網路安全 3+3 資安聯防大作戰

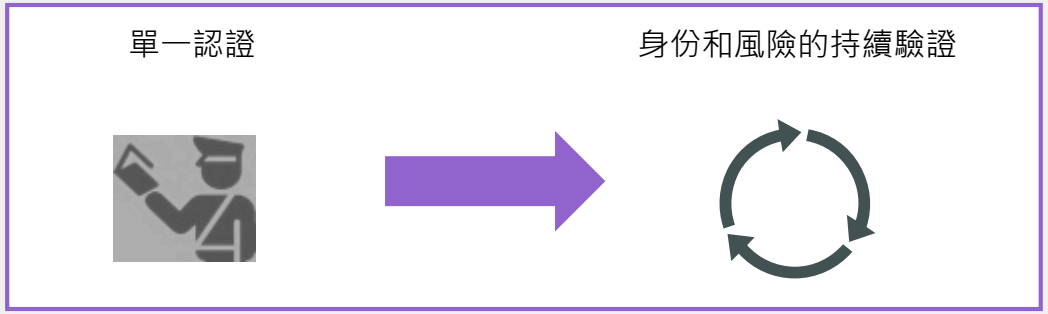
李尚峰 Jarvis Lee
Fortinet 台灣區技術顧問
+e: ljarvis@fortinet.com
1/29/2024

主題大綱

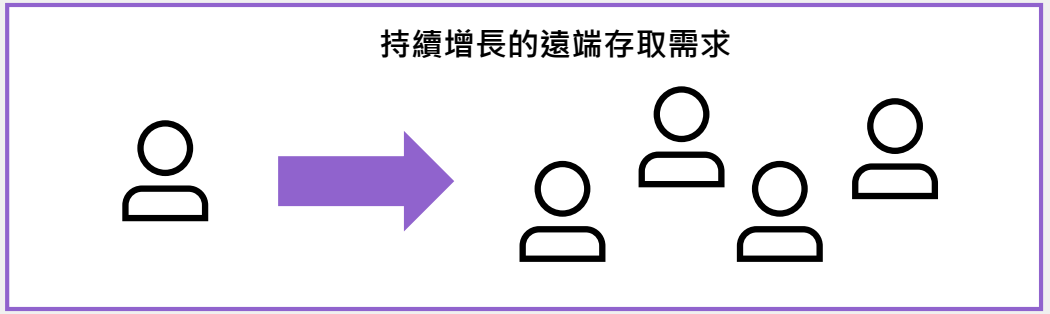
- 趨勢與現況
- 為何選擇 Fortinet
- 新世代 資安鐵三角

© Fortinet Inc. All Rights Reserved.

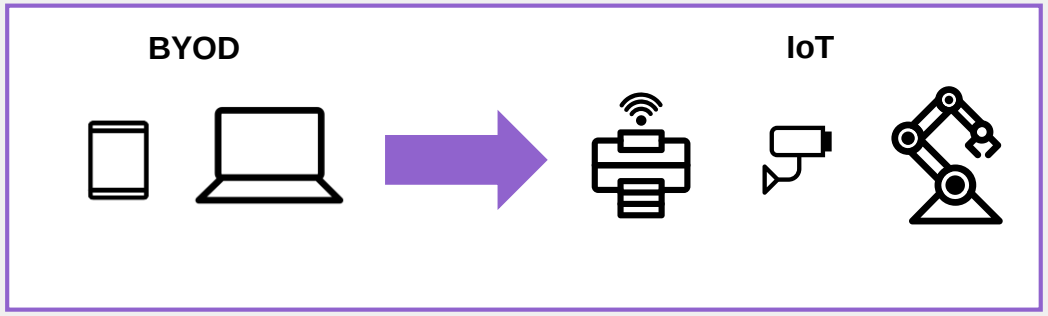
企業網路的存取趨勢演化



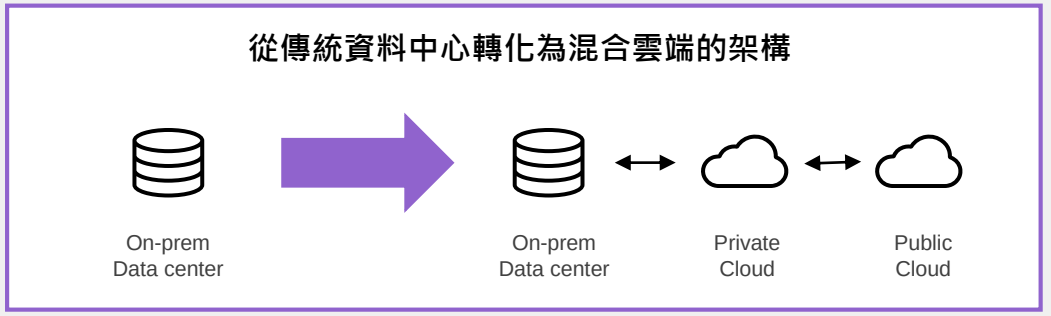
到 2024 年，70% 的應用程序存取將使用多因子認證，遠高於今日的10% *1



到2021年底，透過遠端存取的工作者將從4%成長到30%的幅度 *2



到 2025年, 有超過 120億個IoT 裝置會被安裝啟用 *3



從Gartner 的客戶統計中，IT 建構混合雲的模式日漸普及 *4

1 Gartner Magic Quadrant for Access Management, 12 August 2019
2 Global Workplace Analytics
3 Gartner IoT Forecast
4 Gartner Magic Quadrant for Public Cloud Managed Services, 4 May 2020

© Fortinet Inc. All Rights Reserved.

IT 維運管理的挑戰

© Fortinet Inc. All Rights Reserved.

主題大綱

趨勢與現況

為何選擇 Fortinet

新世代 資安鐵三角

© Fortinet Inc. All Rights Reserved.

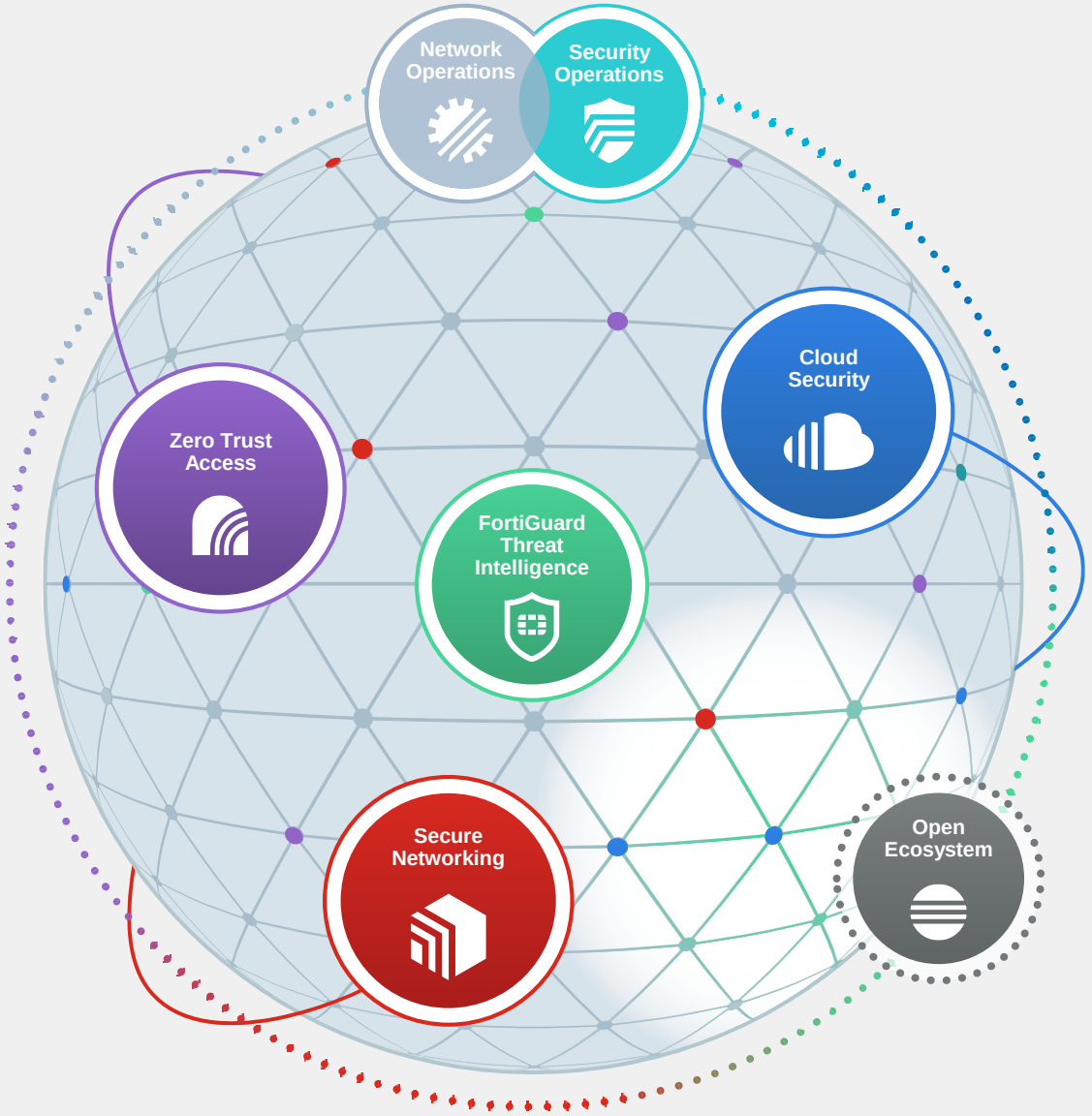
Fortinet Security Fabric

安全織網

Broad
新世代的防護方案需提供高可視度與防護性已涵蓋來自多面向的資訊威脅

Integrated
整合多樣化的技術用以防護偵測進階威脅的入侵攻擊

Automated
整合式的智能系統，經由持續性的自動化檢測評估，確保資安系統自身維持最優化配置



Appliance
Virtual
Hosted
Cloud
Agent
Container

© Fortinet Inc. All Rights Reserved.

