CYBERSEC 2021 臺灣資安大會 | ORGANIZED BY iThome

TRUST: redefined

智慧守護行動與 IoT 時代的自由與安全

陳清淵
Aruba 台灣區技術副總經理

MAY 4-6 臺北南港展覽二館

aruba
a Hewlett Packard
Enterprise company

智慧守護行動與 IoT 時代的自由與安全

Alex Chen 陳清淵
技術副總經理
Aruba, a Hewlett Packard Enterprise Company

ARUBA Edge Service Platform架構

將邊緣資料數據轉化為業務成果

遠端 | 雲端 | 分支機構 | 園區 | 資料中心

ARUBA CENTRAL

3 分析與行動	人工智慧功能可在問題影響業務之前識別問題，並幫助IT部門更快地解決問題	AIOps
2 保護	應用零信任安全性和SASE來提升防護等級，同時簡化操作	零信任安全
1 連接	跨網域和位置的統一網路維運	整合式基礎架構

aruba a Hewlett Packard Enterprise company

現今網路面臨的資安挑戰 - 複雜與難以避免橫向感染

Segmentation
adds Complexity

Complexity
Security

A Segment can be considered as a VLAN

aruba
a Hewlett Packard Enterprise company

Aruba零信任安全架構

安全和網路必須合而為一

aruba
a Hewlett Packard Enterprise company

~~傳統乙太網路交換器端口~~ → 需要更有效率

~~手動配置每個端口設定~~ 配置要能智能動態下發

VLAN 100 ACL 'Headless'

VLAN 200 QoS 'PolicyA'

VLAN 300 ACL 'Desktop'

VLAN 400 ACL 'guest'

Colorless port 功能不需要先前配置好每個端口設定.

VLAN/Access control/QoS 取決於設備接入那一剎那.

