

# IoT Trends and Regulation Impact

Esperanza Tien  
2018/7/5



# Agenda

1

IoT Security Trends and Attacks

2

GDPR Impact for Device Design

3

Secure Trust Anchor

4

Summary

# IoT Trend Affects All Markets

Smart Vehicles	Smart Cities & Energy	Smart Industry & Business	Smart Home & Consumer Devices
Smart Cars	Energy	Factory Automation	Smart Home
Commercial, Agriculture & Construction Vehicles incl. Trucks & Buses	Building Automation	Medical Equipment	Smartphones, Tablets & PCs
Low speed vehicles	Professional Lighting	Other Business	Consumer Electronics & Wearables
Other Transport	Infrastructure		

## Smart ICT

Communication Networks	Data Center / Server Farms
------------------------	----------------------------

# Security is essential

The connected world is further driving the demand for security



Infineon believes in hardware-based security as the essential trust anchor



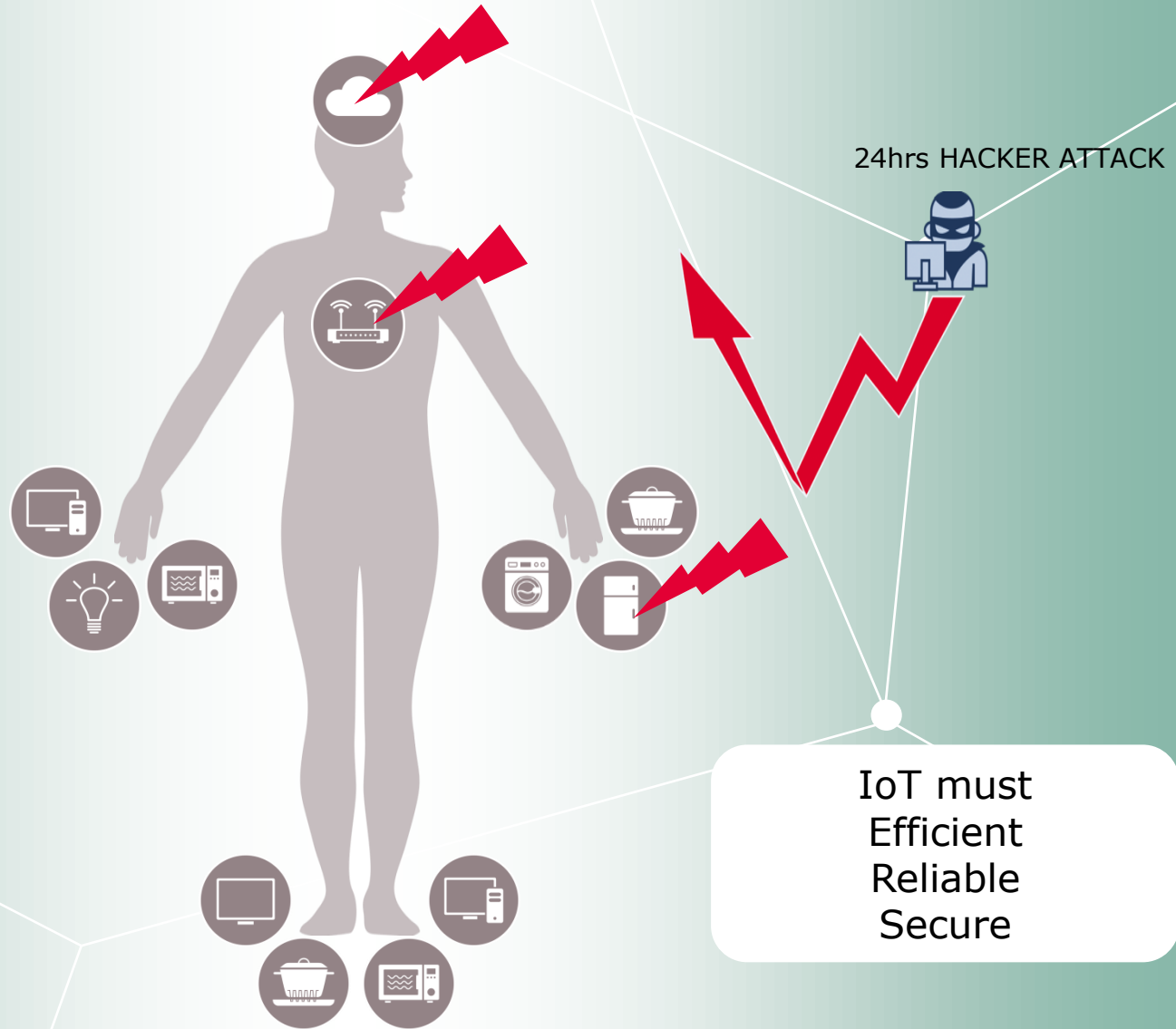
Security is a fundamental need of society with increasing importance

