眺望2020 5G+AI時代 物聯網安全高峰論壇

# 從 IoT 安全防護視角，全方位審視5G部署對策

## 全球行動網路趨勢, 物聯網安全的演進及解決方案, 5G 安全架構

錢小山

首席技術顧問

思科大中華區數據中心架構事業部

二〇一九年十一月


# 全球行動網路趨勢

Source: Cisco VNI Global Mobile Data Traffic Forecast, 2017–2022

# 全球行動數據預測

Mobile
Momentum Metrics

By 2022

| | More Mobile Users | More Mobile Connections | Faster Mobile Speeds | More Mobile Video |
|---|---|---|---|---|
| 2017 | 5.0 Billion | 8.6 Billion | 8.7 Mbps | 59% of Traffic |
| 2022 | 5.7 Billion | 12.3 Billion | 28.5 Mbps | 79% of Traffic |

Source: Cisco VNI Global Mobile Data Traffic Forecast, 2017 – 2022

# 每月全球平均行動用戶和行動流量

| | 2017 | 2022 |
|---|---|---|
| Average Traffic per User |  2.3 GB per month |  13.3 GB per month |
| Average Traffic per Connection |  1.3 GB per month |  6.3 GB per month |

Source: Cisco VNI Global Mobile Data Traffic Forecast, 2017 – 2022

到 2022 年，M2M 通信模塊將佔全球設備和連接總數的 51%（146億個），並將佔全球 IP總流量的 6%（25.3 EB / 月）。

Source: Cisco VNI Global IP Traffic Forecast, 2017 – 2022

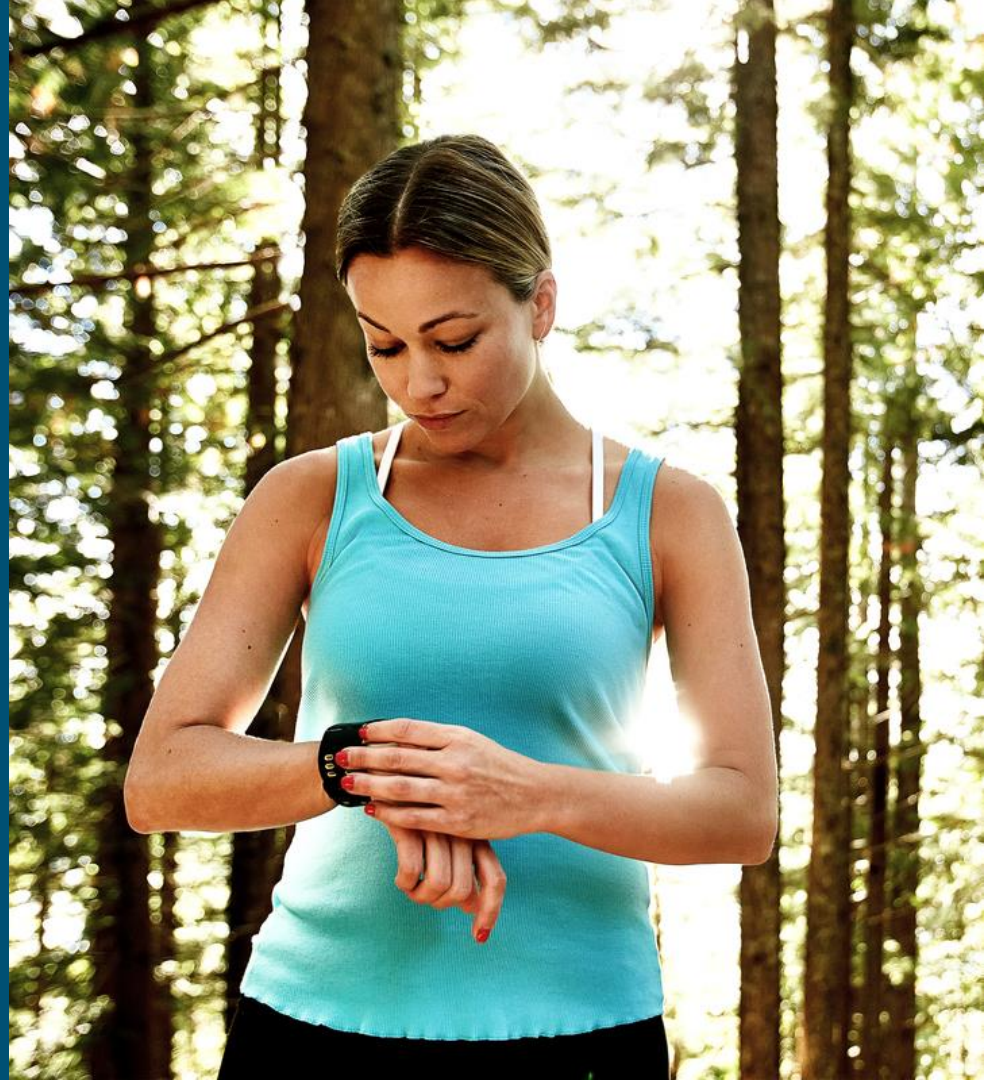


# 到 2022 年，M2M 通信模塊將佔全球行動設備和連接總數的 31%，並將佔行動數據流量的2%（每月1.7 EB）。

Source: Cisco VNI Global Mobile Data Traffic Forecast, 2017 – 2022

# 到 2022 年，全球可穿戴設備總數的 10% 將具有嵌入式行動連接。

Source: Cisco VNI Global Mobile Data Traffic Forecast, 2017 – 2022



# DDoS 攻擊規模和流量持續增加

最高攻擊強度同比增加 174%。*

DDoS 攻擊發生時，最多可到達一個國家/地區總 Internet 流量的 25%。

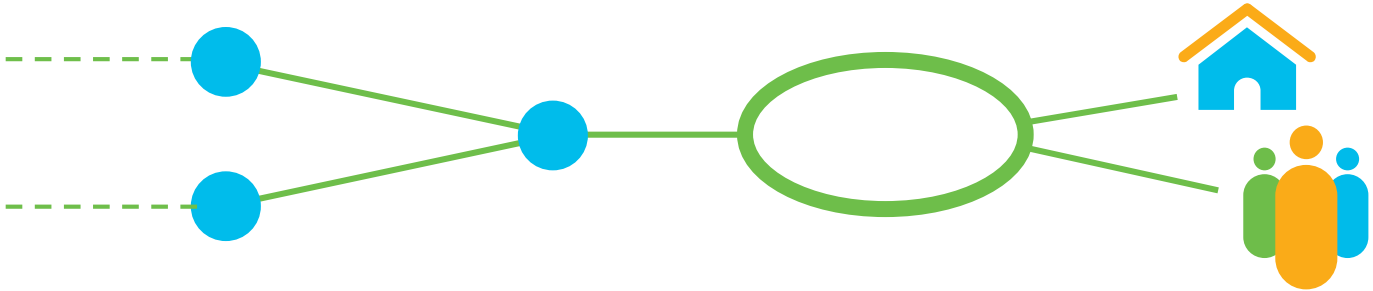
1-2 Gbps 的平均 DDoS 攻擊量同比增長了 37%，比 Internet 流量同比增長 33%快。

* 1H2017- 1H2018



Source: Arbor Networks, Cisco VNI Global IP Traffic Forecast, 2017 – 2022

# 到 2022 年，服務運營商網路流量將會有將近三分之一完全繞過核心網路, 終結在邊緣



Core – Cross-Country
48% in 2017
43% by 2022

Core – Regional
25% by 2017
24% by 2022

Within Metro
27% in 2017
33% by 2022

# *The Future Of Computing Is At The Edge*

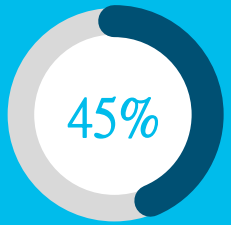
" Around 10% of enterprise-generated data is created and processed outside a traditional centralized data center or cloud. By 2025, Gartner predicts this figure will reach 75%"

https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders/

## Edge Computing Is A Top Of Mind In Securing Industrial IoT


of workload deployments have latency & BW requirements


of large enterprises will integrate edge compute into their 2021 projects




of IoT device data will be stored, processed, analyzed and acted upon close to or at the edge of the network by 2020

