

The Fortinet logo, featuring the word "FORTINET" in a bold, sans-serif font. The letter "O" is stylized with a red and white grid pattern.

2025 Fortinet 資安嘉年華
Resilience Powered by AI and Cybersecurity

安全不分散： 混合時代的資安網路新革命

Lucas Yu 余昇瀚
Fortinet 技術顧問

整個高雄 都是 BLACKPINK 專屬色



市政府



捷運



公車

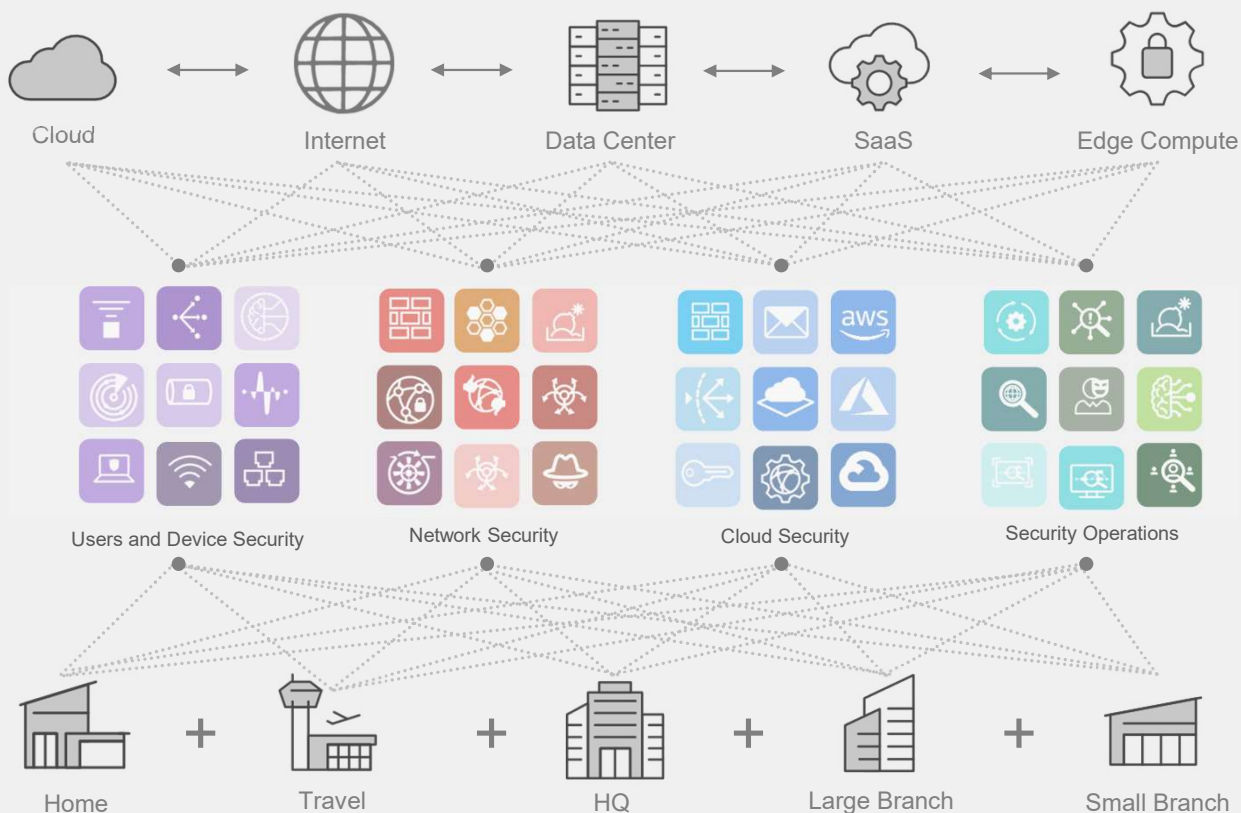


火車



步行

分散的服務、複雜的設備 = 難以管理的環境



混合式環境的核心痛點

環境分散，安全政策難以一致

雲、地政策與工具難以統一，導致政策落差與增加管理負擔。

連通性不佳，體驗不一致

架構太分散、設定太複雜，使用者與營運都跟著受影響。

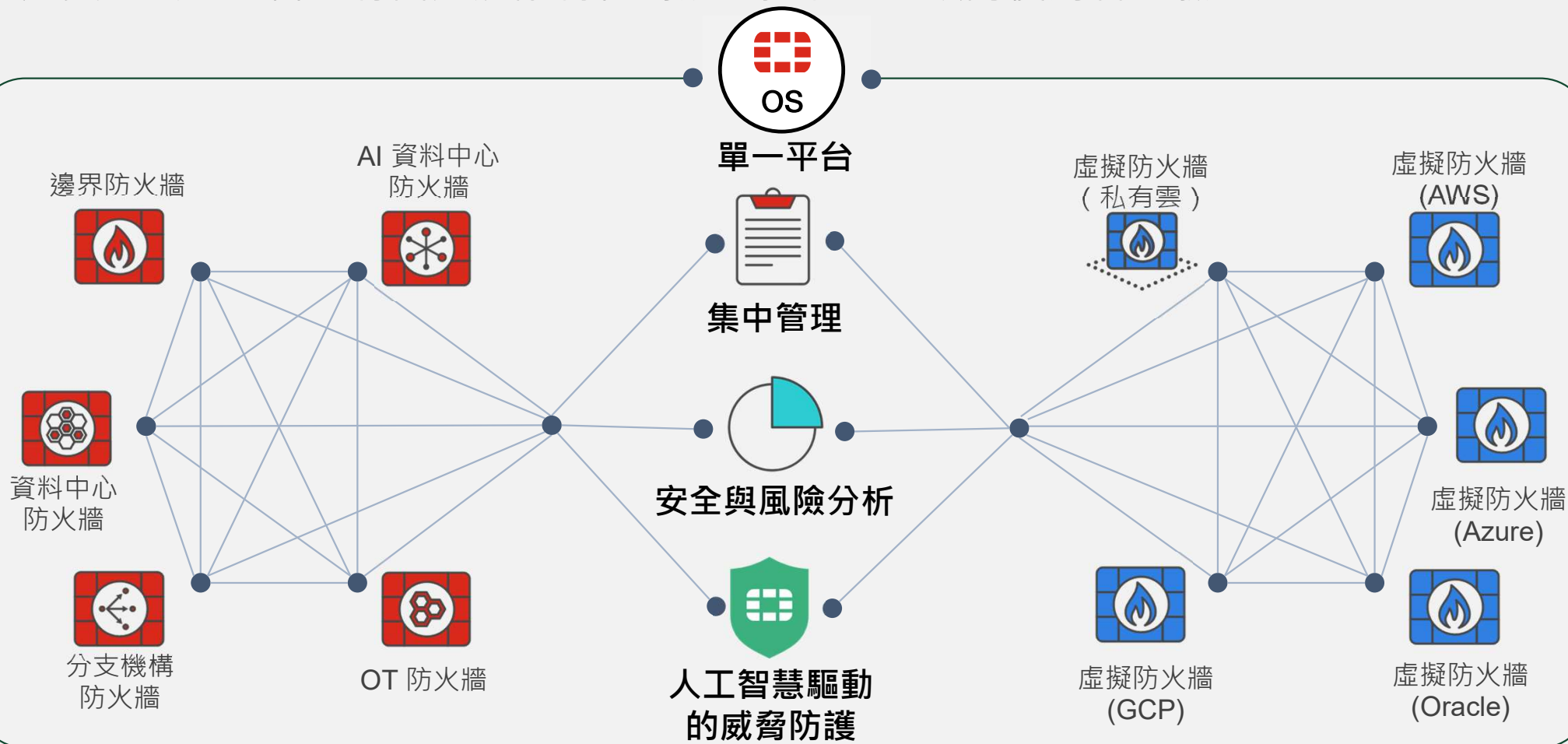
可視性破碎，威脅不易被看見

多套系統與不同平台讓事件資訊分散，降低偵測速度，也放大威脅風險。