# Information & Communication Technologies: the nervous system of IoT

Gather data  
Analyze  
Send commands

Reliably convey data  
and commands

Send and receive  
data and commands





# And in the real world, Attacks are repeating again & again...

## Most comprehensive DDoS attack so far

- › Targeting systems operated by Domain Name System (DNS) provider Dyn
- › Up to 100.000 malicious endpoints used  
- **Mainly Smart Home devices (surveillance cameras)**
- › (top) Effected companies: Airbnb, Amazon, Fox news, PayPal, Shopify, Starbucks, Swedish government, Twitter, Visa
- › More then 65 effected organizations

### How smart home devices are being hijacked to attack Internet

By Matthew Lang | October 22, 2016 | Updated: October 22, 2016 6:59pm



Photo: Jim Cook, iStockphoto.com

Dyn of Manchester, N.H., was the target of a major cyberattack.

The huge cyberattack that crippled the Internet and disabled dozens of websites Friday appeared to be the biggest attack of its kind that the world has ever seen.

<http://www.sfchronicle.com/business/article/How-your-baby-monitors-are-being-used-to-attack.php>

PC REVIEWS BEST PICKS HOW-TO NEWS TIPS BUSINESS EXPLORE

### Web Services Work to Stabilize After Massive DDoS Attack

BY STEPHANIE MILOT, CHLOE ALBANESCU | OCTOBER 21, 2016 03:44PM EST | 6 COMMENTS  
"Our engineers are still investigating and mitigating the attacks on our infrastructure," Dyn says.



**Update 3:45 p.m. ET**  
Shortly after resolving the early morning attack, Dyn reported another DDoS attack "against our Dyn Managed DNS infrastructure," which it said was resolved around 2:45 p.m. "Our engineers are still investigating and mitigating the attacks on our infrastructure," according to Dyn.

<http://www.pcmag.com/news/3489/22/ddos-attack-knocks-twitter-spotify-others-offline>

Technology

### 'Smart' home devices used as weapons in website attack

© 22 October 2016 | Technology | Share



Net-connected cameras are helping attackers in large-scale attacks

Hackers used internet-connected home devices, such as CCTV cameras and printers, to attack popular websites on Friday, security analysts say.

<http://www.bbc.com/news/technology-37738823>

### DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the "primary source of malicious attack" © Major cyber attack disrupts internet service across Europe and US

