model

## IoT-driven enhancement

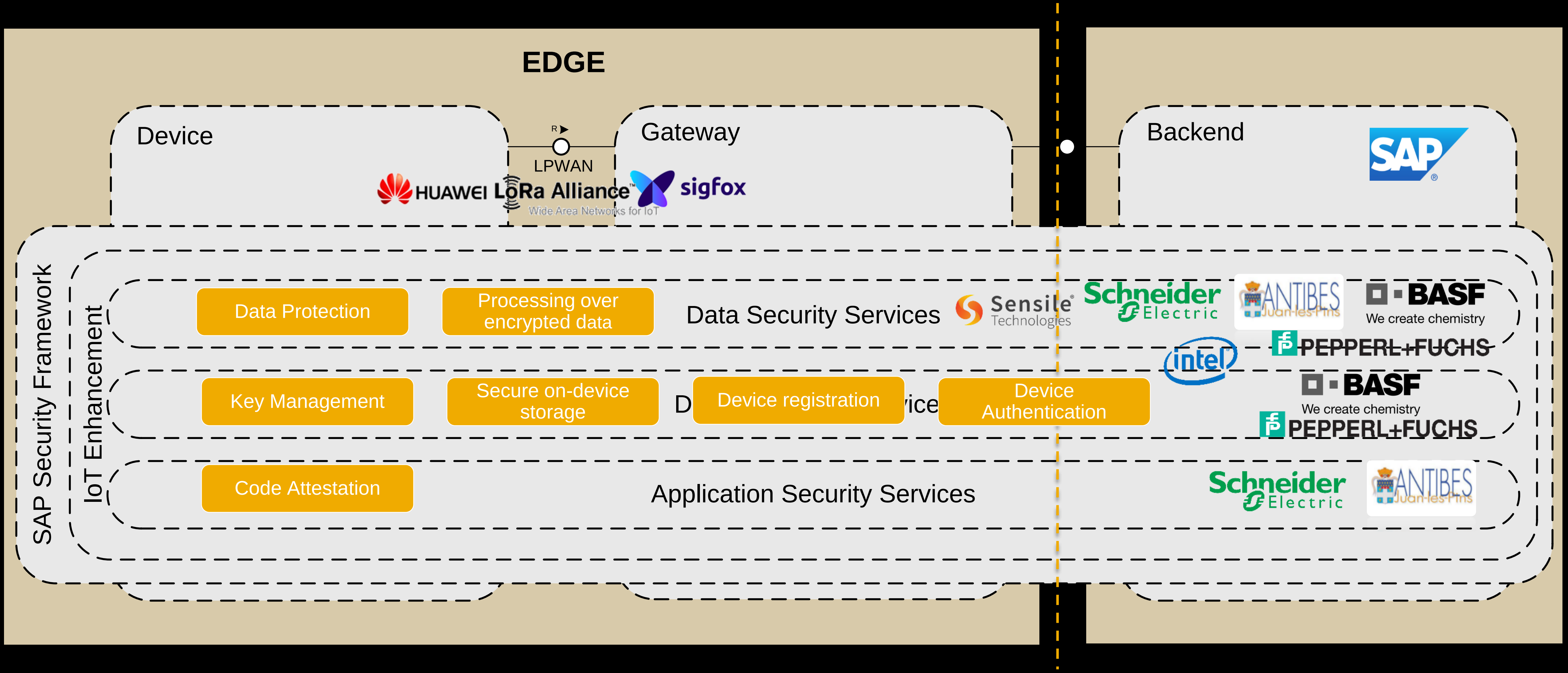
|  |  |  | Edge |  |  |  |
|---|---|---|---|---|---|---|
|  |  |  | Device | Gateway | Back end | Application |
| SAP security framework | End-to-end communication | Data access control |  |  |  |  |
|  |  | Data transmission control |  |  |  |  |
|  |  | Data integrity |  |  |  |  |
|  | Device management | Access control |  |  |  |  |
|  |  | System access control |  |  |  |  |
|  |  | Availability control |  |  |  |  |
|  | Software execution | Data input control |  |  |  |  |
|  |  | Job control |  |  |  |  |
|  |  | Data separation control |  |  |  |  |