最佳解決方案Aruba ClearPass Policy Manager

接入設備即自動取得該存取權限

辨識

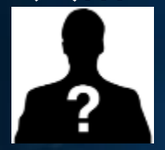
認證

授權

強制派送權限

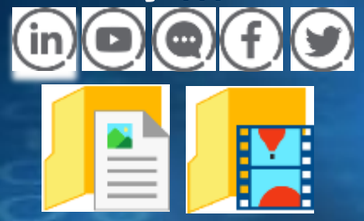
Aruba ClearPass

條件A
人…



＋

條件B
事…



＋

條件C
時…

＋

條件D
地…

＋

條件E
物…

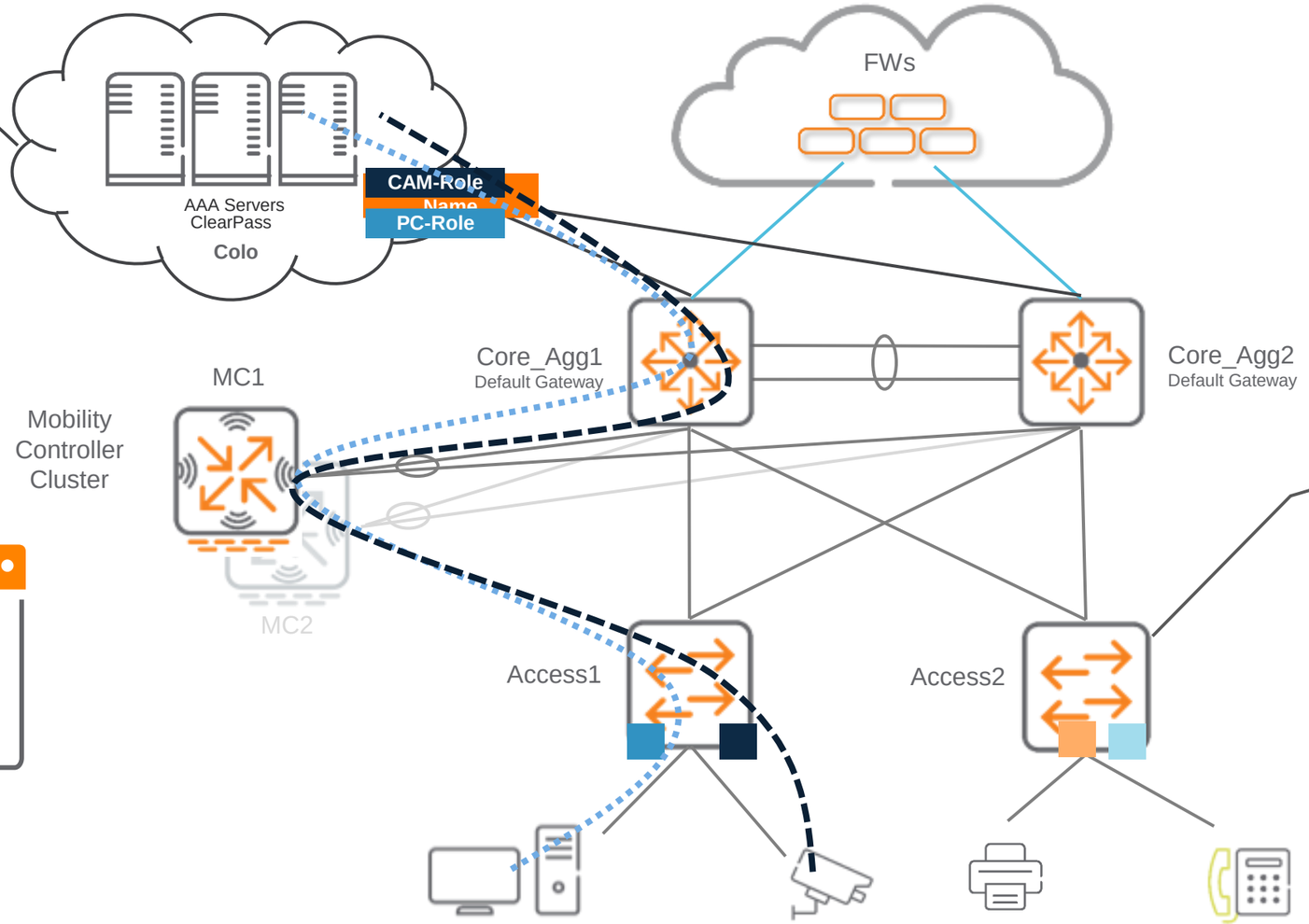
＝ **User-Role**
使用權限

aruba
a Hewlett Packard Enterprise company

User-Roles, Colorless Ports And Dynamic Segmentation

Downloadable User-Role

Vlan 38
CAM-Role
Vlan 37
Printer-Role
Vlan 34
Phone-Role
Vlan 35
PC-Role



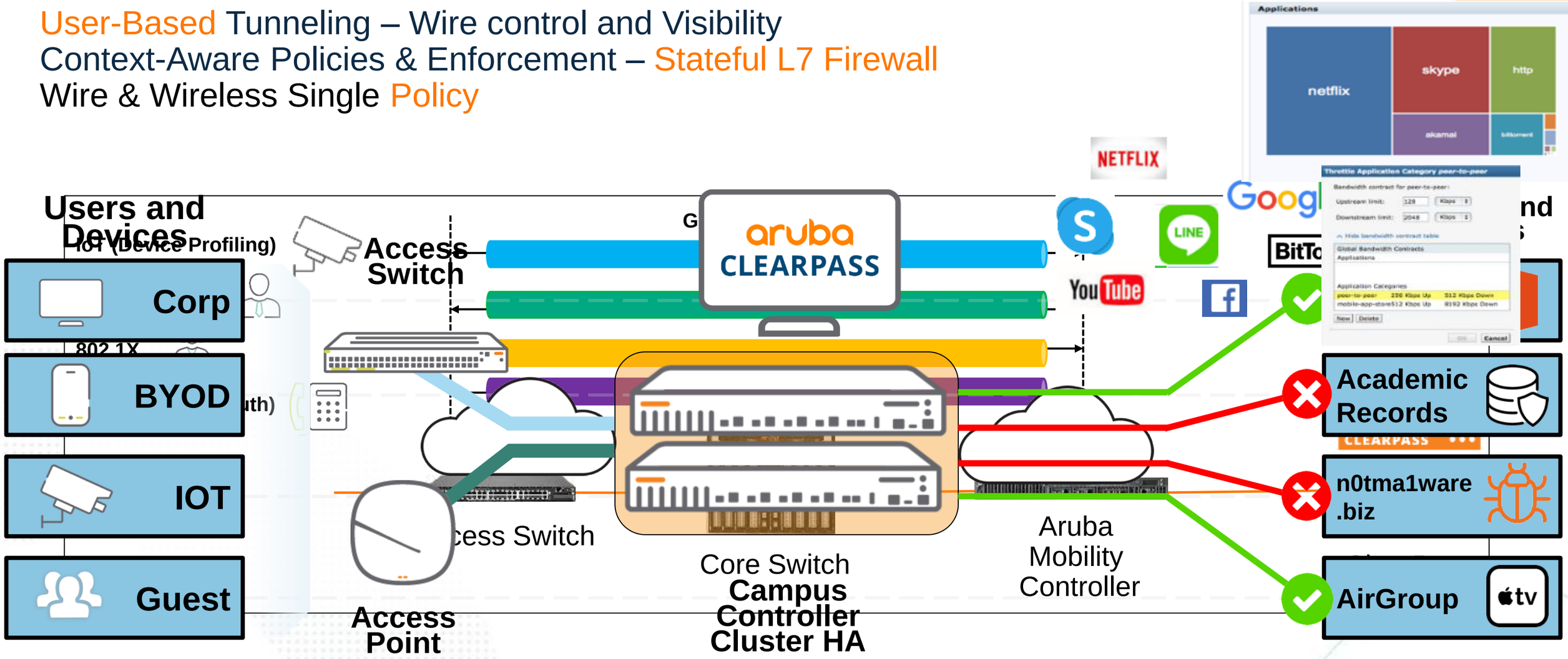
Local User-Role

Vlan 38
CAM-Role
Vlan 37
Printer-Role
Vlan 34
Phone-Role
Vlan 35
PC-Role

CLEARPASS
POLICY MANAGEMENT

動態分割Dynamic Segmentation – Overlay 安全政策

User-Based Tunneling – Wire control and Visibility
Context-Aware Policies & Enforcement – Stateful L7 Firewall
Wire & Wireless Single Policy

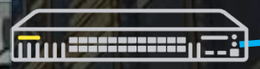


Zero-Trust Infrastructure
Wired Access

DYNAMIC SEGMENTATION

Up to 12-node
Active- Active Cluster

Controller
Gateway

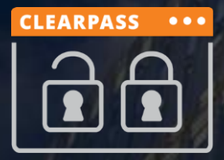


Switch

AP

SWITCH
WHERE YOU
CAN

TUNNEL
WHEN YOU
HAVE TO



ClearPass
Policy Manager

Consultant

TUNNEL to Security GW
- Allow SAP
- Allow Internet
- Deny everything else

UNIFIED POLICY
across Wired, Wireless, Branch and VPN

Alex
External
Consultant

HR

Sarah
HR
Corporate Device

aruba
a Hewlett Packard Enterprise company

Aruba Dynamic Segmentation -減少維運人員的負擔，並且強化管理與問題處理的效率

– 穩定性：

- 具備可以做到在控制器發生故障或斷線時，使用者網路連線不中斷，不影響使用者網路存取。
- 包含無線與有線網路。
- 用戶平衡負載

– 簡化管理性：

- ACL容易管理及營運在控制器,集中控管,所有Switch不需維護。
- 減少ACL數量。
- ACL Session base ,修改後立即生效,不需要重新認證。
- 即時得知ACL Hit及內容(show acl hits)