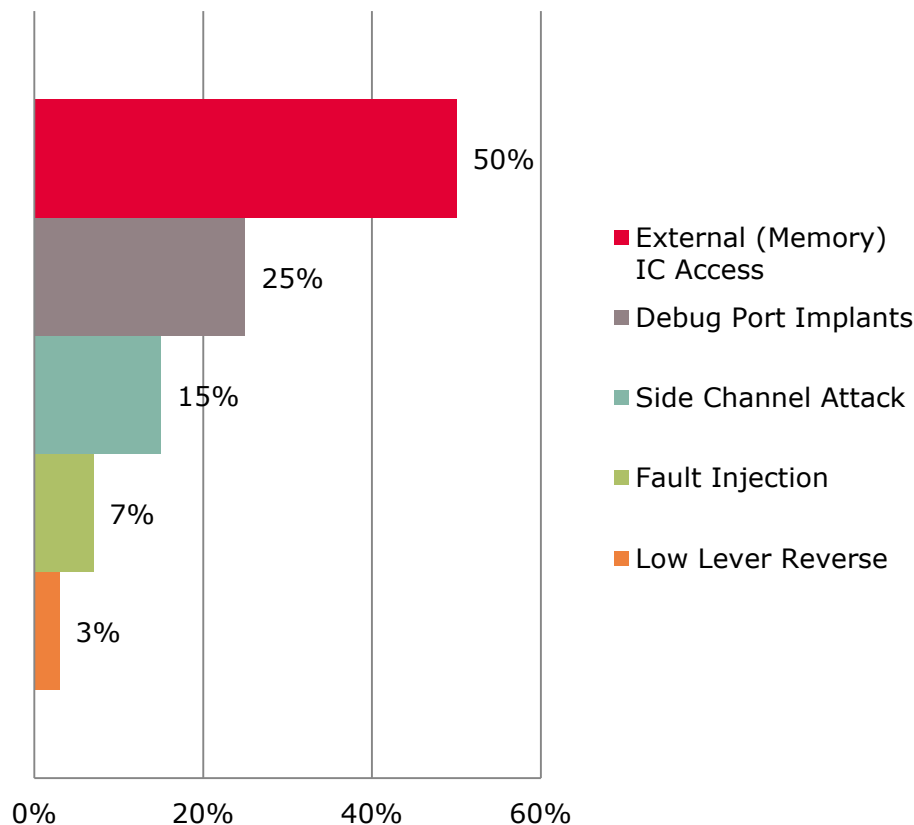


© Dyn estimated that the attack had involved 100,000 malicious endpoints, and the company said there had been reports of an extraordinary attack strength of 1.2 terabits (1,200 gigabytes) per second. Photograph: Alamy

<https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet>

# Penetration Attacks

## Hacker's Way to do Penetration Attack

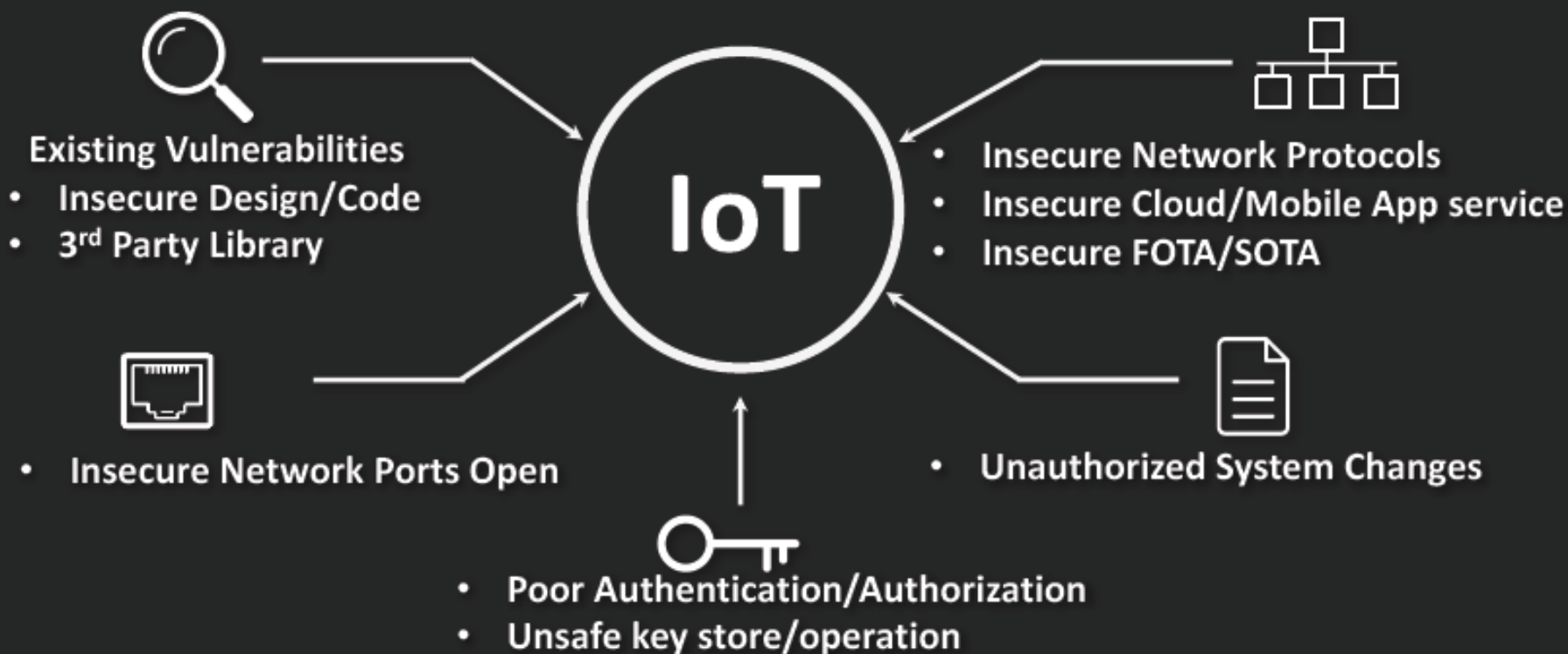


- › External RAM, NVM and Cypto/common co-processor.
- › JTAG/UART/USB for Monitoring and debugging.
- › Internal crypto engines for SW or external storage protections.
- › SoC doesn't have secure key store.
- › Non-certified or low cost security IC.

