Hewlett Packard Enterprise

安全優先！以零信任佈建網路安全網

Alex Chen陳清淵
副總經理, HPE Aruba Networking Taiwan

42001:2023
AIMS

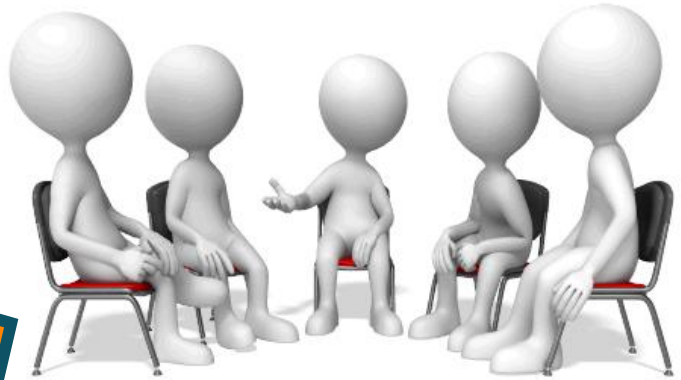
HPE aruba networking

資安：Cybersecurity , Data Privacy and Compliance

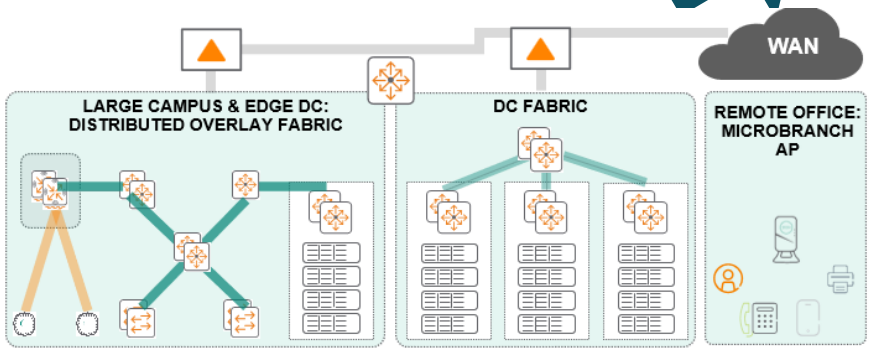
- 可視性
- 管制措施
- 數據安全
- 威脅防護

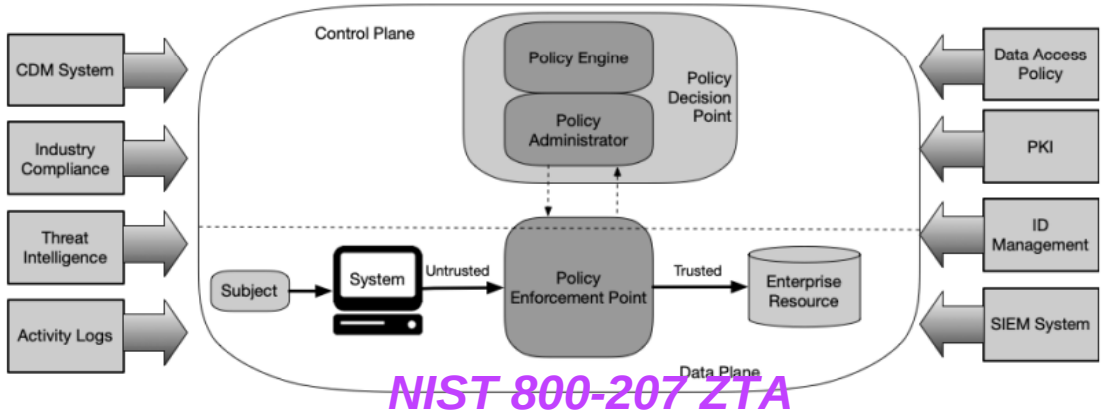
網路安全

交換機、路由器，無線網路，數據中心，遠端分公司以及連接的有線用戶、無線用戶與伺服器



網路安全：架構時時都安全 處處都安全





NIST 800-207 ZTA

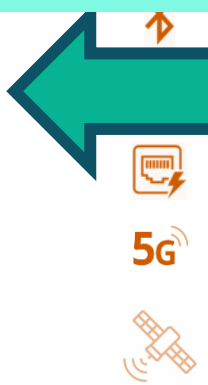
零信任策略結合運用多種既有的技術及方法，
零信任倚重於 <u>最小特權原則</u>等治理政策

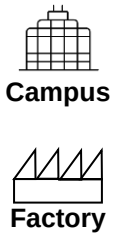
Need to Know ＆ Least Privilege

基於零信任原則的安全優先網路 – Need to Know & Least Privilege

People & Things | **Any Access** | **Anywhere** | **On Prem Enforcement** | **SSE Cloud Enforcement** | **Data and Applications**

網路基礎設施中整合資安，防止其網路免於各種安全威脅的影響





SECURELY

Data Center with CX10K top of rack

SD-Branch

Secure access to SaaS apps

SWG
Secure access to the internet

共用可見性 | 全局的政策 | 邊緣到雲各個決策點 | AI 自動化作業

Security-First AI-Powered Networking

a Zero Trust foundation for powering distinctive, protected experiences

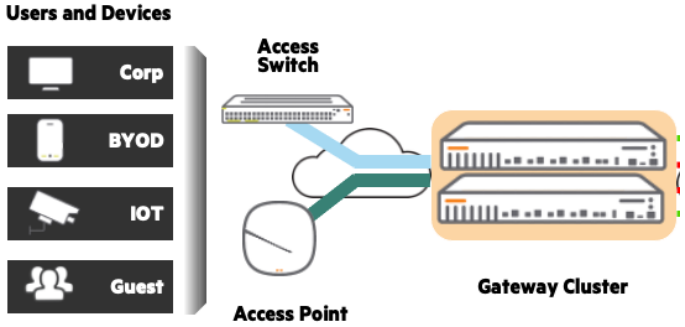
Aruba如何協助網路安全

AI-Power Cloud-Native Central

Role based

Policy Management

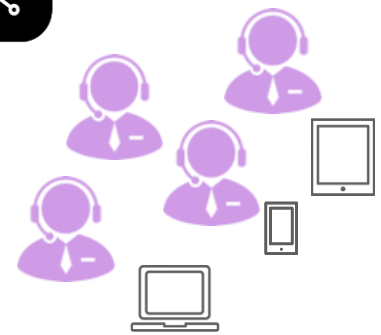
Campus Dynamic Segmentation
動態分片、權限控管、區域聯防