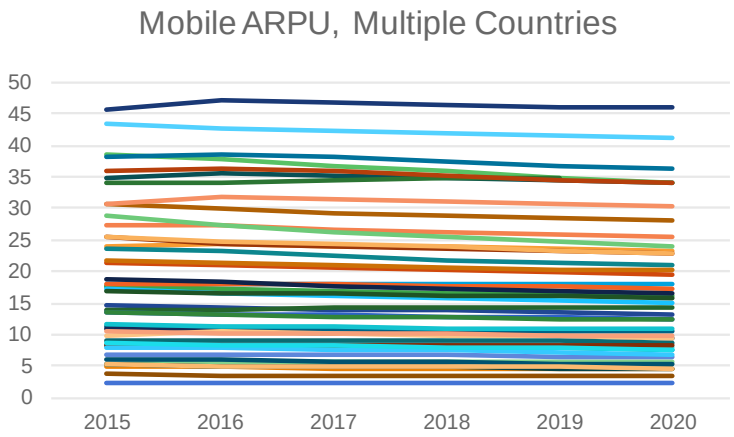

# 物聯網安全的演進

You make security **possible**

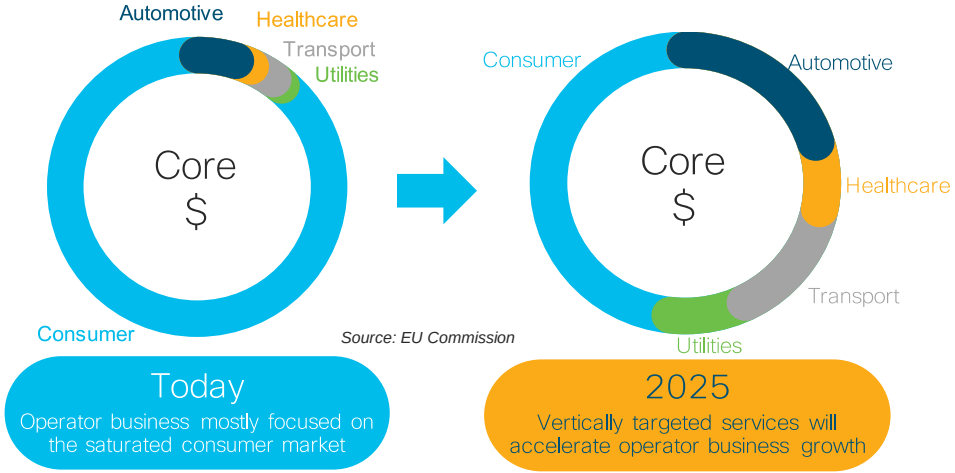
CISCO

# 物聯網是企業網路內部最大的攻擊面之一

# 5G 的生意經?

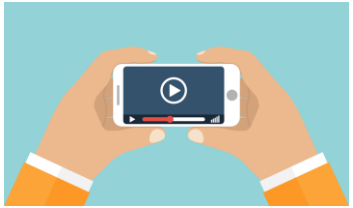



*Consumer ARPUs are Declining or Flat*

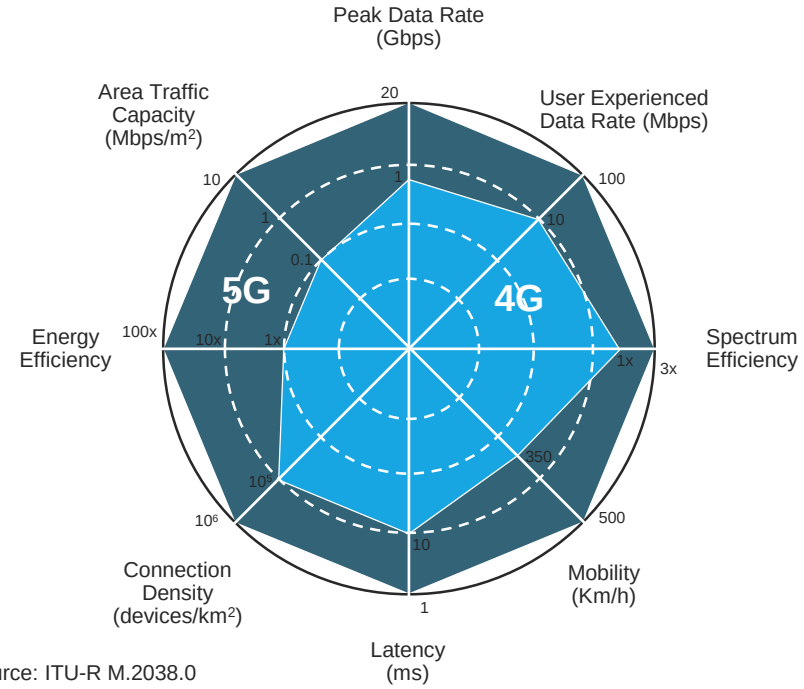



*B2B or B2B2x Market Has Future Growth*

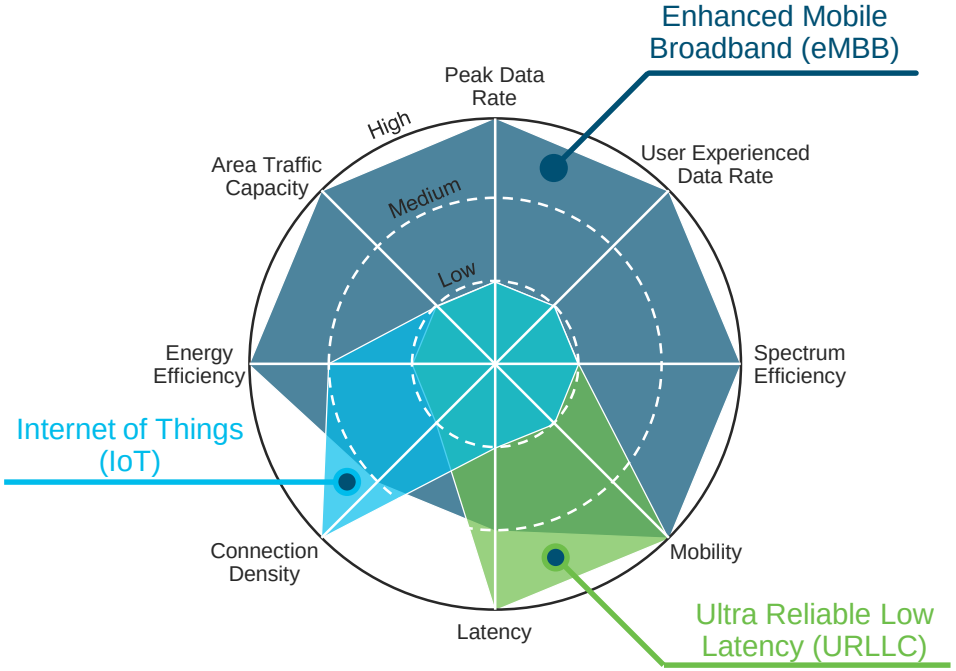
**Low Latency** for better QOE and to Enable New Applications, ***Customer Experience*** Transformation



# 物聯網是 5G 關鍵用例之一

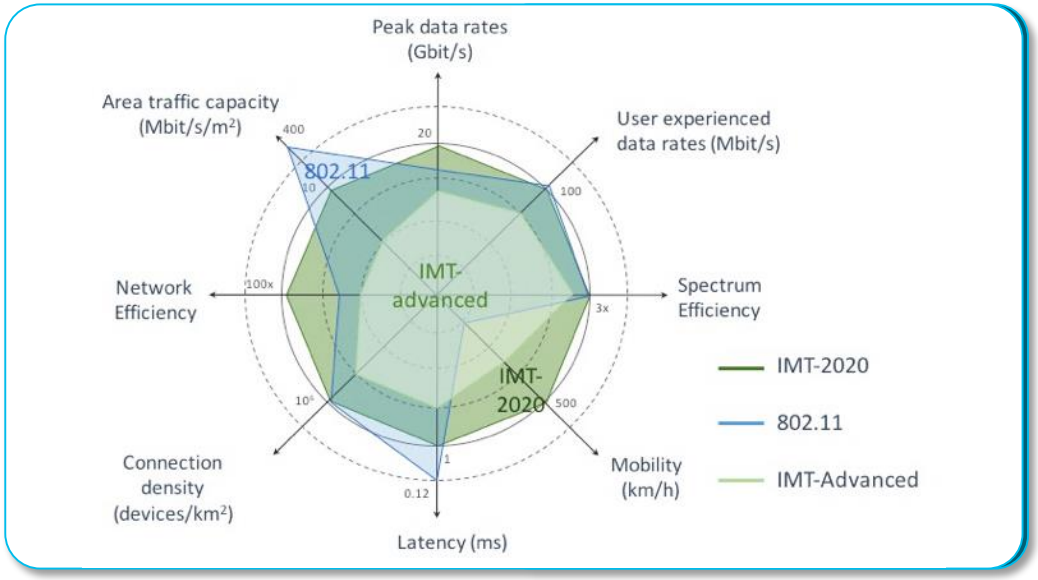



Source: ITU-R M.2038.0




No enhanced to radio access technology planned for IOT in 3GPP R15

# 802.11ax（Wi-Fi 6）和 5G 非常相似


“Evidently, the divergences between 3GPP and IEEE 802.11 MAC designs are set to diminish with the introduction of 802.11ax”

## Connected Home

- Home automation
- Building security
- Network equipment – printers +
- Network infrastructure – routers +
- White goods
- Tracking applications
- Household information devices

## Connected Work

- Office building automation
- Building security
- Office equipment – printers +
- Routers +
- Commercial appliances

## Connected Car

- Fleet management
- In-vehicle entertainment systems, emergency calling, Internet
- Vehicle diagnostics, navigation
- Stolen vehicle recovery
- Lease, rental, insurance management

## Connected Health

- Health monitors
- Assisted living – medicine dispensers +
- Clinical trials
- First responder connectivity
- Telemedicine

## Connected Cities

- Environment and public safety – closed-circuit TV, street lighting, waste removal, information +
- Public space advertising
- Public transport
- Road traffic management

## Retail

- Retail goods monitoring and payment
- Retail venue access and control
- Slot machines, vending machines

## Manufacturing & Supply Chain

- Mining and extraction
- Manufacturing and processing
- Supply chain
- Warehousing and storage

## Energy

- New energy sources – monitoring and power generation support apps
- Smart grid and distribution
- Micro-generation – generation of power, by residential, commercial and community users on their own property

## Other

- Agriculture – livestock, soil monitoring, water and resource conservation, temperature control for milk tanks +
- Construction: Site and equipment monitoring
- Emergency services and national security