› Source from InfoKeyVault. [www.ikv-tech.com](http://www.ikv-tech.com)

# Major IoT Device Security Weakness

Trend Micro identified five major IoT Devices Security weakness in 2016



Source: Trend Micro IoT Security Headline - IoT Devices Security Guideline <https://www.trendmicro.com/jp/iot-security/special/40>



# Agenda

1

IoT Security Trends and Attacks

2

GDPR Impact for Device Design

3

Secure Trust Anchor

4

Summary

# IoT Security by Legislation & Regulation

## 影像監控資安產業標準驗證 明年開跑

2017年12月14日 04:10 工商時報 簡立宗

在經濟部工業局支持下，資策會資安所與台灣資通產業標準協會將於明（107）年開始推動檢測驗證工作，並於12月8日舉辦「影像監控系統系列設備資安產業標準公開說明會暨測試成果發表會」，會中公布資安產業標準最新進度說明及測試成果，宣告物聯網資安標準將正式啟動。大會主席威聯科技總經理張明智表示，資安技術標準的制定，能夠加速產業發展，對台灣科技業有深遠的戰略意義。影像監控是物聯網的重要環節，影像監控產業有明確的資安標準，將有助於將影像監控應用置入物聯網開發框架，擴大影像監控智能化應用範疇，安全地將智能影像分析技術發揮在物聯網的應用當中。

資策會資安所副所長丁綺萍表示，此資安標準是確保物聯網產品資安防護能力的基礎。依循此標準建立資安檢測與認證制度是後續努力的方向。資安所將利用過去累積App資安檢測的成功推動經驗，結合資安所的物聯網資安檢測技術研發能量，未來將會繼續協助政府並與資安業者合作，帶動我國資通產業資安能力的提升。在產官學研專家通力合作下，已順利完成影像監控系統的資安產業標準制定工作，包含IPCAM（影像監控系統網路攝影機）、NVR（數位錄影機）及NAS（數位聯網儲存設備），明（107）年將試行產品檢測及驗證服務，協助國內國產品通過資安檢測驗證，排除外銷障礙，取得產品出口優勢，協助產業在競爭激烈的國際市場中，掌握競爭之優勢。

## Security rules

Oct 5, 2016 (updated)

FRI JAN 7 02:25 PM

## NETWORK-CONNECTABLE PRODUCT

- SMART HOME
- HVAC
- BUILDING AUTOMATION
- ALARM SYSTEMS

## CYBERSECURITY SOLUTION

### TESTING SERVICES

- Fuzz Testing
- Known Vulnerabilities
- Code & Binary Analysis
- Access Control & Authentication
- Cryptography
- Remote Communication
- Software Updates
- Structured Penetration Test

### TRAINING SERVICES

### ADVISORY SERVICES

### REVIEW SERVICES

✓ RISK MITIGATION ✓ INNOVATION ✓ COMPETITIVE ADVANTAGE

TECHNOLOGY NEWS | Fri Dec 2, 2016 | 6:08pm EST

## U.S. presidential commission issues recommendations on cyber security

COMMISSION ON ENHANCING NATIONAL CYBERSECURITY

REPORT ON SECURING AND SHOWING THE DIGITAL ECONOMY

## 《网络安全法》关键点



### 《网络安全法》关键点

《网络安全法》共七章七十九条，明确了多方面的网络安全要求，包括维护国家网络空间主权、保护关键信息基础设施与重要数据、保护个人隐私信息、明确各方网络安全义务等。纵观《网络安全法》，毕马威认为企业及相关组织机构应重点关注以下关键内容：