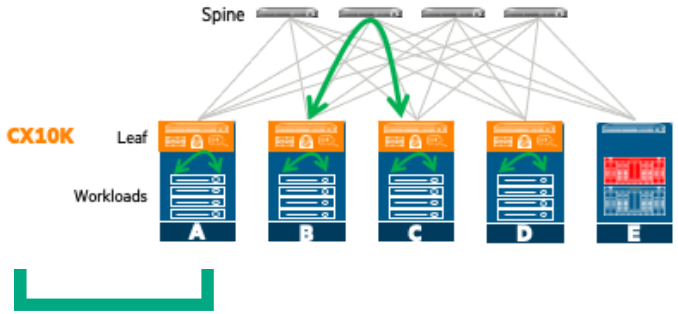
CLEARPASS

ClearPass Access Management

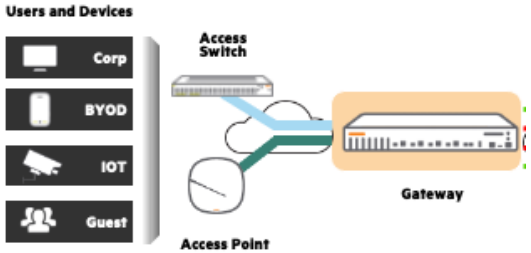
雲端安全- 上網/VPN User Segmentation



DataCenter Micro Segmentation
東西向流量與VMs間管控



Branch Dynamic Segmentation
分支機構動態分片

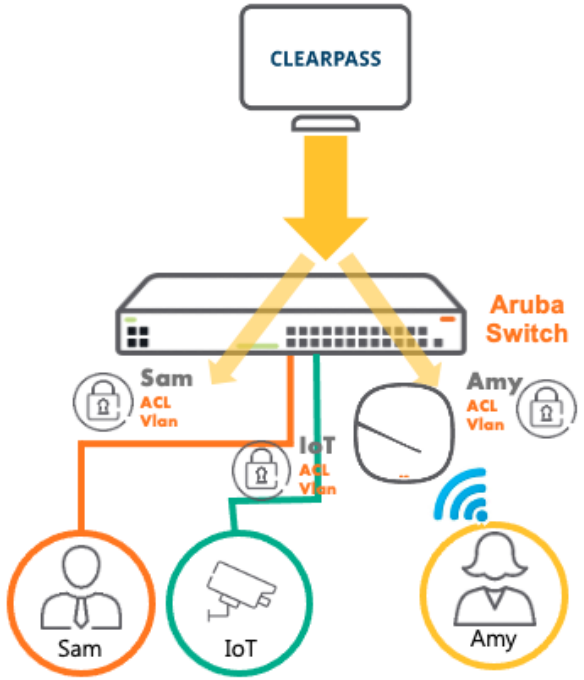


雲端安全- 3rd party Access User Segmentation

動態切片Dynamic Segmentation (per user-device Stateful Firewall)

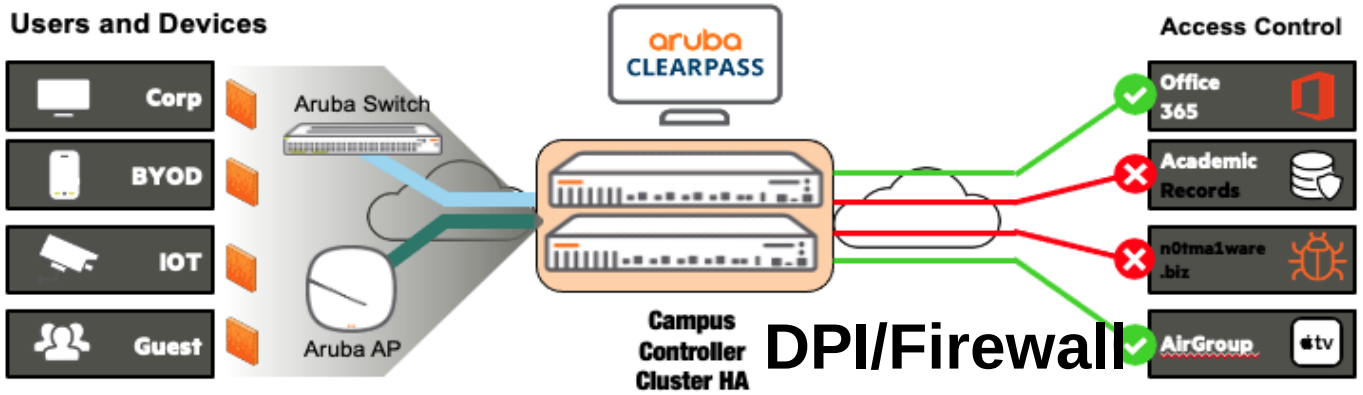
有線網路流量可視性與整網單一存取政策 – Keep it Simple

- 身份識別
- 根據情境進行細緻存取控制
- 實施微分段



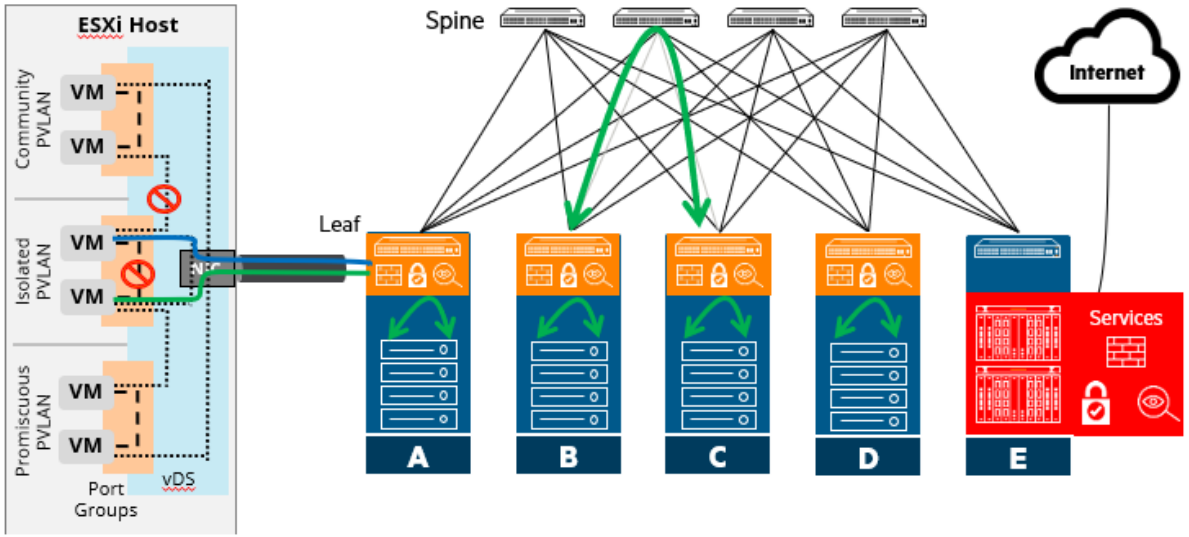
- ✓ VLAN 自動派發
- ✓ 權限(User Role/ACL)自動派發
- ✓ Switch自動套用
- ✓ 大幅減少維運流程
- ✓ 搭配情境動態權限