Fortinet 安全織網（Security Fabric）

一個能夠驅動企業數位化創新的網路安全平臺

© Fortinet Inc. All Rights Reserved.

獲得Gartner第三方認證的肯定

透過單一平台完整涵蓋資安與網路

2022 Magic Quadrant for Network Firewalls

Fortinet Recognized as a Leader

2022 Magic Quadrant for WAN Edge Infrastructure

Fortinet Recognized as a Leader

2022 Magic Quadrant for Wired & Wireless LAN Access Infrastructure

Fortinet Recognized as a Visionary

© Fortinet Inc. All Rights Reserved.

獲得ChatGPT的肯定

GPT-4哦，我有付費買一個月。

fortinet的產品 資安效果如何

Fortinet 的產品在資安效果方面具有很高的聲譽。他們的產品線提供全面的網絡安全解決方案，包括防火牆、入侵防護系統（IPS）、網絡訪問控制、郵件安全、網絡沙箱、安全信息和事件管理（SIEM）等。這些產品旨在保護企業和組織免受各種網絡威脅，如惡意軟件、勒索軟件、分佈式拒絕服務（DDoS）攻擊等。

Fortinet 的核心產品 FortiGate 是一個統一威脅管理（UTM）系統，它結合了多層次的安全防護功能，可識別和阻止各類網絡攻擊。他們還提供不斷更新的威脅情報，以幫助企業及時應對新興的網絡威脅。

在獨立的測試和評估中，Fortinet 的產品經常獲得優異的成績，表明其資安效果可靠。然而，值得注意的是，沒有任何安全產品能夠提供100%的保護，企業和組織應該採取多層次的安全策略，結合其他安全措施（如安全意識培訓、定期備份等）來確保網絡的安全。

總之，Fortinet 的產品在資安效果方面具有很高的聲譽和良好的性能，但您應該根據自己的需求和網絡環境進行評估，並結合其他安全措施以實現更全面的保護。

et 已經成為全
企業和組織免

。許多企業、政
，Fortinet 的產
。

網絡環境來進
擇。

主題大綱

趨勢與現況

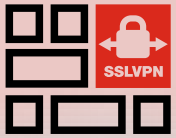
為何選擇 Fortinet

新世代 資安鐵三角

© Fortinet Inc. All Rights Reserved.

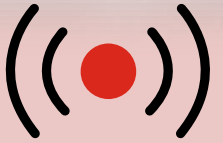
2018 Fortinet 安全織網 – 資安鐵三角

單設備最大可提供 SSL VPN
連接 30,000 使用者



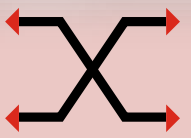
FortiGate

FortiAP



單設備最大可連接
4,096 個 APs

FortiSwitch

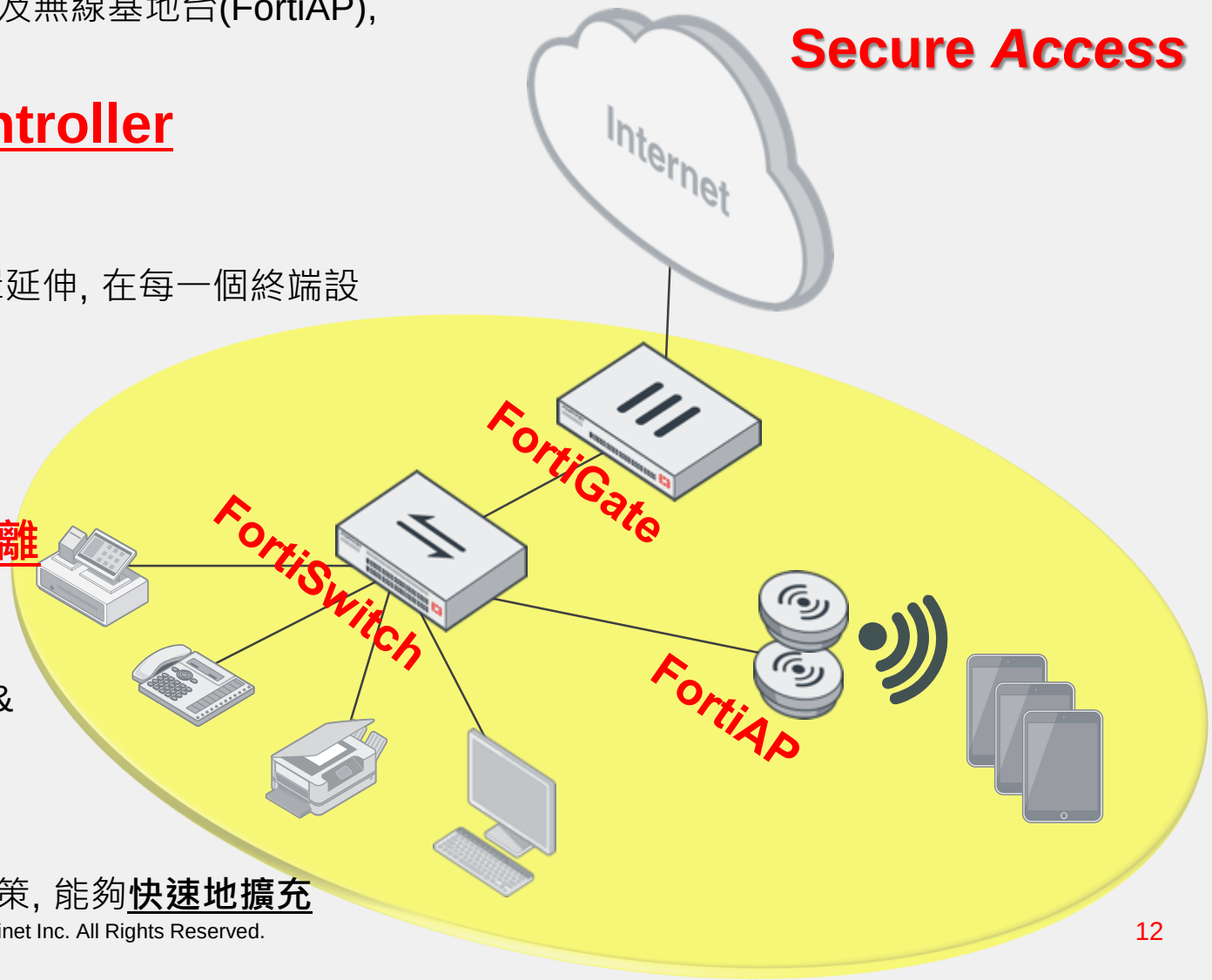


單設備最大可串接管控
256 台 Switches

© Fortinet Inc. All Rights Reserved.