### 个人信息保护

《网络安全法》明确了对于个人信息收集、使用及保护的要求。



### 关键信息基础设施

“关键信息基础设施”的保护要求在《网络安全法》中反复提及。



### 网络运营者

“网络运营者”：网络的所有者、管理者和网络服务提供者。《网络安全法》明确了网络运营者的多项安全职责。



### 敏感信息保存

《网络安全法》要求在境内运营收集或产生的个人信息/重要数据，应在境内存储。



### 安全产品认证

网络关键设备和网络安全专用产品应在安全认证合格后，方能销售或提供。



### 法律责任

对于违反《网络安全法》的企业及组织机构，最高处罚金额可达100万元人民币。

### > History

Directive 95/46/EC  
of 24 October 1995

72 Prefaces / 7  
Chapters / 34 Articles

Data Protection Act  
(DPA) of  
EU Member states



REGULATION (EU) 2016/679 OF  
THE EUROPEAN PARLIAMENT  
AND OF THE COUNCIL of 27 April  
2016

on the protection of **natural persons** with  
regard to the **processing of personal  
data** and on the free movement of such  
data, and repealing Directive 95/46/EC  
(General Data Protection  
Regulation)

173 Prefaces / 11 Chapters / 99  
Articles

### > Who does the GDPR apply to?

#### > GDPR applies to ‘controllers’ and ‘processors’.

- > A controller determines the purposes and means of processing personal data.
- > A processor is responsible for processing personal data on behalf of a controller.

[https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules\\_en](https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en)

# GDPR Short Summary

- › 執行日期 2018年5月25日
- › 違反GDPR有關控制者與處理者之義務、認證機構之義務或監管機構之義務者，最高處以一千萬歐元之行政罰鍰，如維企業，最高處以前一會計年度全球營業額之百分之二，以較高者為準。

## 規範對象

對歐盟境內人民提供商品、服務、客戶中有歐盟公民、雇用歐盟員工。

## 個資定義

包括電話號碼、地址、行動裝置 ID、社群網站等，會暴露個人身份的資料，以及血統、政治意見、宗教、生物特徵、性傾向等個人特徵都算。

## 當事人權利

更正權、刪除權、個資可攜權、拒絕權。

## 企業責任

知悉個資遭侵害，需 72 小時內通報與通知、個資保護影響評估、個資保護設計及預設。

Source Business Next

<https://www.bnext.com.tw/article/49249/gdpr-general-data-protection-regulation-eu->

# GDPR Technical Impact- Encryption

- › Encryption: GDPR Articles 5(1)(f) and 32(1)(a)
- › 依據適合風險安全級別，GDPR明確將加密做為一項重要技術措施。
- › 可能需要加密，如通過網路傳輸個人數據或儲存在諸如筆記型電的移動設備上時。此外，可以使用加密來實線訪問控制機制，如用於數據庫漢被分儲存。
- › 適用對象:產品（必須）/服務（必須）
- › 與產品(product)、個人數據控制者(controller)服務與個人數據處理者(processor)相關問題:
  - 通過媒體漢不安全網路進行數據傳輸，是否加密?
  - 加密是否用於訪問控制(例如，數據庫或備份)?
  - 如果產品不包含加密功能，那麼對手冊中的用戶提供建議?
  - 加密是否有效?(密要長度，演算法及加密算法已知弱點)
  - 加密密鑰如何管理?
  - 金鑰遺失/遺忘的影響?
  - 密鑰是否以安全的方式傳輸(例如，託管服務器硬碟加密的密鑰)?