零信任網路/Micro-Segmentation/ Wire Client traffic visibility

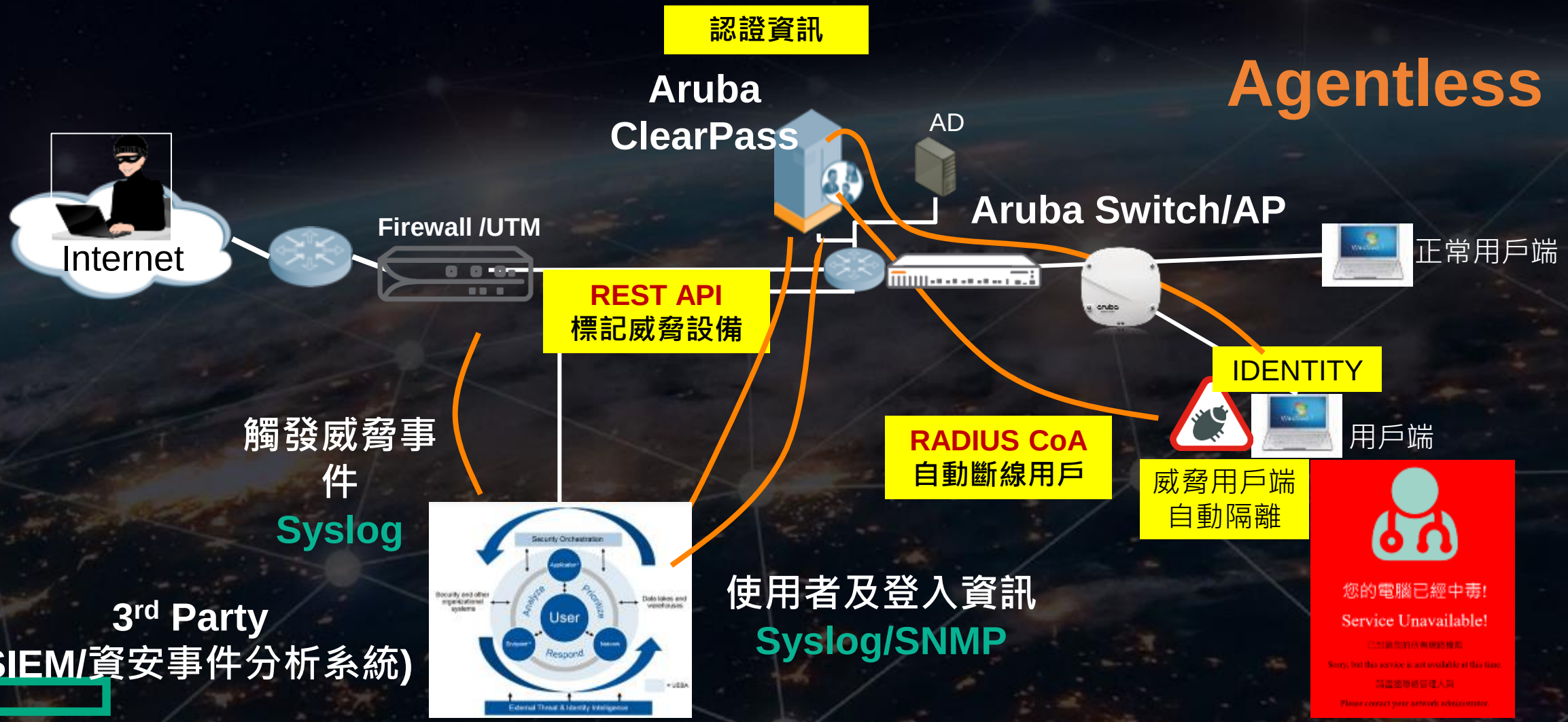


中間網路設備不需更換

數據中心微分割- 東西向控管



通過即時適應進行持續監測-安全協調、自動化和回應(SOAR)



勒索病毒

隔離機器

Ransomware

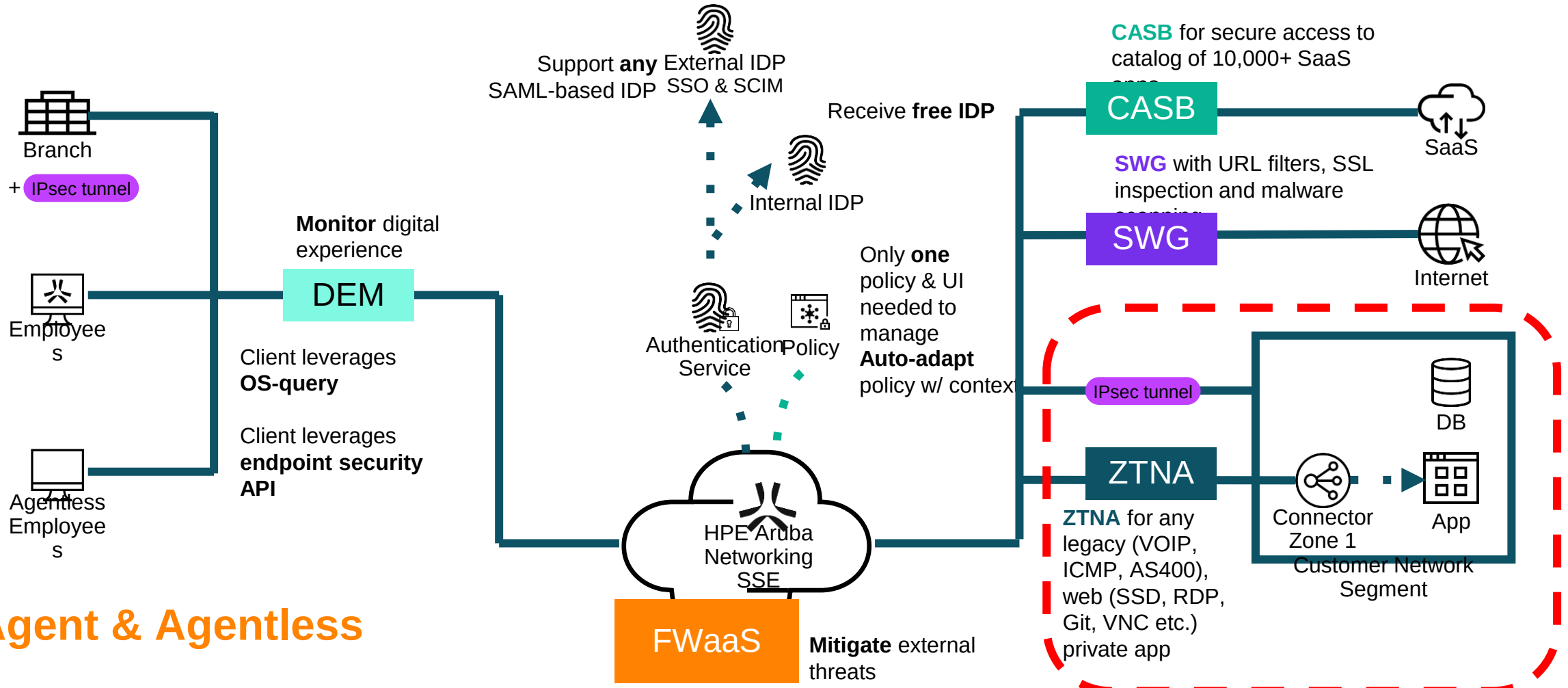
遏制傳播

Aruba零信任網路/Dynamic-Segmentation 的優勢

優　　勢	HPE Aruba + ClearPas
分隔使用者最小單位 ，**per-device Role可以是：人、事、時、地、物組合條件**	✅
存取控制方法 **Stateful Firewall**	✅
判斷使用者角色、Domain Computer， **不安裝 Client Agent**	✅
使用者**角色變換**時 (例如AD部門更新)，**立即存取政策變更**	✅
是否支援 Client Agent ，**偵測用戶端是否啟用防火牆、防毒，是否安裝禁止的應用程式**	✅
同網段設備互相限制存取權限 (Micro-Segmentation)	✅
同一個 switch port，**同時支援不同用戶端設備政策**	✅
整合資安平台,做到內部網路**資安聯防SOAR**	✅
可否支援**串接 3rd party switch/hub**	✅