# 物聯網的需求

## Automation & Monitoring

50 – 500kbps | High
Fixed | 10 Years

## Security & Surveillance

0.5 – 8Mbps | Low
Fixed | Connected

## Fleet Management

100s of Kbps | Low
10 – 150Km/h | ~3 months

## Smart Cities

50 – 500Kbps | Low
Fixed | 10 Years

## Automotive / Telematics

10s of Mbps | Low
10 – 150Km/h | Vehicle

## Wearables

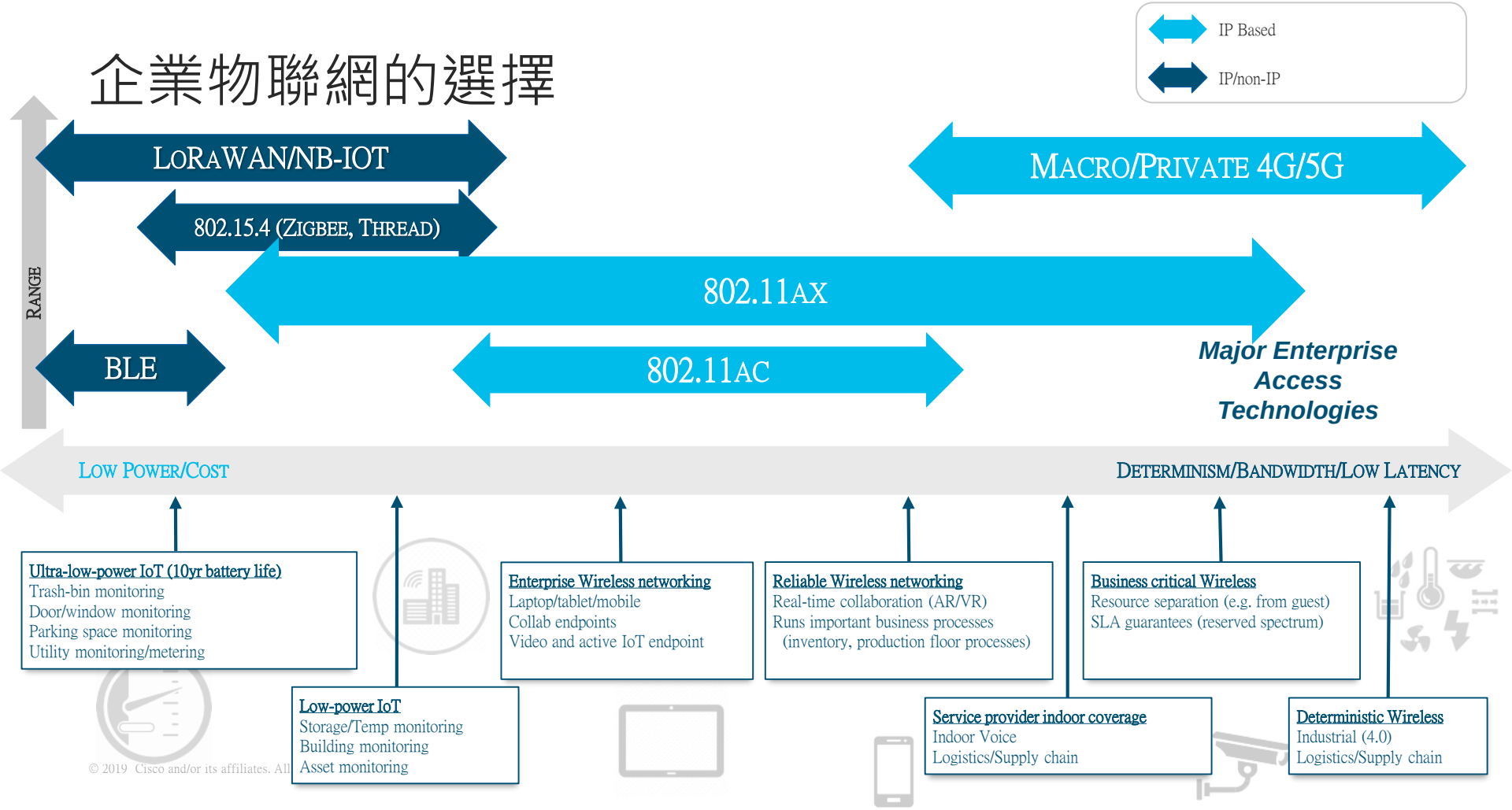
10s of Mbps | Low
~5Km/h | ~1 week

# 低延遲的用例 (5G & WiFi 6)

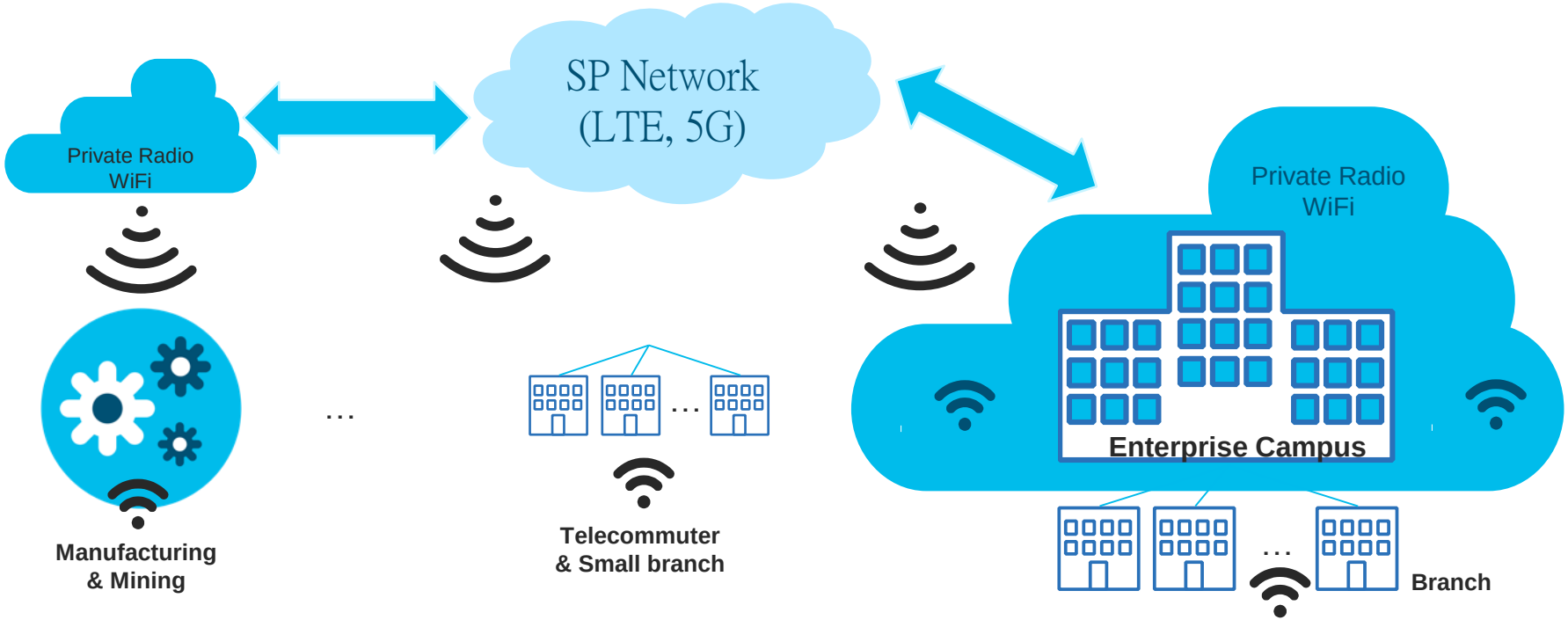
| Use Case | | Description | $RTT$ / $PLR$ |
|---|---|---|---|
| Factory Automation |  | Real-time control of machines and systems in production lines | $0.25 - 10\ ms$<br>$PLR \sim 10^{-9}$ |
| Intelligent Transportation |  | Autonomous driving and optimization of road traffic (platooning and overtaking) | $0 - 100\ ms$<br>$PLR \sim 10^{-3} - 10^{-5}$ |
| Robotics and telepresence |  | Remote control with synchronous visual-haptic feedback | $10 - 100\ ms$ |
| Virtual Reality/ Augmented Reality/gaming |  | Other applications for VR/AR and gaming exist beyond prior discussion. See reference | $1\ ms - 40\ ms$ |
| Health care |   | Tele-diagnosis, tele-surgery | $1 - 10\ ms$ |
| Smart Grid |  | Switching on/off electrical sources to compensate for demand fluctuations | $100\ ms$ |

Source: Parvez, I., et al. (2017). "A Survey on Low Latency Towards 5G: RAN, Core Network and Caching Solutions." arXiv preprint arXiv:1708.02562.