適用於現代分散式網路的 Fortinet 混合式網狀防火牆

虛實、雲地整合，將營運混亂轉化為統一控制、一致的使用者經驗



Fortinet 專利 ASIC – 滿足 AI 資料中心需求



安全處理器

(security processor) 整合了網路和內容處理，提供快速的應用程式識別、智能導流



網路處理器

(network processors) 為網路提供無與倫比的效能，奠定超大規模防火牆的基石

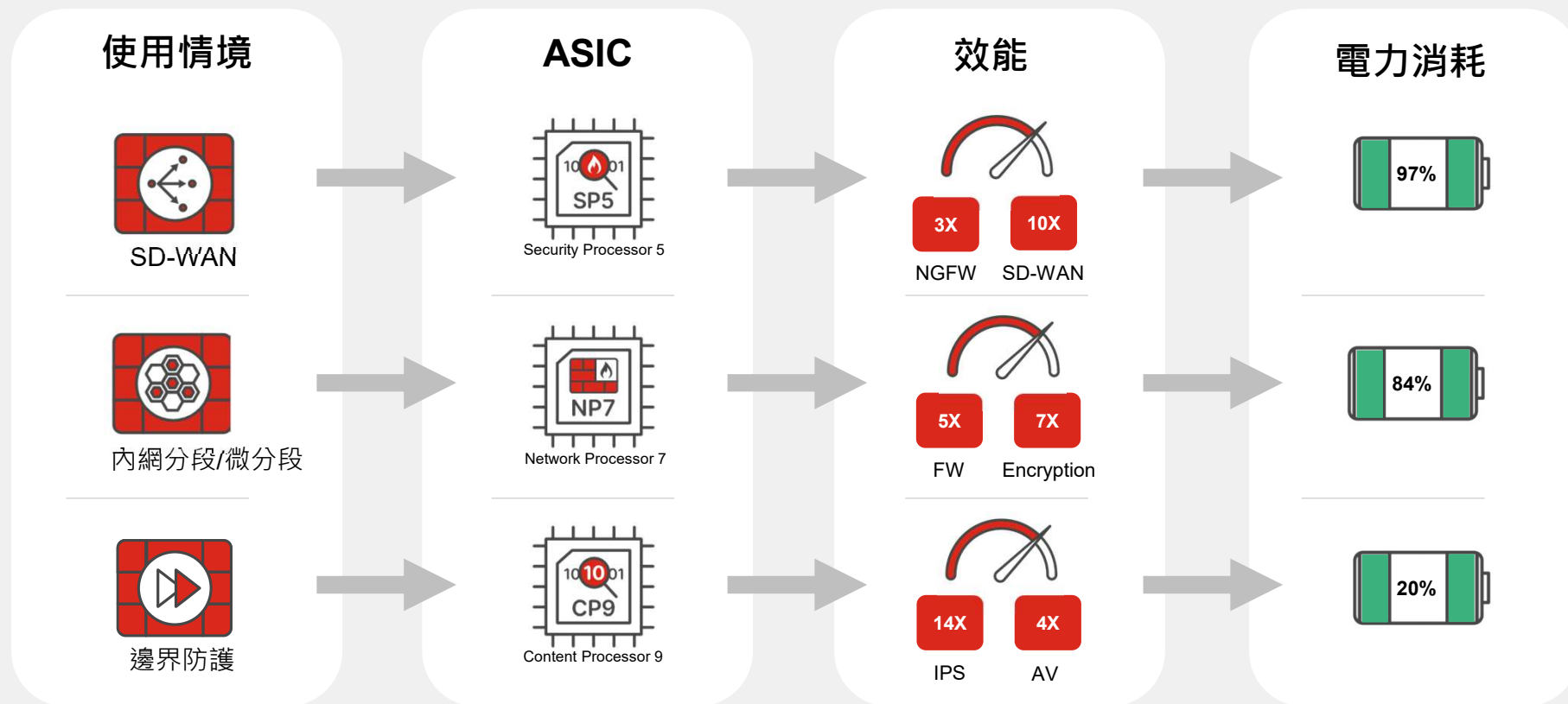


內容處理器

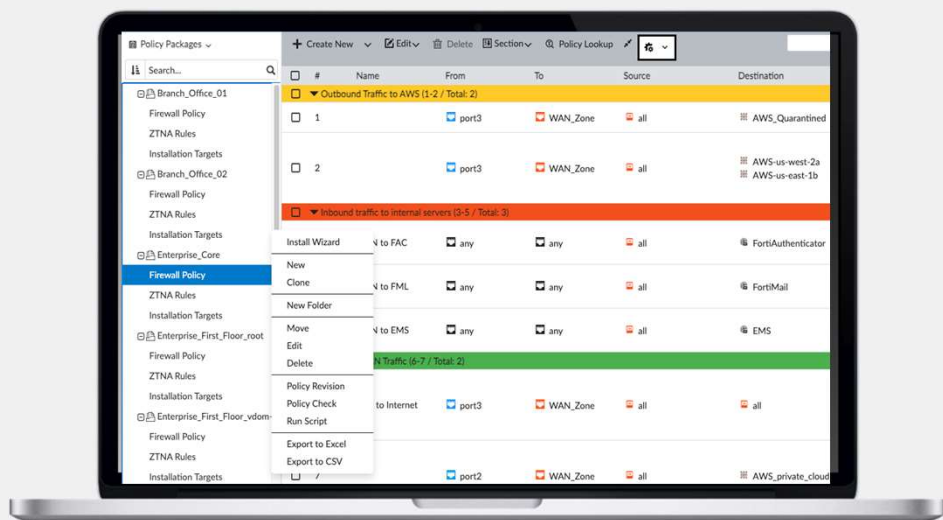
(content processor) 可以加速惡意流量辨識並增進內容檢查，以強化安全功能



效能來自 Fortinet 持續研發的專用安全晶片

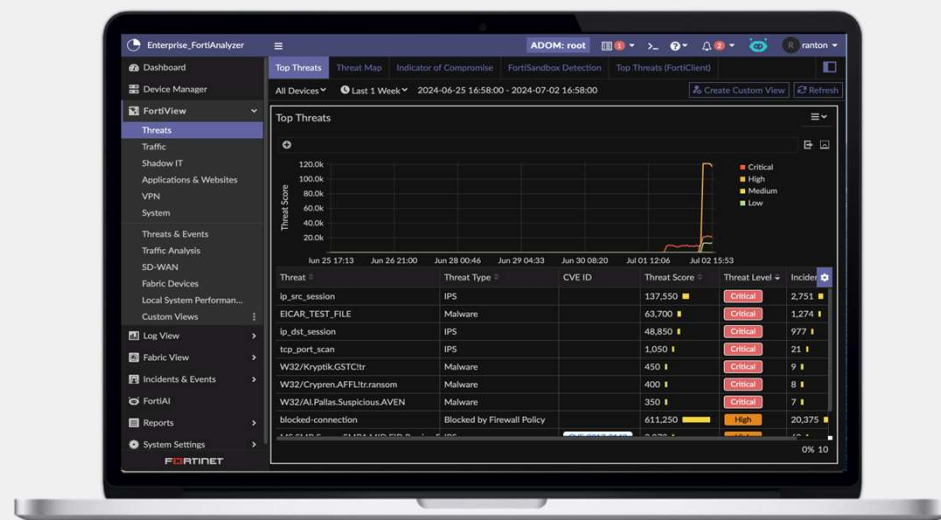


每台強大防火牆背後，都有強大的管理與分析



防火牆管理

集中化、規模化的管理所有設備，讓所有設備的變更、佈署更快速、更一致、更安全。



安全維運分析

集中日誌、事件關聯與自動化分析，讓威脅更快被看見、問題更快被處理。



AI 智能防護 讓防禦更聰明!



