



# AI驅動的端點防護，密碼小偷哭哭了 ，迎接WiFi 7的到來！

Marty Chang

Fortinet 技術顧問

[mchang@fortinet.com](mailto:mchang@fortinet.com)



## 資安/網路 維運中心



FortiAnalyzer

Central Log & report



FortiNAC

IoT Access Control



FortiSandbox

File Analysis



FortiAI

Virtual Security Analyst™



FortiSIEM

SIEM / UEBA



FortiXDR

XDR



FortiManager

Central Device Mgmt.



FortiAuthenticator

User Access Mgmt.



FortiTester

Network Tester



FortiDeceptor

Honeypot



FortiSOAR

SOAR



FortiPAM

PAM



## 雲端服務 / 雲端託管

### Cloud mgmt.

FortiGate Cloud | FortiLAN Cloud | FortiExtender Cloud | FortiManager Cloud | FortiAnalyzer Cloud | FortiClient EMS Cloud | FortiToken Cloud | FortiSOAR Cloud

### Cloud services

FortiPresence | FortiMail Cloud | FortiPhish | FortiGSLB | FortiConverter | Fortinet SOCaaS | FortiSASE | FortiPenTest | FortiWeb Cloud | FortiSandbox Cloud | FortiVoice Cloud | FortiMonitor