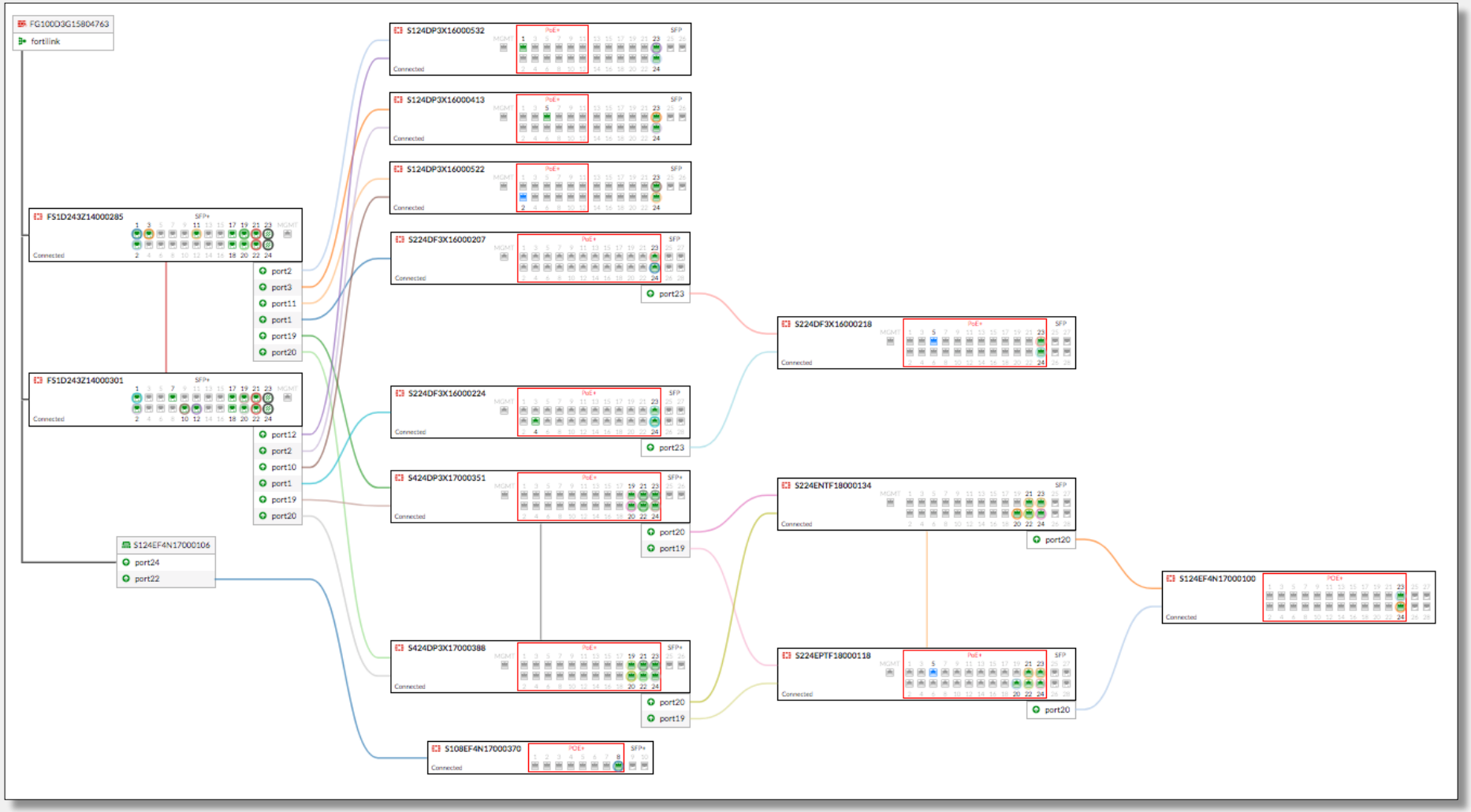
2018 Fortinet 資安鐵三角 特點

- **容易管理**
  - 整合防火牆(FortiGate), 交換器(FortiSwitch)以及無線基地台(FortiAP), 在統一的接入介面管理
  - **FortiGate 就是 AP及 Switch的 Controller**
- **內外網的安全**
  - 讓 FortiSwitch及 FortiAP成為 FortiGate的邏輯延伸, 在每一個終端設備的前面, 進行內網**端點的資安管控**
- **及時控管**
  - 網路拓樸及流量監控**可視化**
  - 針對發生資安問題的終端設備做 **Layer 2隔離**
- **節省成本**
  - FortiSwitch與 FortiAP不需要額外的授權成本 & 學習成本
- **彈性擴充**
  - 透過彈性的架構因應客戶的網路環境及管理政策, 能夠**快速地擴充**



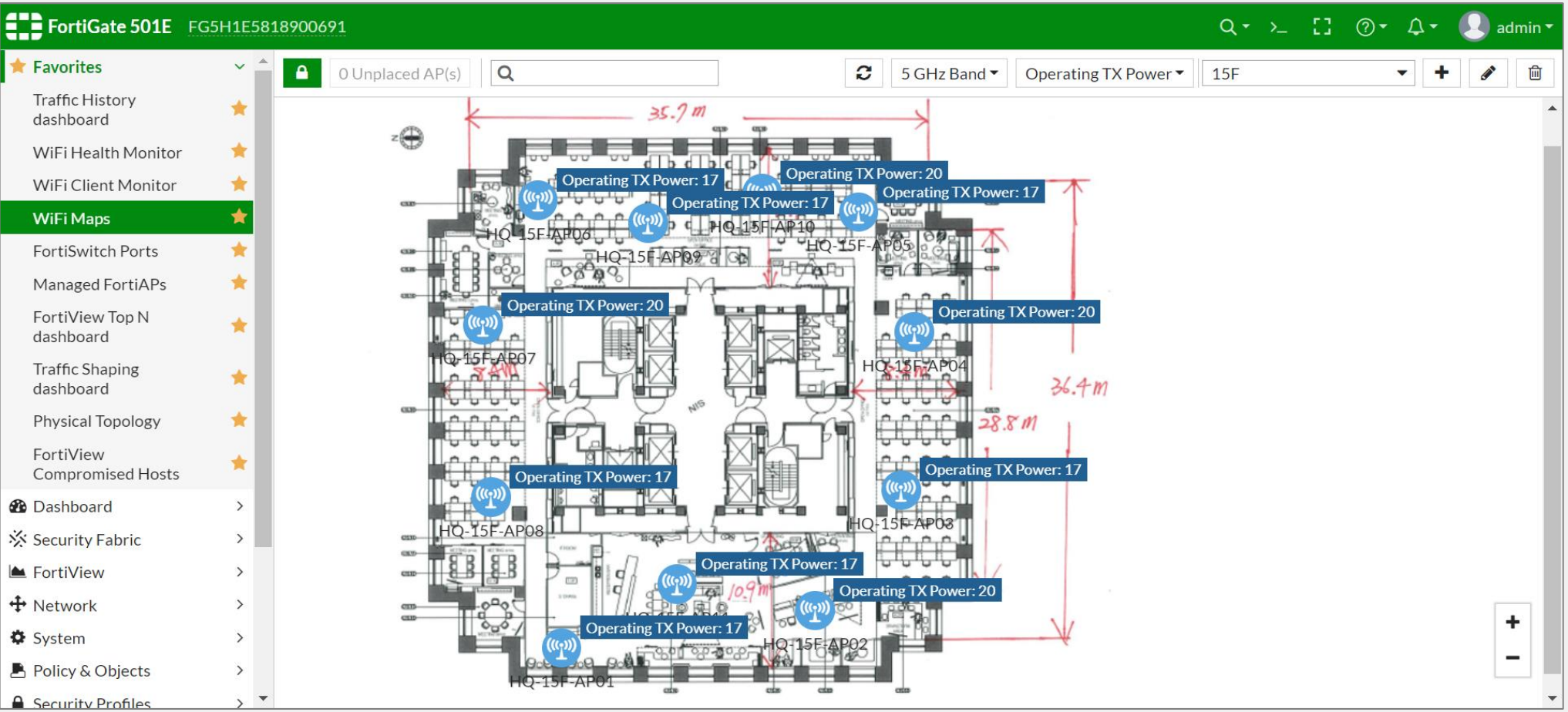
© Fortinet Inc. All Rights Reserved.

FortiSwitch - 自動產生拓樸圖



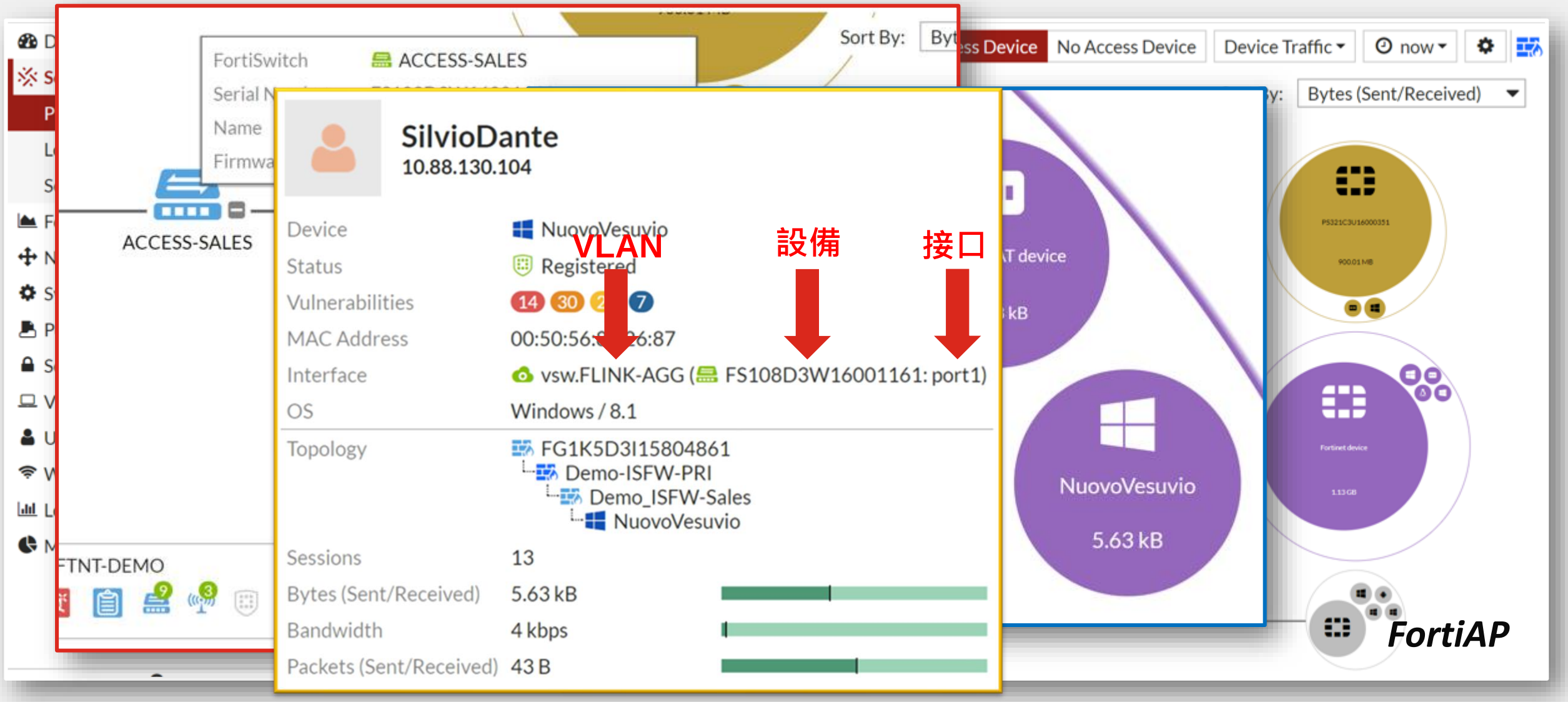
© Fortinet Inc. All Rights Reserved.