FortiGuard AI 驅動的安全服務的廣度和規模

偵測範圍廣

來自數百萬個 Fortinet 端點
網路和應用程式的遙測數據

6M

Firewalls

300M

Emails

150M

Endpoints

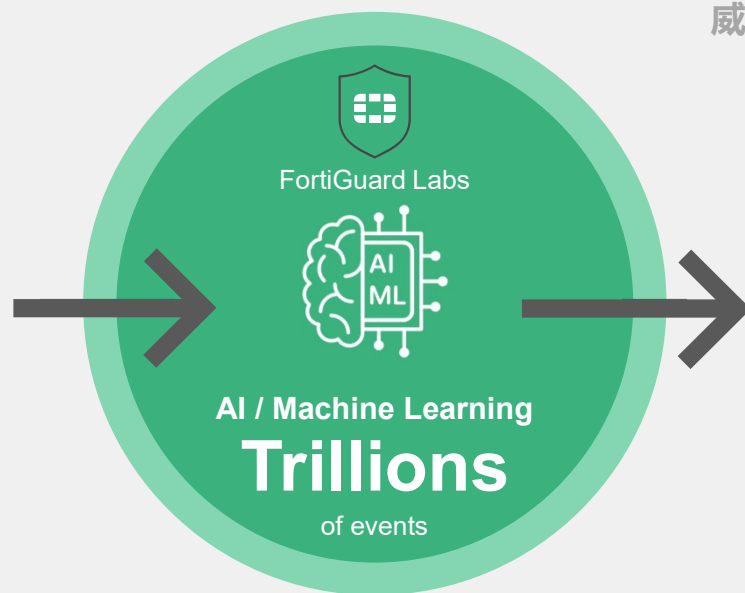
40M

Sandbox Files

未知狀態



主動偵測 & 快速反應

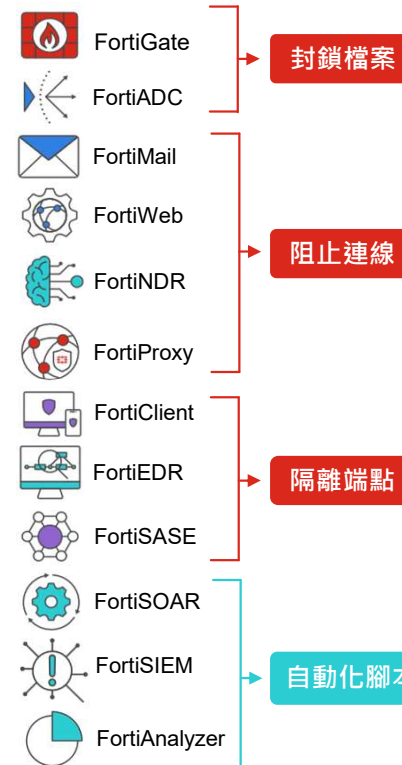


威脅情資



全面的防護

橫跨 Fortinet 安全織網



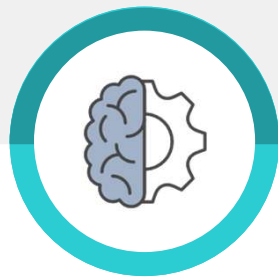
AI 智能防護

FortiGuard – AI 驅動的安全服務



AI / ML IPS 智能引擎

利用 AI /ML 增強
威脅偵測與阻擋
(如 Cobalt Strike)



Gen AI 應用程式控管

全方位辨識 Gen AI
應用程式，方便管控



URL 過濾檢測

有效防禦網路釣魚
(Web Phishing)



Inline 惡意程式 防禦

防禦規避型惡意軟體
(Evasive Malware)



AI 智能防護

FortiGuard – AI / ML IPS 智能引擎

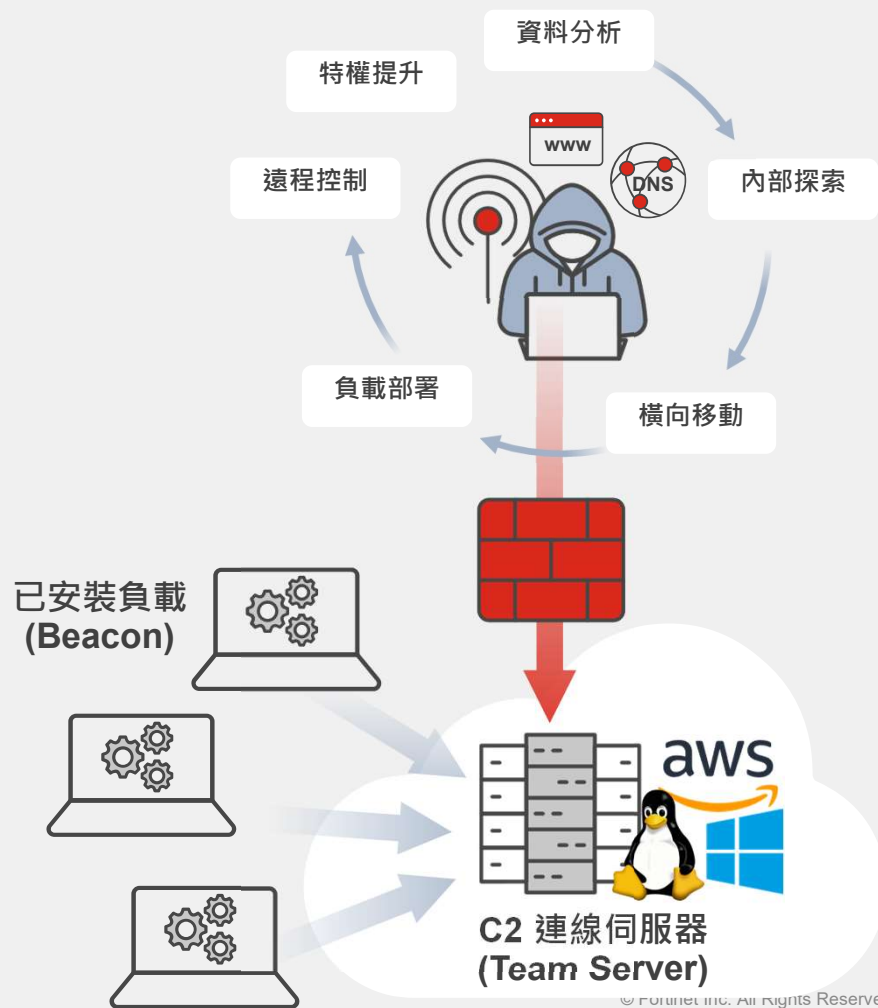
- **Cobalt Strike 是滲透測試和攻擊方模擬套件**

專為大規模長時間和漏洞利用而設計，可執行命令和控制 (C2) 通訊。高度可客製化，常被駭客濫用成為入侵攻擊工具。

- **FortiGuard – IPS 特徵碼資料庫可偵測 Cobalt Strike 惡意負載 (Beacon)**

- **FortiGuard – AI / ML IPS 智能引擎**

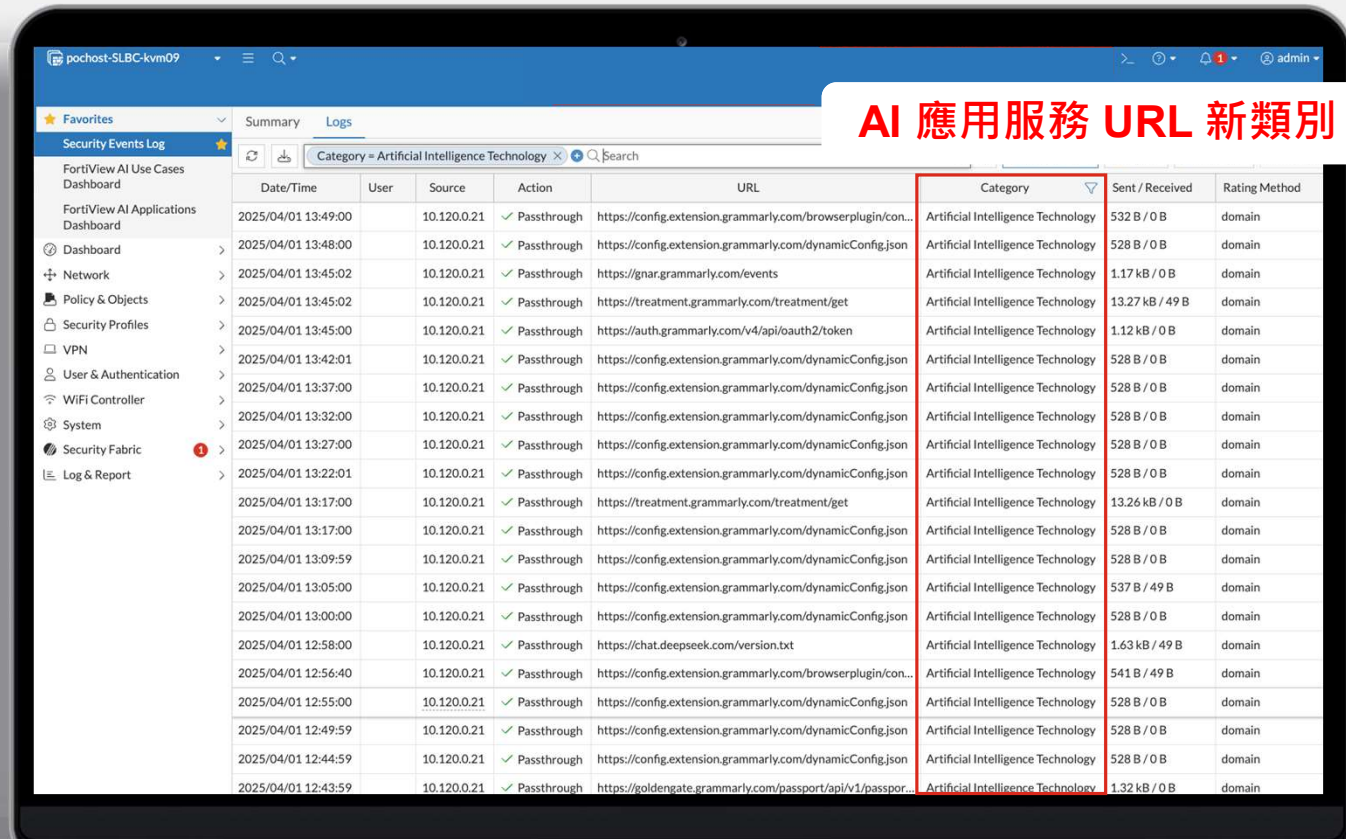
利用 C2 流量 (如 HTTP(S) / DNS / SMB / TCP...) 訓練 ML 模型，讓隨機 C2 流量的捕獲率大幅提升。



AI 智能防護

FortiGuard – URL 過濾檢測

- FortiGuard URL 過濾功能，已經對超過 6,000+ 種 URL 進行分類
- 自 7.4.2 版本起，為 GenAI 增加了新類別以利管理



The screenshot displays the FortiGuard Security Events Log interface. The log is filtered by the category 'Artificial Intelligence Technology'. The table below shows the details of the events, including Date/Time, User, Source, Action, URL, Category, Sent / Received, and Rating Method.