## 終端行動用

戶

384629

FortiToken

2 Factor OTP Token



FortiClient / FortiEDR

VPN, ZTNA, EPP, and SASE Client



SaaS

FortiCASB

FortiCWP

Secure SD-WAN

IPsec / SSL VPN

SASE



FortiGate

Security Gateway

ZTNA



FortiDDoS

L7 D/DOS Mitigator



FortiADC

Load Balancer



FortiMail

Mail Sec. Gateway



FortiWeb

Web App. Firewall



FortiIsolator

Browser Isolation



FortiProxy

Secure Web Gateway



## 外點/分公司

司



FortiWiFi

Secure WiFi Access



FortiExtender

3G/4G/5G WAN



FortiSwitch

Switch



FortiAP

Wireless Access Point



FortiRecorder

Surveillance Manager



FortiVoice

IP PBX



FortiCamera



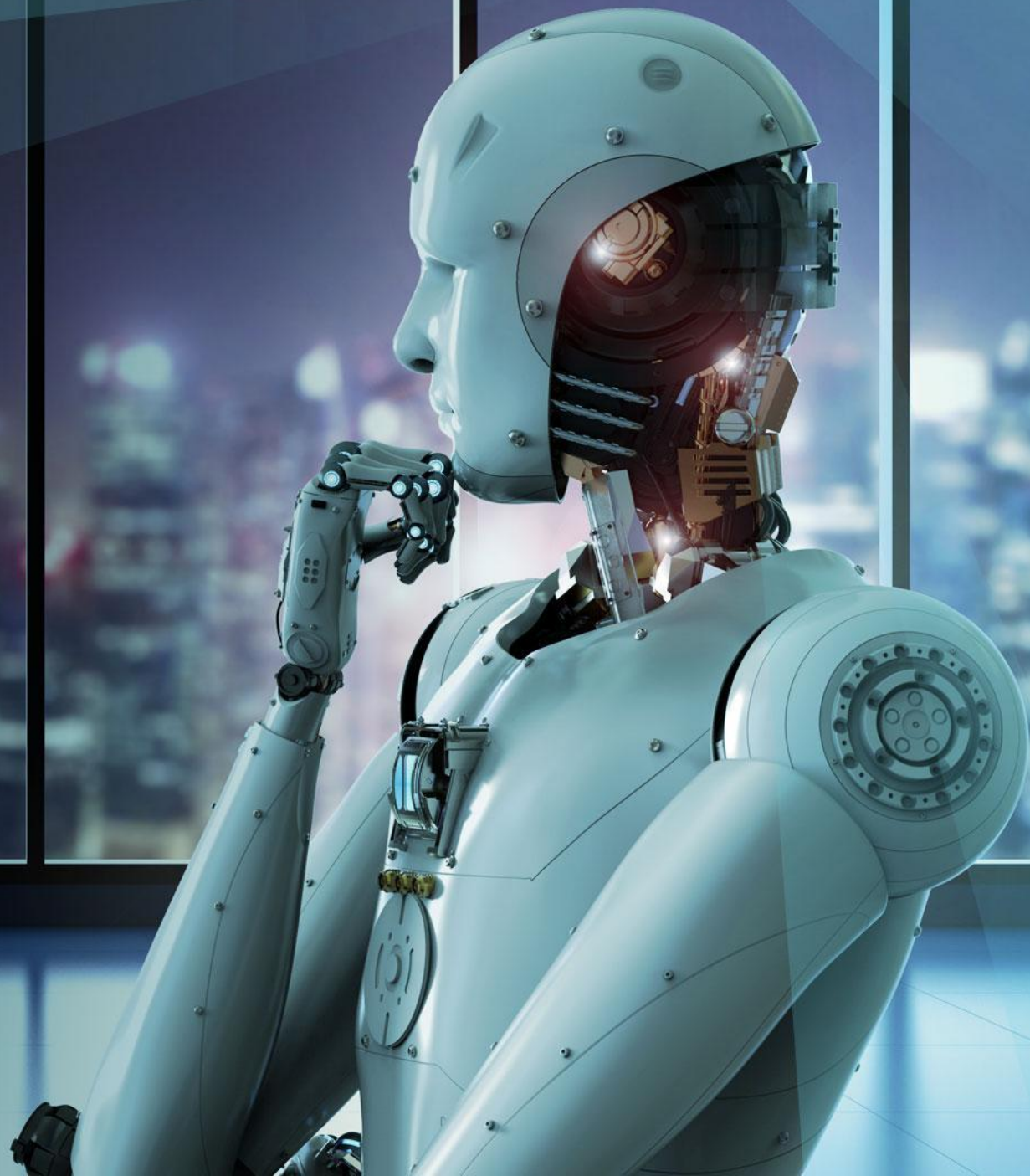
FortiFone

業界最完整且全面的資安佈局



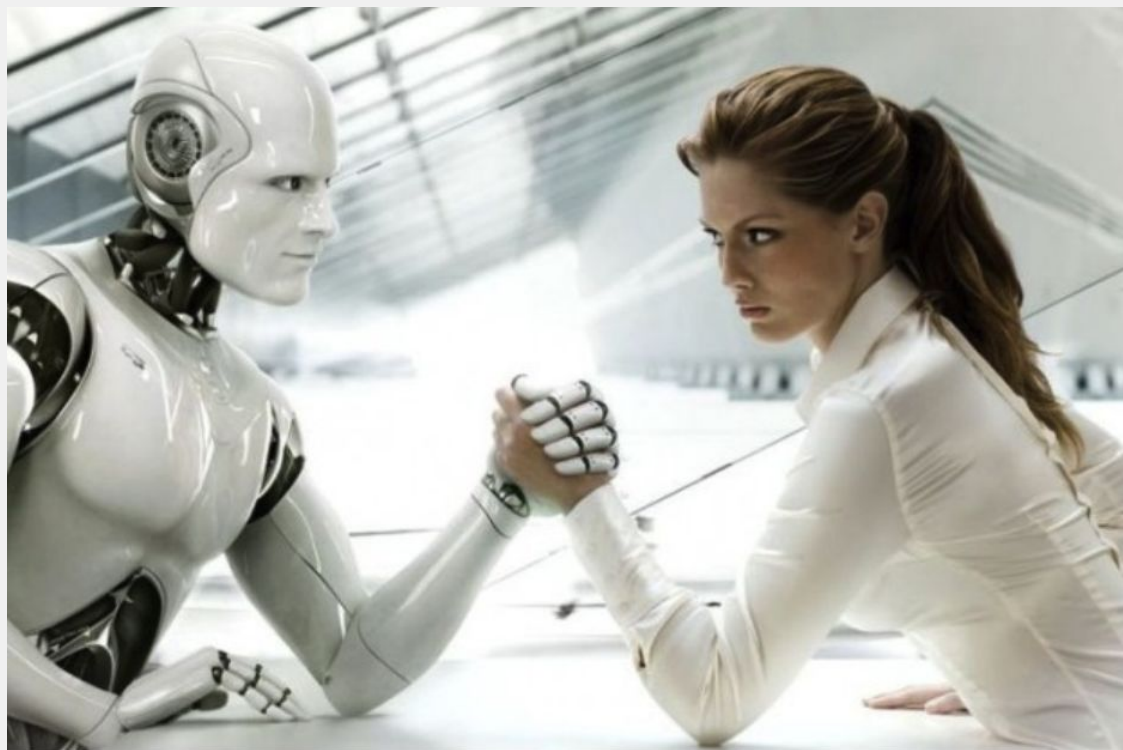
資料中心

# AI驅動的端點防護



# 別讓人力去對抗新型態資安威脅

資安威脅正 AI 武裝化，犯罪即服務（Crime-as-a-Service）讓攻擊更容易得逞



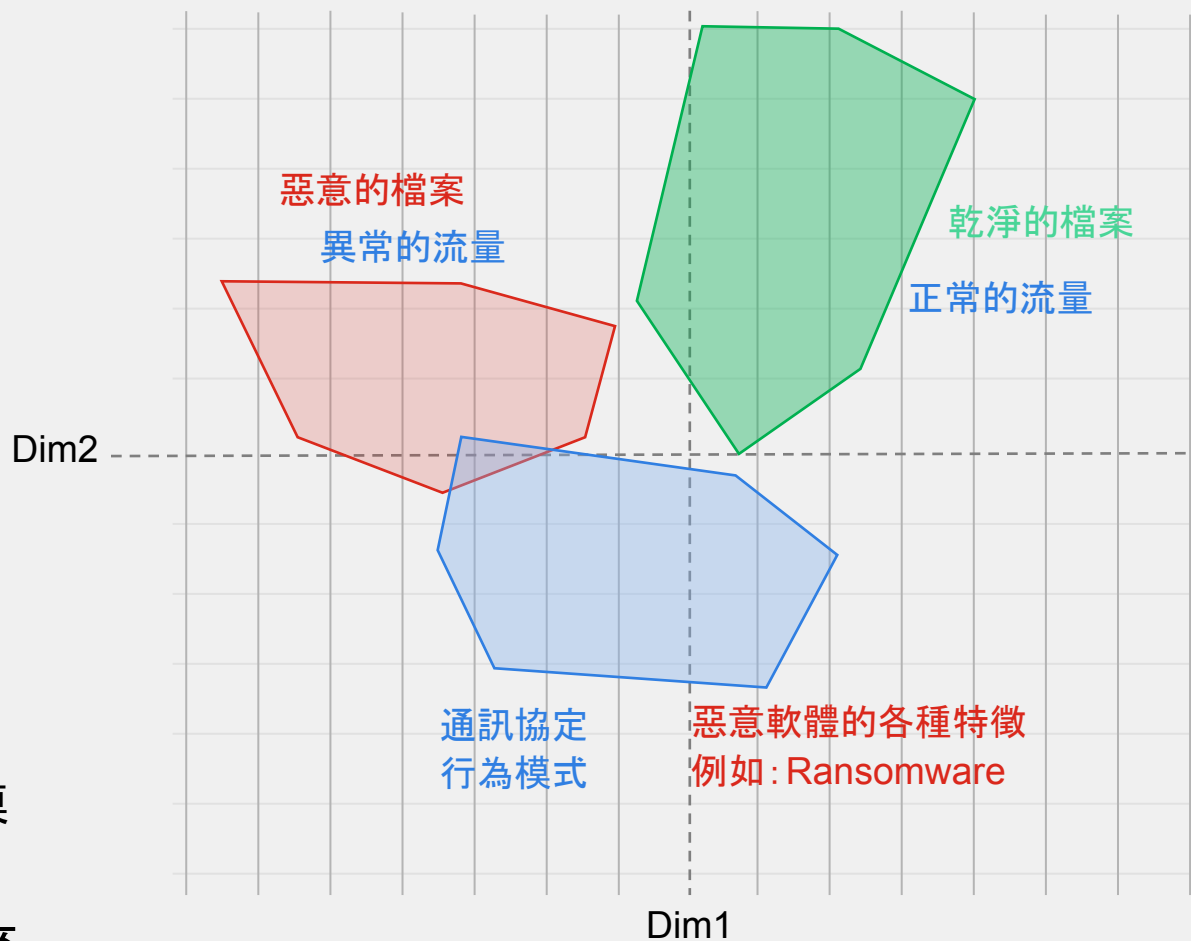
讓機器去處理適合機器處理的問題，將寶貴人力放在核心業務上  
透過 AI-驅動的安全營運防護，填補零信任框架下的資安人才需求





# AI / 機器學習：可以用來做些甚麼？

- 運用 AI / 機器學習來發掘模式 (PATTERN)
- 識別與群組特徵 (FEATURES), 也就是圖中的點
- 可運用在各種的分析, 例如:
  - 語音及面部辨識
  - 社群媒體內容分析
  - **惡意內容的分類** (FortiNDR 用許多乾淨、惡意的檔案以及許多特徵內容來訓練系統 (例如: Ransomware), 藉以識別超過20+ 種以上的惡意軟體形式/場景)
  - **網路流量的分析** (FortiNDR 用許多流量模式訓練系統來偵測異常流量行為)
- 學習的監督回饋 – 來自 FortiGuard 或是來自用戶本地網路的學習回饋



# 苦 命 的 MIS

老闆的電腦又中毒了.....