# SAP security reference model

IoT-driven enhancement

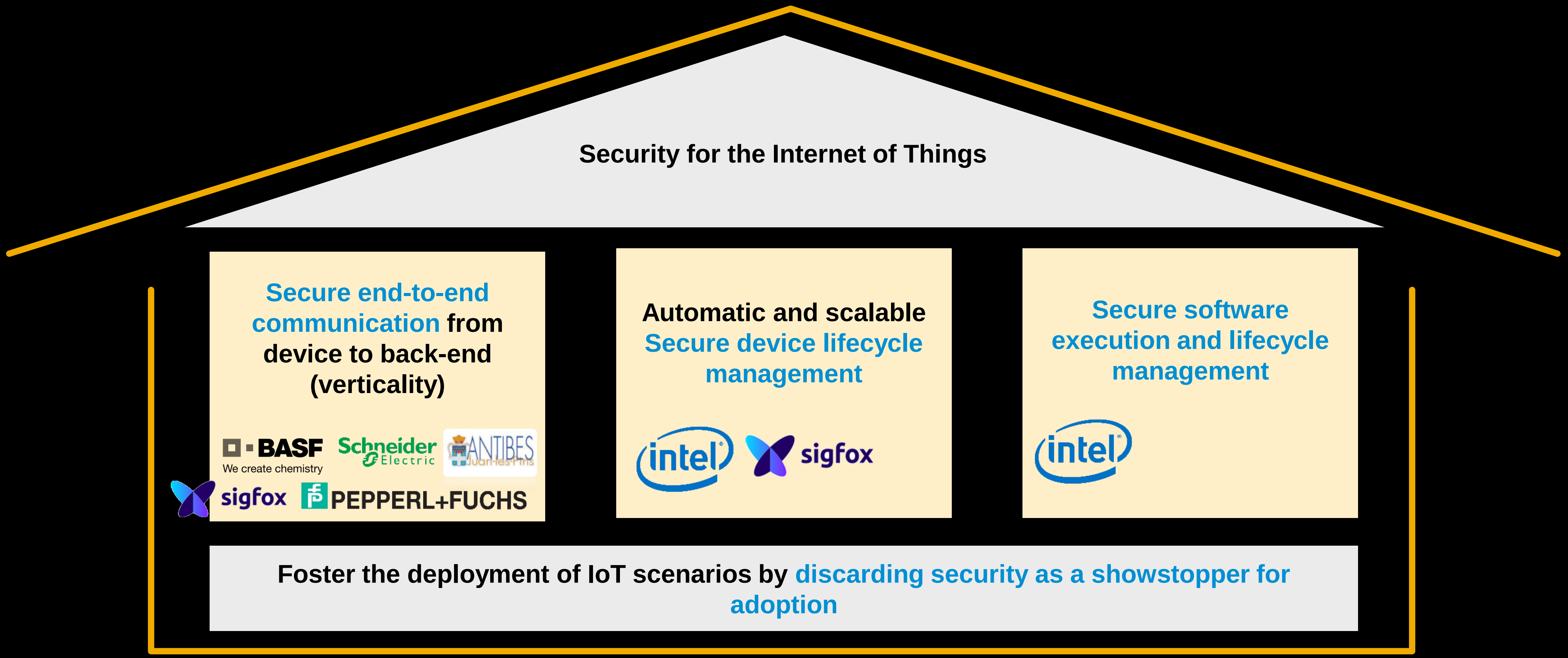


# Reference architecture



# Security as enabler for the Internet of Things

## Security pillars



Security for the Internet of Things

**Secure end-to-end communication** from device to back-end (verticality)

Automatic and scalable **Secure device lifecycle management**

**Secure software execution and lifecycle management**

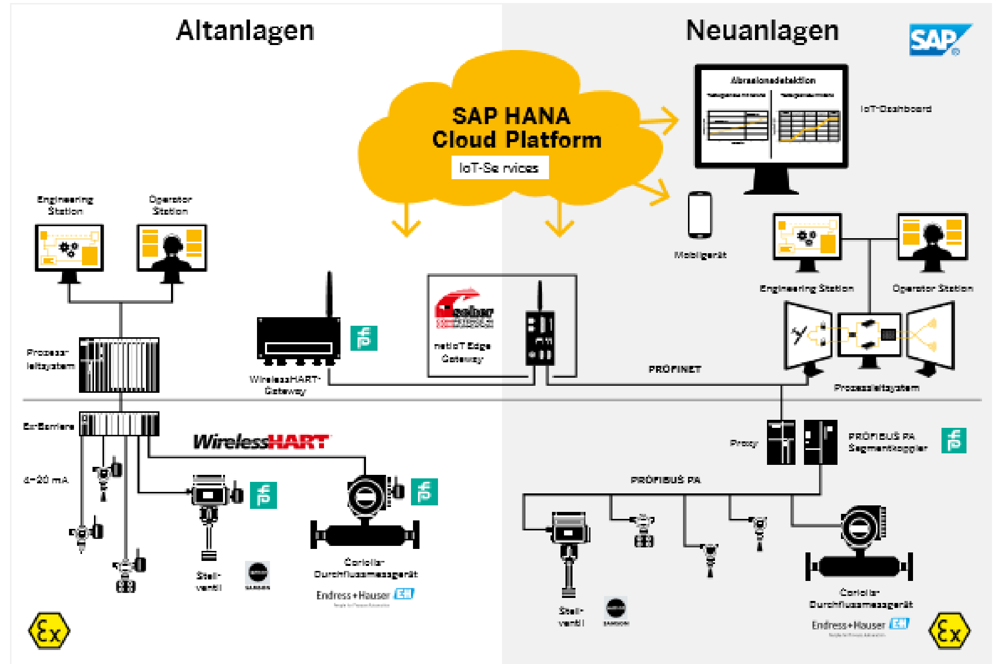
Foster the deployment of IoT scenarios by **discarding security as a showstopper for adoption**