Date/Time	User	Source	Action	URL	Category	Sent / Received	Rating Method
2025/04/01 13:49:00		10.120.0.21	✓ Passthrough	https://config.extension.grammarly.com/browserplugin/con...	Artificial Intelligence Technology	532 B / 0 B	domain
2025/04/01 13:48:00		10.120.0.21	✓ Passthrough	https://config.extension.grammarly.com/dynamicConfig.json	Artificial Intelligence Technology	528 B / 0 B	domain
2025/04/01 13:45:02		10.120.0.21	✓ Passthrough	https://gnar.grammarly.com/events	Artificial Intelligence Technology	1.17 kB / 0 B	domain
2025/04/01 13:45:02		10.120.0.21	✓ Passthrough	https://treatment.grammarly.com/treatment/get	Artificial Intelligence Technology	13.27 kB / 49 B	domain
2025/04/01 13:45:00		10.120.0.21	✓ Passthrough	https://auth.grammarly.com/v4/api/oauth2/token	Artificial Intelligence Technology	1.12 kB / 0 B	domain
2025/04/01 13:42:01		10.120.0.21	✓ Passthrough	https://config.extension.grammarly.com/dynamicConfig.json	Artificial Intelligence Technology	528 B / 0 B	domain
2025/04/01 13:37:00		10.120.0.21	✓ Passthrough	https://config.extension.grammarly.com/dynamicConfig.json	Artificial Intelligence Technology	528 B / 0 B	domain
2025/04/01 13:32:00		10.120.0.21	✓ Passthrough	https://config.extension.grammarly.com/dynamicConfig.json	Artificial Intelligence Technology	528 B / 0 B	domain
2025/04/01 13:27:00		10.120.0.21	✓ Passthrough	https://config.extension.grammarly.com/dynamicConfig.json	Artificial Intelligence Technology	528 B / 0 B	domain
2025/04/01 13:22:01		10.120.0.21	✓ Passthrough	https://config.extension.grammarly.com/dynamicConfig.json	Artificial Intelligence Technology	528 B / 0 B	domain
2025/04/01 13:17:00		10.120.0.21	✓ Passthrough	https://treatment.grammarly.com/treatment/get	Artificial Intelligence Technology	13.26 kB / 0 B	domain
2025/04/01 13:17:00		10.120.0.21	✓ Passthrough	https://config.extension.grammarly.com/dynamicConfig.json	Artificial Intelligence Technology	528 B / 0 B	domain
2025/04/01 13:09:59		10.120.0.21	✓ Passthrough	https://config.extension.grammarly.com/dynamicConfig.json	Artificial Intelligence Technology	528 B / 0 B	domain
2025/04/01 13:05:00		10.120.0.21	✓ Passthrough	https://config.extension.grammarly.com/dynamicConfig.json	Artificial Intelligence Technology	537 B / 49 B	domain
2025/04/01 13:00:00		10.120.0.21	✓ Passthrough	https://config.extension.grammarly.com/dynamicConfig.json	Artificial Intelligence Technology	528 B / 0 B	domain
2025/04/01 12:58:00		10.120.0.21	✓ Passthrough	https://chat.deepseek.com/version.txt	Artificial Intelligence Technology	1.63 kB / 49 B	domain
2025/04/01 12:56:40		10.120.0.21	✓ Passthrough	https://config.extension.grammarly.com/browserplugin/con...	Artificial Intelligence Technology	541 B / 49 B	domain
2025/04/01 12:55:00		10.120.0.21	✓ Passthrough	https://config.extension.grammarly.com/dynamicConfig.json	Artificial Intelligence Technology	528 B / 0 B	domain
2025/04/01 12:49:59		10.120.0.21	✓ Passthrough	https://config.extension.grammarly.com/dynamicConfig.json	Artificial Intelligence Technology	528 B / 0 B	domain
2025/04/01 12:44:59		10.120.0.21	✓ Passthrough	https://config.extension.grammarly.com/dynamicConfig.json	Artificial Intelligence Technology	528 B / 0 B	domain
2025/04/01 12:43:59		10.120.0.21	✓ Passthrough	https://goldengate.grammarly.com/passport/api/v1/passpor...	Artificial Intelligence Technology	1.32 kB / 0 B	domain

AI 應用服務 URL 新類別

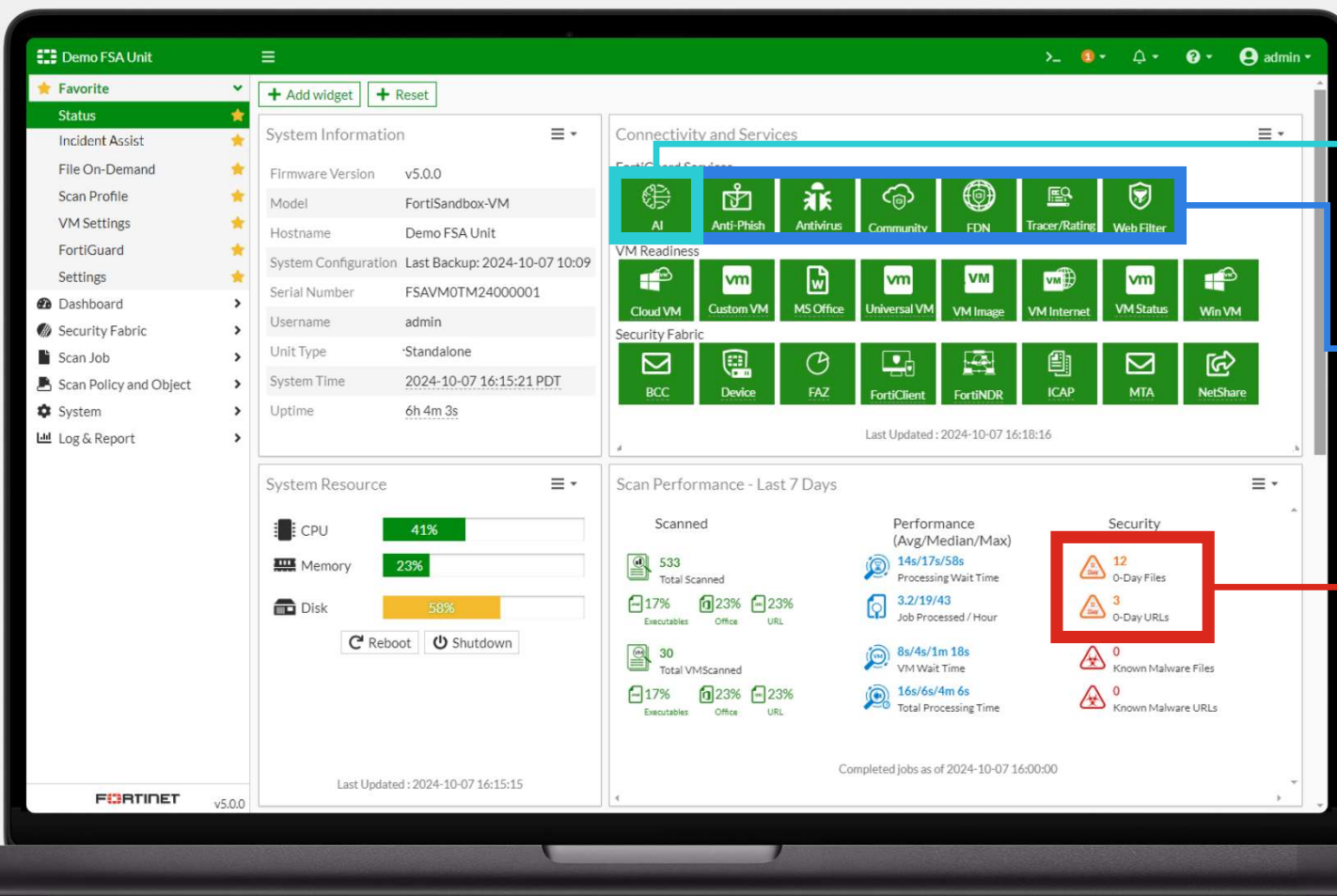


AI 智能防護

FortiGuard – Inline 惡意程式防禦



FortiSandbox
智能沙箱服務



持續更新的進階
AI 智能引擎

進階的 AI 智能
威脅偵測服務

0-Day 零日威脅偵測

A man with glasses is sitting at a desk in a server room, looking at several computer monitors. The monitors display network diagrams with nodes and connections. The background shows server racks with cables and lights. The text "AI 智能管理 讓維運更簡單!" is overlaid on the image in a semi-transparent box.