WiFi Maps - 圖面顯示樓每一台AP



© Fortinet Inc. All Rights Reserved.

Security Fabric 清楚呈現網路拓樸結構

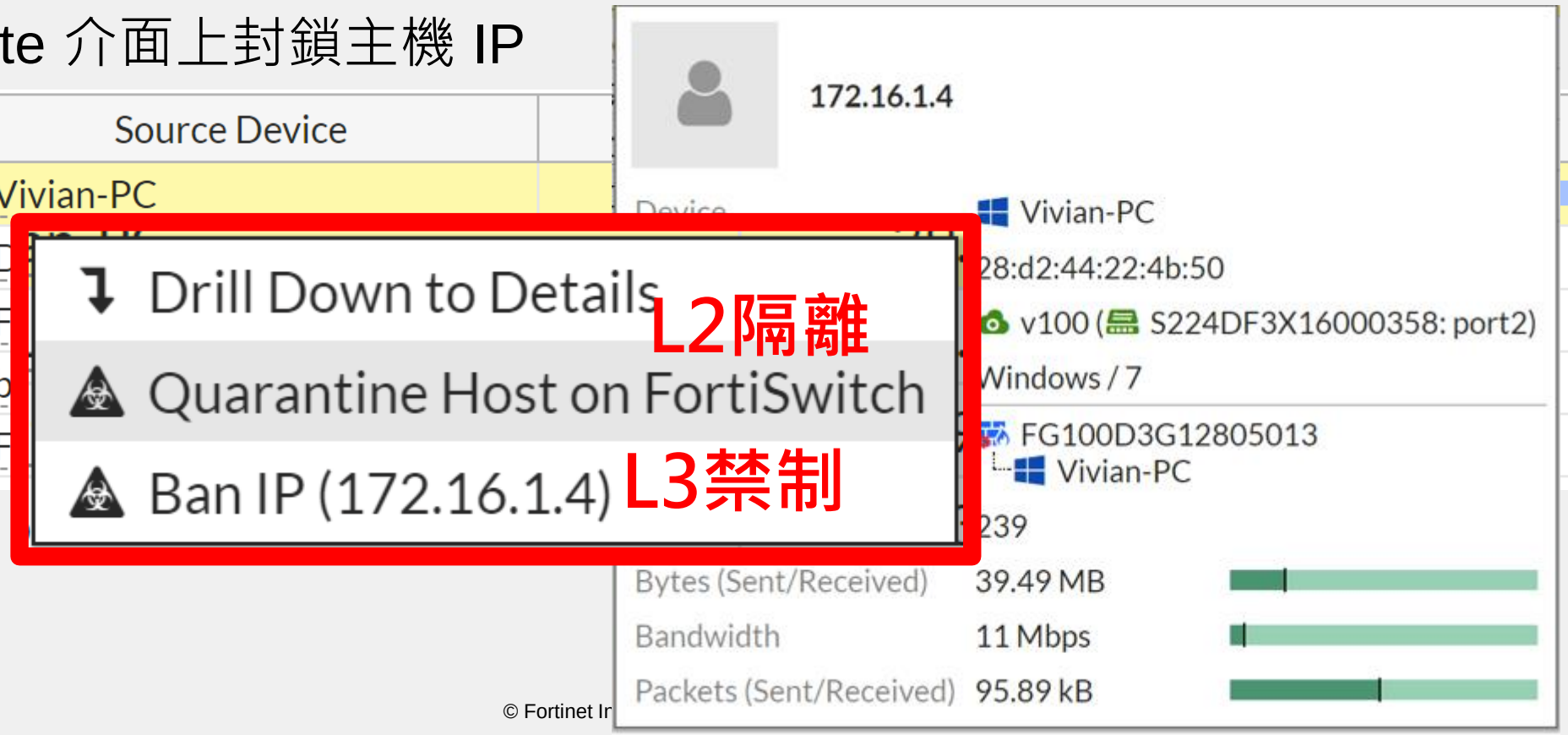


© Fortinet Inc. All Rights Reserved.

將問題主機攔阻在 FortiSwitch 及 FortiAP 上

- 在FortiSwitch 及FortiAP 上直接隔離有問題的主機 (隔離 VLAN)
  - 採用 VLAN 隔離的方式, 將問題主機放入該隔離 VLAN 中
    - By **MAC address**
- 在FortiGate 介面上封鎖主機 IP

Source	Source Device
172.16.1.4	Vivian-PC
172.16.1.6	D
172.16.1.8	F
172.16.1.5	b
172.16.1.7	F

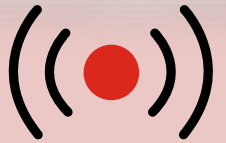


© Fortinet Ir

新世代 資安鐵三角

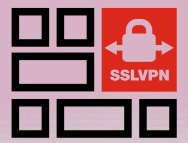
新世代 - 資安鐵三角

FortiAP



單設備最大可連接
4,096 個 APs

單設備最大可提供 SSL VPN
連接 30,000 使用者

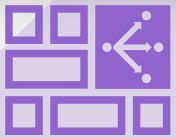


FortiGate

FortiSwitch

單設備最大可串接管控
256 台 Switches

SD-WAN

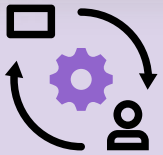


透過應用導向並整合資安防護
達成最佳路徑選擇

FortiToken

結合手機載具，完備身份驗證

ZTNA



持續性的檢測從用戶身份辨識
到設備安全

© Fortinet Inc. All Rights Reserved.

新世代 - 資安鐵三角

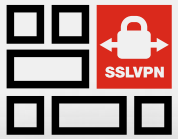
FortiAP

單設備最大可連接
4096 個 APs

FortiSwitch

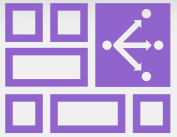
單設備最大可串接管控
256 台 Switches

單設備最大可提供 SSL VPN
連接 30,000 使用者



FortiGate

SD-WAN

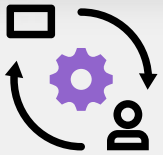


透過應用導向並整合資安防護
達成最佳路徑選擇

FortiToken

結合手機載具，完備身份驗證

ZTNA



持續性的檢測從用戶身份辨識
到設備安全

© Fortinet Inc. All Rights Reserved.

Fortinet 提供高效且安全的 SD-WAN 方案

01 以應用程序為導向的控制

廣泛的應用程序辨識與控制技術，提供更好的用戶使用體驗

02 業界唯一透過硬體加速技術

業界最早使用 SD-WAN ASIC WAN Edge，可用於各式各樣部署環境

03 簡化的管理機制整合安全管控

將網路安全、SD-WAN 和 SD-Branch 集中統一管控和報表分析，簡化企業運營負擔

© Fortinet Inc. All Rights Reserved.