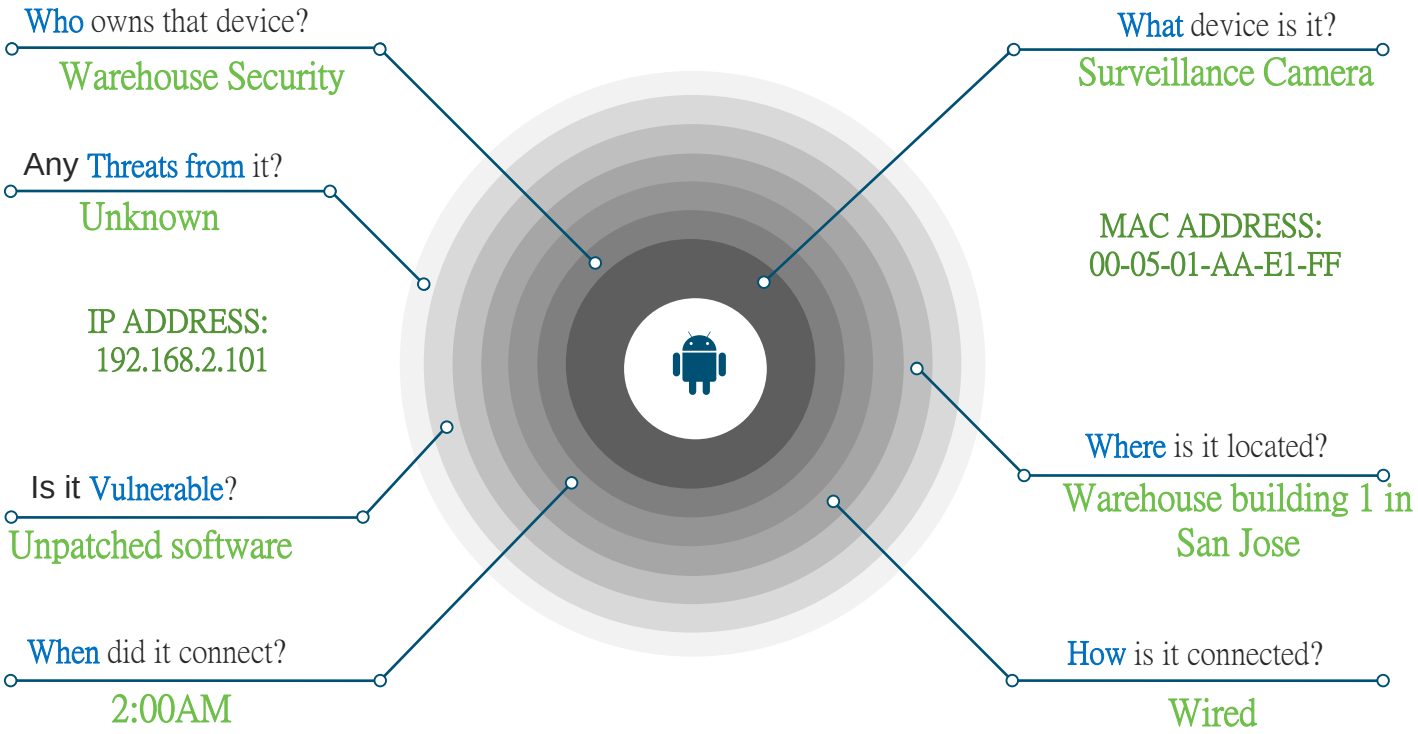
# 企業物聯網的選擇



# 並且需要多重網路訪問連接



# 物聯網的安全顧慮之一 - 缺乏可見度



# 物聯網設備的安全挑戰 – 能見度, 策略, 標準

## Device Visibility

Do you know devices well enough to differentiate service?

## Intent-based Policy

Does customer knows behavior of devices to build their policy?

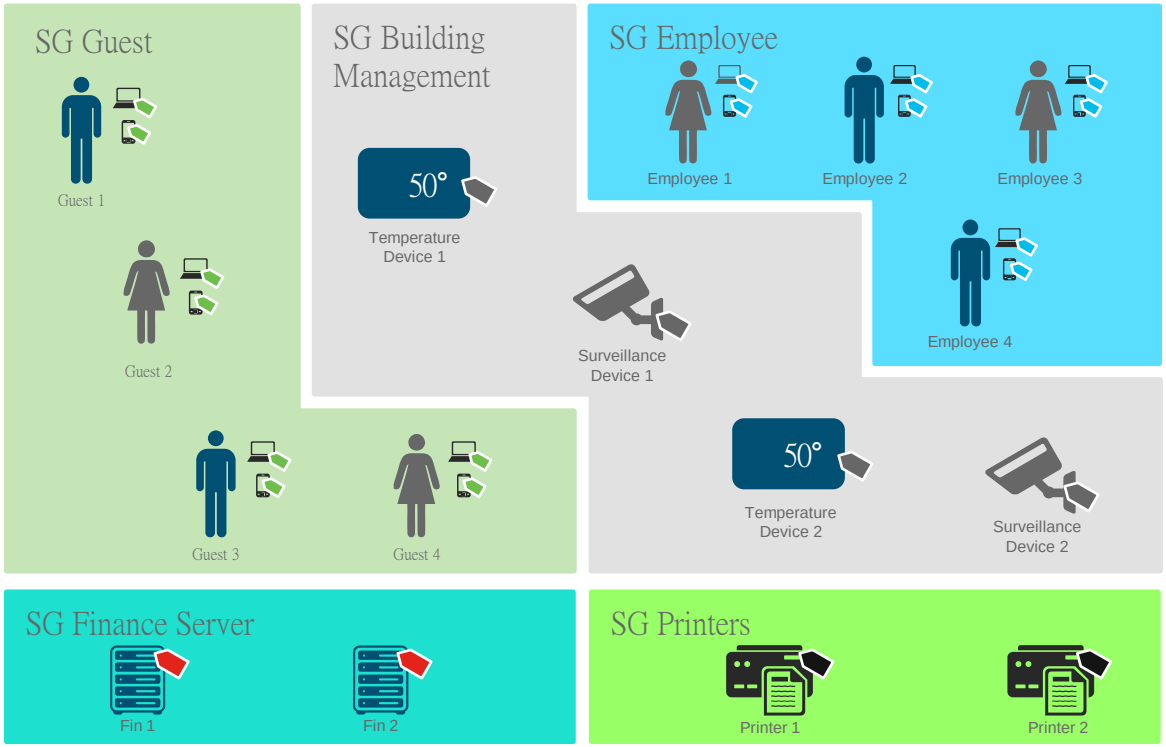
## Standard based

Is there any industry standard way of connecting IoT devices to enterprise network?

# 基於能見度的的安全細分

- Intent based groupings to provide consistent policy and access independent of network topology
- Leverage attributes such as location and device type to define group assignments

SG → Scalable Group aka Security Group



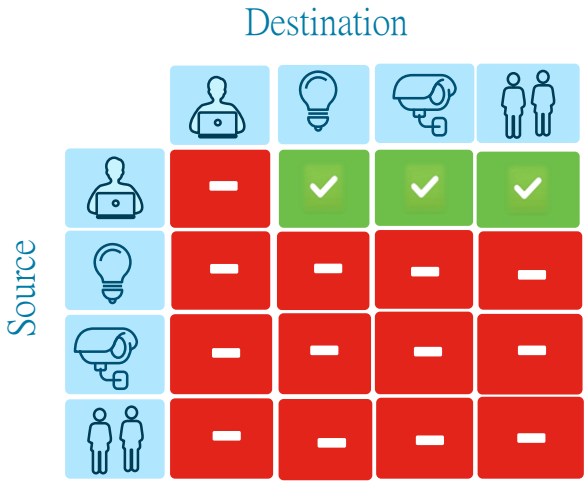
# 物聯網安全解決方案

- Group based policies
- Manufacturer Usage Description
- IOT Visibility with MUD 1.0
- Protecting IOT using MUD and Group based policy
- IT/OT Convergence
- DevNet

# Group based policy 建構區塊

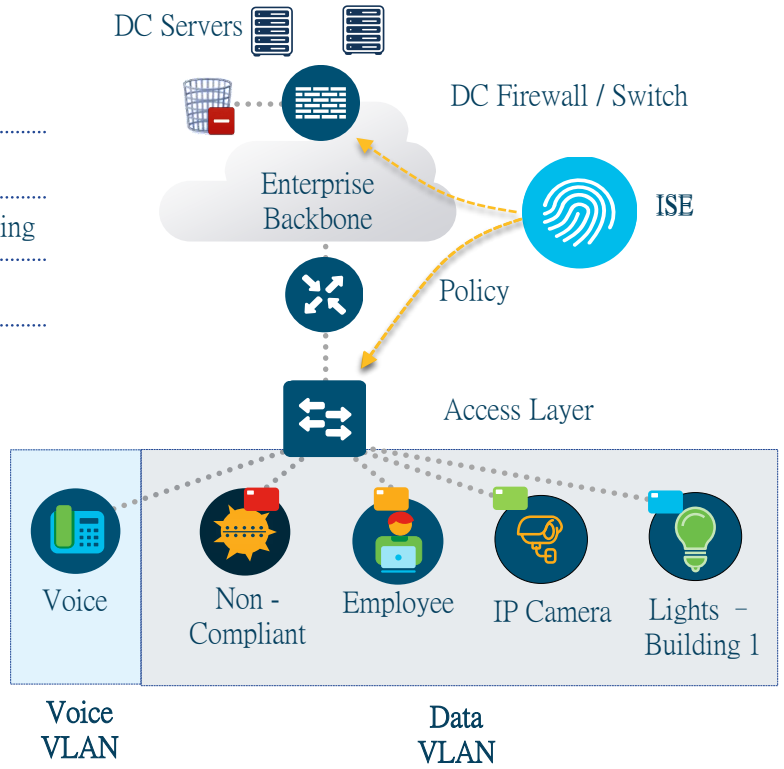
## Scalable Groups (SGT)


