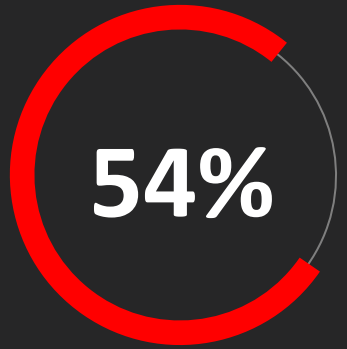
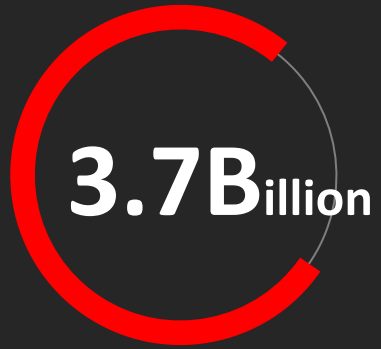
智慧城市安全嗎？

Bob Hung
Trend Micro TW/HK GM

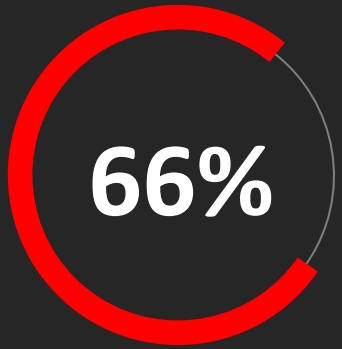
為什麼要讓城市“聰明”？



目前世界上有一半以上(54%)的人口居住在城市地區，而在50年代只有30%。



2009年，全球人口估計為68億，居住在城市的人口約37億。

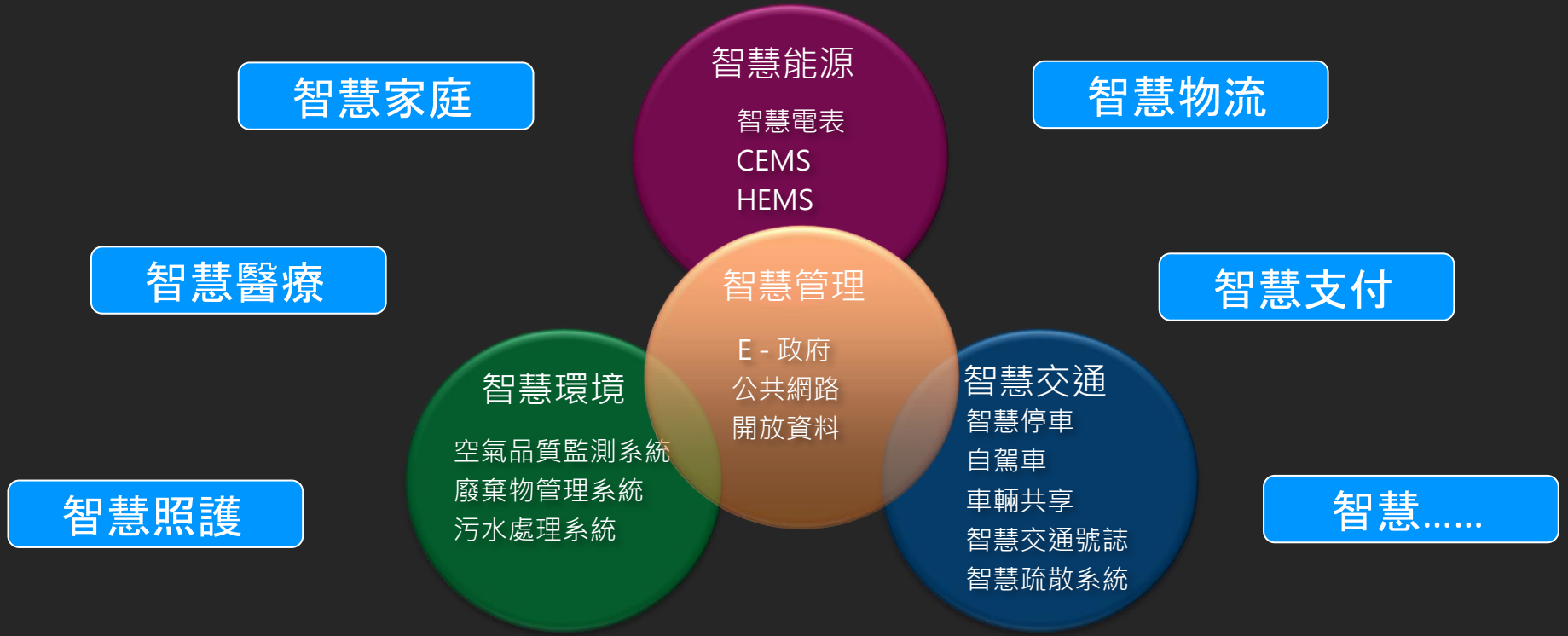


到2050年，所有人中有66%是城市居民

為了應對這些社會，經濟和環境挑戰，公共和私營部門大力投資智慧城市技術

https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-smart-cities

智慧城市的關鍵領域


智慧家庭
智慧能源
智慧電表
CEMS
HEMS
智慧物流
智慧醫療
智慧管理
E - 政府
公共網路
開放資料
智慧支付
智慧環境
空氣品質監測系統
廢棄物管理系統
污水處理系統
智慧交通
智慧停車
自駕車
車輛共享
智慧交通號誌
智慧疏散系統
智慧照護
智慧.....

智慧城市- 安全威脅

- 城市佔全球能源消耗的70%左右，佔世界各國生產總值（GDP）的70%
- 任何形式的惡意入侵，破壞和情報收集都將對智慧城市造成以下重大影響


公共安全


經濟損失


社會混亂


政治不安


法律與秩序失衡

https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-smart-cities

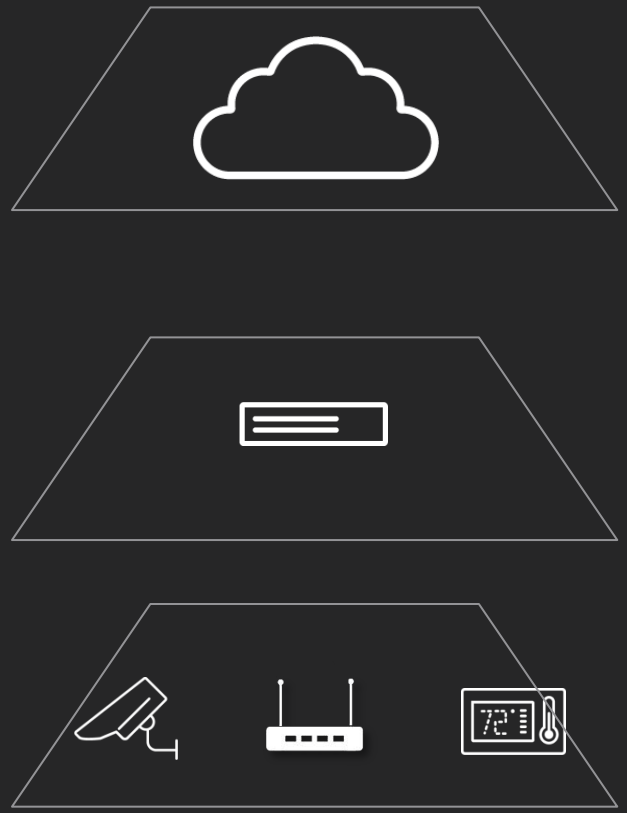
TREND MICRO

物聯網資訊基礎架構

1 雲端層
Data Landing

2 網路層
Data Transmission

3 裝置層
Data Collection



TREND MICRO

“物” 改變了

過去

- 個人
- 中小企業
- 大型企業

現在與未來

- 個人
- 中小企業
- 大型企業
- 工業
- 關鍵基礎設施
- 城市
- 政府
- 國家

TREND MICRO

智慧城市的風險因素

更新困難	多樣曝險位置	無人管理	系統限制	資安難以確保
				
與傳統系統共存更新和修補困難	多樣可攻擊點;設備，網路閘道，網絡和雲	資訊安全管理權責不明	設備裝置的系統限制導致資安方案導入困難	沒有良好的測試方法或規定，設備製造商難以測量安全性

https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-smart-cities

TREND MICRO

Hotel Smart Keys System

Ransomware hijacks Austria hotel smart keys to lock guests out of their rooms.

http://thehackernews.com/2017/01/ransomware-hotel-smart-lock.html

US baby monitor hacked

Stranger hacks baby monitor and talks to child at night.

http://kdvr.com/2015/04/21/couple-whose-baby-monitor-was-hacked-has-message-for-other-families/

Hijack a Jeep's digital system remotely

Take control of steering and braking systems.

https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

HID Door Controllers

Remote Control all of alarm and locking functionality via vulnerability

http://blog.trendmicro.com/let-get-door-remote-root-vulnerability-hid-door-controllers/

The City's Emergency Sirens System

The emergency sirens system was hacked in US, 156 emergency sirens were activated for 2 hours.