透過 SD-WAN ASIC 達到業界最佳性價比

適用於Edge 端的各個機型

01

Apr 2019
FGT 100F
發表業界第一顆
SD-WAN ASIC 晶片

02

Oct 2019
FGT 60F
將 SD-WAN 功能與次世代防火牆無縫整合

03

Feb 2020
FGT 40F
發表業界最高信性價比的SD-WAN 專用機

04

July 2020
FGT 80F
發表內建 Bypass 的機種
是用在OT/IT 等重要基礎建設場域的機種

05

Oct 2020
FGT 200F
發表市場上同級距最強效能的多功能機種，適合在用於企業行內網防護與多功能同時執行SD-WAN與NGFW的最佳設備

06

May 2022
FGT 70F
提供企業在分點部署上有更多的選擇
兼具 SD-WAN + NGFW

07

Jul. 2023
FGT 90G
基於Desktop機種上具備10G SFP+ 介面擁有高效傳輸特性

SP4

SP5

多樣化的型號與變化便於各式各樣的場域環境

Built-in LTE

Built-in Wireless

POE+

Built-in POE

Bypass

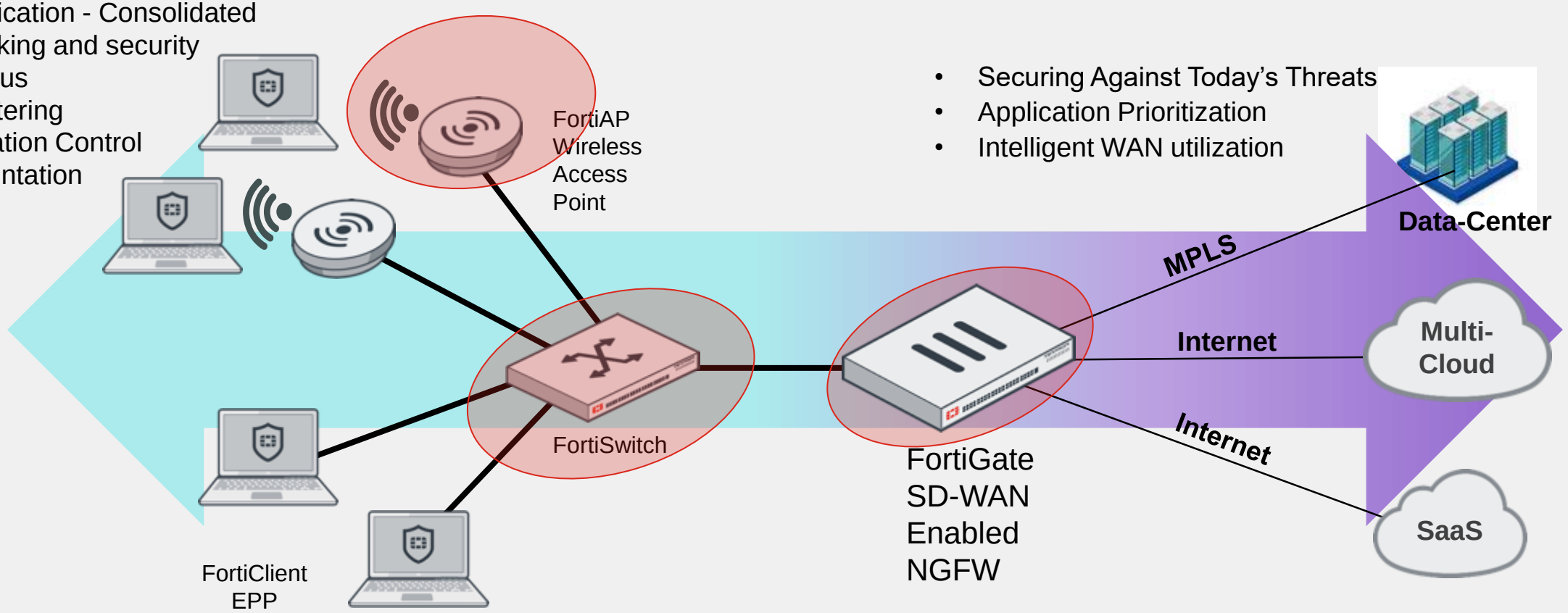
Built-in Bypass

© Fortinet Inc. All Rights Reserved.

Fortinet 鐵三角涵蓋內外網的所有資安管控需求

FortiGate 是網路資安核心管理設備

- Simplification - Consolidated networking and security
- Anti-virus
- URL filtering
- Application Control
- Segmentation



- Securing Against Today's Threats
- Application Prioritization
- Intelligent WAN utilization

管理單一減少維運負擔

功能與安全無縫整合

投資回報最大化

新世代 – 資安鐵三角

FortiAP

單設備最大可連接
4096 個 APs

FortiSwitch

單設備最大可串接管控
256 台 Switches

單設備最大可提供 SSL VPN
連接 30,000 使用者

FortiGate

SD-WAN

透過應用導向並整合資安防護
達成最佳路徑選擇

FortiToken

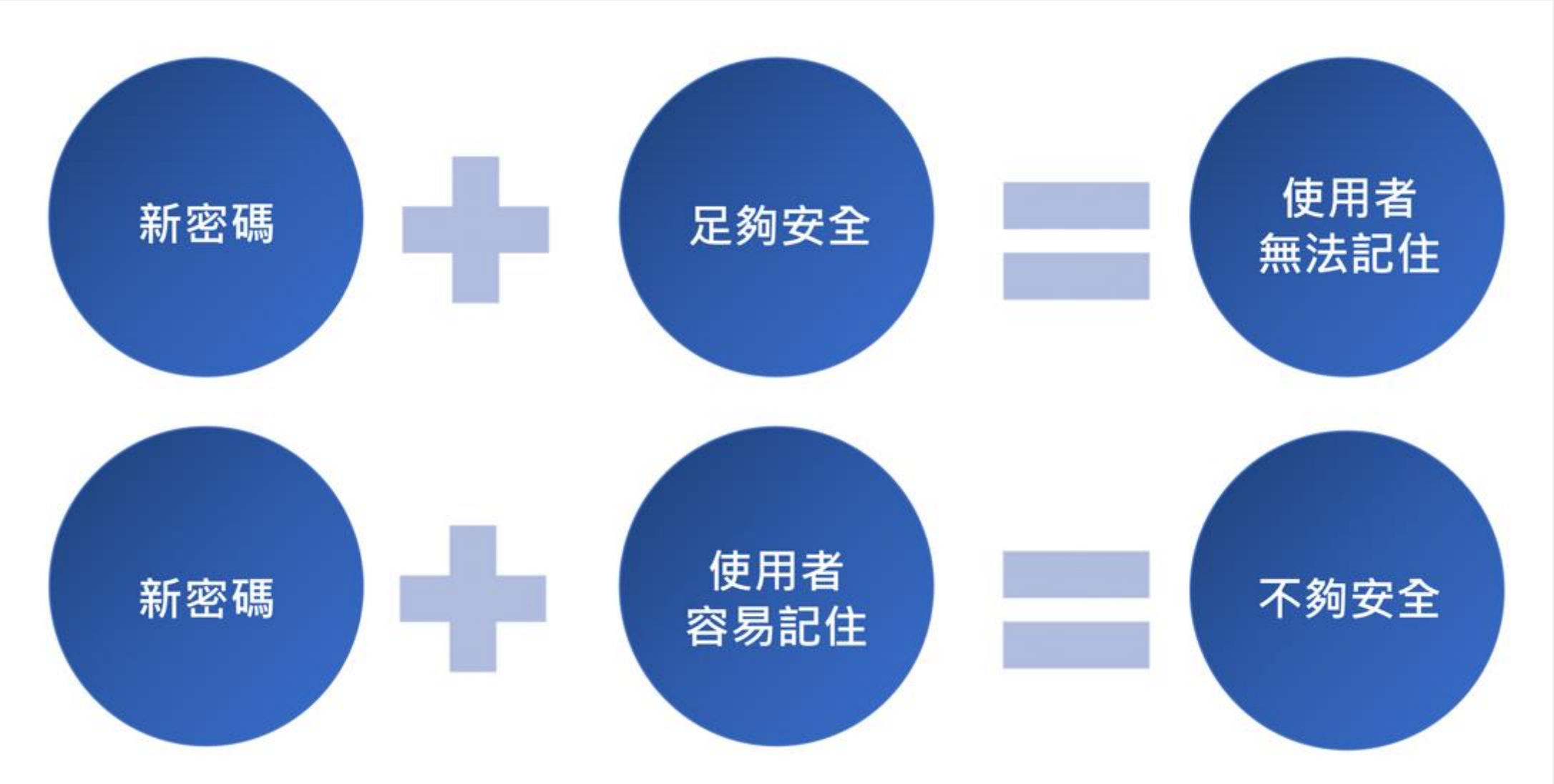
結合手機載具，完備身份驗證

ZTNA

持續性的檢測從用戶身份辨識
到設備安全

© Fortinet Inc. All Rights Reserved.

夠安全又能記住的密碼是一項挑戰…



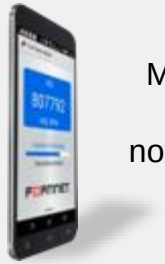
© Fortinet Inc. All Rights Reserved.

FortiToken 提供多樣化選擇

永久授權，每年不需再付授權費用

- 彈性購買包裝，單一購買從 5 組到 10,000 自由組合
- 硬體樣式 – USB 憑證載具, 卡片式, 體積小；強固外殼便於攜帶
- 軟體樣式 – APP 軟體載具於 Apple Store / Play Store 直接下載，確保來源安全無變造，支援主動推播通知便利使用
- 最新的 FTK-400 通過 FIDO 機構認證(無密碼) 安全金鑰技術，支援 FIDO2 U2F 等級

FortiToken Mobile



Multi platform OATH OTP application with push notification of login attempts and one tap approval

FortiToken Cloud

Subscription Service
Centralized token management
No additional Hardware, Software, or Firewall reconfiguration

FortiToken 220

A mini credit form factor OTP token

FortiToken 200B / 200BCD

Durable, large display, OATH OTP token with FortiGuard activation or optional encrypted activation file.

FortiToken 300

- Driverless USB Device
- FIPS-140 compliant
- Economical PKI authentication. Use with cryptography apps, VPN, web-based apps