## Group based Policy



# Group based policy 用例 – 安全細分

- Micro Segmentation
- Central Policy Provisioning
- No Topology Change
- No VLAN Change

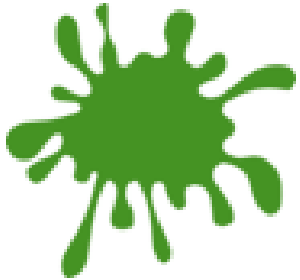



- Employee Tag
- IP Camera Tag
- Lights – Building 1 Tag

Use existing topology and automate security policy to reduce OpEx

Tag (short for Scalable Group Tag)

# 物聯網安全解決方案



- Group based policies
- Manufacturer Usage Description
- IOT Visibility with MUD 1.0
- Protecting IOT using MUD and Group based policy
- IT/OT Convergence
- DevNet

# 新的物聯網標準

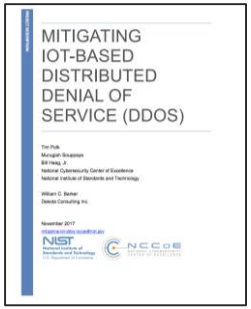
Addresses visibility and segmentation challenges for IoT devices

IETF®

RFC 8520
March 19, 2019

https://datatracker.ietf.org/doc/rfc8520/

NIST




https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos

# MUD 回答兩個問題

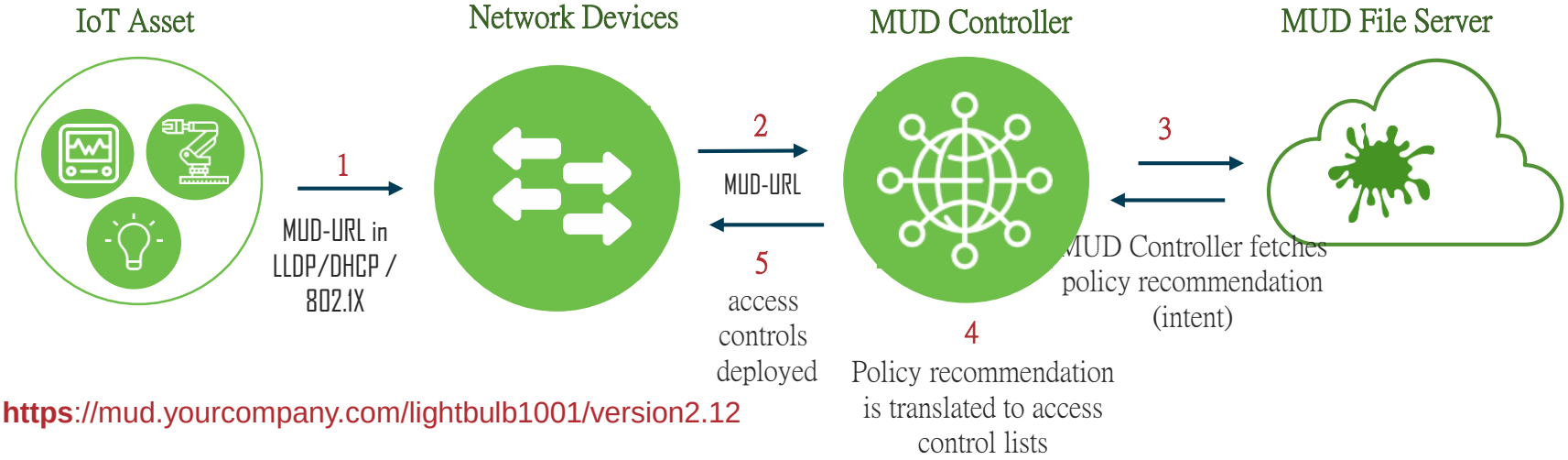
What type of Thing is this?

What policies are appropriate for it?

# Manufacturer Usage Description (MUD)


The URL points to a file in a file server or Manufacturers web server. If you are a customer using an IOT device then this URL will be automatically embedded by the manufacturer and your infra would forward this.

# MUD 運作架構




**https**://mud.yourcompany.com/lightbulb1001/version2.12

# 將意圖轉化為訪問控制策略

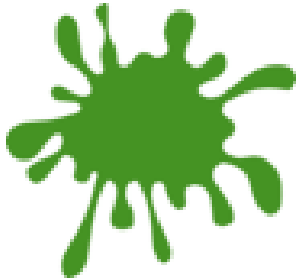
Allow traffic to manufacturer web server hosting the service

permit host mud.yourcompany.com

Deny access for the rest

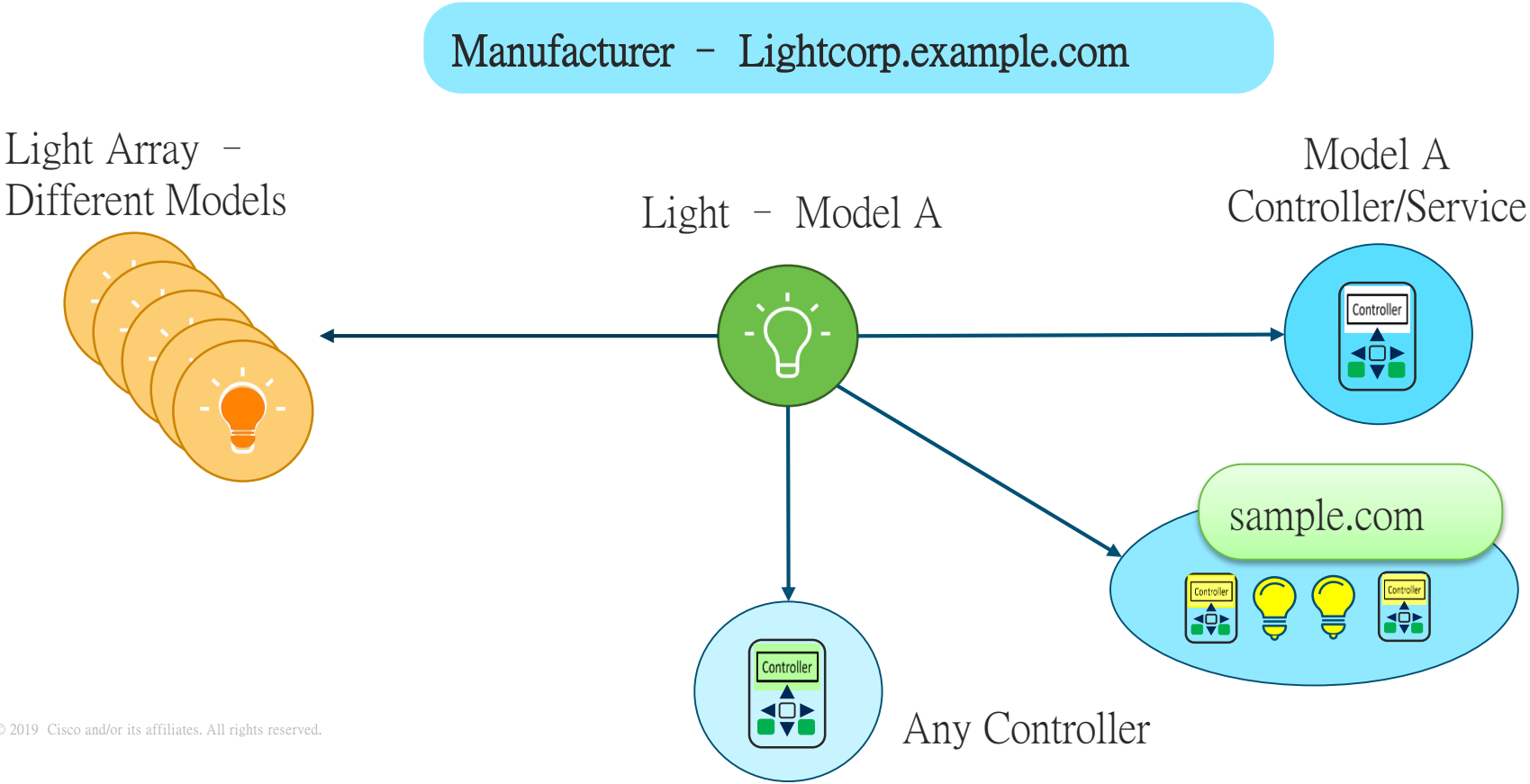
deny any

# 物聯網安全解決方案



- Group based policies
- Manufacturer Usage Description
- IOT Visibility with MUD 1.0
- Protecting IOT using MUD and Group based policy
- IT/OT Convergence
- DevNet

# 這個燈泡與控制器需要什麼通道？



# MUD 下燈泡的訪問控制

## MUD Access Controls

- Internet communication
- Controller specific to IOT device
- Access to any Controller
- Local communication
- Devices with MUD URL
- Devices from same Manufacturer

# MUD 下物聯網安全的三步驟

Step 1

Profiling/ Visibility

Identify IOT device using a MUD URL

Step 2

Scalable Group Assignment

Assign Scalability/ Scalable Groups based on Classification

Step 3

Group based Policy enforcement

Apply Group based policy for access control of the IOT device

# 確認 MUD 設備及其策略

## Step 1: Identify the MUD Access controls for IOT devices

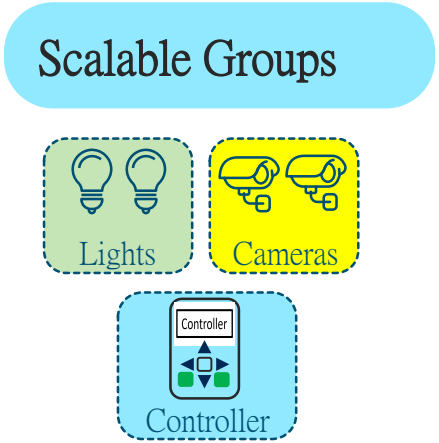
| MUD Access Controls | Group based policy (Access control) |
|---|---|
| Controller specific to IOT device | Access to device controller specific to an IOT device. |
| Device from same Manufacturer | Access between IOT devices from same manufacturer. |