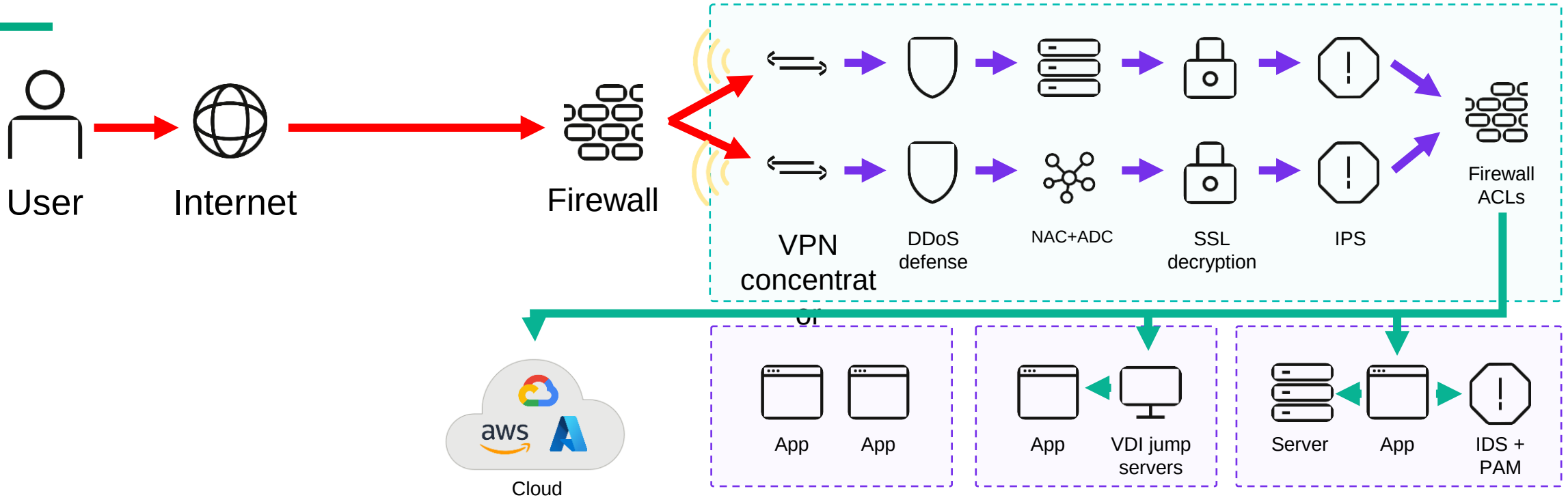
上網安全 ：SSE可以成為訪問任何資源的可見性和控制層

為所有用戶和設備提供全面保護



Agent & Agentless

傳統VPN網路
遠端工作使用者的安全旅程

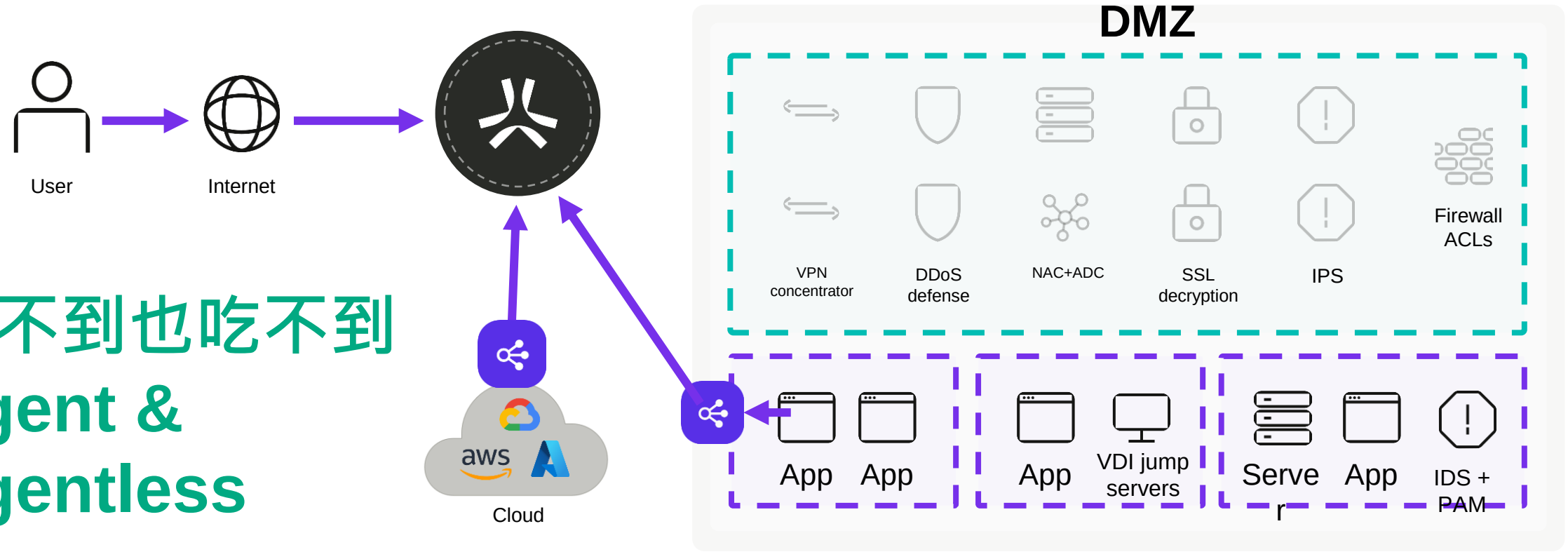


VPN 暴露IP。
VPN 就像信標，等待被發現。因此，IP 會暴露出來，從而形成可利用的攻擊面。

VPN 過度擴展網路訪問.
來自未知裝置的未知使用者擴展了網路訪問許可權，從而增加了攻擊面.

VPN 管理起來很複雜。
擴展物理 VPN 閘道會增加網路複雜性，並且成本高昂。
團隊跨多個UI管理多個配置和策略非常耗時且容易出錯。

HPE Aruba SSE ZTNA



看不到也吃不到 Agent & Agentless

無形的網路

由內而外的連接使應用程式完全不可見，**永遠不會暴露在互聯網上。**

應用程式訪問

遠端使用者只能獲得對授權應用程式的訪問許可權，而**不會將使用者或設備置於公司網路上**。

精細的最低許可權訪問

應用程式到使用者連接提供內置的應用程式分段，而無需複雜的網路分段。一對一連接使**未經授權的用戶無法橫向移動**。

Zero Trust Made Simple

Why use AI for Networking

The Benefits of AI for Networking

優化的性能

流量模式分析、網路擁塞預測，並在潛在瓶頸出現之前識別它們

減少停機時間

增強的流量監控以識別潛在問題，並自動採取糾正措施來**防止中斷**

預測分析

分析歷史數據，在潛在**網路問題**發生之前進行預測

自動化管理

自動執行日常網路管理任務，例如**配置、監控和故障排除。**

提高安全性

主動阻止潛在威脅，識別異常網路行為，並自動採取措施防止網路攻擊

中斷預測

分析網路流量允許通過數據分析和**機器學習來預測網路中斷**

自適應學習

隨著時間的推移，從新數據中學習，不斷**提高效率和安全性。**

網路性能

通過**分析流量模式、預測擁塞**和動態調整頻寬分配來優化網路

預測性維護

除了預測網路中斷外，AI 還支援主動維護以防止網路停機

員工效率

自動執行重複性任務，減少錯誤並促進更好的決策

HPE Aruba Networking AI for Networking Series

AI for Networking in HPE Aruba Networking New Central

AI for Networking in Wireless

AI for Networking in Switching

AI for Networking in Security

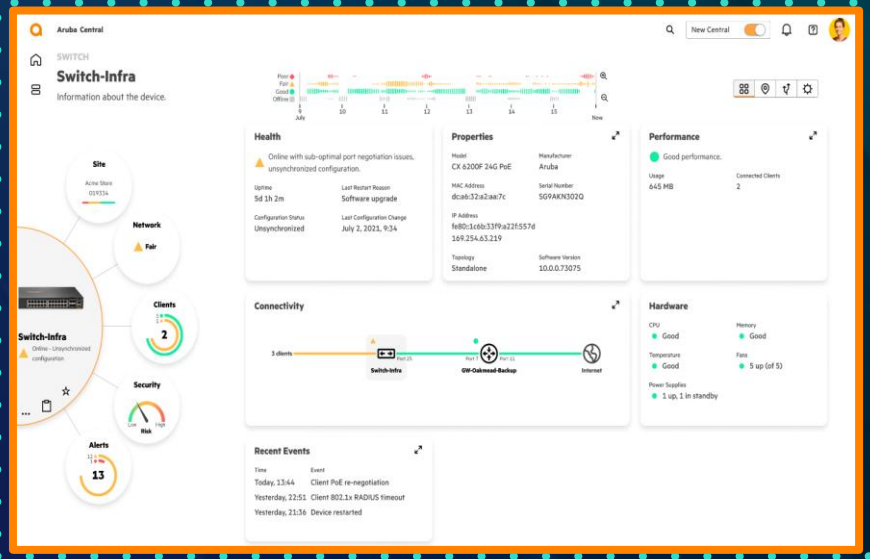
AI for Networking in verticals

Access Points / Switch/ Gateway send various types of telemetry data to HPE Aruba Networking Central

4.7M+ Network Device
1.6 B+ Clients

Client Behavior
Threat Detection
Traffic Metrics
Network Errors
Roaming
Location Services
Diagnostics
Anomalies
IoT Sensors
Policy Violations
Configuration Sync
Event Logs
Client Identification
Firewall Data
Threat Detection
Client Metrics
Wi-Fi and Radio Statistics
DPI
AP Details
Hardware Metrics
Health Status
Firmware Info
Security Insights
Power Save