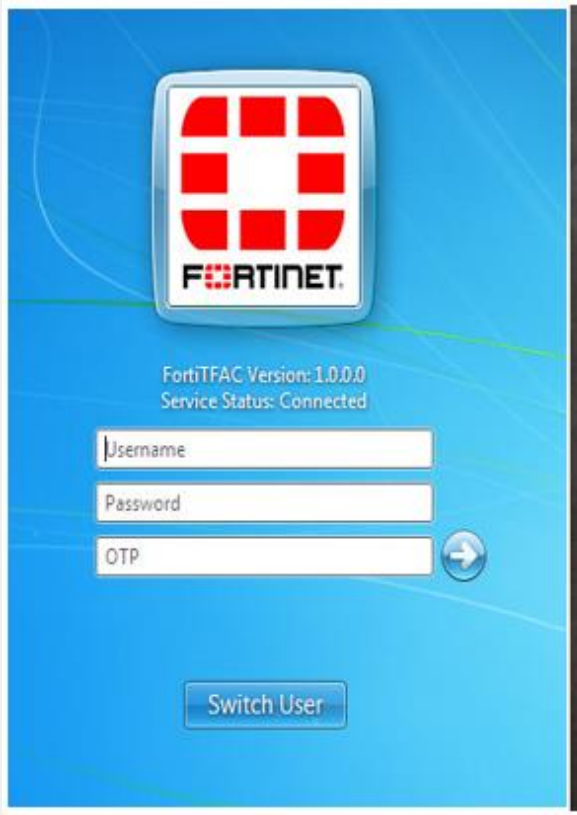
FortiToken 400

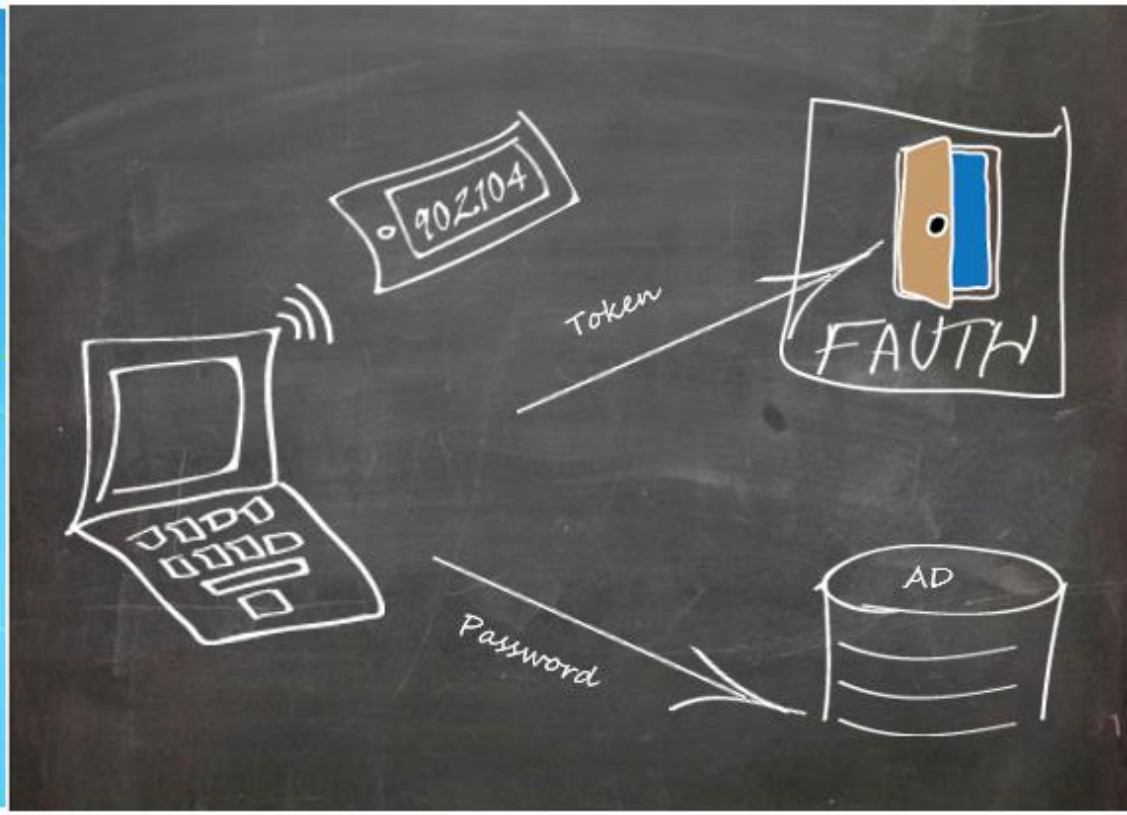
- FIDO certified
- Passwordless security key
- Use with SSL/VPN, SaaS, or FIDO2 supported browsers

© Fortinet Inc. All Rights Reserved.

應用場景 – 強化作業系統的身份驗證

- 強化作業系統登入使用雙因子驗證
  - Credential Provider Plugin Installed in the Client PC
  - Split Authentication Process:
    - Token Authentication to the FAC
    - Password Authentication to DC
    - Protects PC from brute forcing
    - Utilizes SSL API rather than RADIUS





© Fortinet Inc. All Rights Reserved.

新世代 – 資安鐵三角

FortiAP

單設備最大可連接
4096 個 APs

FortiSwitch

單設備最大可串接管控
256 台 Switches

單設備最大可提供 SSL VPN
連接 30,000 使用者

FortiGate

SD-WAN

透過應用導向並整合資安防護
達成最佳路徑選擇

FortiToken

結合手機載具，完備身份驗證

ZTNA

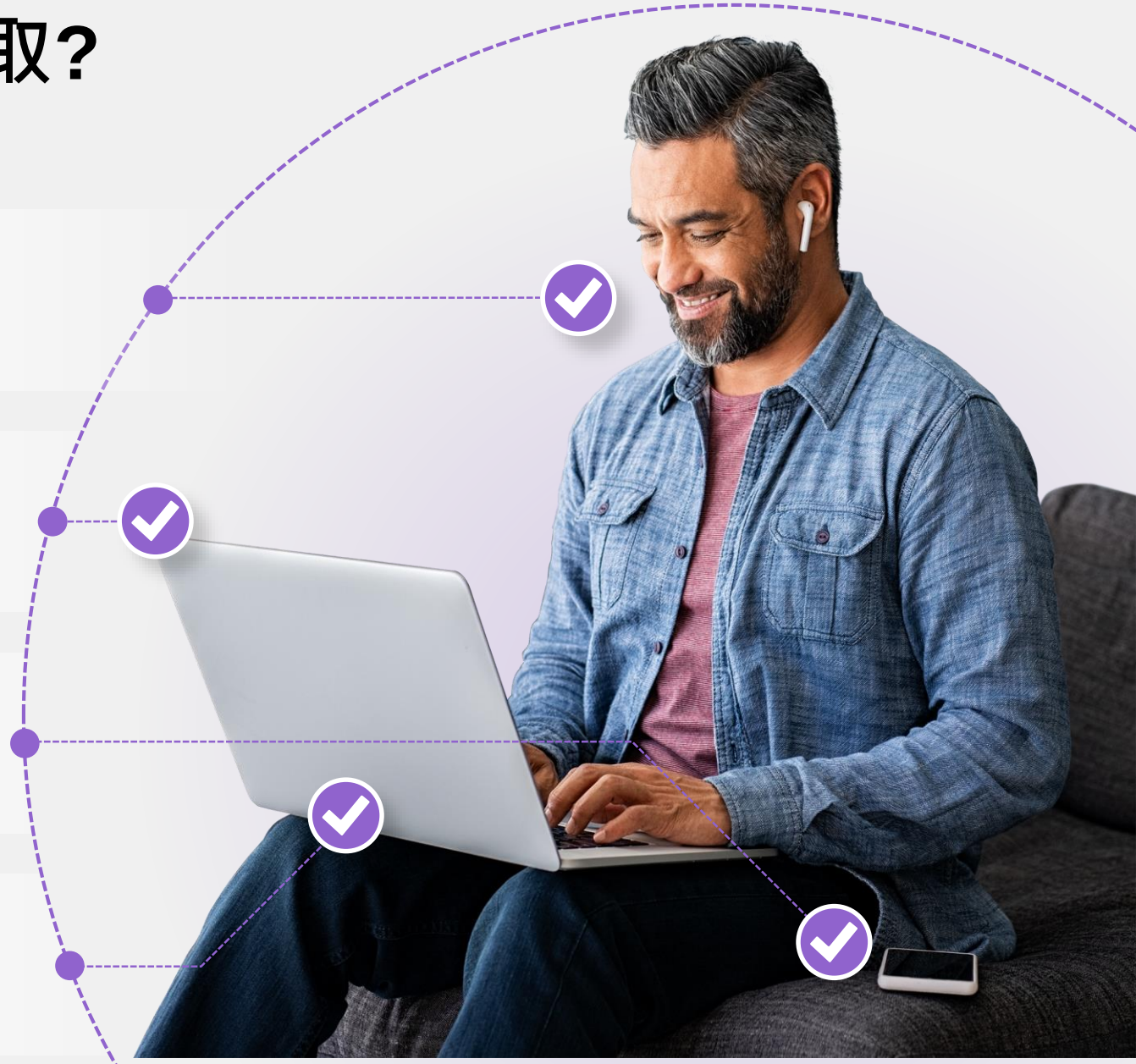
持續性的檢測從用戶身份辨識
到設備安全

© Fortinet Inc. All Rights Reserved.

什麼是 ZTNA 零信任存取?