Example: Manufacturer > Light Corp

Note: SGT is Scalable Group Tags

# 將 MUD 的控制策略貼上 Group Based Policy 的標籤

## Step 2: Create Scalable Groups for IOT devices in ISE




- Light bulb → SGT 10
- Camera → SGT 20
- Controller → SGT 30

Note: SGT is Scalable Group Tags

# Group Based Policy 標籤的執行

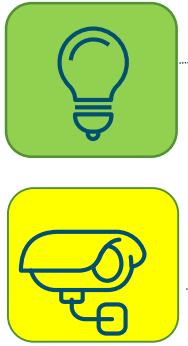
## Step 3: Create Group based Policies in ISE

# 將 MUD 功能整合到網路設備

Supported versions:

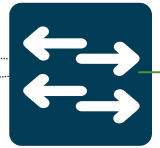
**Device Identification/Visibility**: ISE 2.6
**IOS**: 16.9.1 and 15.2.6(2)
**Switch**: Catalyst 9k,3850 and CDB

1. Device Identification
2. Visibility



IOT Device

MUD-URL in LLDP/DHCP



Catalyst Switch

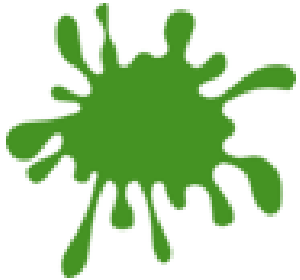
MUD-URL in RADIUS Accounting

ISE 2.6

Turn on
1. Device Sensor
2. AAA and Radius Accounting
3. MacAuthBypass

Add the switch as AAA client in ISE

# 物聯網安全解決方案

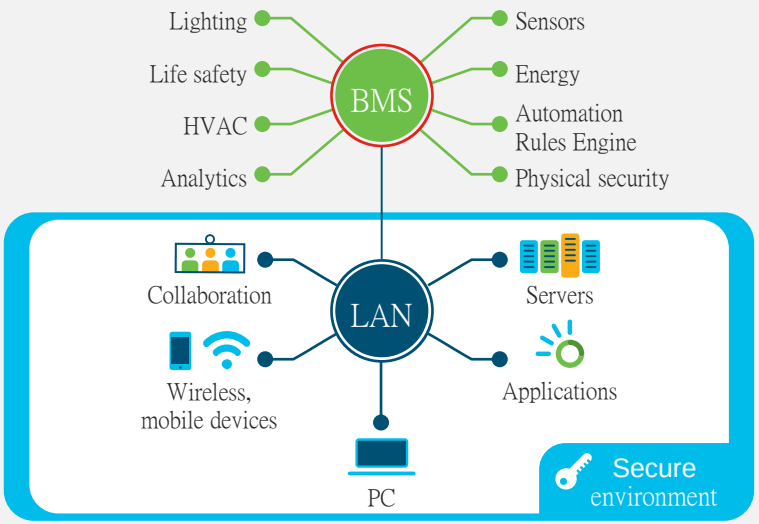


- Group based policies
- Manufacturer Usage Description
- IOT Visibility with MUD 1.0
- Protecting IOT using MUD and Group based policy
- IT/OT Convergence
- DevNet

# IT / OT 融合

## Traditional approach

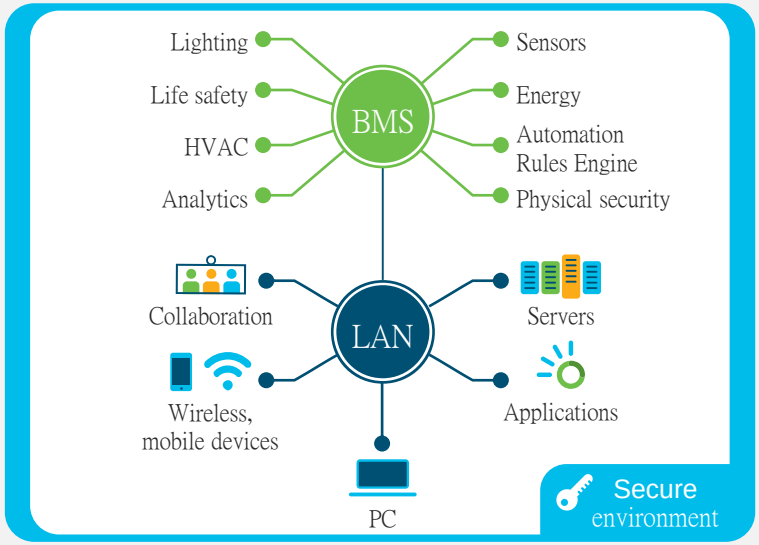
Although BMS is connected to the LAN,
advanced security features are not used.




Cisco security applied to traditional networked devices

## Converged approach

BMS and all smart building automation and
control systems are connected by Cisco technology.




Cisco security applied to all networked devices including BMS

# 物聯網安全解決方案

- Group based policies
- Manufacturer Usage Description
- IOT Visibility with MUD 1.0
- Protecting IOT using MUD and Group based policy
- IT/OT Convergence
- DevNet