# Scenario owner: BASF

Predictive maintenance

BASF
We create chemistry

PEPPERL+FUCHS



## BASF

- BASF owns and operates a chemical factory, instrumented by sensors
- Situation: Need for operational continuity of chemical processes while preserving the physical integrity of workers and factory. Process automation and predictive maintenance have been identified as one aspect of the digital transformation.

## Solution

- Data fusion between IT and OT data
- Remote physical assets diagnostics
- Engineering rules and predictive models
- Indicators-based planning
- Dynamic optimization of maintenance schedules

## Benefits

- Connect operational levels to automation process
- High resolution management

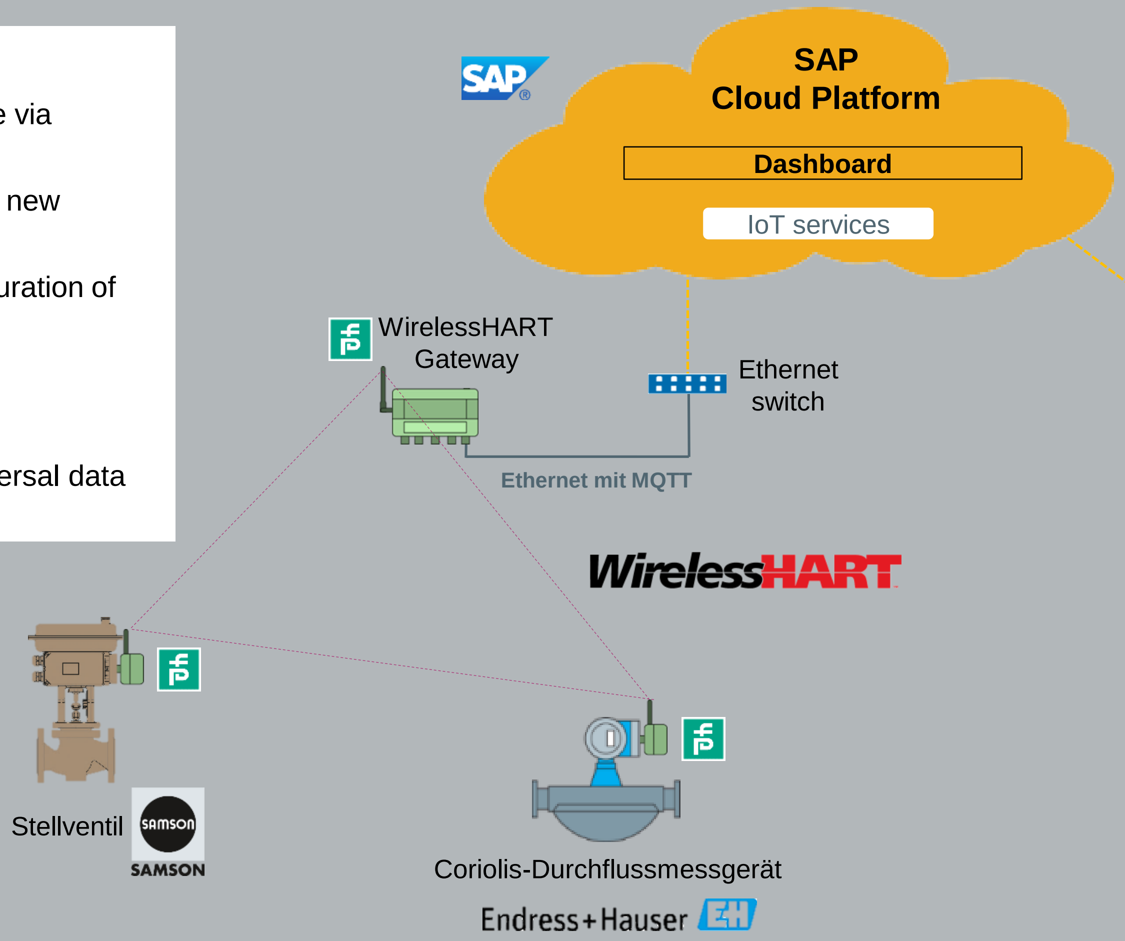
## Security requirements

- End-to-end data protection
- Scalable secure device management

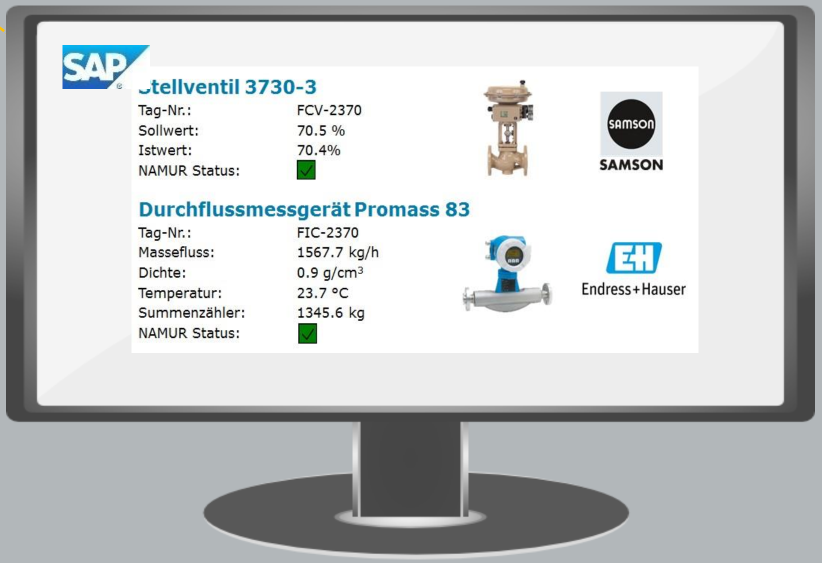
# Predictive maintenance

## Solution

- Retrofit on installed base via WirelessHART
- Automatic recognition of new devices
- Minimal one-time configuration of WHA-GW
- Full NE107 status
- Transparent integration
- Future extension to universal data access possible