–自動化與智動化：

- 提供網路連線裝置的設備識別能力，防止未經授權的連線裝置在網路上使用，並且包含無線與有線網路。
- 無線與有線網路一體。

–流量可視性：

- 提供應用程式(第七層)網路使用的可視性並具備管理能力。
- 簡單易管的維運系統，提供人員、設備、訊號的全面管理。

aruba
a Hewlett Packard Enterprise company

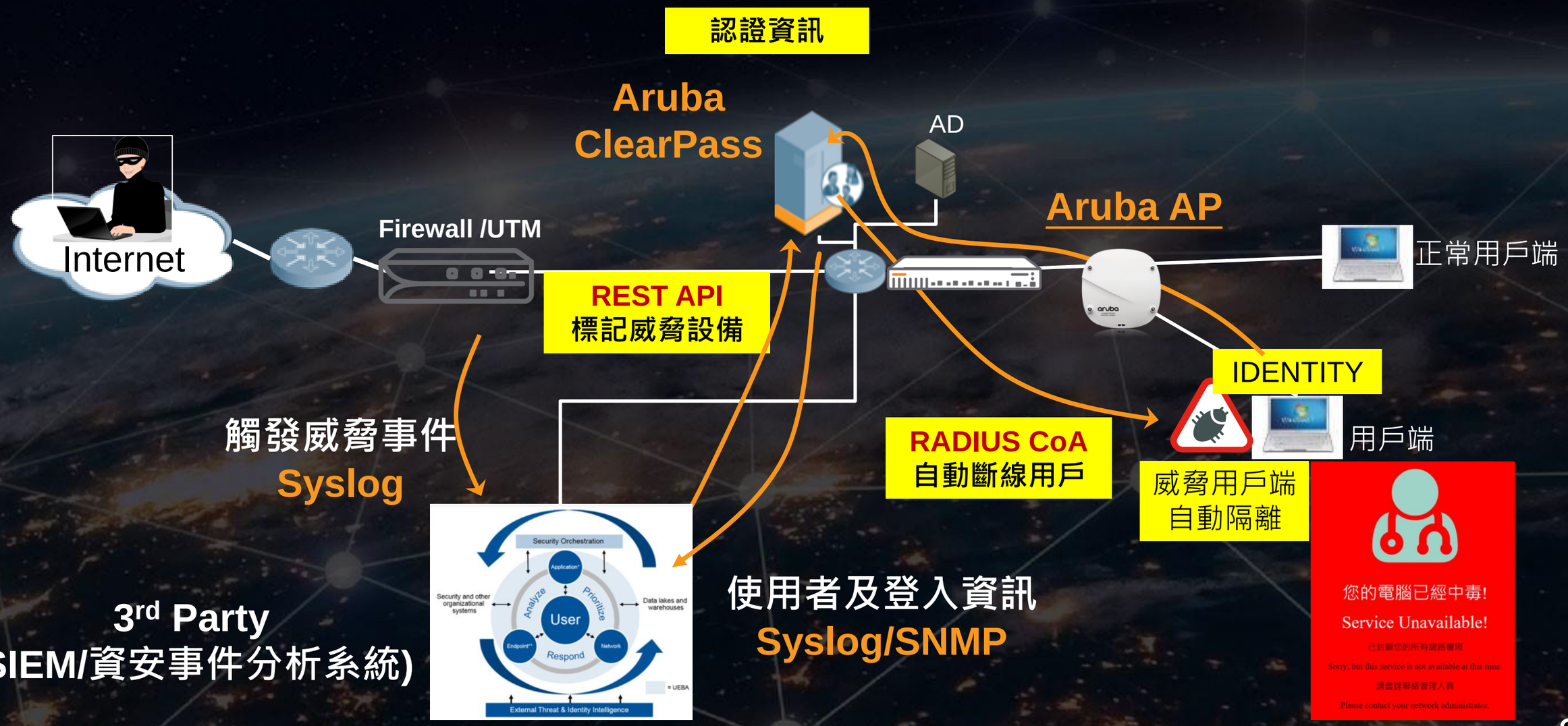
SIMPLE AND SECURE

…似乎是天秤的兩端

Aruba NAC – Agentless Agent Based

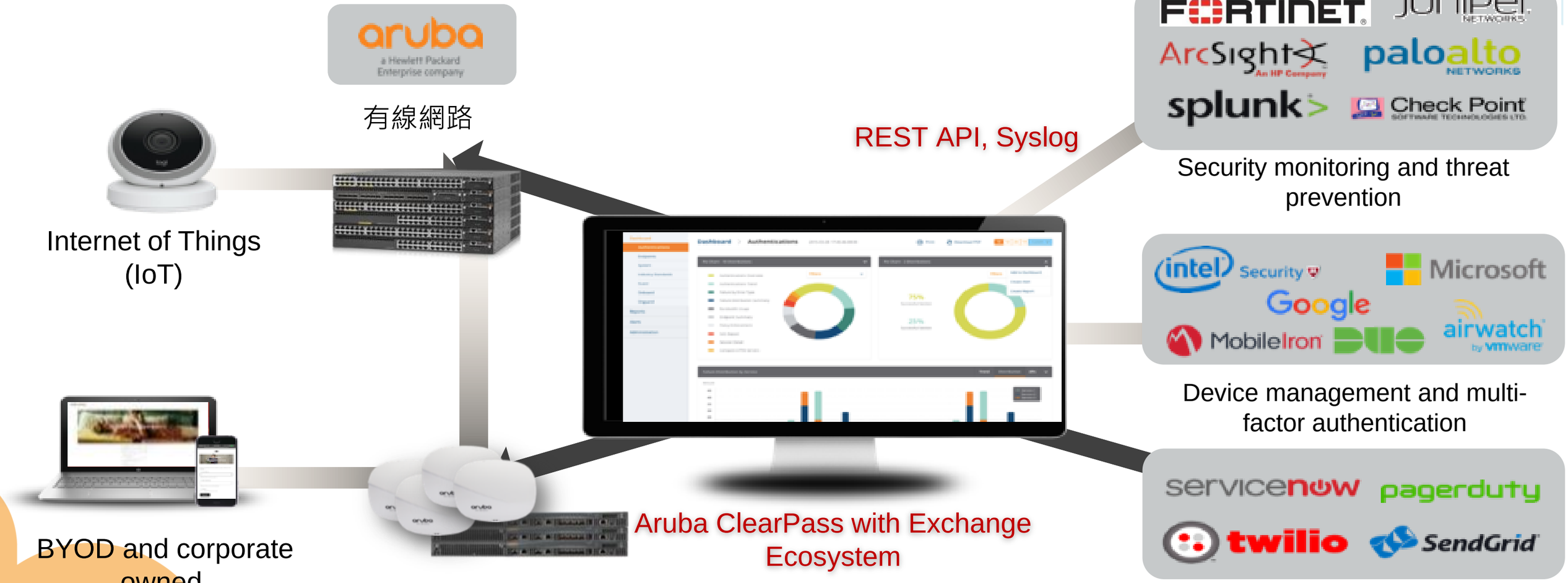
Agent

對於流量內容檢測的生態系統整合 - 持續監控並即時作動

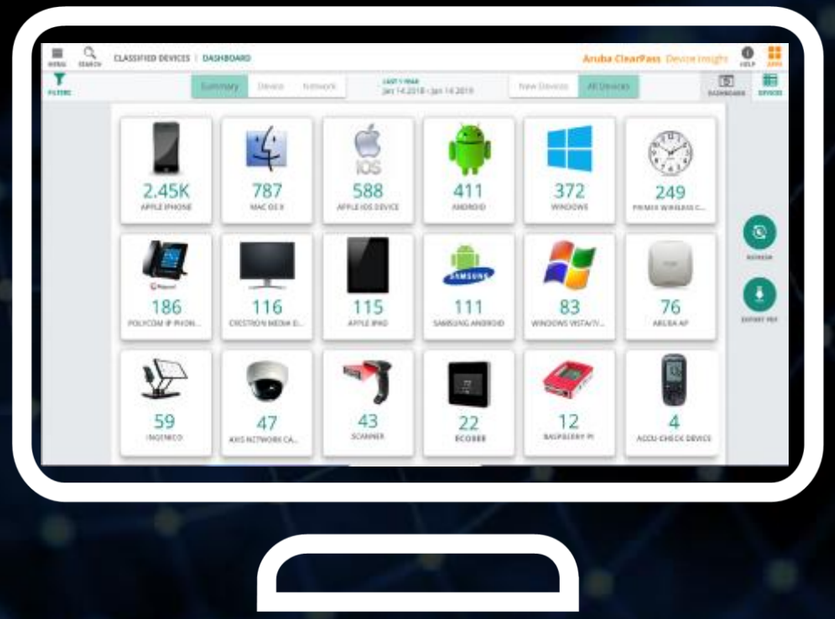