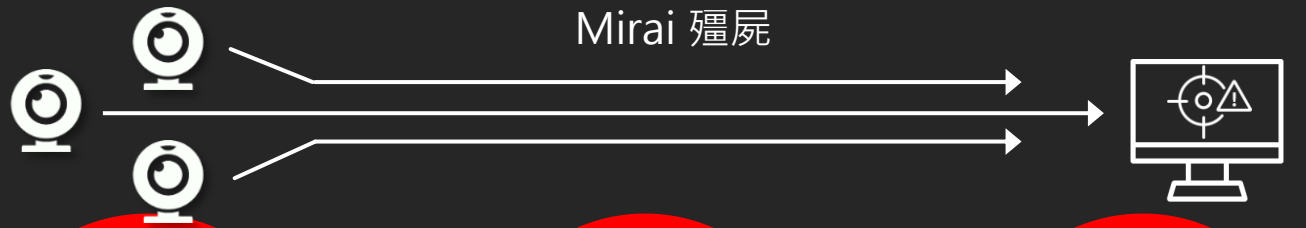
https://www.cnet.com/news/hackers-blamed-for-activating-emergency-sirens-in-dallas/

Power Plants in Ukraine

Power outage affecting ~225,000 customers was work of hackers.

https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

Mirai 阻斷式攻擊 - 2016年 10月21號



1.2Tbs → 500M → 75

創下史上巨量的阻斷式攻擊

Dyn 轉址服務受到超過 5億個 IP 位置要求 執行網域名稱轉址服務 (DNS lookup)

主要網站受到影響（ 例如 Twitter, Netflix, Spotify ...)

Mirai 只利用數十萬的連網裝置 (IPCam, Router)，當天早上就摧毀了美國東海岸的大部分地區，之後遍及到德州，華盛頓州和加州的數據中心都出現了問題甚至完全關機。

TREND MICRO

IPCam資安現況

a 15% 的 IPCam 直接暴露在 Internet上. 佈建流程脆弱

b 暴力破解是主要攻擊事件

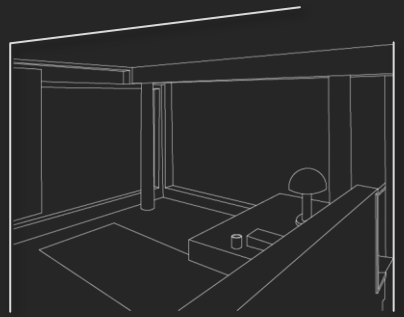
c 4% 的事件是駭客利用已知漏洞的攻擊

智慧家庭資安現況

a 15.44% 家庭曾遭網路攻擊

b **2.95% 家庭物聯網設備遭入侵**

c **對內攻擊 vs 對外攻擊 比例 3.5 : 1**



物聯網資訊安全架構

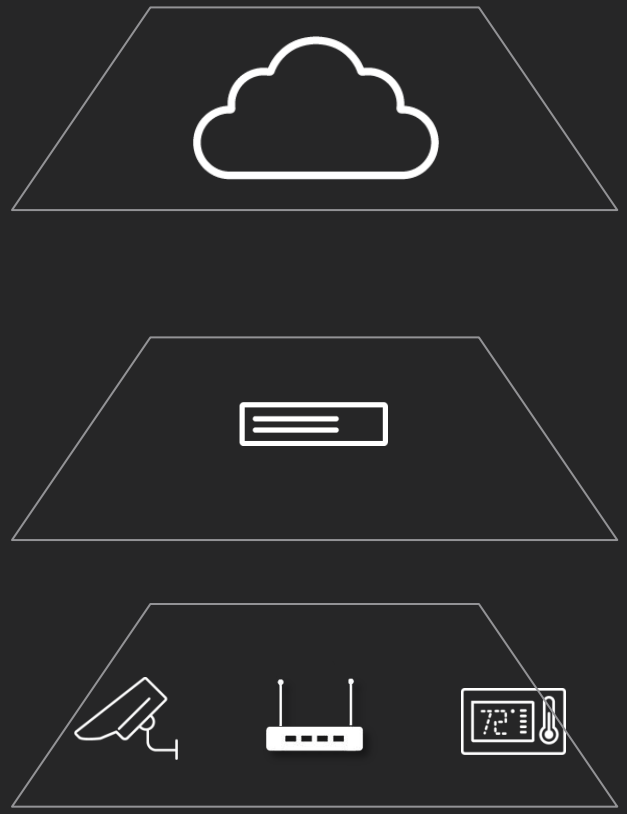
1 雲端層
Data Landing
雲端資料保護

2 網路層
Data Transmission
網路場域保護

3 裝置層
Data Collection
裝置端點保護

Keeps it Secure

Builds it Secure



安全管理

進行弱點測試
訂定資訊安全要求
成立資安事件應變組織
確保軟體持續安全更新
使用週期年限規劃
考慮資料隱私處理
連線管道加密與認證
手動停止的機制
容錯處理的系統設計
確保服務的連續性

Thank You!