IoT Dashboard



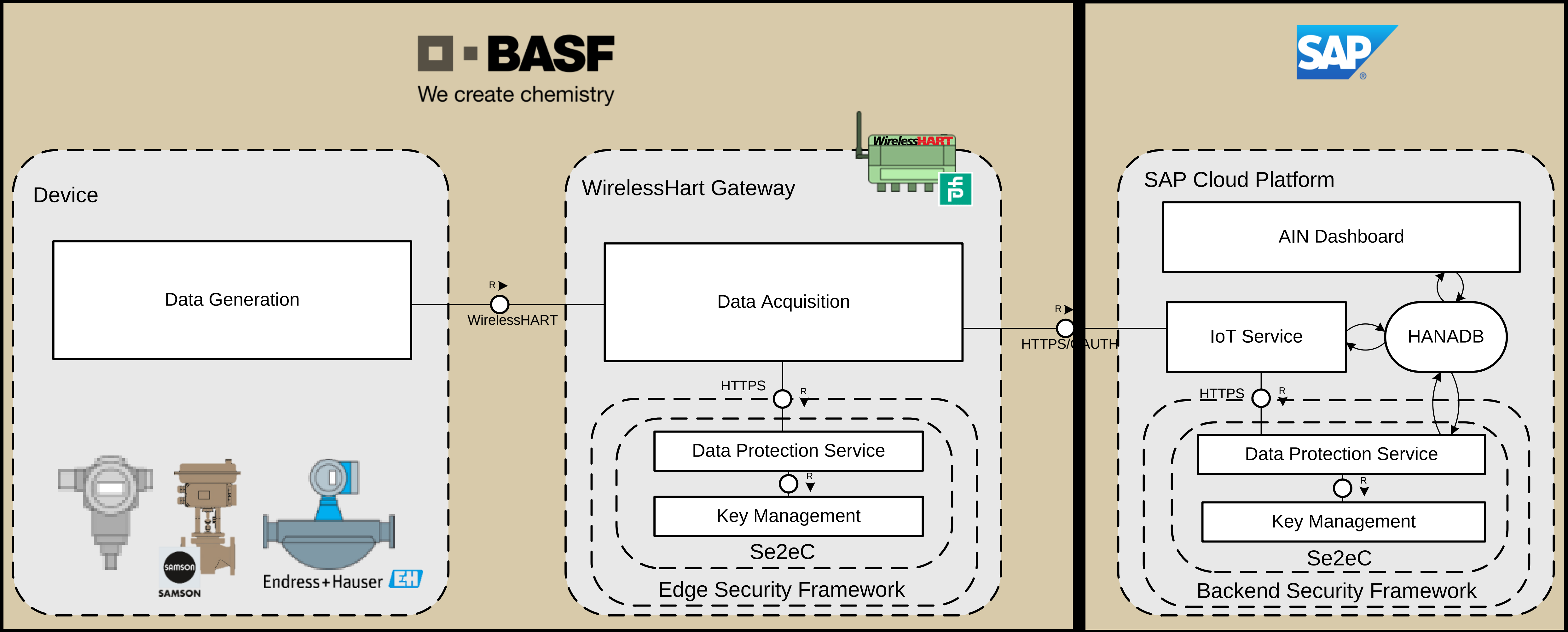
### Stellventil 3730-3

| | |
|---|---|
| Tag-Nr.: | FCV-2370 |
| Sollwert: | 70.5 % |
| Istwert: | 70.4% |
| NAMUR Status: | ✓ |

### Durchflussmessgerät Promass 83

| | |
|---|---|
| Tag-Nr.: | FIC-2370 |
| Massefluss: | 1567.7 kg/h |
| Dichte: | 0.9 g/cm³ |
| Temperatur: | 23.7 °C |
| Summenzähler: | 1345.6 kg |
| NAMUR Status: | ✓ |

# Architecture realization



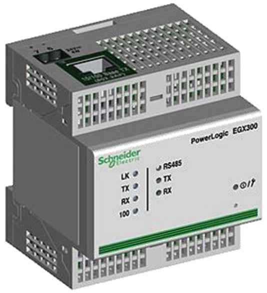
# Scenario owner: Schneider Electric

## Secure system decentralization

Schneider Electric

### Schneider Electric

- Schneider operates a factory with production lines instrumented with status sensors (such as voltage, anomaly) in a 1,300 $m^2$ facility in Nice.
- Industrial automation is used for production-line processes.
- Situation: No visibility into the status of company production machines and working station. Replace manual injection of this data to the system by connecting IoT infrastructure to the back end. Predictive maintenance has been identified as one aspect of the digital transformation.



### Solution

- Custom solution on SAP HANA
- Data fusion between IT and OT data
- Multidimensional assets description
- Remote machinery diagnostics
- Engineering rules and predictive models
- Dynamic optimization of maintenance schedules