Telemetry Data from Switch/AP/Gateway to Central

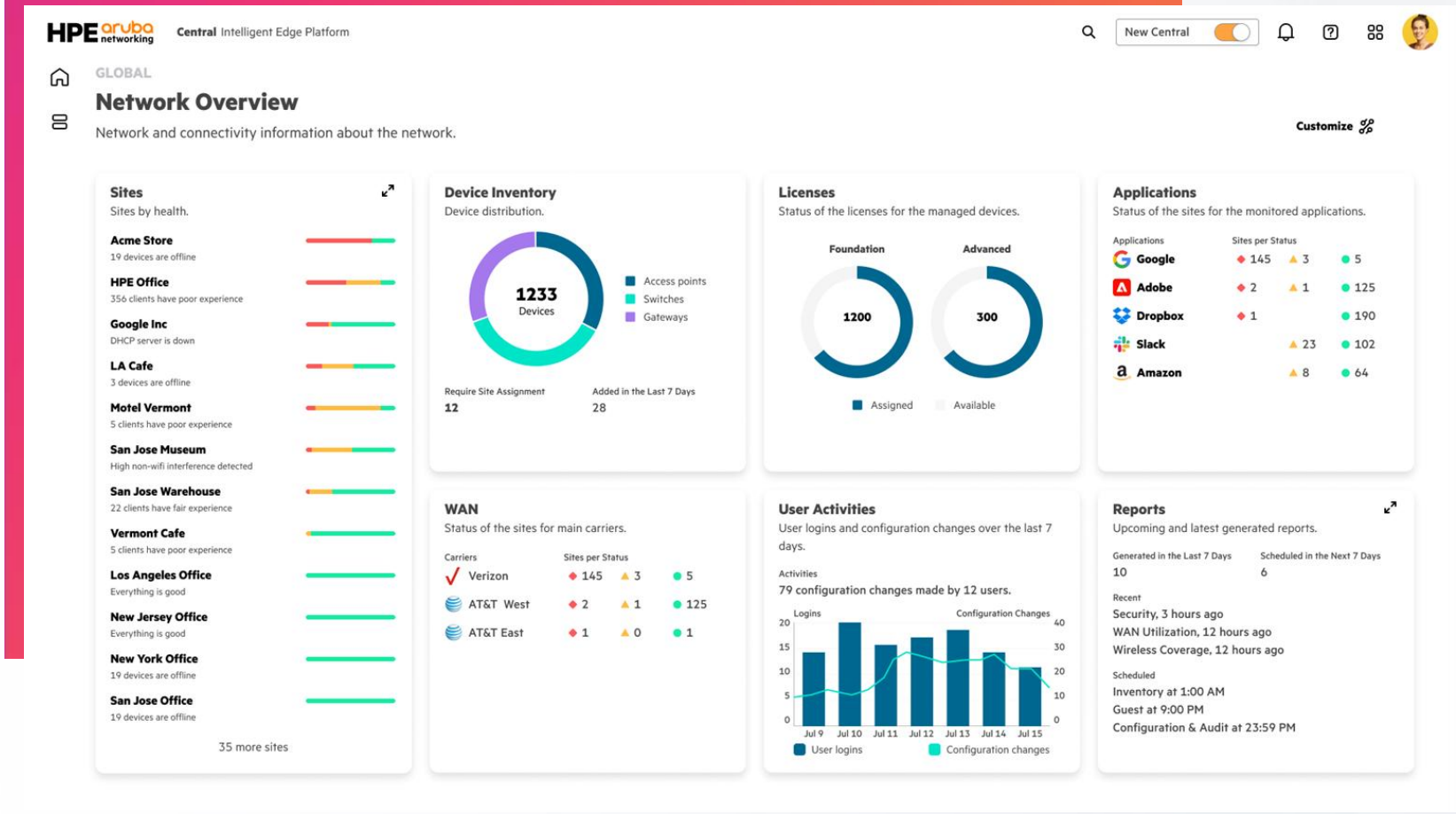


AI-powered, operator-centric experience

遙測Telemetry允許即時監控**網路流量**、**設備性能**和**應用程序行為**。這種可見性有助於**及時檢測異常**、**性能瓶頸**或**安全威脅**，從而及時進行干預。

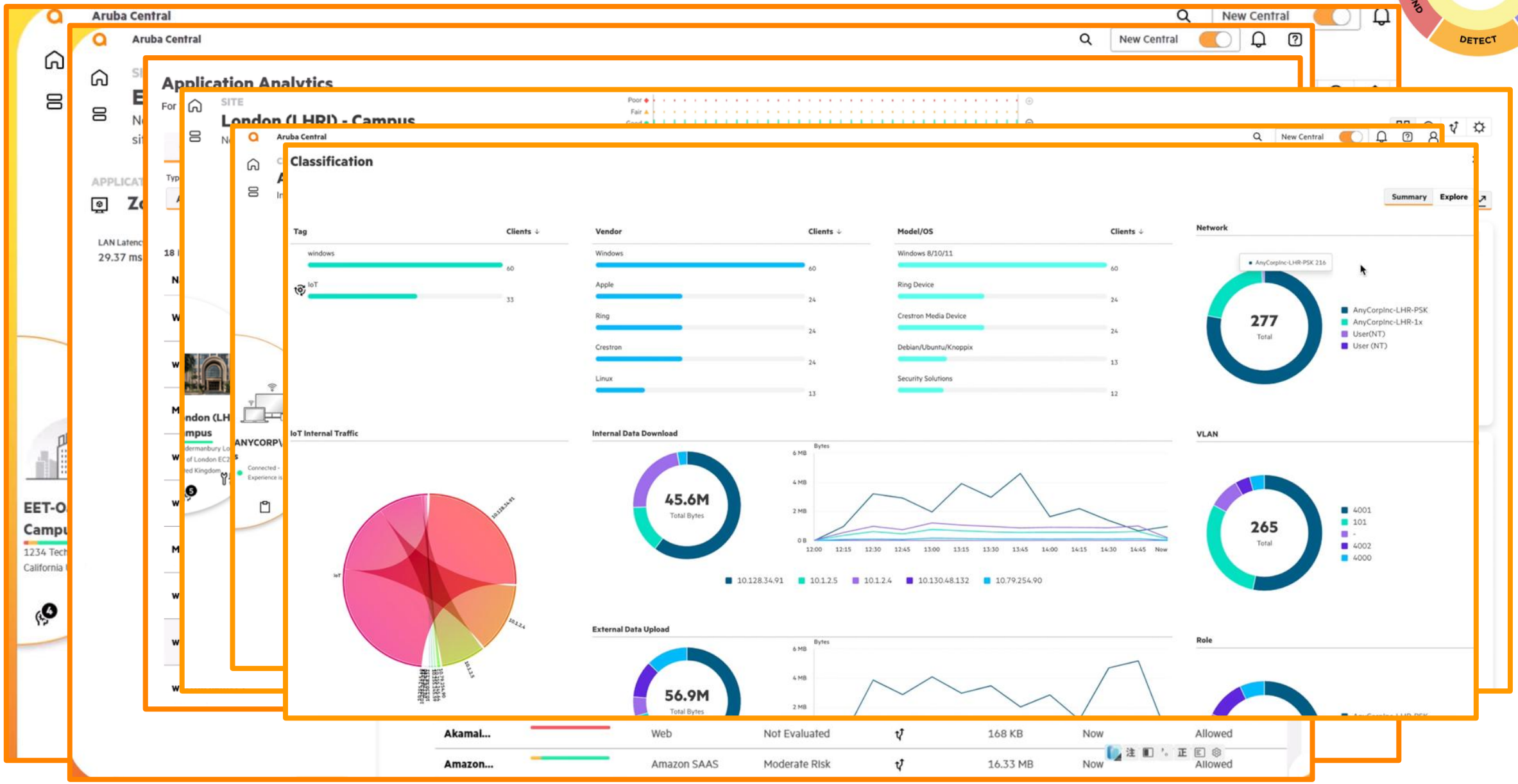
AI 驅動的網路運營儀錶板

Powerful ‘command center’ view to direct operator attention



- **統一的網路檢視**，用於快速評估網站運行狀況、應用程式體驗、設備清單等
- 優化網路運營的**「待辦事項」**清單
- **混合多樣指標**突出了需要**立即關注**的問題