Source : Techknowledge Services Group



# Agenda

1

IoT Security Trends and Attacks

2

GDPR Impact for Device Design

3

Secure Trust Anchor

4

Summary

# Main security concerns for end customers



Identity Protection  
against **Fake Devices**



Protection against  
**Eavesdropping**



Protection against the  
**Manipulation of the  
Data**



Protection against  
**illegal Update of  
Firmware**

# Trust Anchors: The best way to protect keys



Key security is **essential** for system security

1

Compromised keys = no security

2

Cloning of key leaves no traces

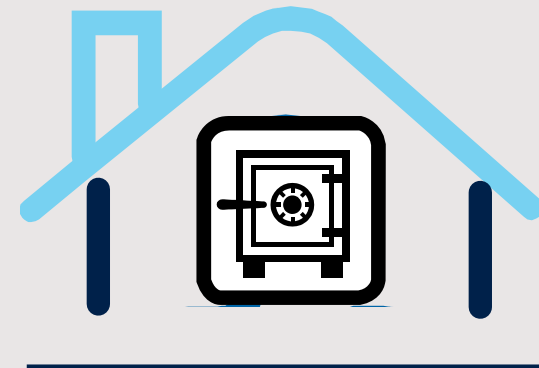
3

Key handling must be secured through the whole lifecycle including manufacturing




## Trust Anchors

- › Key store
- › Crypto operation
- › Key management

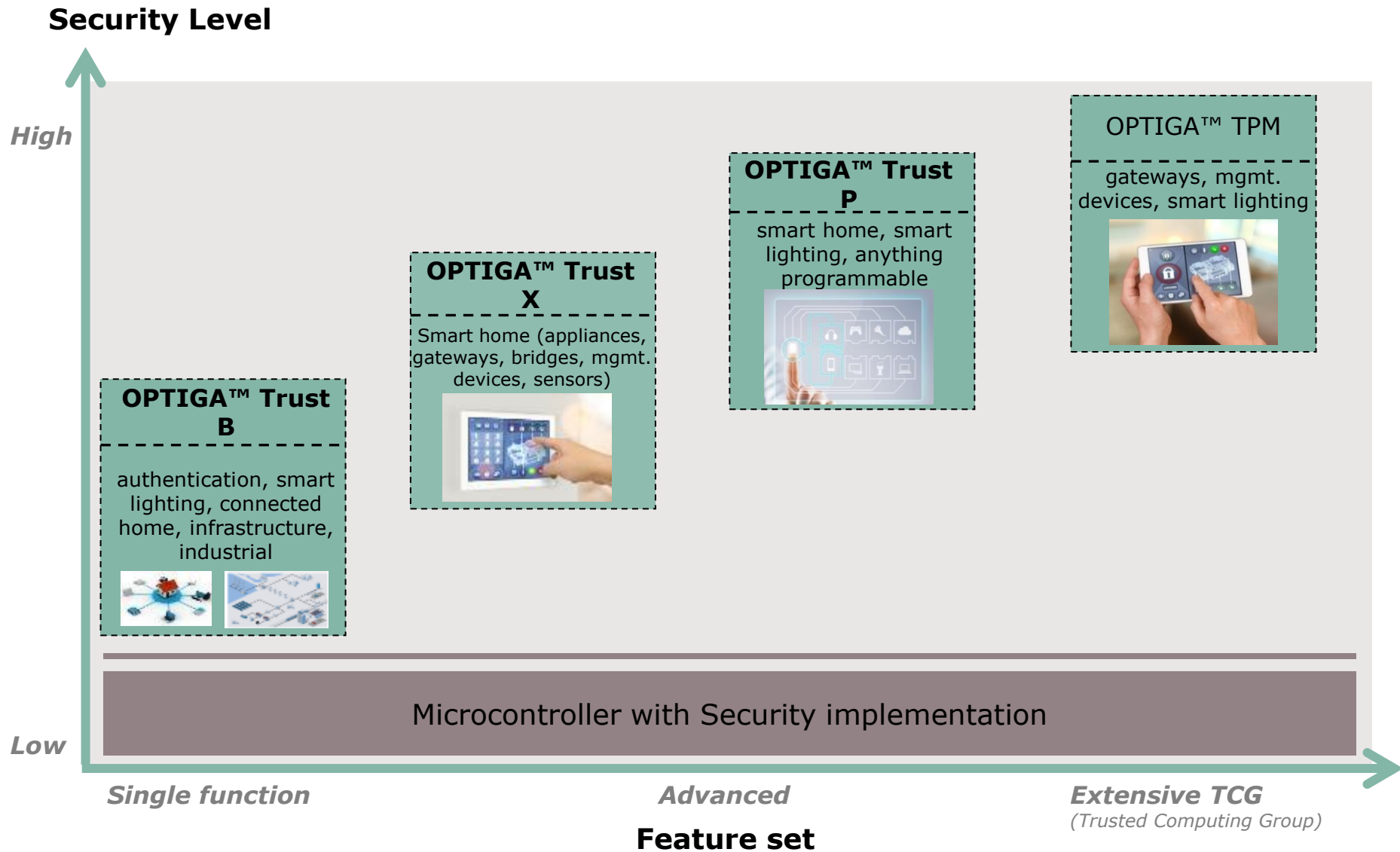


# Why hardware security in IoT device?



	Main CPU    Software		Main CPU    Software    Hardware 		
Crypto functionality	✓			✓	
Strong isolation	—			✓	
Security-certified	—			✓	
Tamper-resistant	—			✓	
Manufactured using security-certified processes	—			✓	
Resistant to IP theft	—			✓	