**AI 智能管理
讓維運更簡單!**

AI 智能管理

FortiAI on FortiManager – 簡化複雜設定

FortiAI 可以幫忙的

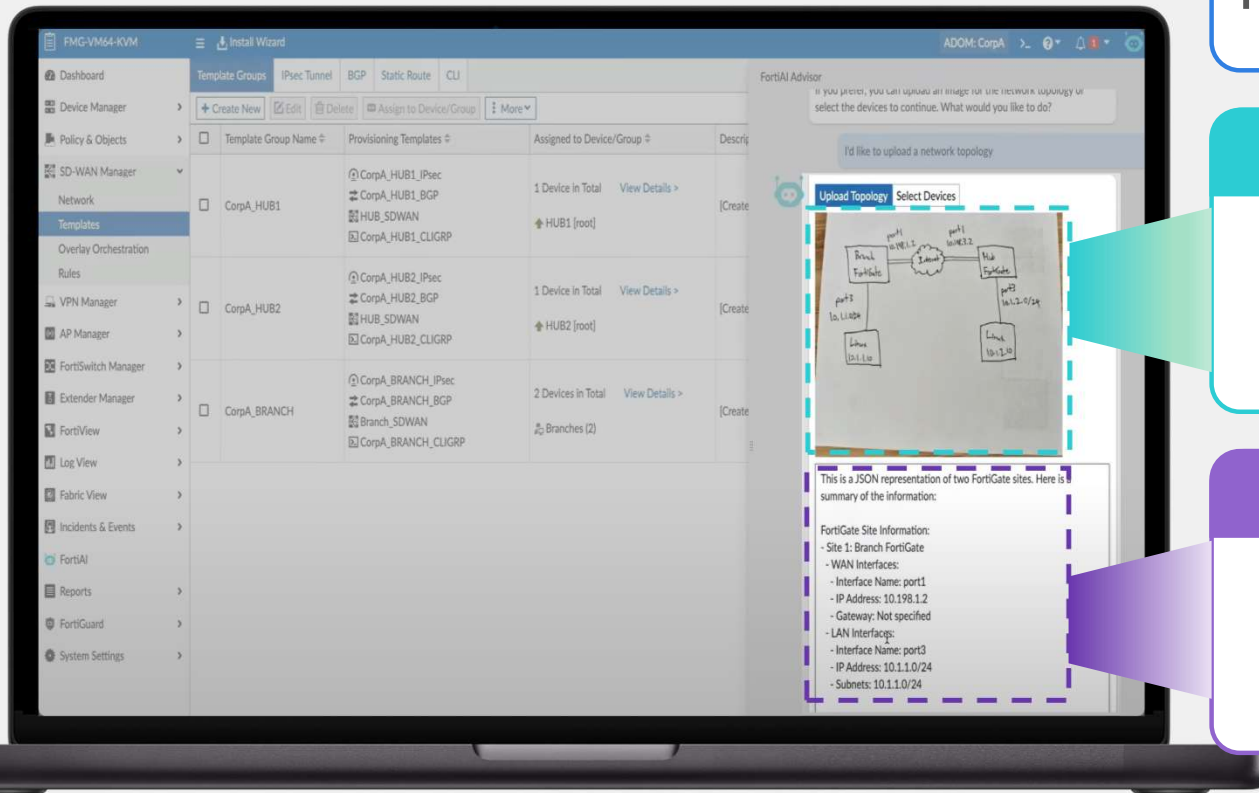
只要你會畫圖！
FortiAI 就能幫你做設定！

FortiAI 看到的

看到的
手繪 VPN 架構圖

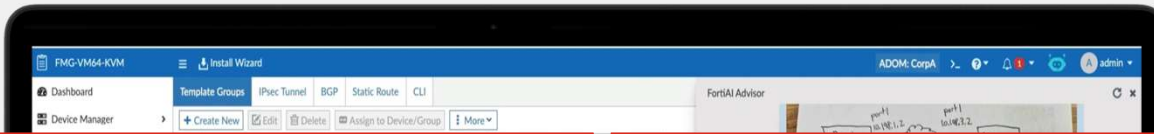
FortiAI 理解的

VPN 網路架構
並請求確認



AI 智能管理

FortiAI on FortiManager – 簡化複雜設定



```
Br-1_VPN_SCRIPT

config firewall address
  edit "to_HUB-1_local"
    set allow-routing enable
    set subnet 20.1.1.1/24
  next
  edit "to_HUB-1_remote"
    set allow-routing enable
    set subnet 20.1.2.1/24
  next
end

config vpn ipsec phase1-interface
  edit "to_HUB-1"
    set interface port4
    set peertype any
    set net-device disable
    set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes
    set comments "VPN: to_HUB-1 [Generated by FortiAI]"
    set remote-gw 14.1.1.4
    set psksecret <PLACEHOLDER_FOR_YOUR_PRESHARED_KEY>
  next
end
```

```
HUB-1_VPN_SCRIPT

config firewall address
  edit "to_Br-1_local"
    set allow-routing enable
    set subnet 20.1.2.1/24
  next
  edit "to_Br-1_remote"
    set allow-routing enable
    set subnet 20.1.1.1/24
  next
end

config vpn ipsec phase1-interface
  edit "to_Br-1"
    set interface port4
    set peertype any
    set net-device disable
    set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes
    set comments "VPN: to_Br-1 [Generated by FortiAI]"
    set remote-gw 14.1.1.2
    set psksecret <PLACEHOLDER_FOR_YOUR_PRESHARED_KEY>
  next
end
```

FortiAI 生成的
生成可部署的
VPN 組態設定檔

```
Branch FortiGate_VPN_SCRIPT

config firewall address
  edit "Branch FortiGate_to Hub FortiGate_to local"
    set allow-routing enable
    set subnet 10.1.1.0/24
  next

Hub FortiGate_VPN_SCRIPT

config firewall address
  edit "Hub FortiGate_to Branch FortiGate_to local"
    set allow-routing enable
    set subnet 10.1.2.0/24
  next
```



AI 智能管理

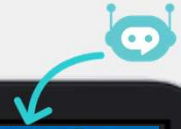
FortiAI on FortiAnalyzer - 透過自然語言互動應答，即時解析資安事件



The screenshot displays the FortiAI interface on a laptop screen. The main dashboard shows a 'Last 4 Hours' view from 2024-11-07 13:36:00 to 17:36:00. It features three summary cards: '1 High Severity Incidents', '0 Outbreak Alerts', and '1 Compromised Host'. Below these is an 'Events Map' showing incident severity levels (critical, high, medium, low) funneling into a central node for 'client001' with an 'endpoint 18 95%' and a 'Denial of Service (D)' incident category. A chat window on the right is titled 'FortiAI' and shows a user query: 'Do we have an incident for client001'. The chat response is 'Getting incidents...' followed by a large blue box containing the text 'FortiAI 找了找...'. At the bottom of the chat window, the user's question is repeated: '我們是否有針對端點 client001 的資安事件?'. The interface also includes a sidebar with navigation options like 'Dashboards', 'Status', 'Email Metrics', 'SOC Dashboard', 'Device Manager', 'FortiView', 'Log View', 'Fabric View', 'Incidents & Events', 'FortiAI', 'Reports', and 'System Settings'. The Fortinet logo is visible in the bottom left corner of the interface.

AI 智能管理

FortiAI on FortiAnalyzer - 透過自然語言互動應答，即時解析資安事件



The screenshot displays the FortiAI interface on a tablet. The left sidebar shows navigation options like Dashboards, Status, Email Metrics, SOC Dashboard, Device Manager, FortiView, Log View, Fabric View, Incidents & Events, FortiAI, Reports, and System Settings. The main content area is split into two panels. The left panel, titled 'Incident Details for client001', shows incident information for ID IN00000004, including Name, Endpoint, Category, Severity, Status, Description, and Reporter. A red box highlights the Name, Endpoint, and Category fields. The right panel, also titled 'Incident Details for client001', shows the same information and includes a chat input field with the text 'Do we have an incident for client001'. A blue arrow points from the chatbot icon to the chat input field.