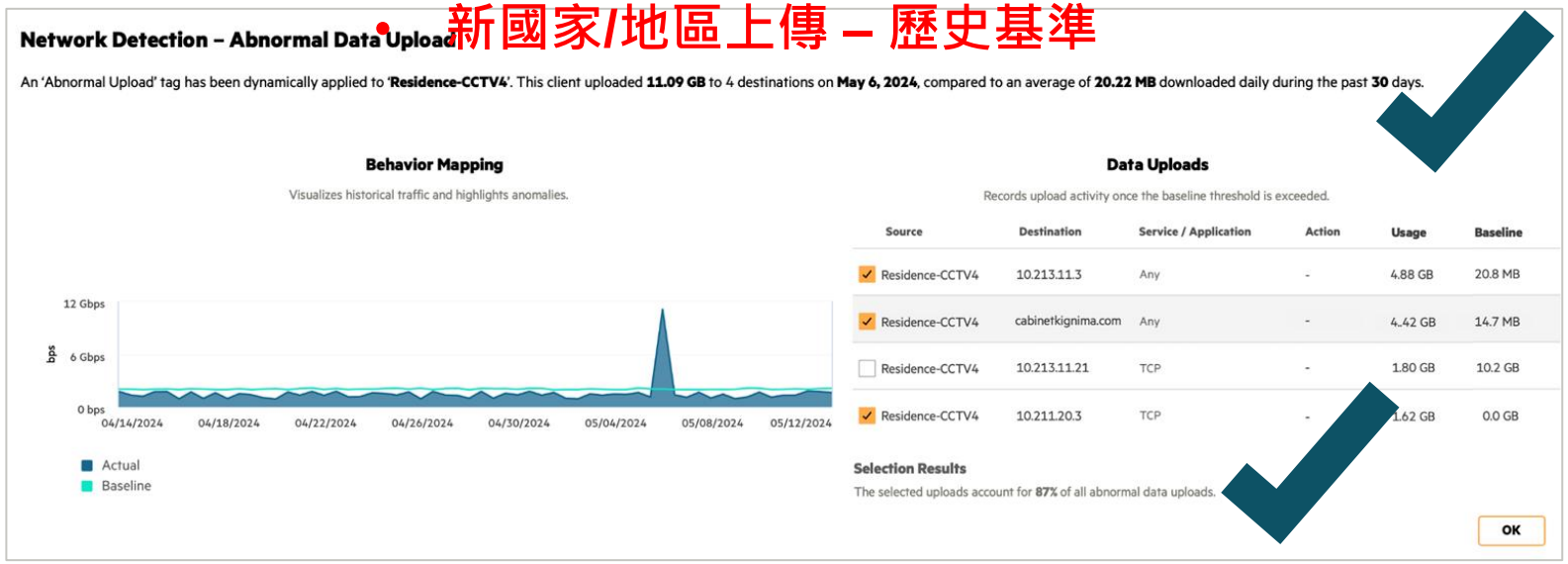
識別：使用 Client Insights 實現 AI 驅動的可見性和分析

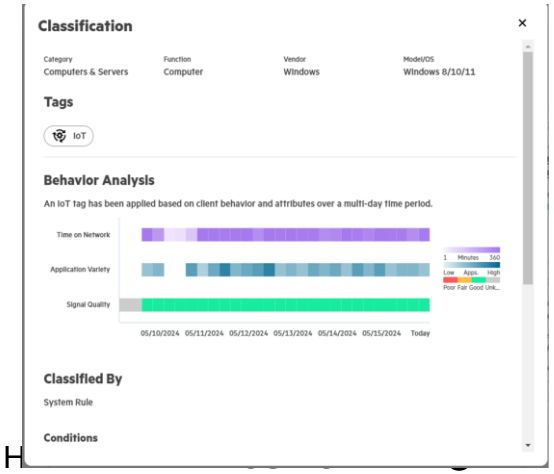


AI 驅動的、基於網路的網路檢測和回應（NDR）

- 檢測高風險 IoT 設備的危害
- 來至於行業領先的 HPE Aruba Networking Central 可觀測性數據湖
- 建立設備行為基線，檢測異常行為，併發出警報進行調查
- 內置於 HPE Aruba Networking Central 中，具有本機遙測功能，無需額外設備

- 異常數據下載 – 歷史基線
- 數據上傳異常 – 歷史基線
- 新國家/地區上傳 – 歷史基準





Representative screenshots subject to change.

AI 驅動的建議- Security Risk & Firmware

Network
Good
19 devices

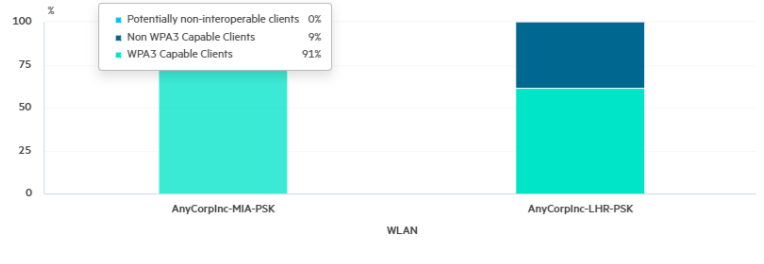
AI-Powered Network Optimization
in depth analysis for **London (LHRI) - Campus.**

Enable WI-FI 6 to Improve WLAN Performance
Improve average transmission rate by up to 13% on your WLANs by enabling WiFi 6
Yesterday at 5:30 AM

Enable WPA3 for Better Security
WiFi security will improve for up to 90% of Clients by enabling WPA3
Today at 5:30 AM

Power-Save Recommendation Available for Access Points
You have Power-Save recommendations available for 2 site(s) that can provide up to...
Yesterday at 5:30 AM

WPA Capable Clients by WLAN



Actions
Change the current Wi-Fi authentication to WPA3

WLAN	Current Authentication	New Authentication
AnyCorpInc-MIA-PSK	wpa2-psk-aes	wpa3-sae-aes
AnyCorpInc-LHR-PSK	wpa2-psk-aes	wpa3-sae-aes

Actions
No clients detected that are likely to have connectivity issues when WPA3 is enabled.

AI-Powered Network Optimization
in depth analysis for **QDSM Office.**

Access Point Firmware Recommendation
New firmware recommendation available for 2 access point(s) in the site. These upgrades provide new features and bug fixes.
Today at 4:00 AM

Available Firmware Recommendation - Access Points
Review the list in Classic Central for device specific AI-driven recommendations and apply the recommended upgrade there.

Firmware Info

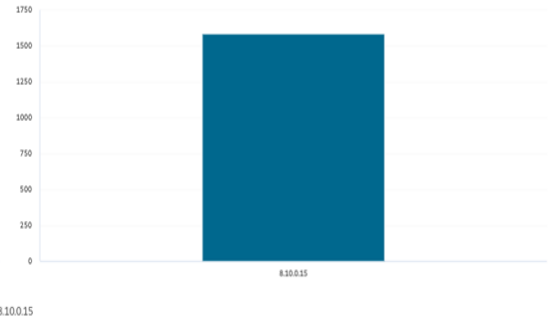
Firmware Recommendation Summary - Access Points
Firmware recommendations based on Model and Current Firmware.
Note: CVE-2024-3596, CVE-2024-6387 currently do not have fixed firmware versions available. To mitigate this vulnerability, implement workarounds mentioned in the security advisory issued by Aruba Threat Labs.