叫他不要上有的沒有的網站,就是不聽!!

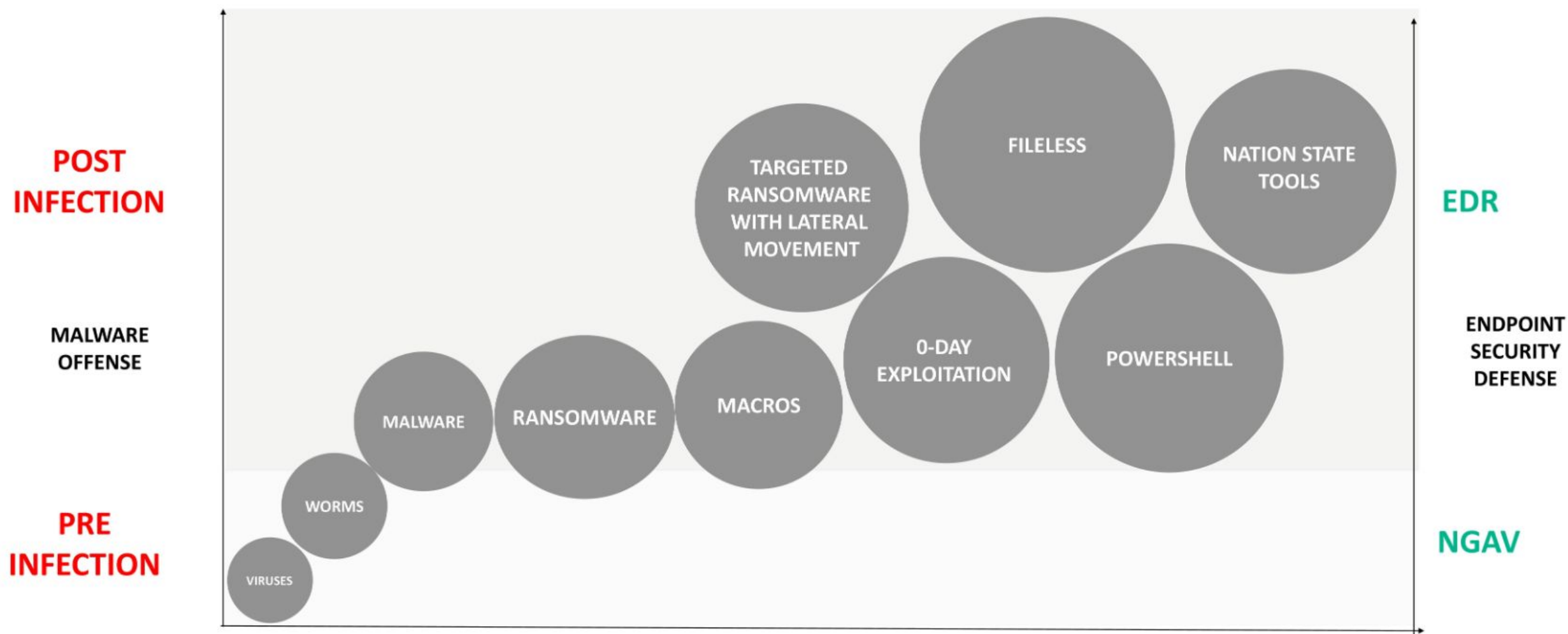
這次更慘了,中了勒索病毒 !!