aruba
a Hewlett Packard Enterprise company

Aruba ClearPass 開放的生態系統，整合資安控管平台
與資安廠商偕同提供全方位的內部網路資安聯防



瞭解哪種類型的用戶端連接您的網路與流量行為

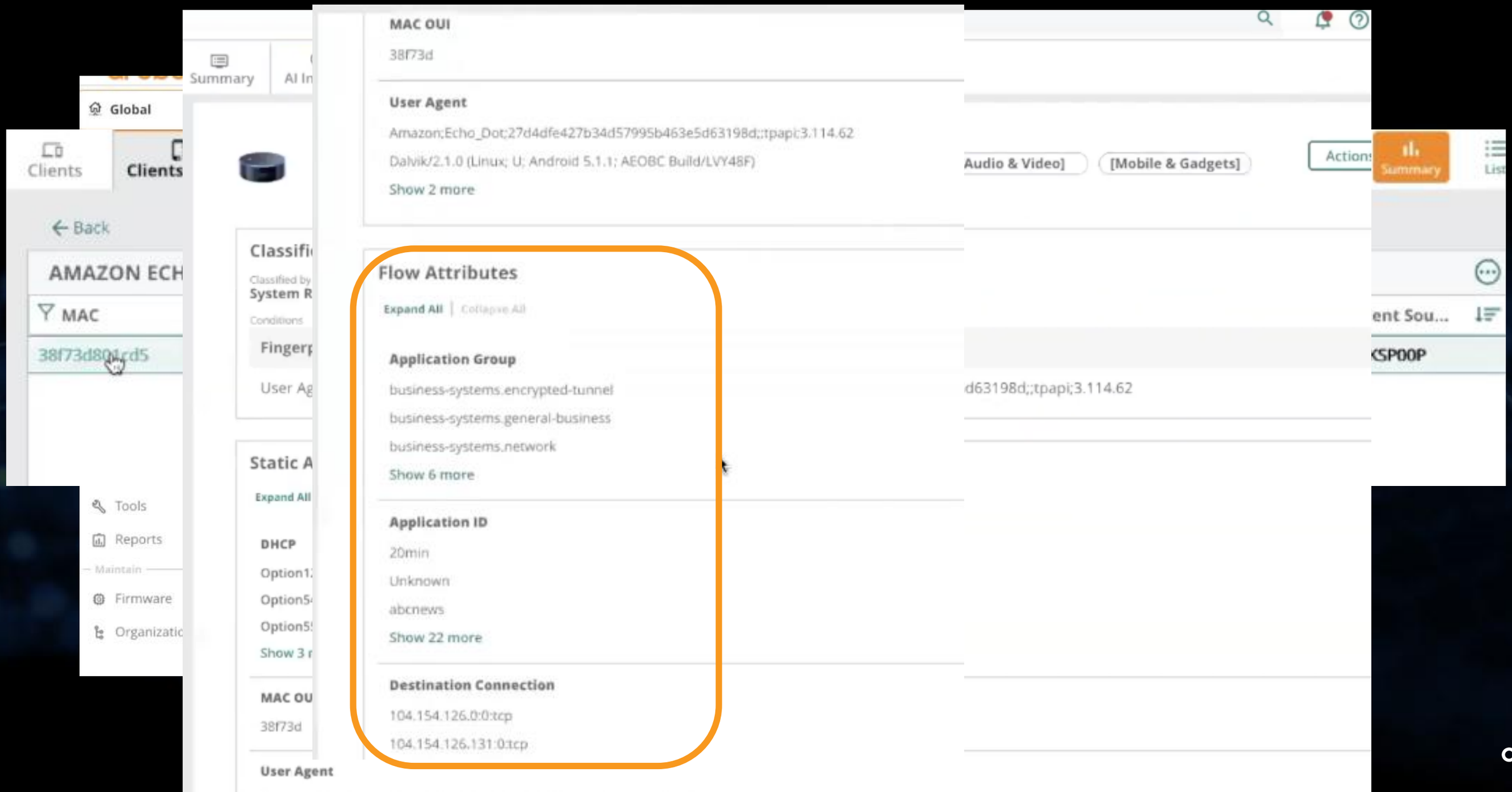


CLEARPASS DEVICE INSIGHT

- AI-Powered
- Cloud-Enabled
- Enhanced by Crowdsourcing
- Integration with CPPM Policy Manager

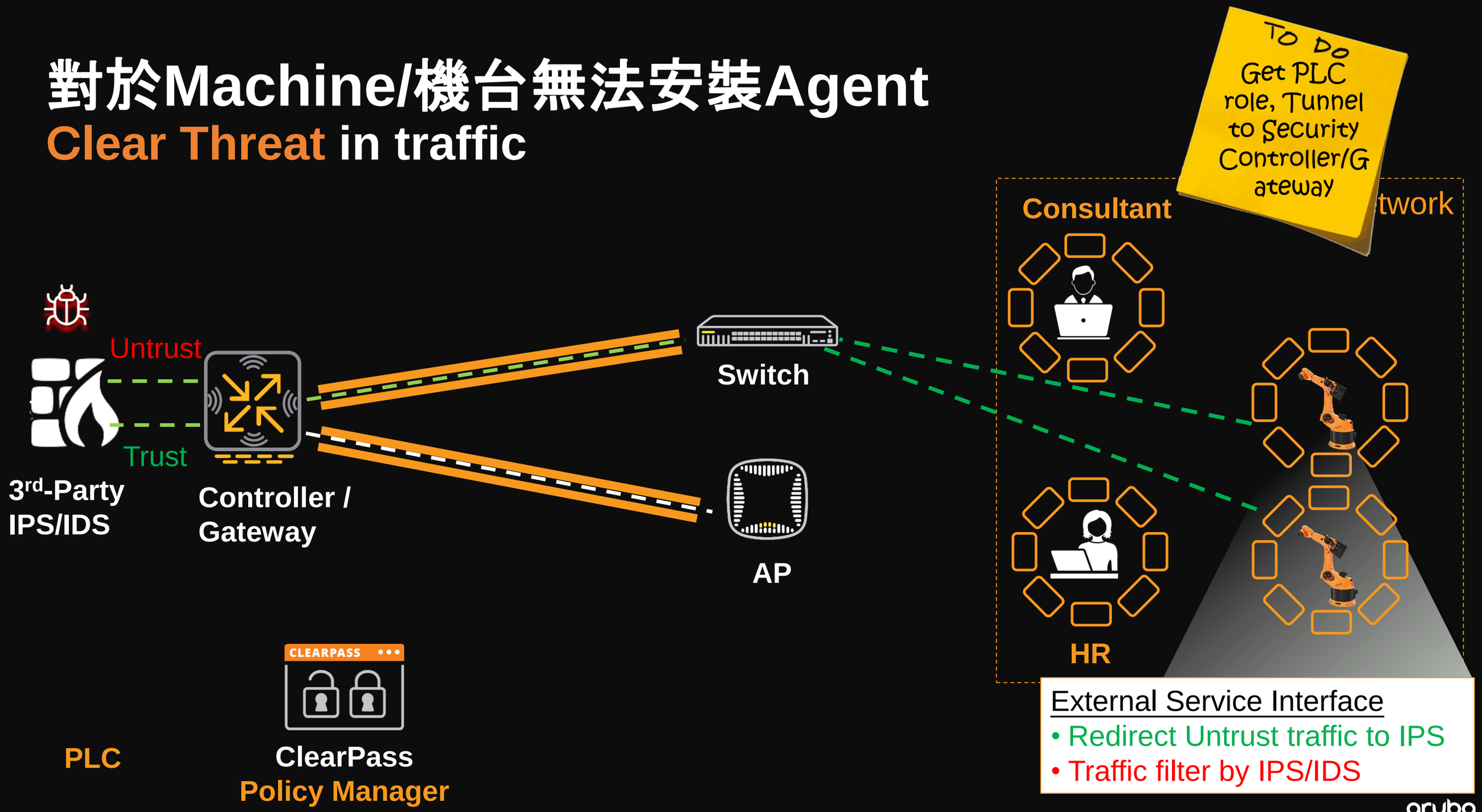
Device Visibility is key to proper segmentation

ClearPass Device Insight



aruba
a Hewlett Packard Enterprise company

對於Machine/機台無法安裝Agent
Clear Threat in traffic



aruba
a Hewlett Packard Enterprise company

IoT 設備的爆炸性增長不僅推動自動化和效能...也帶來挑戰

2023 年將產生 51B 連網裝置*

分支機構的挑戰：

- **物聯網裝置易受攻擊**
- **橫向感染的威脅**
  - e.g.,駭客從受感染的HVAC設備取得POS終端
- **必須分段/隔離設備流量**
- **傳統解決方案將設備分配給唯一的VLANs**
  - VLAN數量=設備類型數量
  - 難以管理，無法擴展
- **SASE風格的解決方案需要端點代理**
  - 不適用於IoT裝置