Model	Current Firmware	Recommended Firmware	Number of Devices	Recommendation Reason
AP-515	8.10.0.3_84941	**8.10.0.15_91324**	2	Minimizing firmware security vulnerabilities

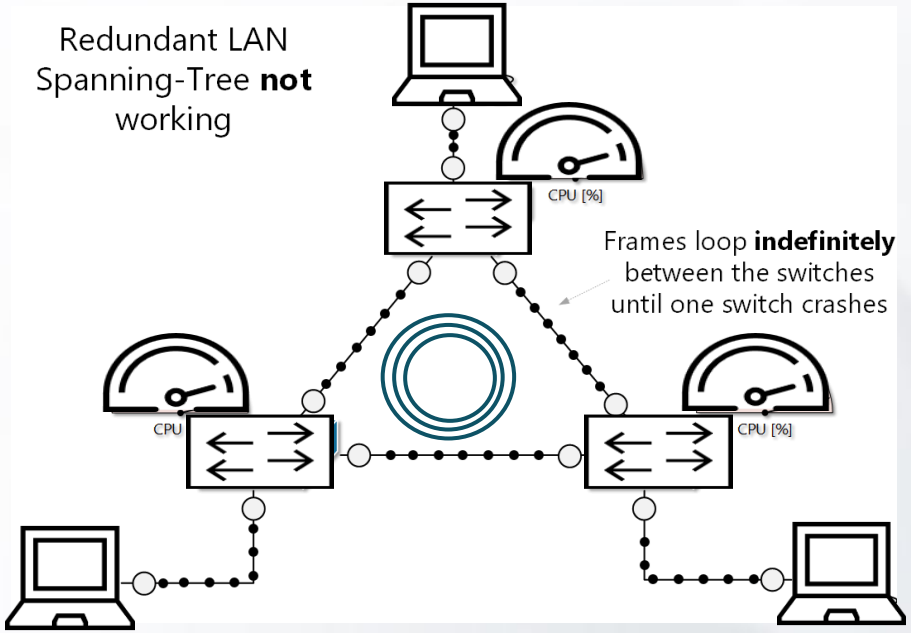
Popularity of Recommended Firmware
Charts provide details on adoption of the recommended firmware.

Device Count by Firmware Version

Customer Count by Firmware Version



When a Loop is Detected in a Network



問題癥狀

- **High CPU** utilization on the network switches
- Excessive **broadcast** or **multicast** traffic
- Network **slowdown** or outage
- Users' devices, IP Phone, CCTV Cameras, getting **disconnected** on wired and wireless network.

Manual Troubleshooting Mode Enabled

故障排除步驟和時間 - 1到6小時

所有IT團隊的人現在都專注於一個問題，並在不同的工具中進行故障排除.

運營影響、業務影響和 SLA 降級

IT 團隊解決迴圈所花費的時間

Time Estimates:

- Minor Loop (Single Switch Misconfiguration) – 30 minutes to 2 hours
- Moderate Loop (Impacting Multiple Switches) – 2 to 6 hours
- Major Loop (Enterprise-Wide Outage) – 6 hours to 2+ days

Detect and Recover – Loop detection and Analysis

AI Powered Alerts – For Spanning Tree Loops in the

Summary

Switch BO-MIAI-EGSW02 has an L2 loop with itself.

First Occurred: January 21, 2025 4:25 PM
Last Occurred: January 30, 2025 11:35 AM
Occurrences: 1579
Priority: Very High

Impact

Clients: No impact
Access Points: No impact
Switches: 34% (1/3)
Gateways: No impact

Action

Root Cause
Loop(s) was detected and it consists of the following connections:
- BO-MIAI-EGSW02 1/1/12 <-> BO-MIAI-EGSW02 1/1/11

Action
Check topology and STP configuration

Health

Online with High port utilization with frame drops, high port utilization, high broadcast traffic.

Uptime: 14w 5d 13h 8m
Last Restart Reason: Reboot requested by user, Version: FL.10.10.1140 18 Oct 24 18:29:03 : Switch bo...
Configuration Status: Synchronized
Last Configuration Change: October 24, 2024 10:02 AM

Properties

Model: CX-6300F
Manufacturer: Aruba
MAC Address: e4:de:40:ee:90:40
Serial Number: SG39KN5013
IP Address: 172.31.0.55
Deployment Mode: Standalone
Software Version: FL.10.14.1010

Connectivity Performance

High broadcast traffic, high port utilization, high port utilization with frame drops

Usage: 6.38 TB (7.59 MB of Uplink usage)
Uplink Utilization: 0 % (3.48 kbps) 0 % (2.19 kbps)
Connected Clients: 0

Connectivity

0 clients — BO-MIAI-EGSW02 — Internet

Hardware

CPU: Good
Memory: Good
Temperature: Good
Fans: 3 up of 3
Power Supplies: 1 up of 1
PoE Capacity: 370 W
PoE Output: 7.70 W

Events

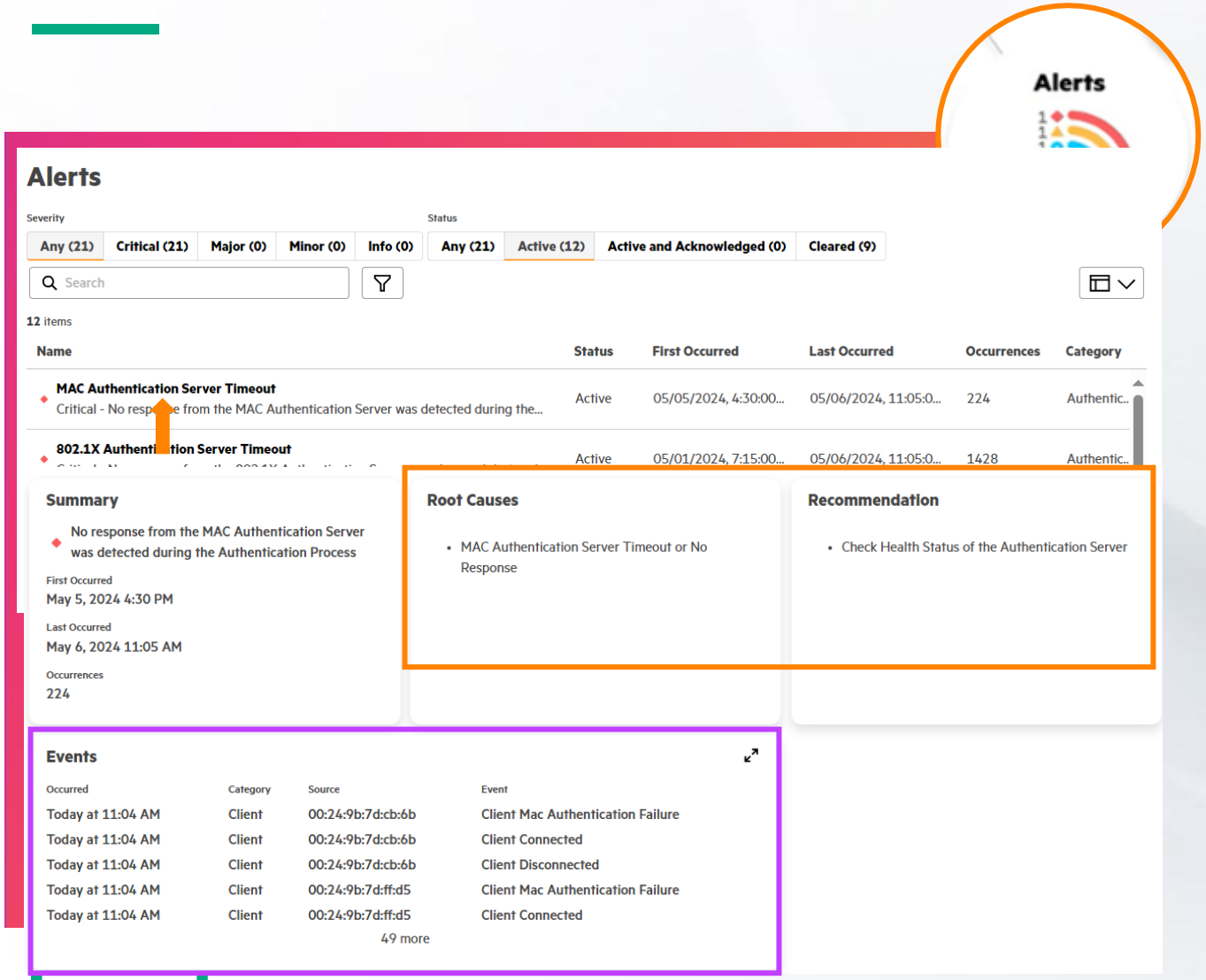
Occurred	Category	Source	Event
Today at 8:39 AM	Connectivity	BO-MIAI-EGSW02	Aruba Central Connection Failure