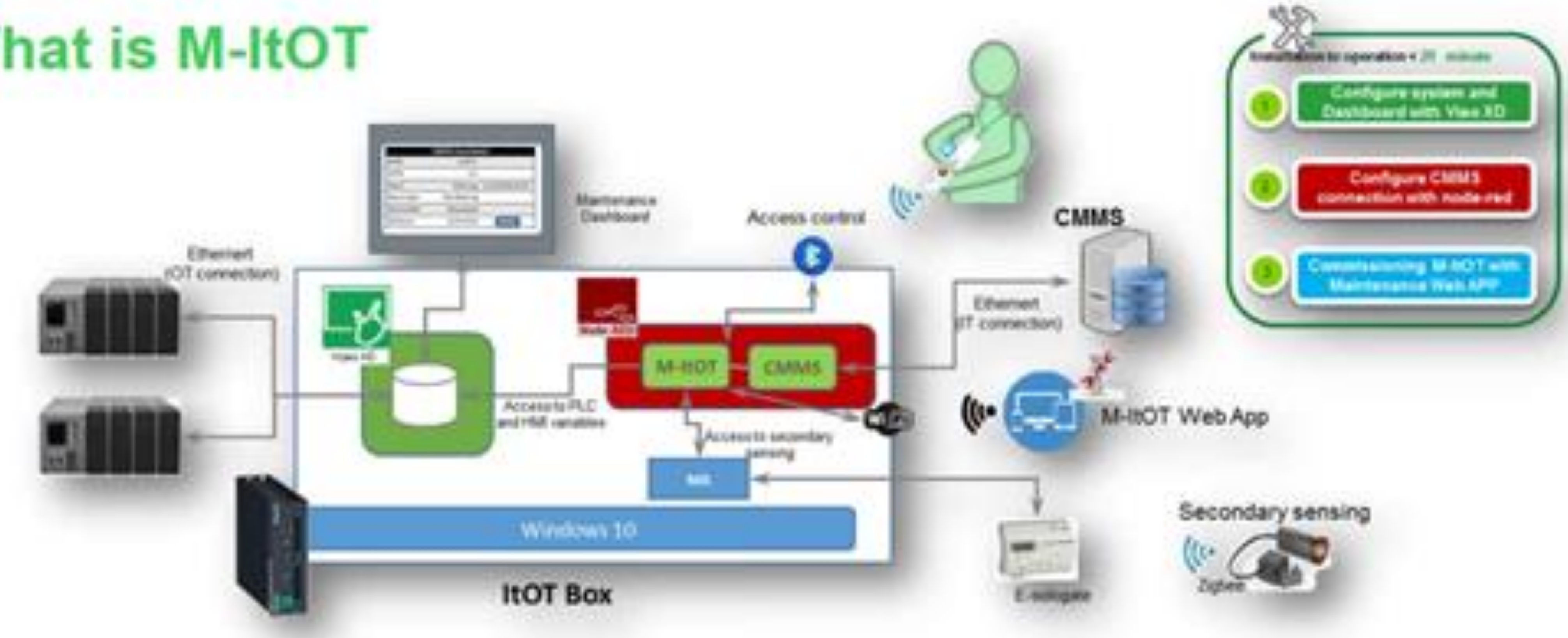
### Benefits

- Higher asset availability leading to higher passenger satisfaction
- Less effort for corrective maintenance