FortiAI 檢視 client001 相關事件後：

- 發現 client001 有存取外部惡意網站 (Malicious Website) 的資安事件

AI 智能管理

FortiAI on FortiAnalyzer - 透過自然語言互動應答，即時解析資安事件



The screenshot shows the FortiAnalyzer SOC Dashboard with the FortiAI chat interface open. The dashboard displays metrics for High Severity Incidents (1), Outbreak Alerts (0), and Compromised Hosts (1). The Events Map shows a flow from critical, high, medium, and low severity incidents to a client001 endpoint with 18 incidents (95% Denial of Service (DoS)). The Incident Details for client001 show an Incident ID of IN00000004, Name: FortiAI-Demo: Web request to Malicious Websites detected, Endpoint: client001, Category: Denial of Service (DoS), Severity: High, Status: Draft, Description: (Not provided), and Reporter: Auto-Raised. The chat interface shows a user query: "Can you show me the web filter logs for srcip 192.168.0.2 for today?" and a response: "Do we have an incident for client001".

1 High Severity Incidents | 0 Outbreak Alerts | 1 Compromised Host

Events Map

critical

high

medium

low

client001 endpoint 18 95%

Denial of Service (DoS) 1

Incident Category

Incident Details for client001

Incident ID: IN00000004

- Name: FortiAI-Demo: Web request to Malicious Websites detected
- Endpoint: client001
- Category: Denial of Service (DoS)
- Severity: High
- Status: Draft
- Description: (Not provided)
- Reporter: Auto-Raised

Do we have an incident for client001

Can you show me the web filter logs for srcip 192.168.0.2 for today?

What's new in FortiAnalyzer 7.6 | What can I do with FortiAI

Monthly token usage 0.0% | 0/1024

請幫我列出 192.168.0.2 (client001) 今天的 web filter 上網事件清單

AI 智能管理

FortiAI on FortiAnalyzer - 透過自然語言互動應答，即時解析資安事件



The screenshot displays the FortiAnalyzer interface. On the left, a sidebar contains navigation options like Dashboards, Device Manager, FortiView, Log View, and Reports. The main area shows a log table with columns for #, Date/Time, Device ID, User, Source, Destination IP, Service, and Host. A red box highlights the first four rows of the table, which all have a source IP of 192.168.0.2. On the right, a chat window titled 'FortiAI' shows a user query: 'Do we have an incident for client001'. The AI assistant responds with 'Incident Details for client001' and lists details such as Incident ID, Name, Endpoint, Category, Severity, Status, and Reporter. A follow-up query asks for web filter logs for the source IP 192.168.0.2, and the AI assistant confirms that the logs are displayed in the web filter log view section.

#	Date/Time	Device ID	User	Source	Destination IP	Service	Host
1	2024-11-07 1	FGVM01TM2400		192.168.0.2	104.18.29.80	HTTPS	coin
2	2024-11-07 1	FGVM01TM2400		192.168.0.2	104.18.28.80	HTTPS	coin
3	2024-11-07 1	FGVM01TM2400		192.168.0.2	208.94.116.246	HTTP	malv
4	2024-11-07 1	FGVM01TM2400		192.168.0.2	208.94.116.246	HTTP	malv

FortiAI 列出有關 **192.168.0.2 (client001)** 今天的 Web filter 事件清單，您可以在 Web filter event 部分查看日誌。
如果您需要任何進一步的分析或其他操作，請告訴我。

FortiAI 列出有關 **192.168.0.2 (client001)** 今天的 Web filter 事件清單，您可以在 Web filter event 部分查看日誌。
如果您需要任何進一步的分析或其他操作，請告訴我。

What's new in FortiAnalyzer 7.6 What can I do with FortiAI

Monthly token usage 0.0%

0/1024

AI 智能管理

FortiAI on FortiAnalyzer - 透過自然語言互動應答，產生報表

幫我產生一份Report，是過去7天所有來源ip的頻寬使用狀況，並用chart呈現

A

切換到Logview頁面，以便繪製來源IP的頻寬餅狀圖

A

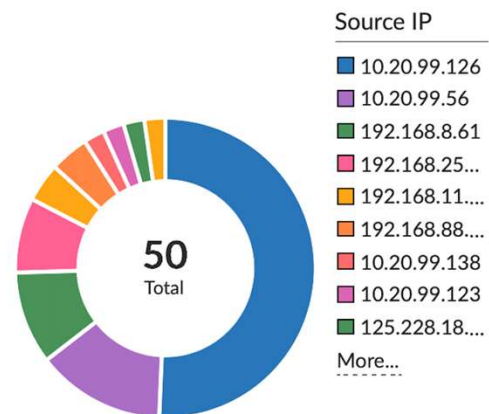


已切換到 Logview 的 Traffic 頁面並設定時間範圍為過去7天。

請問現在要以來源IP為分類繪製頻寬使用情況的餅狀圖嗎？

是

A



AI 智能管理

FortiAI on FortiAnalyzer - 透過自然語言互動應答，產生報表



儲存此圖表

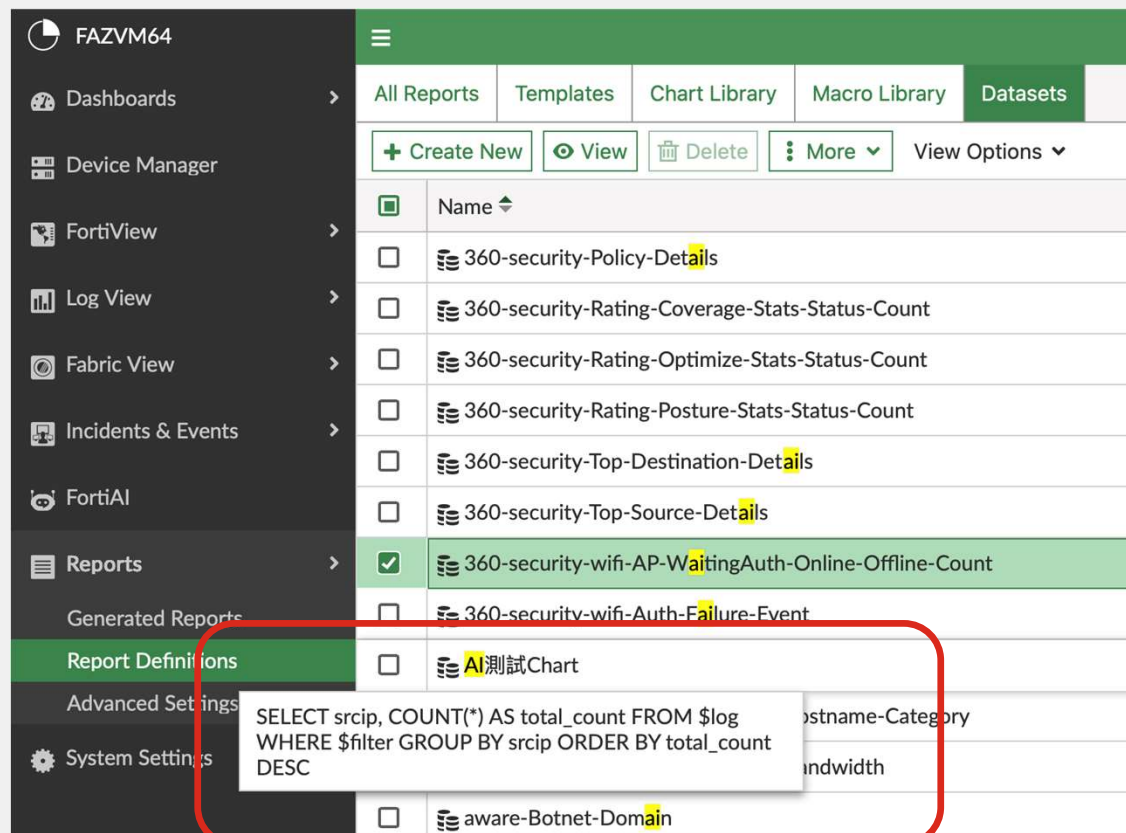
請問您想要此圖表以什麼名稱儲存？另外，您希望存為報告中的圖表還是單獨匯出圖片檔？