解決方案：Branch Gateway零信任安全動態分段

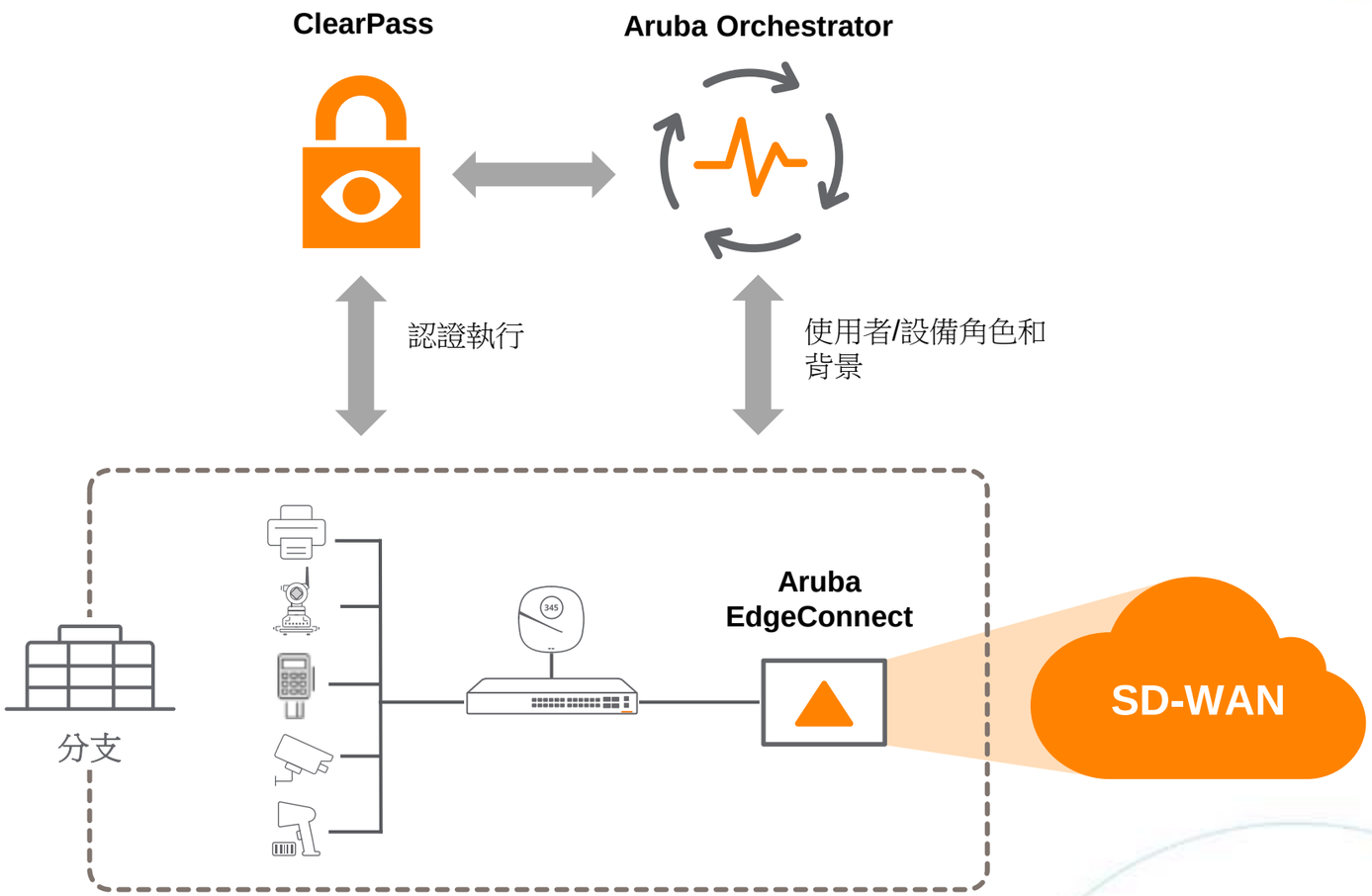
IDC, Future of Industry Ecosystems: Shared Data and Insights, September 2020