### Security requirements

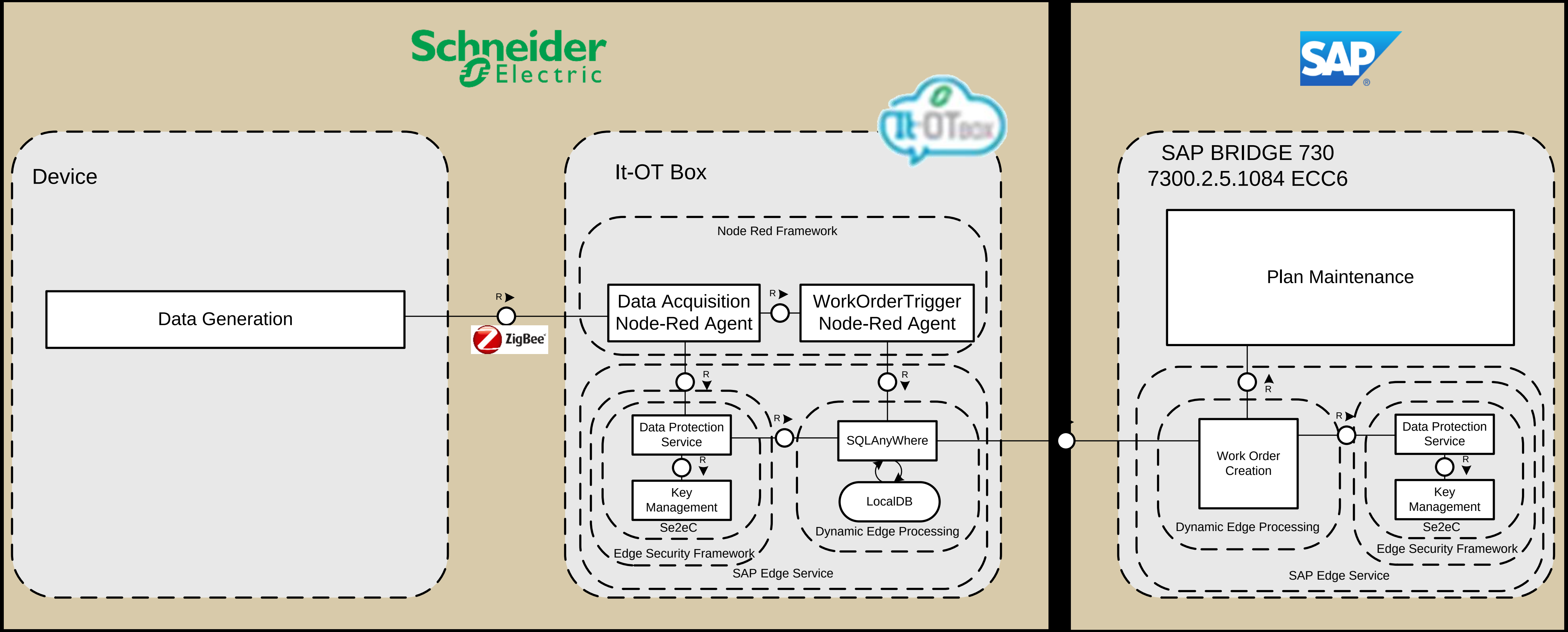
- Secure end-to-end communication over low-power connectivity
- Secure software execution