- **High Broadcast traffic,**
- **High port utilization with frame drops**

立即發現問題，並指導 IT 團隊找到根本原因以快速解決。

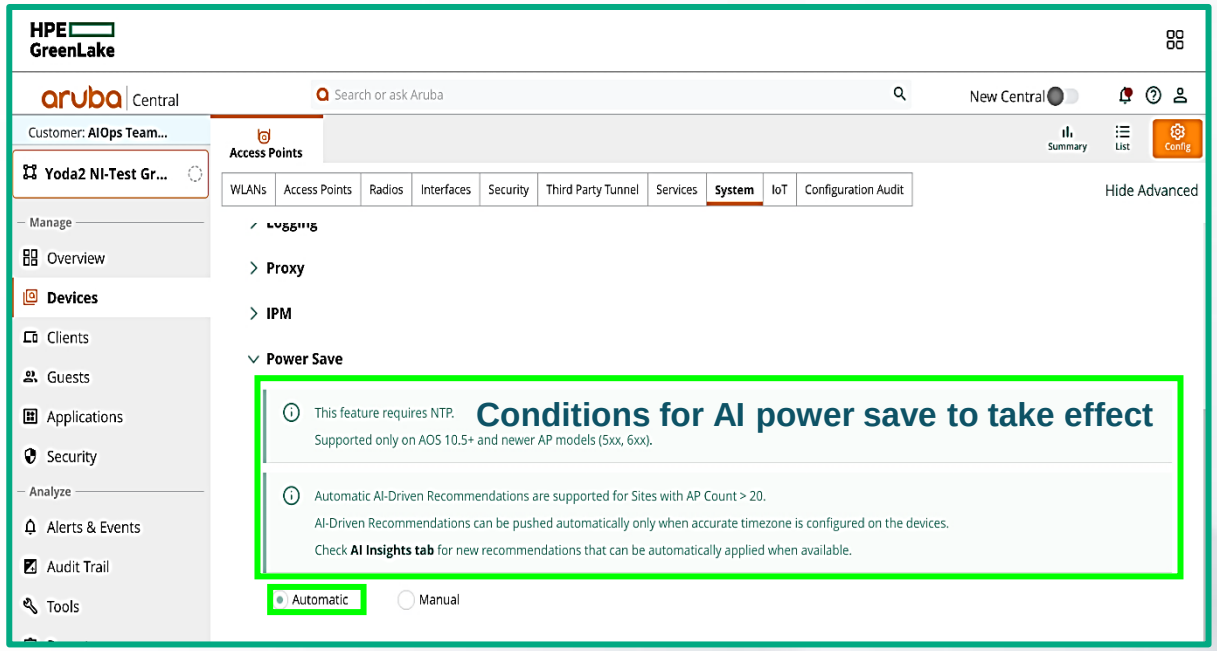
無運營影響和業務影響以及維護 SLA

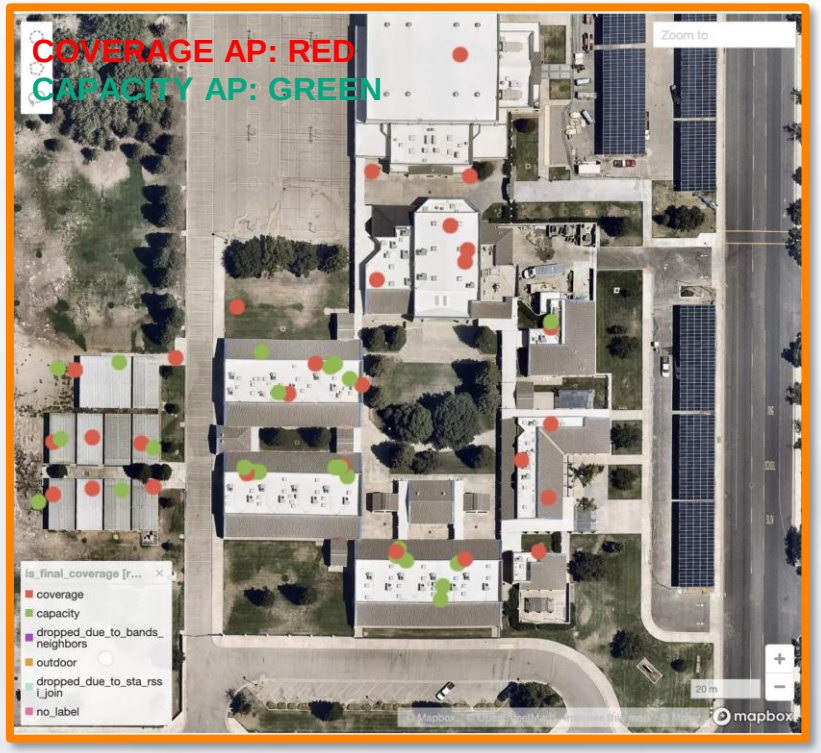
AI 驅動的保障和警報
Accelerate troubleshooting across skill levels



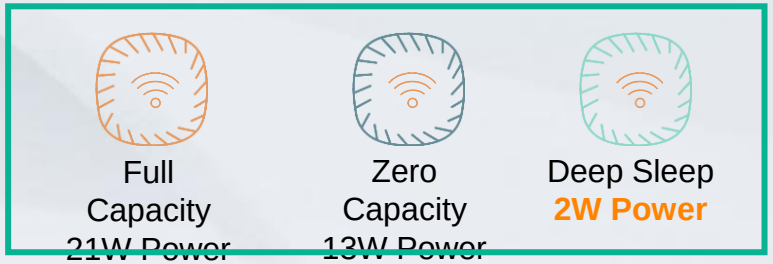
- 在 <5 分鐘內從事件到洞察，提供近乎即時的警報，加快 MTTR
- 具有精確根本原因、建議和影響的全棧關聯
- 通過整合觸發事件清單減少警報疲勞
- 設備運行狀況和客戶體驗的保證指標，用於快速診斷

AI 驅動 Power Saving





- Access Points draw power from **PoE switches around 10W to 30W,** based on the user connectivity and services.
- Which has impact on **energy consumption, cost and CO2 Emission**.
- With **AI Intelligence** we are now able to solve this issue in a **dynamic way** and support organization to **save energy cost and get down the CO2 Emission.**



Green Wi-Fi is using AI to dynamically adjust AP PoE power based on the site conditions and behavior.

AFT Tool :- Wireless Power Saving Calculator

HPE aruba networking

統一、安全、簡化的網路基礎設施，
提供各式連接方式並保護以及加速業務成果

Connect + Protect + Automate

Public cloud

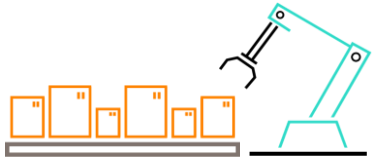
aws Microsoft Azure

Colocation

Private DC

Campus

Edge / Branches



Routing | SD-WAN | VPN/VPC | 25-400G/VXLAN | Wired POE/Wireless
6E | Private 5G

Thank you

8合1轉接器

填問卷送好禮

QR Code