Aruba EdgeConnect 整合ClearPass

可視性、控制、反應

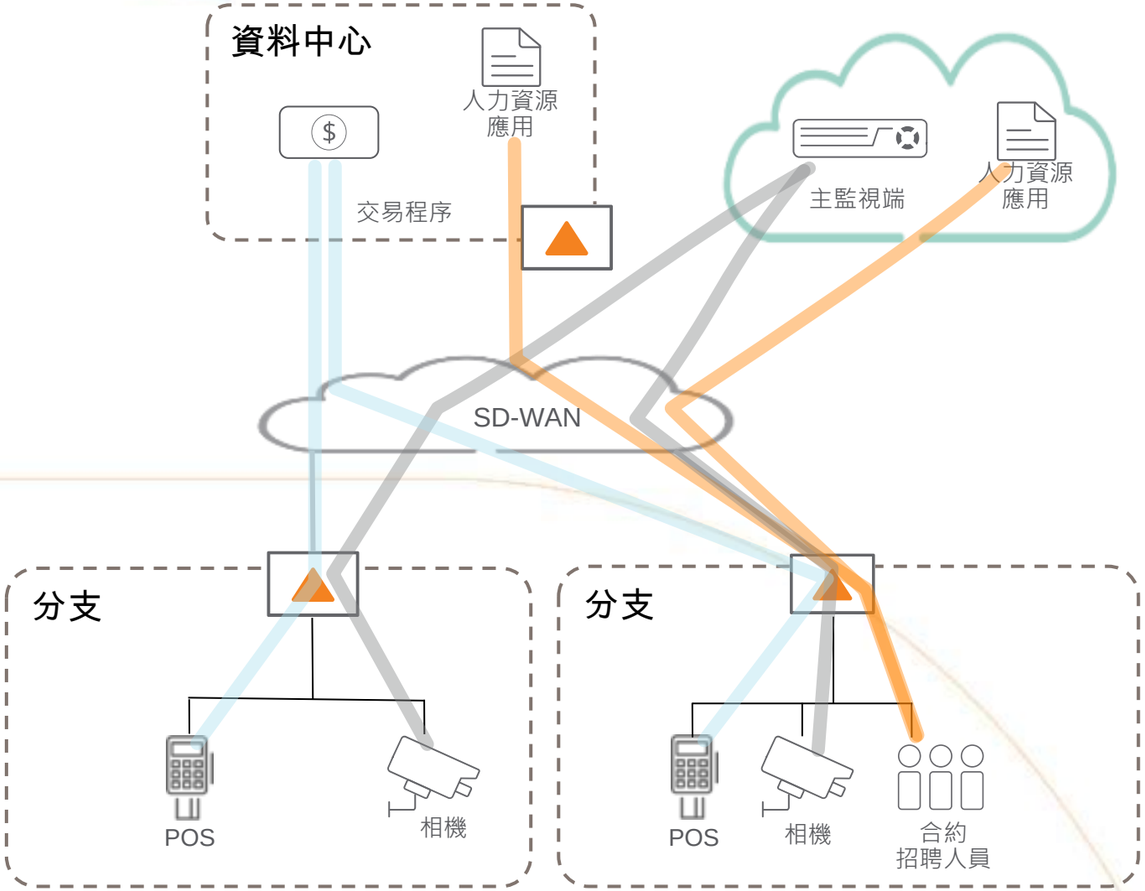
單一平台可自動化企業範圍內的情境感知，套用基於角色的策略

- **可視性與自動化：**
  - 內置探索功能、分析和儀表板
- **控制：**
  - 取得使用者/設備的控制
- **反應：**
  - 主動式反應和動態分段
- **360 度安全整合：**
  - 超過 150 個安全夥伴的生態系統
- **利用多個身份儲存：**
  - 支援 AD, LDAP, SQL, Internal dB, BYOD, 第三方整合



零信任安全動態分段

使用者/設備只能與其角色一致的終端進行通訊



- 藉由身份、角色和安全態勢識別使用者和設備
- 根據內容動態分段和隔離應用程式流量
- 業務驅動的政策範例

	相機	**主監視端**	POS終端	**交易程序**	約聘人員	人力資源應用
相機	✗	✓	✗	✗	✗	✗
主監視端	✓	✓	✗	✗	✗	✗
POS終端	✗	✗	✗	✓	✗	✗
交易程序	✗	✗	✓	✓	✗	✗
約聘人員	✗	✗	✗	✗	✗	✓
人力資源應用	✗	✗	✗	✗	✓	✓

Edge to Cloud 安全接入服務邊緣 –SASE

進階 SD-WAN 邊緣 + 雲端交付安全

採用 SASE 架構時的理想補充

- SD-WAN
- 路由
- 進階區隔
- ZB FW
- WAN 最佳化
- UTM

+

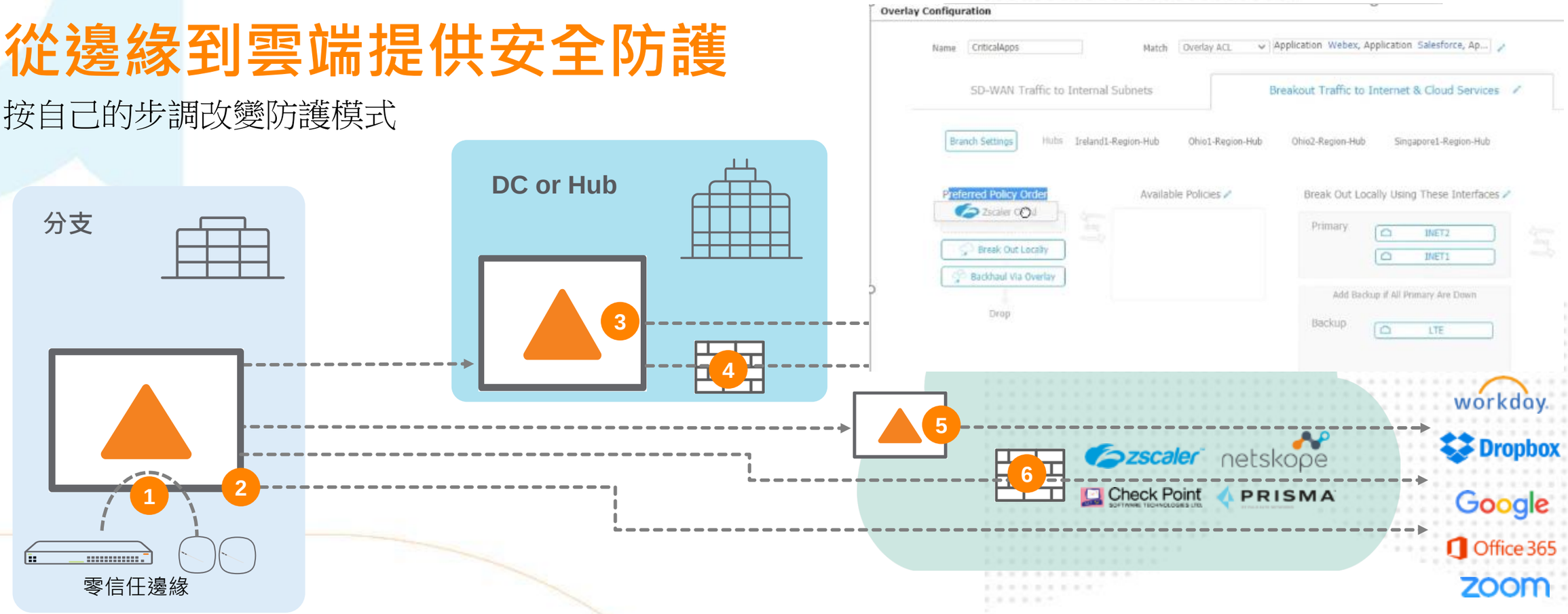
- SWG
- FWaaS
- IDS/IPS
- A/V
- ZTNA
- DLP
- Sandbox
- CASB
- DDoS