# What is M-ItOT


Installation to operation < 20 minute
1
Configure system and Dashboard with Vijeo XD
2
Configure CMMS connection with node-red
3
Commissioning M-ItOT with Maintenance Web APP
Maintenance Dashboard
Access control
CMMS
Ethernet (OT connection)
Ethernet (IT connection)
Vijeo XD
Node-RED
M-ItOT
CMMS
Access to PLC and HMI variables
Access to secondary sensing
Windows 10
M-ItOT Web App
Secondary sensing
Zigbee
E-sologate
ItOT Box

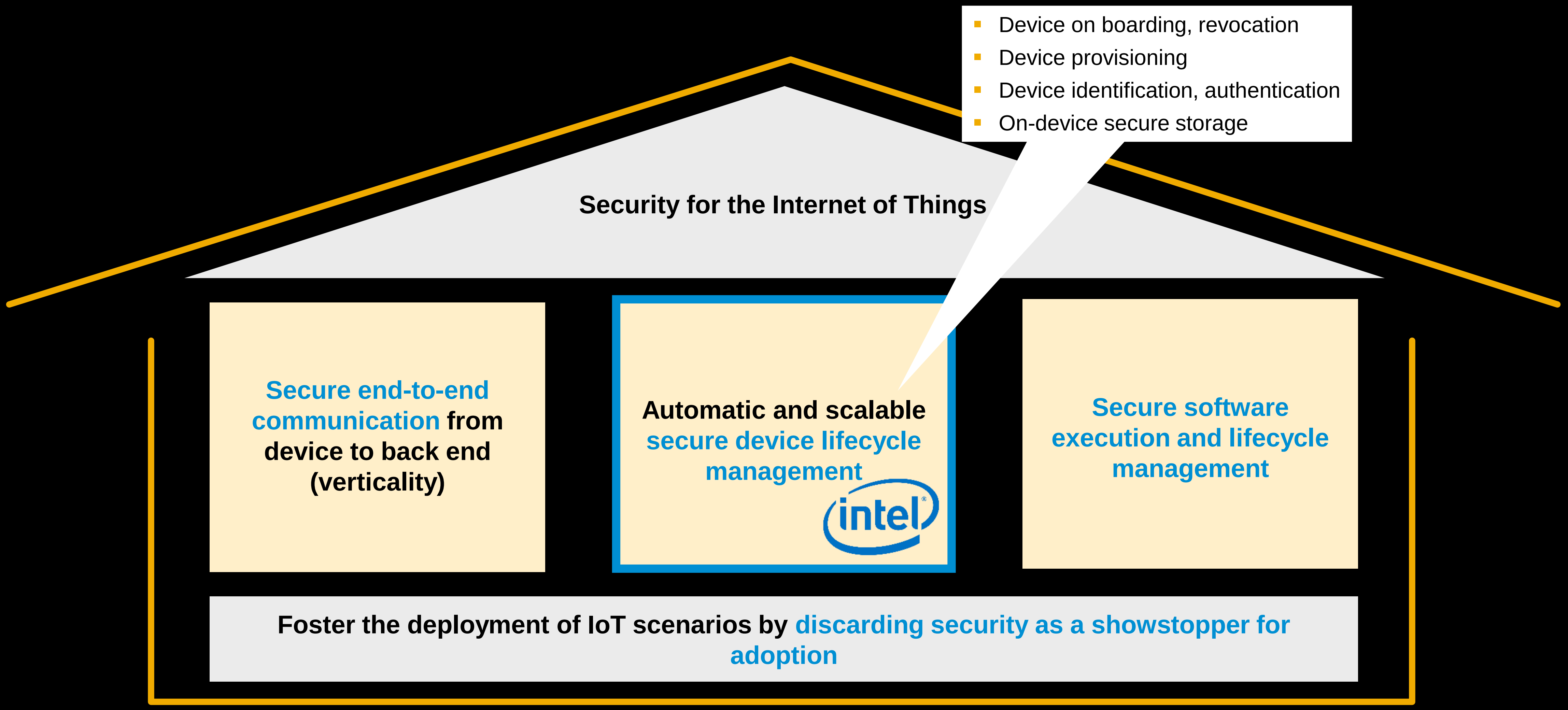
1. nodes to:
   a) Calculate machine operating times using power consumption Zigbee sensor.
   b) HMI maintenance dashboard.
   c) Handle maintenance work order using CMMS connection and HMI dashboard.
   d) Sense deviation of machine behavior using PLC variables or secondary sensing.
   e) Interface Maintenance Web App
   f) Connection to CMMS software (SE, partners, SAP, IBM Maximo)
2. Vijeo XD Maintenance template (dash board, maintenance work order handling).
3. M-ItOT App for setting and monitoring.
4. Electronic access control for maintenance crew members.