# Infineon security products address multiple security requirements





# Agenda

1 IoT Security Trends and Attacks

2 GDPR Impact for Device Design

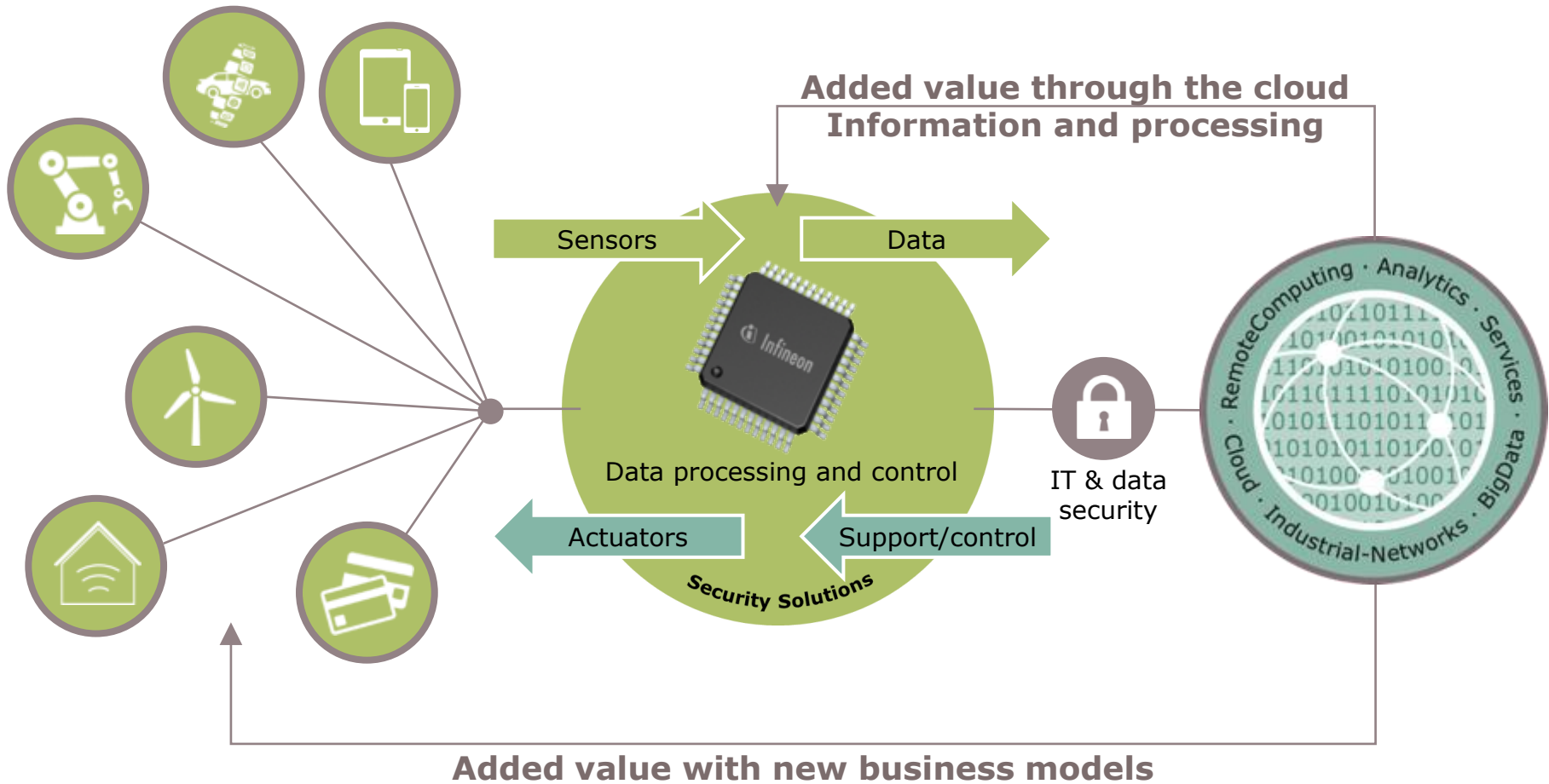
3 Secure Trust Anchor

4 Summary

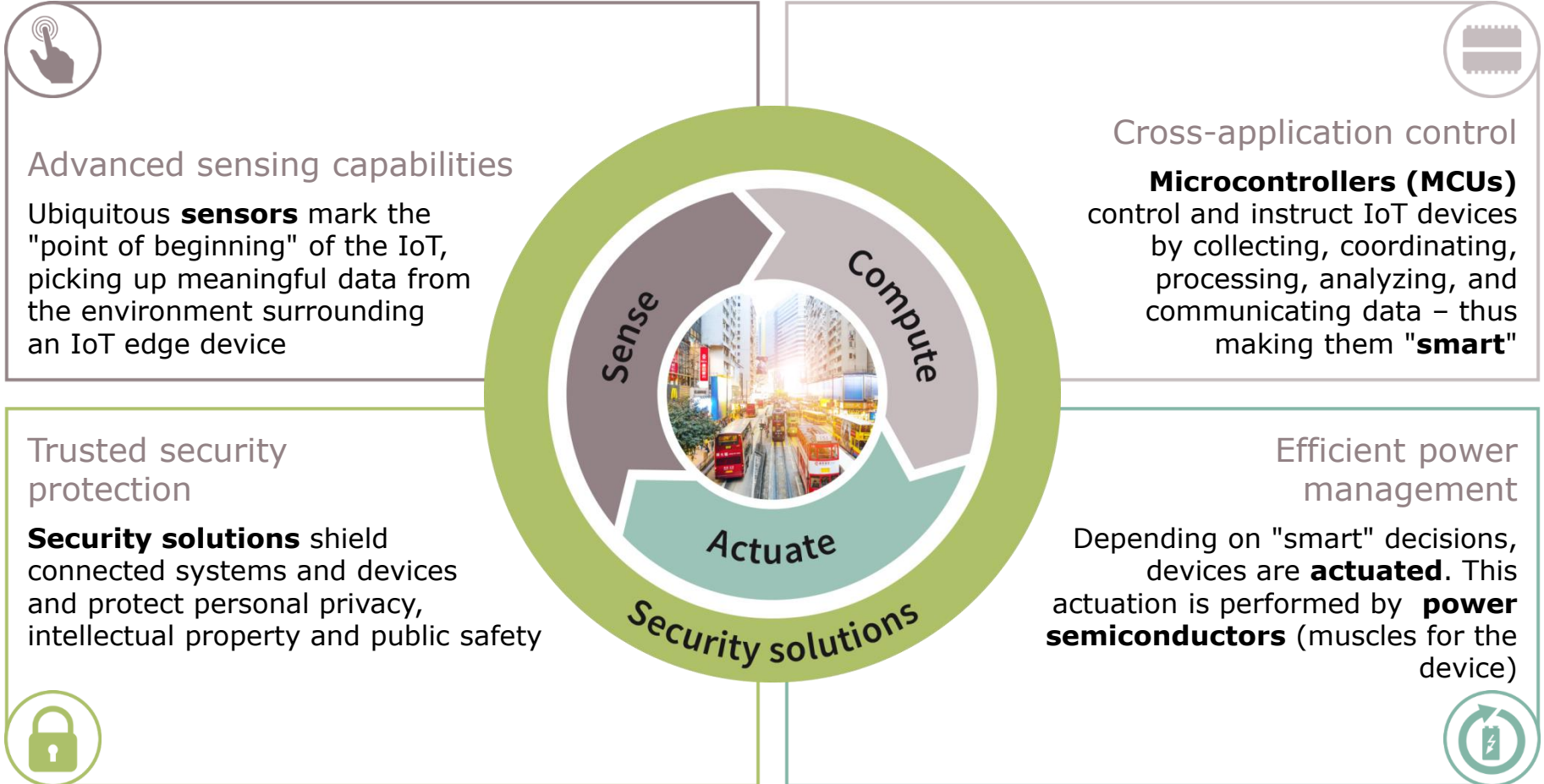
# Our belief: hardware-based security

- › Hardware security can be integrated into any system
- › Hardware security avoids extra work for users and can even simplify user experience
- › Hardware security provides the best available protection

# Semiconductors are the crucial link between the real and digital worlds



# Infineon helps to create sustainable IoT success for its customers



Making the Internet of Things smart, secure and power-efficient – based on our understanding of connected systems

# 全球半導體解決方案的領導者

我們的願景  
現實與數位世界的連結

企業價值  
承諾 合作  
創新 成效

我們的使命  
讓生活  
更加便利、安  
全和環保

## 美好生活 定義未來