永不信任，持續驗證和確認

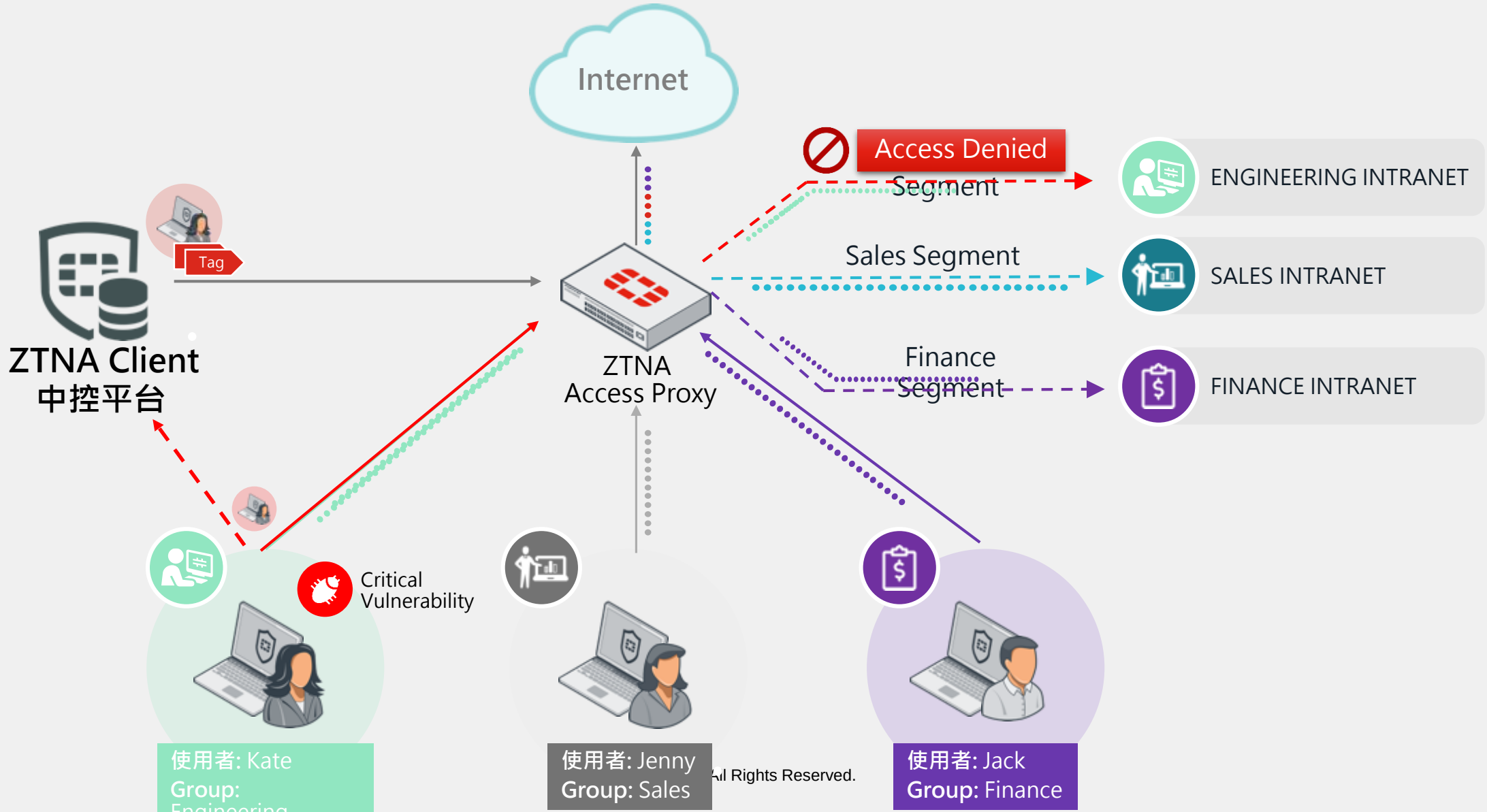
- 用戶身份驗證
- 設備終端驗證
- 終端健康狀態驗證
- 最小權限存取



© Fortinet Inc. All Rights Rese

ZTNA 應用場景

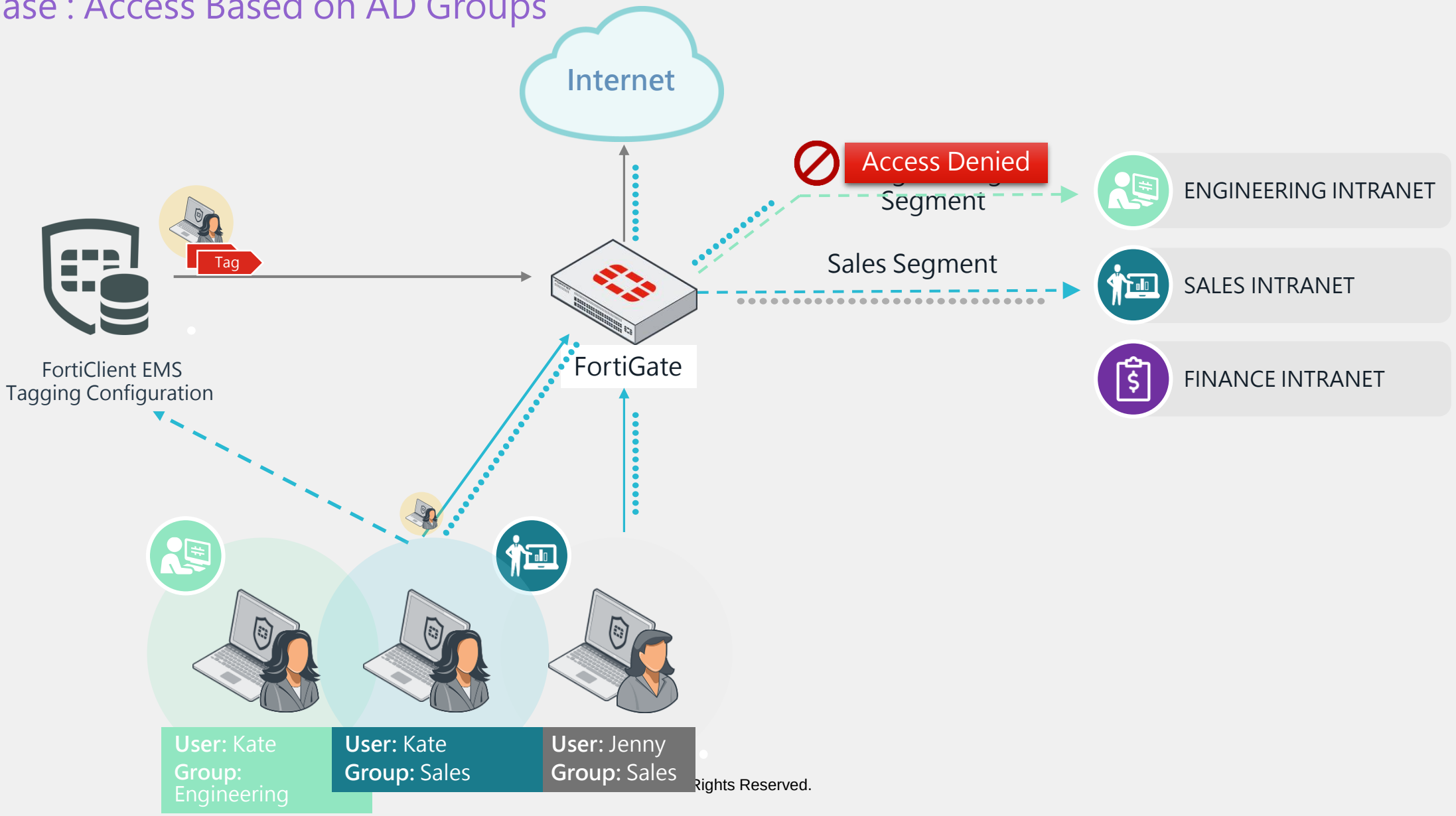
Use Case : Block Access for Security Risk Endpoints



All Rights Reserved.

ZTNA 應用場景

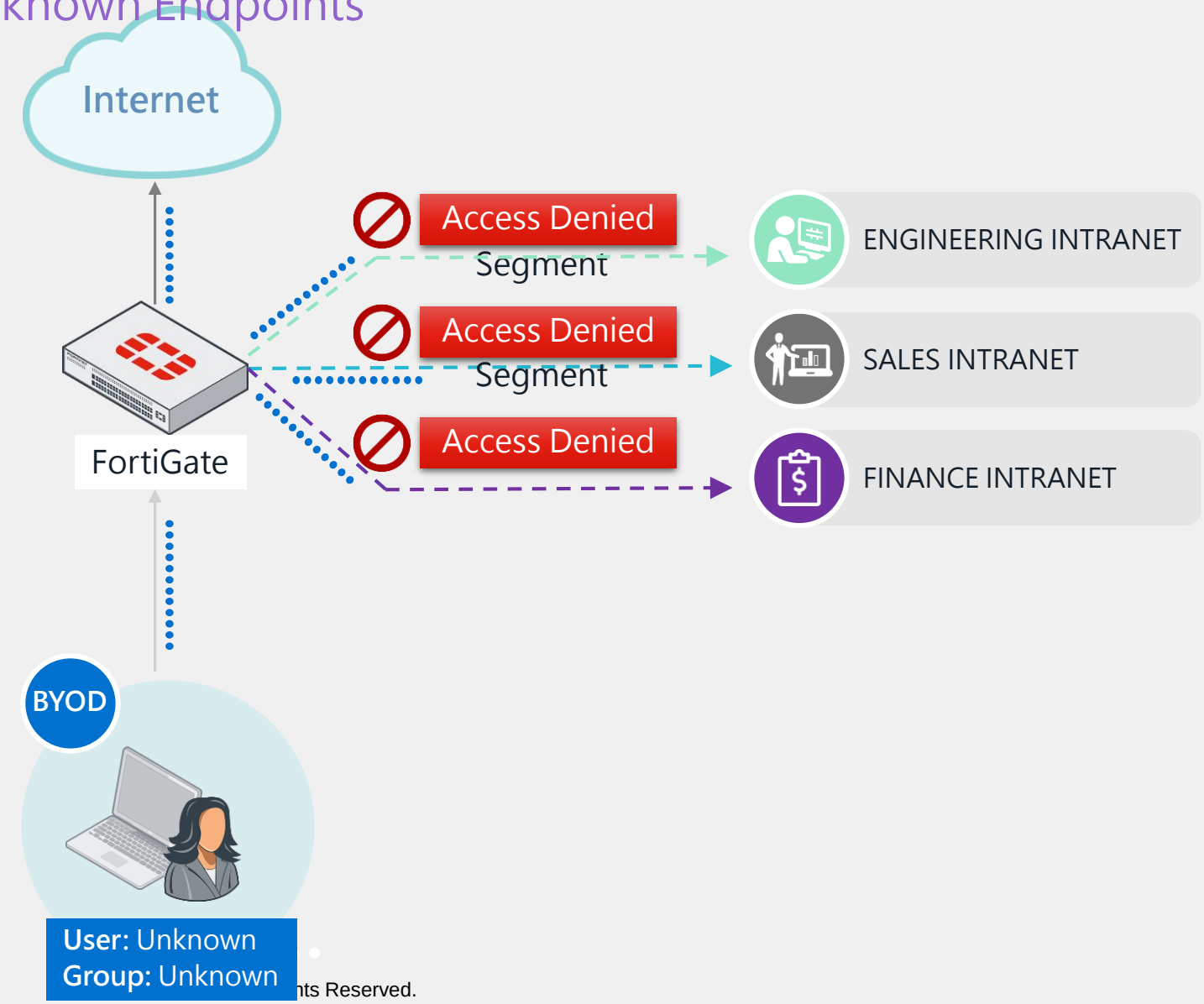
Use Case : Access Based on AD Groups



Rights Reserved.