# Architecture realization



# Security for the Internet of Things

## Automatic and scalable secure device lifecycle management



- Device on boarding, revocation
- Device provisioning
- Device identification, authentication
- On-device secure storage

Security for the Internet of Things

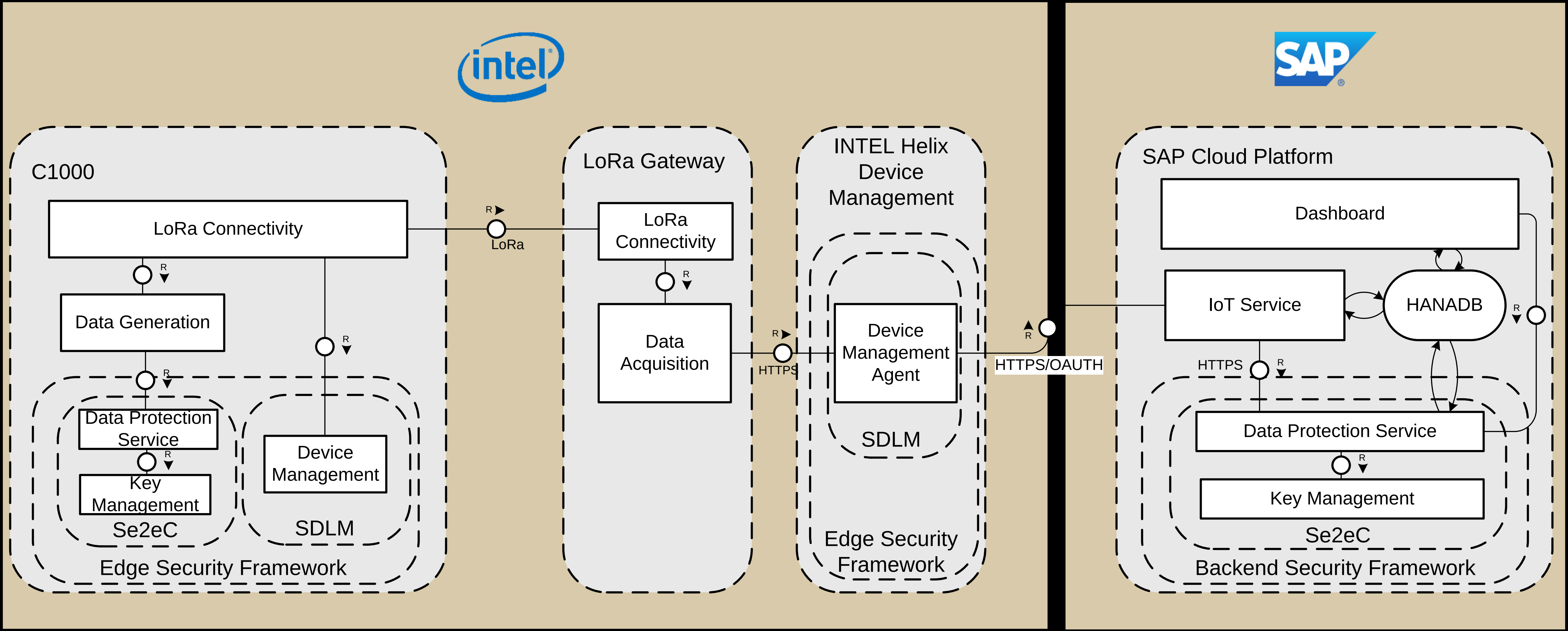
**Secure end-to-end communication from device to back end (verticality)**

**Automatic and scalable secure device lifecycle management**

**Secure software execution and lifecycle management**

**Foster the deployment of IoT scenarios by discarding security as a showstopper for adoption**

# Architecture realization



# Thank you.

Contact information:

**Dr. Laurent Gomez**
SAP Product Security Research
laurent.gomez@sap.com

**Dipl.-Inf. José Márquez**
IoT Central Architecture
jose.marquez@sap.com

Run Simple