# 思科開放 MUD DevNet 網站支持開發人員使用


Intro to MUD


Developers Guide


- Sample Code
- MUD Maker Tool
- Sandbox

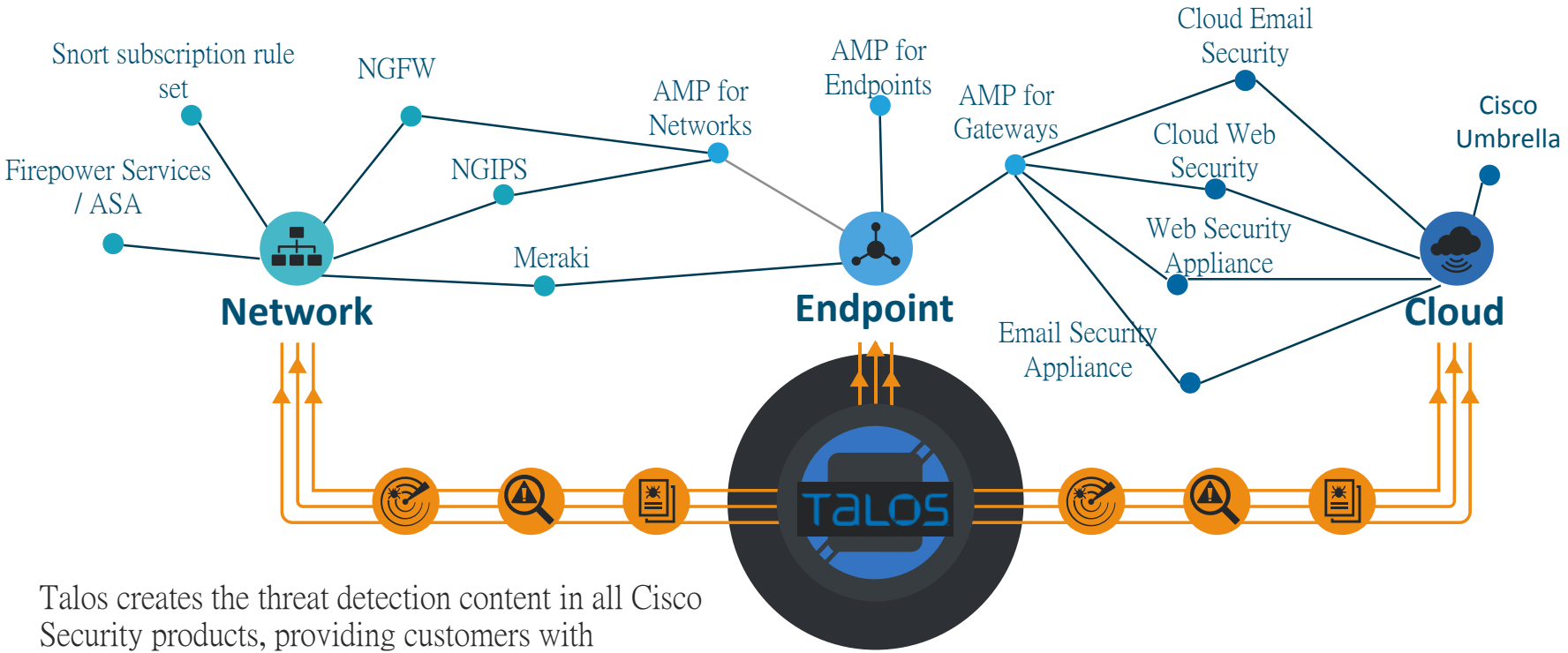
http://cs.co/iotmud

https://developer.cisco.com/site/mud/


# 5G 安全架構

cisco

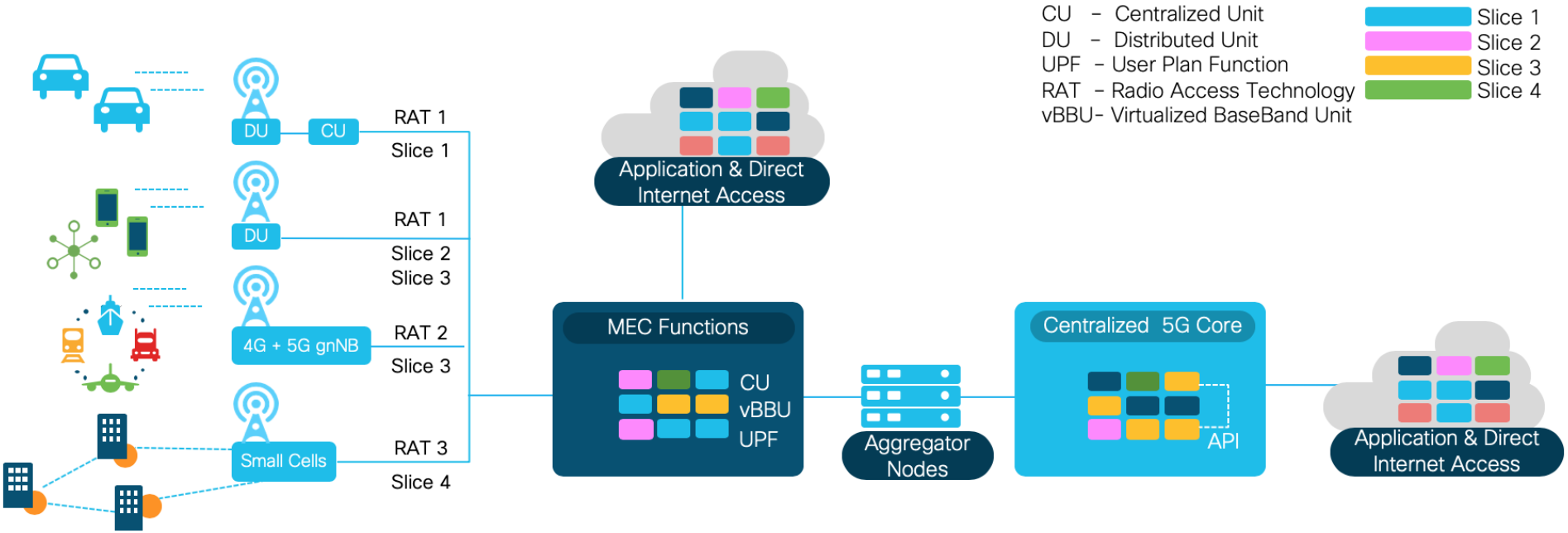
# 思科端到端的網路安全骨幹




Talos creates the threat detection content in all Cisco Security products, providing customers with comprehensive solutions from cloud to core.

# 5G 不斷發展架構中的安全挑戰

| | |
|---|---|
| IoT & M2M | • Weak inbuilt security in IoT devices, peer to peer attacks |
| Virtualization | • Increased complexity in mitigating side channel attacks and securing cloud native architectures |
| Distributed Architectures | • Increased threat vectors due to distributed DC, edge computing and Network slicing |
| New and Legacy Technologies | • Multiple Technology convergence, threat migration between technologies |
| Cross domain policy Transparency/Visibility | • ENTERPRISE policy ambiguity/definition, identity … vs. what’ s in SP domain<br>• Rick, Scott ATT team |




**Device Threats**

Malware
Bots DDoS
Firmware Hacks
Device Tampering
Sensor Susceptibility
TFTP MitM attacks

**Air Interface Threats**

MitM attack
Jamming

**RAN Threats**

Rogue Nodes
Insecure S1, X2
Insecure Xx, Xn

**MEC & Backhaul Threats**

DDoS attacks
LI Vulnerabilities
Insecure Sx
Insecure N6
CP / UP Sniffing
MEC Backhaul sniff
Side Channel attacks
NFVi Vulnerabilities

**5G Packet Core & OAM Threats**

Virtualisation
LI Vulnerabilities
Improper Access Control
Network Slice security
API vulnerabilities
IoT Core integration
Roaming Partner
DDoS & DoS attacks

**SGi / N6 & External Roaming Threats**

IoT Core integration
VAS integration
App server vulnerabilities
Application vulnerabilities
API vulnerabilities

# Trusted Critical Infrastructure (*)

## Requires Trusted Service Provider Networks

### Trust begins in hardware
Anti-counterfeit and trust anchor infrastructure

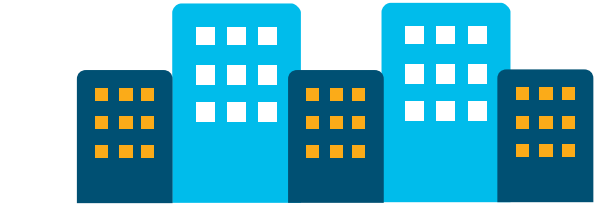
### Verifying trust: Network OS
Image signing and secure boot infrastructure

### Maintaining trust at runtime
Run-time defense, encrypted transport, ddos protection

### Visualize and report on trust
Integrity measurement and verification infrastructure. Trust insight in roadmap of crosswork portfolio

.

8+ years of CSDL devotion
30+ years of leadership



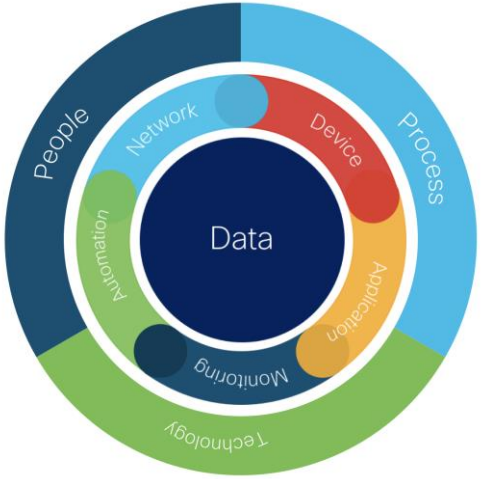
Protect your brand | Unlock new revenue | Reduce cost

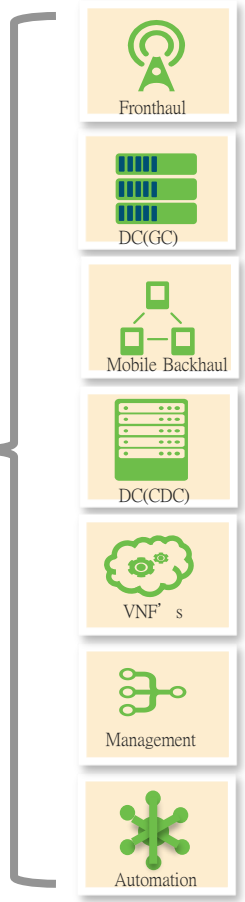
Click here for more details on IOS-XR security

(*) This is embedded in the current hardware and operating system

# 零信任，零接觸網路的 6 個步驟

1. Strong Identity using Certificates
2. Validated Secure Configuration
3. Segmentation of Network Services
4. Visibility of Network Activities
5. Restricted Access to Network Elements
6. Strong Security Perimeters



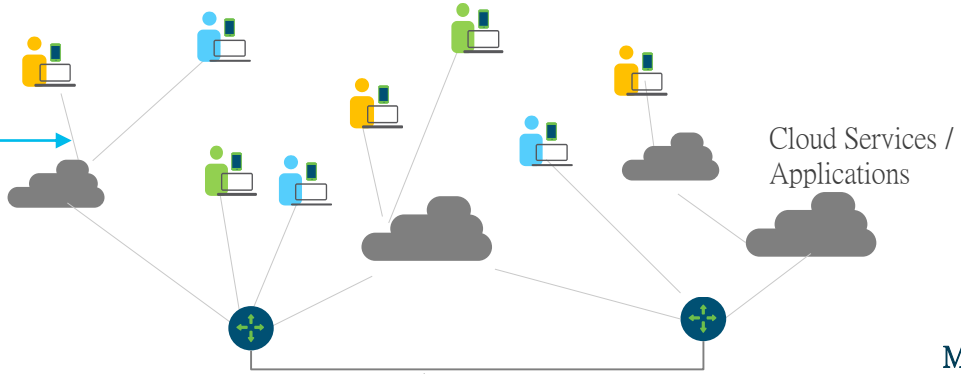
# 電信雲和 5G NFV/Container 虛擬化架構的安全性

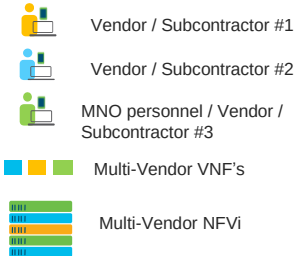
| | | | | |
|---|---|---|---|---|
| Orchestration | Securing Orchestration management & interfaces, Securing Policy Enforcement within Orchestration and between Orchestration and network components, Visibility | | | Cisco ACI<br>Cisco Tetration Analytics |
| User Access | Segmentation, User Access, DNS protection | | | Cisco Umbrella |
| Network | Securing NW interfaces, securing Cloud interfaces – and workloads, Segmentation, Policy enforcement, Securing, Peering & Roaming interface | | | |
| Applications | Securing 3rd Party application interfaces, Application Security, Segmentation, Enforcing policies in cloud, Securing API | | | Cisco ACI<br>Cisco Cloudlock<br>Cisco AppDynamics<br>Cisco Tetration Analytics |
| VNF | Securing VNF, securing Software Lifecycle, Isolation – between VNS, detecting malicious virtual functions | | | |
| Infra | Hardening of NFVI, perimeter security, securing – E-W traffic | AMP | ISE, Stealthwatch, Firepower | Cisco Tetration Analytics |