*「安全存取服務邊緣 (SASE) 是一種新興產品，將全面的 WAN 功能與全面的網路安全功能（例如 SWG、CASB、FWaaS 和 ZTNA）相結合，滿足數位化企業的動態安全存取需求。」***

**Gartner,「The Future of Network Security is in the Cloud」（網路安全的未來在雲端），2019 年 8 月 30 日* Gartner

從邊緣到雲端提供安全防護

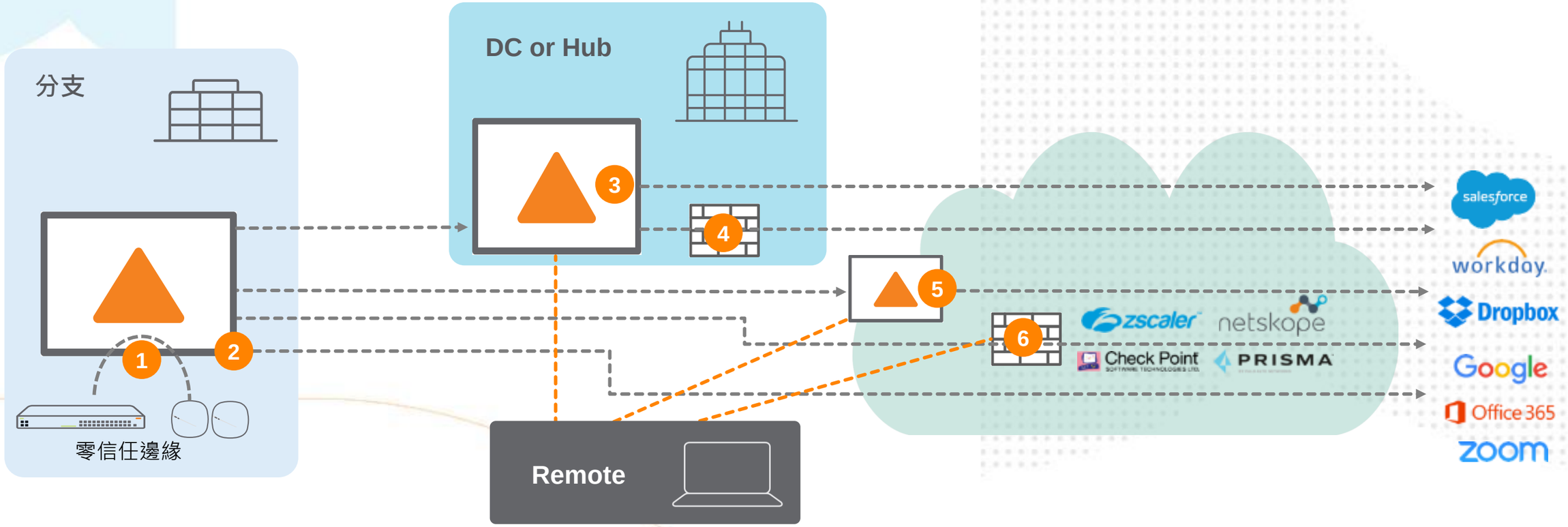
按自己的步調改變防護模式



1. 利用Aruba UTM @ Edge 進行東西向分割 (嵌入EC和SDB中)
2. 使用Aruba UTM @ Edge直接進入網路 (嵌入EC和SDB中)
3. 使用Aruba UTM @ Hub進行集中管理(嵌入EC-V / VPNC)
4. 整合第三方UTM @ Hub (Check Point, PAN…)
5. 使用Aruba UTM雲端傳輸 (EC-V/VPNC in AWS, Azure, GCN)
6. 使用第三方SWG, CASB 雲端傳輸(Zscaler, Netskope, Check Point….)

從邊緣到雲端的安全佈署

按自己的步調改變安全模型



1. 利用Aruba UTM @ Edge 進行東西向分割 (嵌入EC和SDB中)
2. 使用Aruba UTM @ Edge直接進入網路 (嵌入EC和SDB中)
3. 使用Aruba UTM @ Hub進行集中管理(嵌入EC-V / VPNC)
4. 整合第三方UTM @ Hub (Check Point, PAN…)
5. 使用Aruba UTM雲端傳輸 (EC-V/VPNC in AWS, Azure, GCN)
6. 使用第三方SWG, CASB 雲端傳輸(Zscaler, Netskope, Check Point….)

ARUBA 零信任安全架構

WIRED　WiFi　SD-BRANCH

UNIFIED INFRASTRUCTURE - ONE SECURITY ARCHITECTURE - ZERO TRUST

CORPORATE HQ

BRANCH

WAREHOUSE

HOME

SIMPLE

- ✓ 減少網路分段數量
- ✓ 智動化下發權限減少配置
- ✓ 辨識設備與角色規則
- ✓ 端點無需植入代理程式
- ✓ 單一策略橫跨有線無線分支單位

＋

SECURE

- ✓ 精細的訪問權限
- ✓ 動態微分段區隔
- ✓ 端點360°全方位可視性
- ✓ 多供應商生態系統，區域聯防即時隔離
- ✓ 全面的防護與邊緣安全

aruba
a Hewlett Packard Enterprise company

定義您的零信任安全旅程

驅動企業數位轉型

邊緣服務平台

- 智慧連接
- 資安防護
- AI分析與作動
- 簡化管理流程

建構安全邊緣

- 完整的資安聯防
- 整合最新 SASE、CPPM
- 結合業界超過150家的廠商

安全和網路必須合而為一

Edge Service Platform | Dynamic segmentation
Zero-Trust networking | IoT Visibility | SASE

Thank You

aruba
a Hewlett Packard
Enterprise company