圖表

請提供您希望以什麼名稱，方便我幫您儲存。

測試Chart

已成功將圖表儲存。您現在需要進行下一步操作嗎？



FAZVM64

Dashboards > All Reports | Templates | Chart Library | Macro Library | Datasets

Device Manager > + Create New | View | Delete | More | View Options

FortiView >

Log View >

Fabric View >

Incidents & Events >

FortiAI >

Reports > 360-security-wifi-AP-WaitingAuth-Online-Offline-Count

Generated Reports > 360-security-wifi-Auth-Failure-Event

Report Definitions > AI測試Chart

Advanced Settings >

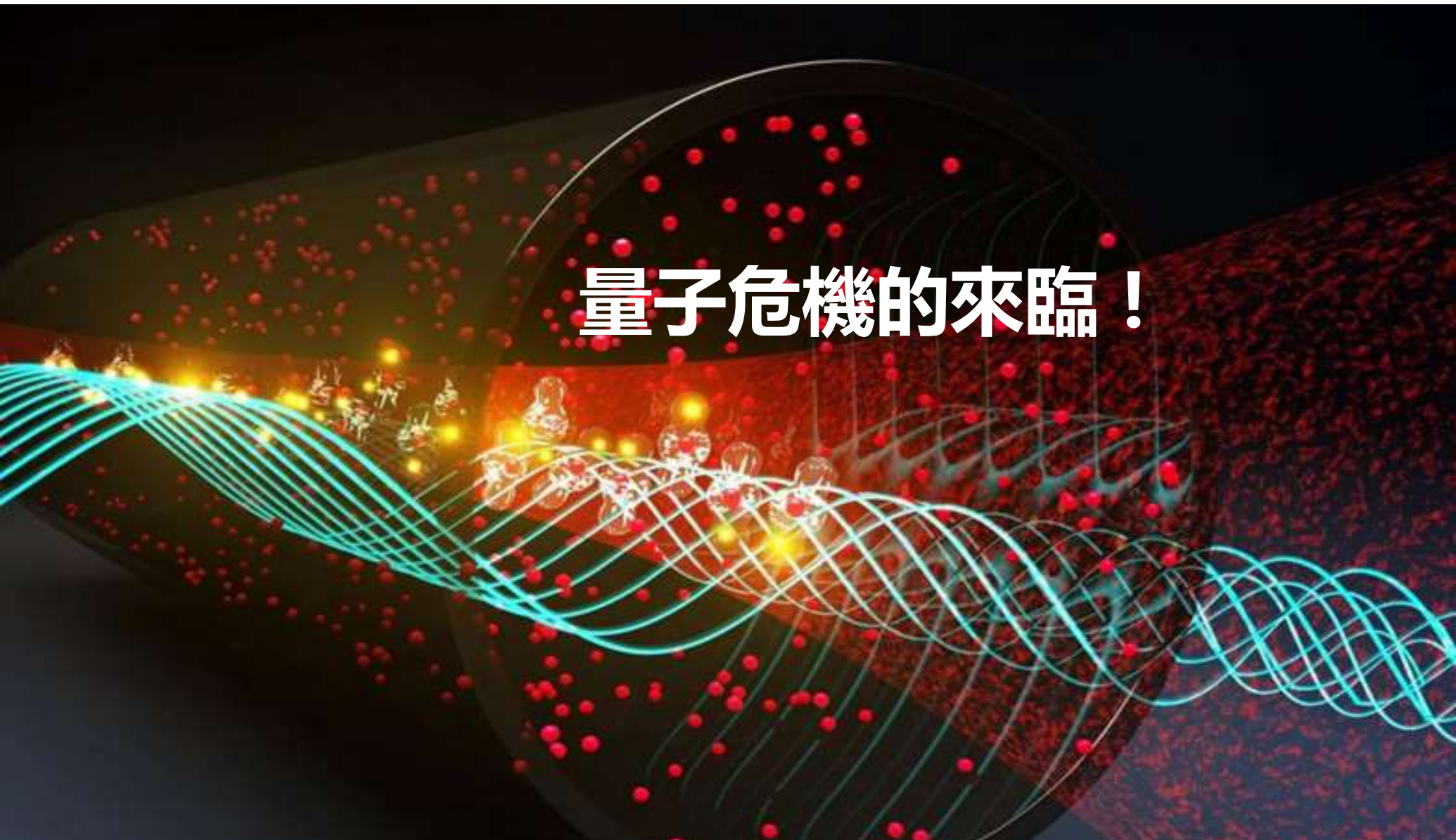
System Settings >

```
SELECT srcip, COUNT(*) AS total_count FROM $log WHERE $filter GROUP BY srcip ORDER BY total_count DESC
```

aware-Botnet-Domain



量子危機的來臨！



企業面臨量子威脅風險

加密被破解：

量子電腦能針對特定演算法快速破解，從而暴露企業系統的脆弱性。

資訊不安全：

一旦加密被破解，企業和個人持有的大量資訊能面臨被竊取的風險。

法規要求：

CNSA（Commercial National Security Algorithm Suite）2.0 要求自 2027 年起，所有新採購的國安系統必須支援 PQC。傳統非對稱密碼技術，如 RSA、ECDSA、EdDSA、ECC 等，2030 年棄用，於 2035 年禁用。

Fortinet 量子安全解決方案 – QKD



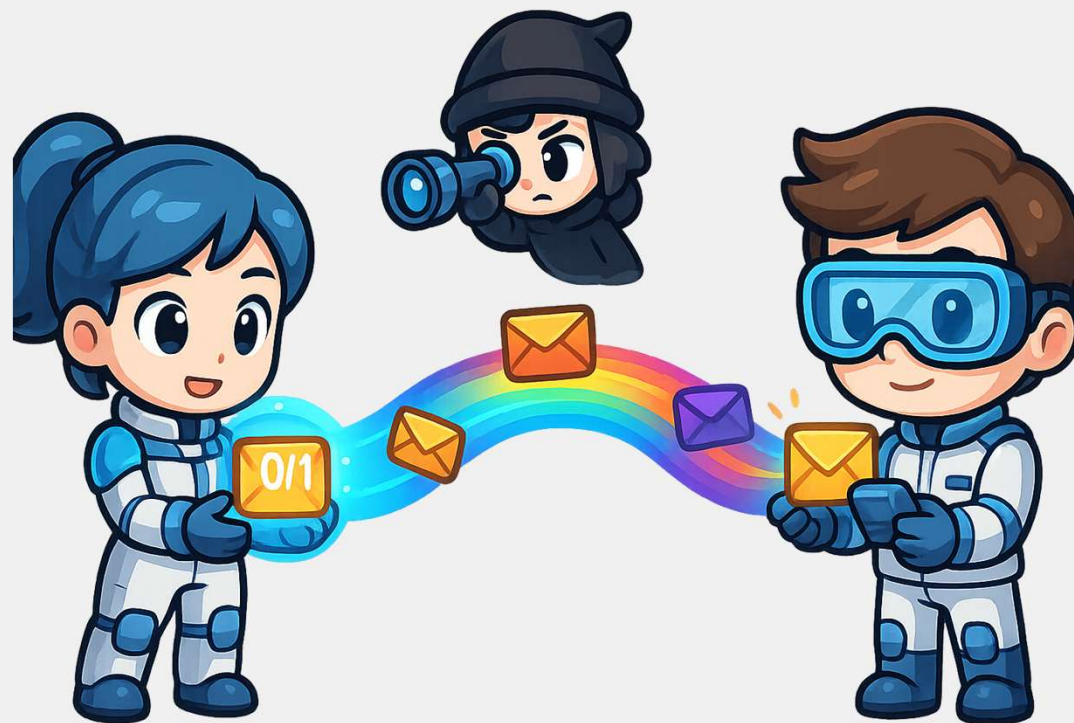
QKD

Quantum Key Distribution

量子金鑰分配

採用量子物理方式

確保安全



Fortinet 量子安全解決方案 – QKD



QKD

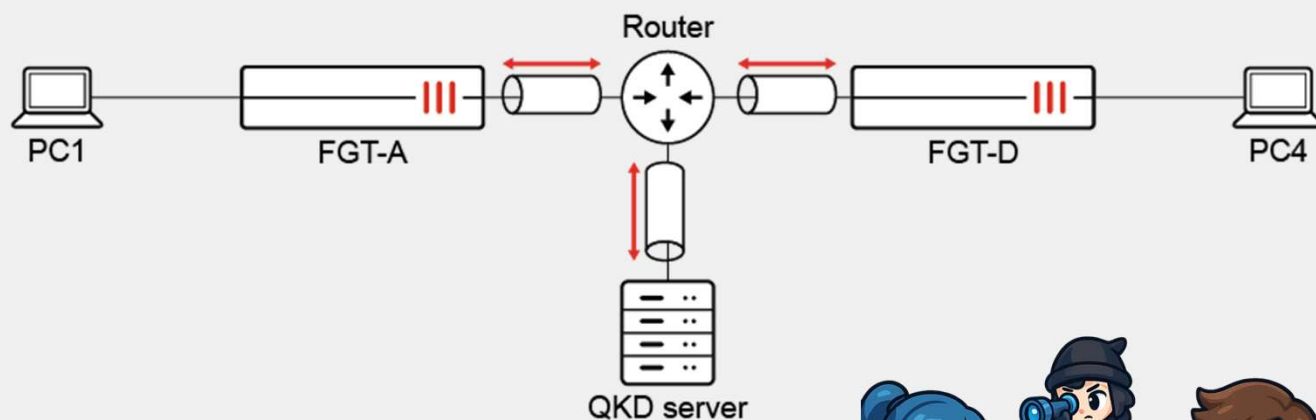
Quantum Key Distribution

量子金鑰分配

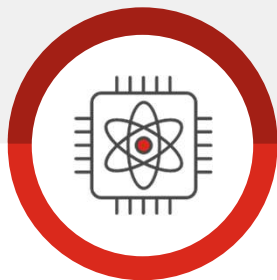
採用量子物理方式

確保安全

Quantum Key Distribution (May 2023)