Problem | Multiple NFVi / NF Vendors, Contractors, Sub-contractors, employees accessing the network during configuration

Anyconnect VPN

1




Solution | Zero Trust Access Security based on VPN (Anyconnect), Multi-Factor Authentication (MFA) and enhanced visibility (Stealthwatch)

Benefits | Verifies and re-verifies the access of the user to specific VNF or NFVi

Stealthwatch

3

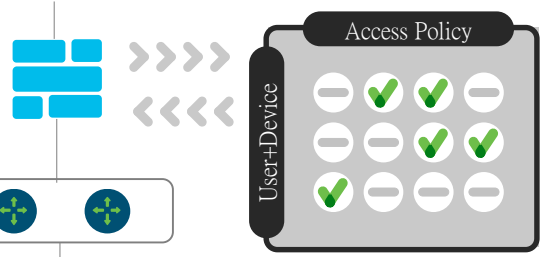
Multi-Factor Authentication

2

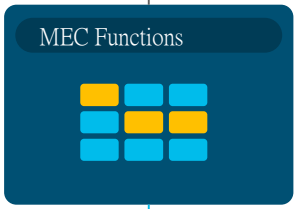
pxGrid integration

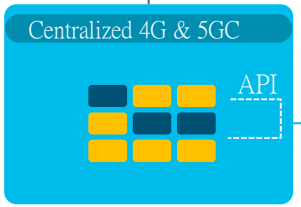
ISE

Policy Control & Enforcement



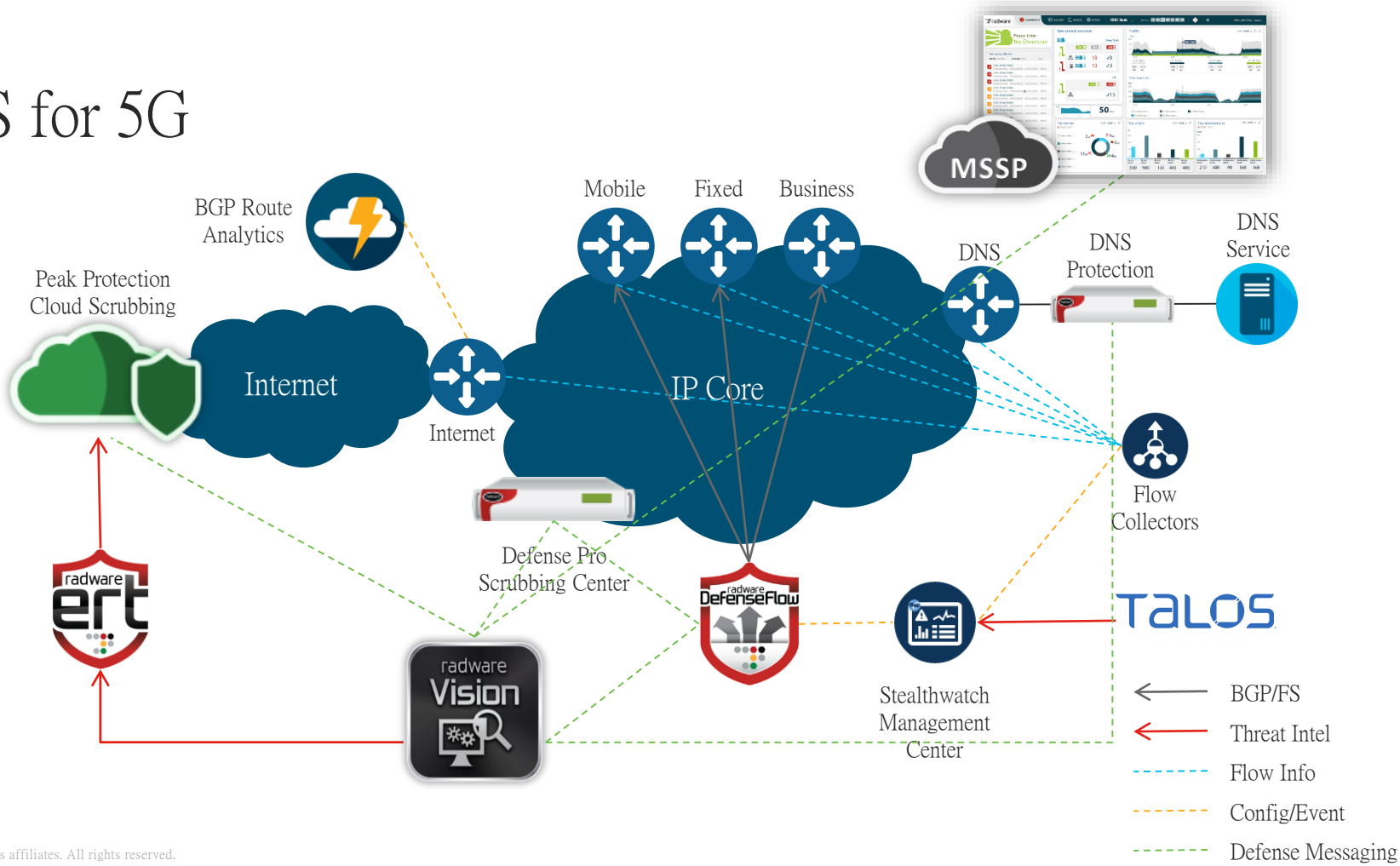

TrustSec

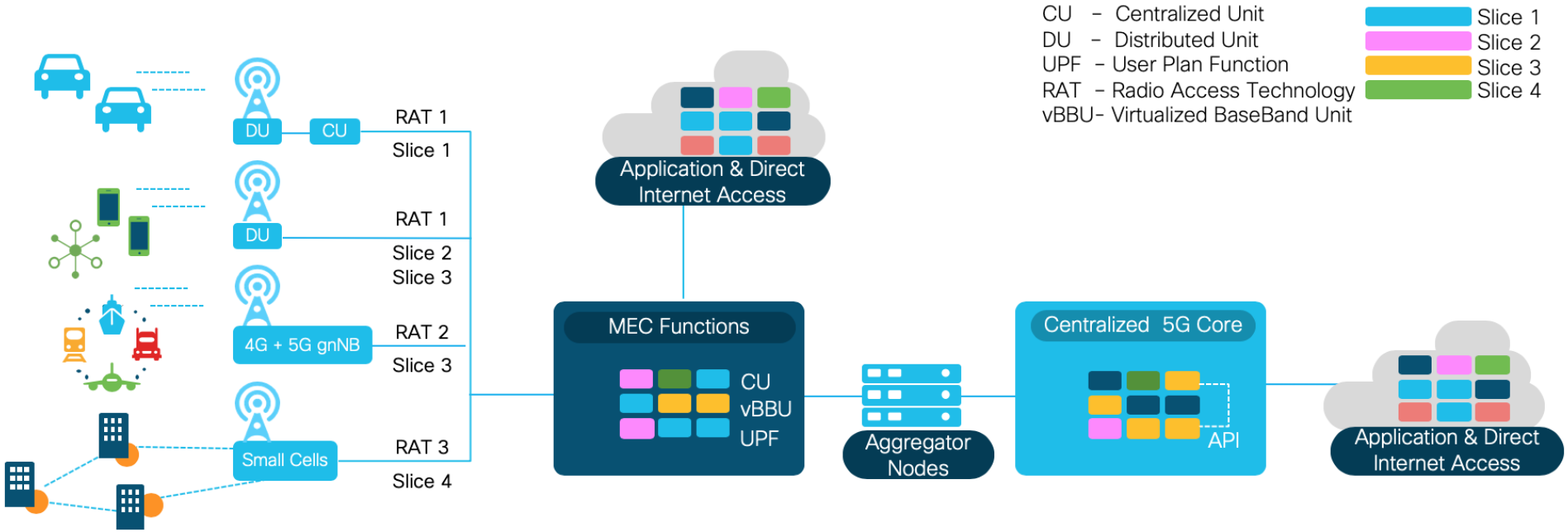


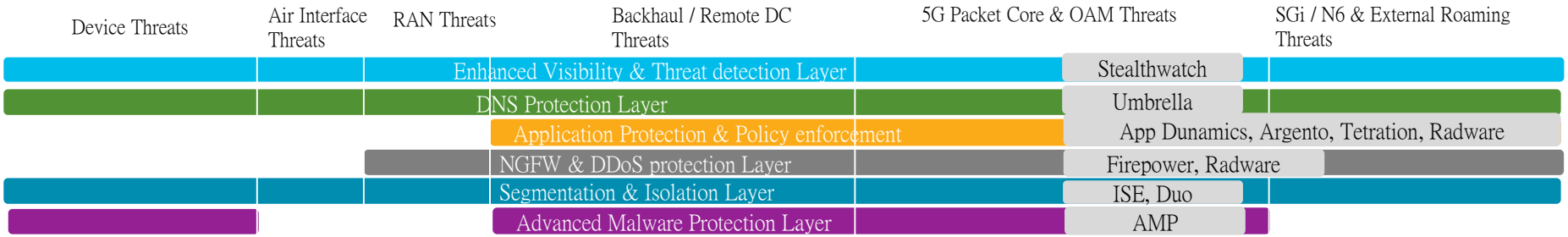




Device flows
VM metadata

# DDoS for 5G





# Thank You

CISCO