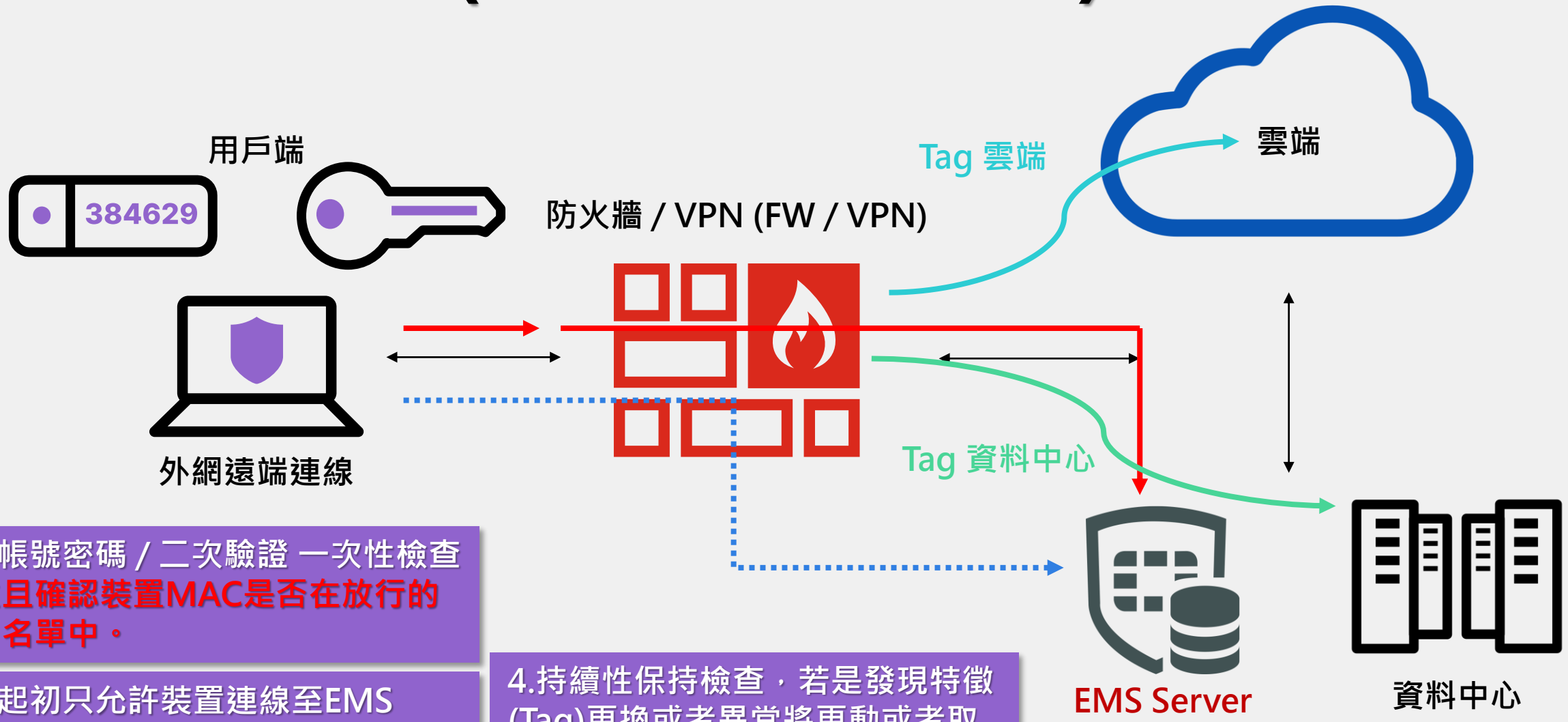
ZTNA 應用場景

Use Case : Restricted Access for Unknown Endpoints



nts Reserved.

初期導入ZTNA (SSLVPN + ZTNA)



1.帳號密碼 / 二次驗證 一次性檢查
並且確認裝置MAC是否在放行的白名單中。

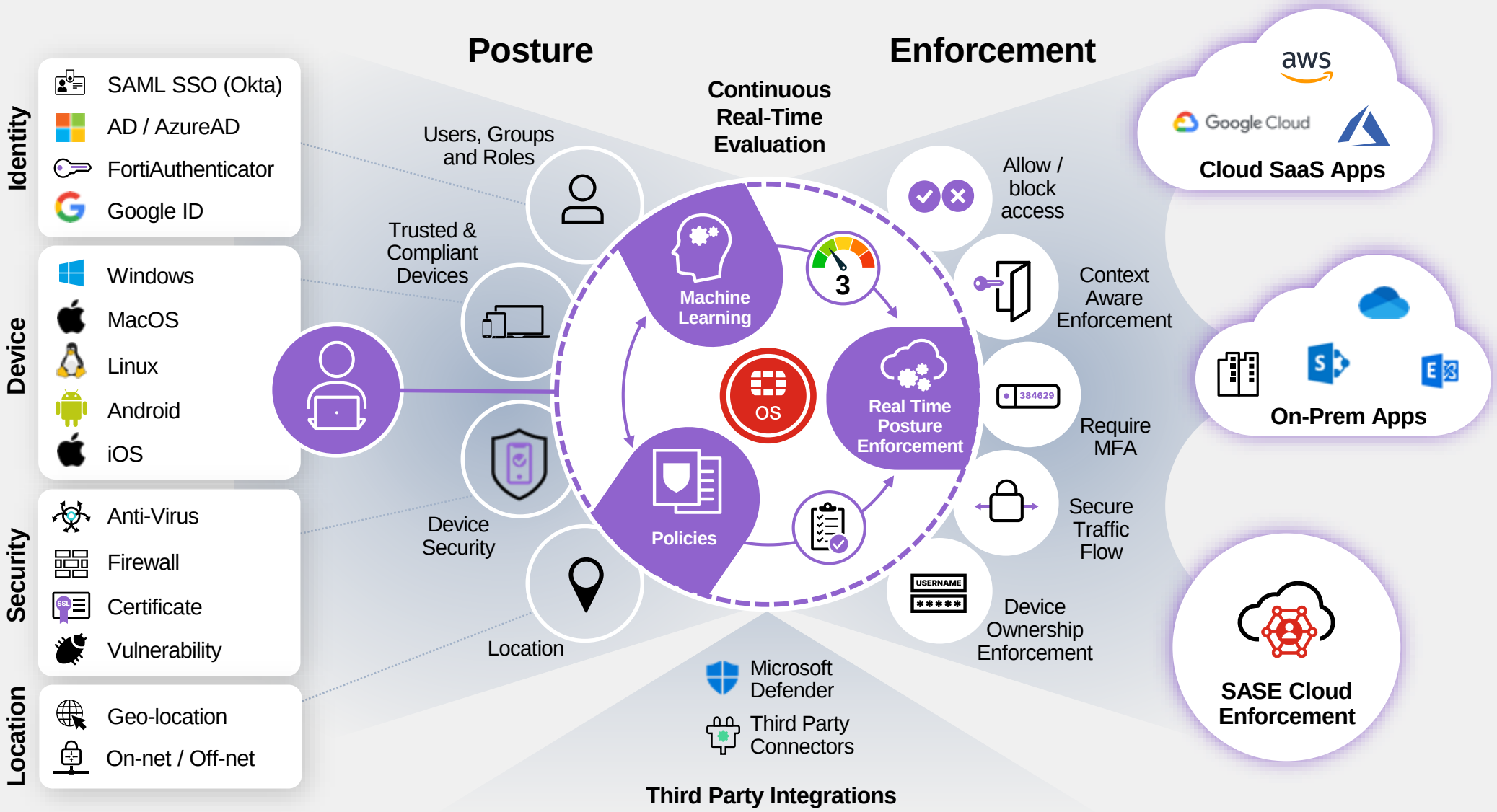
2.起初只允許裝置連線至EMS Server。

3.確認裝置特徵(tag)是否能夠存取資料中心設備 or 雲端設備。

4.持續性保持檢查，若是發現特徵(Tag)更換或者異常將更動或者取消存取權限。

© Fortinet Inc. All Rights Reserved.

Zero Trust 概觀總結



© Fortinet Inc. All Rights Reserved.

Fortinet 新世代 – 資安鐵三角

FortiAP

單設備最大可連接
4096 個 APs

FortiSwitch

單設備最大可串接管控
256 台 Switches

單設備最大可提供 SSL VPN
連接 30,000 使用者

FortiGate

SD-WAN

透過應用導向並整合資安防護
達成最佳路徑選擇

FortiToken

結合手機載具，完備身份驗證

ZTNA

持續性的檢測從用戶身份辨識
到設備安全

© Fortinet Inc. All Rights Reserved.