Fortinet 量子安全解決方案 – PQC



PQC

Post-Quantum Cryptography

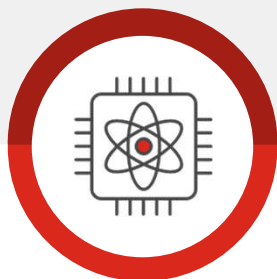
後量子加密

採用演算法

對抗量子電腦



Fortinet 量子安全解決方案 – PQC



PQC

Post-Quantum Cryptography

後量子加密

採用演算法

對抗量子電腦

Post-Quantum Cryptography (August 2024)



Quantum-resistant key exchange method

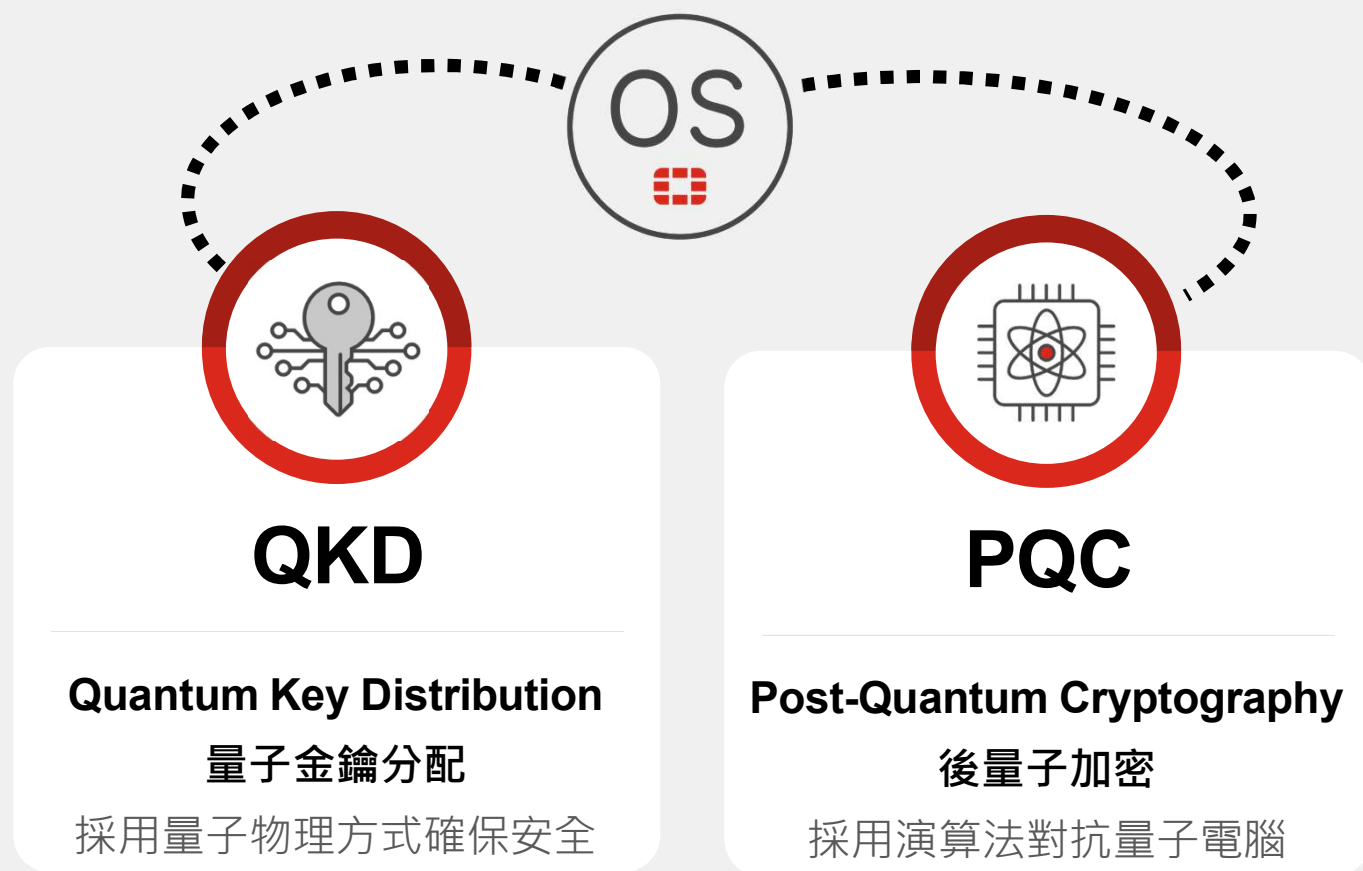
Post Quantum Cryptography Additional Key Exchanges

Transform type	KE groups
<input type="checkbox"/> ADDKE1	ML-KEM-768
<input type="checkbox"/> ADDKE2	HQC192



Fortinet 企業量子安全無縫接軌

- **量子金鑰分配 (QKD)** : 透過 QKD 供應商實現量子安全的金鑰交換機制。
- **後量子加密 (PQC)** : FortiOS 內建演算法包含 Crystals Kyber、ML-KEM、BIKE、HQC 和 Frodo 等。
- **混合模式** : 傳統公鑰與後量子加密並存，支援企業現有系統的相容性與量子遷移優勢。
- **演算法堆疊** : 結合多種加密演算法，以創造更有韌性的安全解決方案。



《混合式網狀防火牆》 魔力象限領導者



首屆評比，即獲得肯定！

單一管理平台

• 政策一致、全域可視

AI 驅動的威脅分
與回應

• 讓防禦更快、更聰明

彈性部署模式

• 靈活應變基礎架構變化

內建量子抗性加密

• 守護未來的資料安全



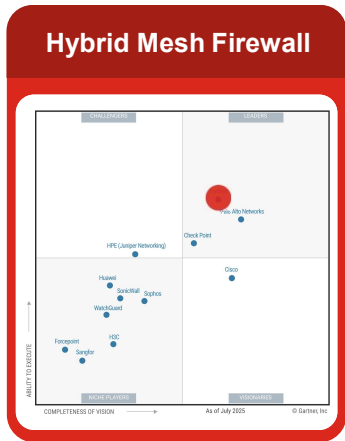
#1 最多第三方驗證

Fortinet 持續獲得 Gartner、IDC 和 Forrester 等主要行業分析公司超過 140 份研究報告的認可，並且在 10 個 Gartner 魔力象限中獲得認可。



- Hybrid Mesh Firewalls
- SASE Platform
- SD-WAN
- Security Service Edge
- Wired and WLAN
- SIEM
- Endpoint Protection Platforms
- Email Security Platforms
- Access Management
- Privileged Access Management

← FortiOS Operating System →



Gartner® Magic Quadrant™ for Hybrid Mesh Firewalls – Published 25 August 2025 – Rajpreet Kaur, Adam Hills, Charanpal Bhogal, Esraa ElTahawy, Feng Gao, Tiffany Taylor



Gartner® Magic Quadrant™ for SD- WAN – Published 30 September 2024 – Jonathan Forest, Karen Brown, Nauman Raja



Gartner® Magic Quadrant™ for Enterprise Wired and Wireless LAN Infrastructure – Published 25 June 2025 – Mike Leibovitz, Christian Canales, Nauman Raja, Tim Zimmerman



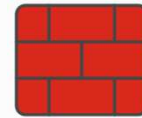
Gartner, Magic Quadrant™ for SASE Platforms – Published 9 July 2025 – Jonathan Forest, Neil MacDonald, Dale Koepfen



Gartner® Magic Quadrant™ for Security Service Edge – Published 20 May 2025 – Charlie Winckless, Thomas Lintemuth, Dale Koepfen, Charanpal Bhogal



FORTINET



全能防火牆



單一平台



AI 智能助理



集中管理



安全與風險分析



AI 威脅防護





FORTINET

2025 Fortinet 資安嘉年華
Resilience Powered by AI and Cybersecurity