**付 錢 < > 重 灌  
??**



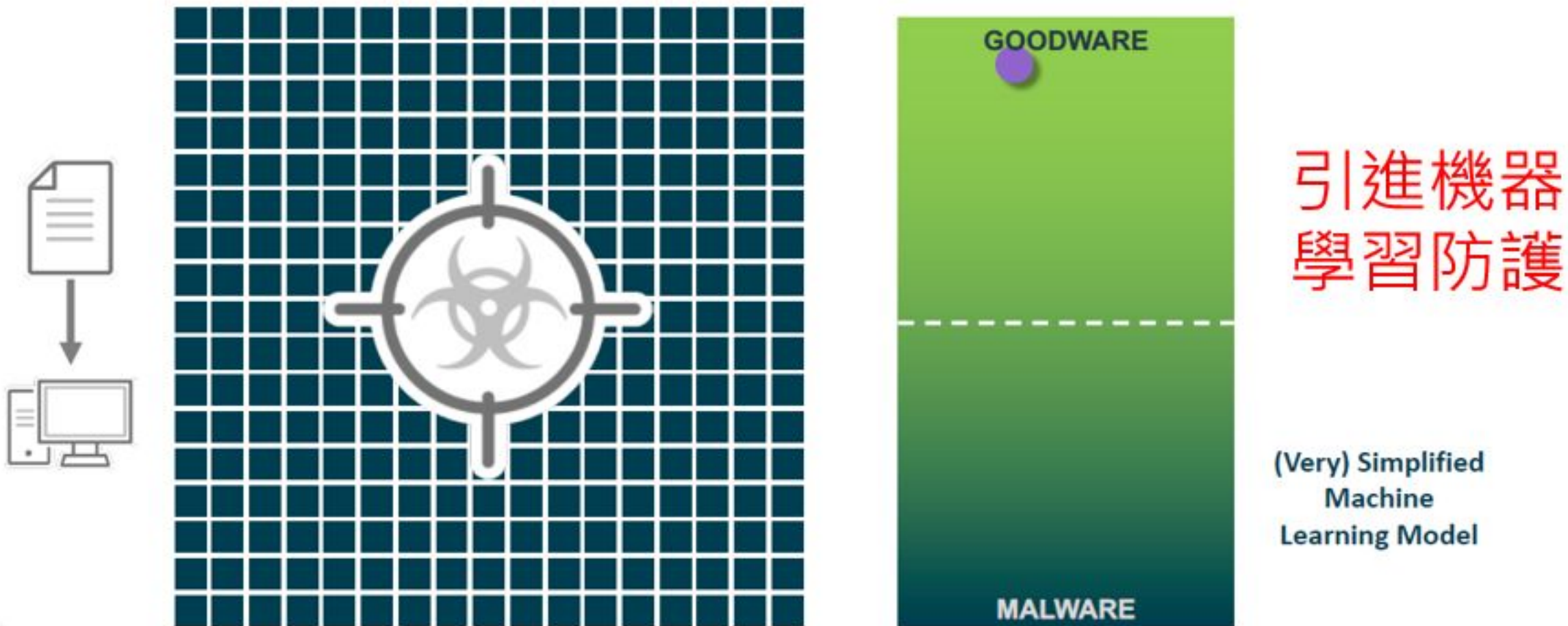
此相片 (作者: 未知的作者) 已透過 [CC BY-NC-ND](#) 授權

# 惡意軟體的演進與資安 產品的因應之道



# 病毒防範的演進與攻防

## Last Decade: Rise of Machine Learning

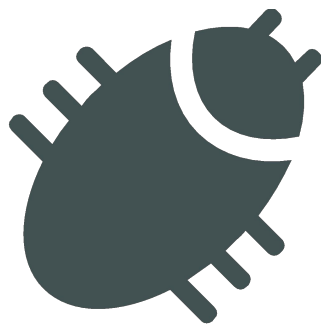




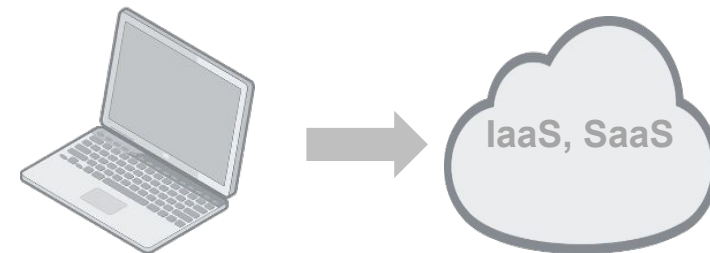
# 端點防護的挑戰



威脅層面  
與日俱進



系統弱點  
不斷暴露



雲端應用  
規避檢測

**Gartner**®

The security mindset has shifted to acknowledge that prevention alone is not enough; security and risk management leaders must be able to more easily harden endpoints and perform more detailed incident response to resolve alerts.

Notes/Sources:

1. Gartner Magic Quadrat for Endpoint Protection Platforms, August 2019.

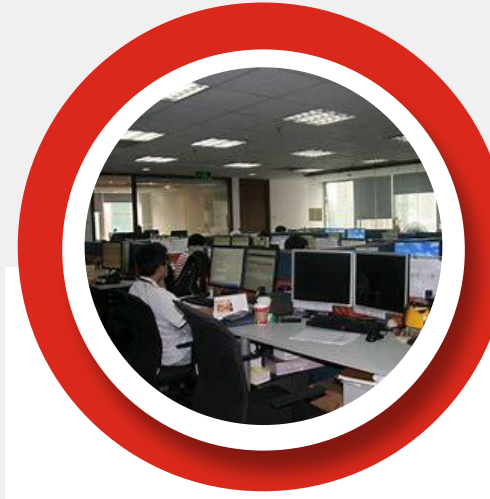
# 持續進階威脅



資料竊取



勒索加密



運作停擺



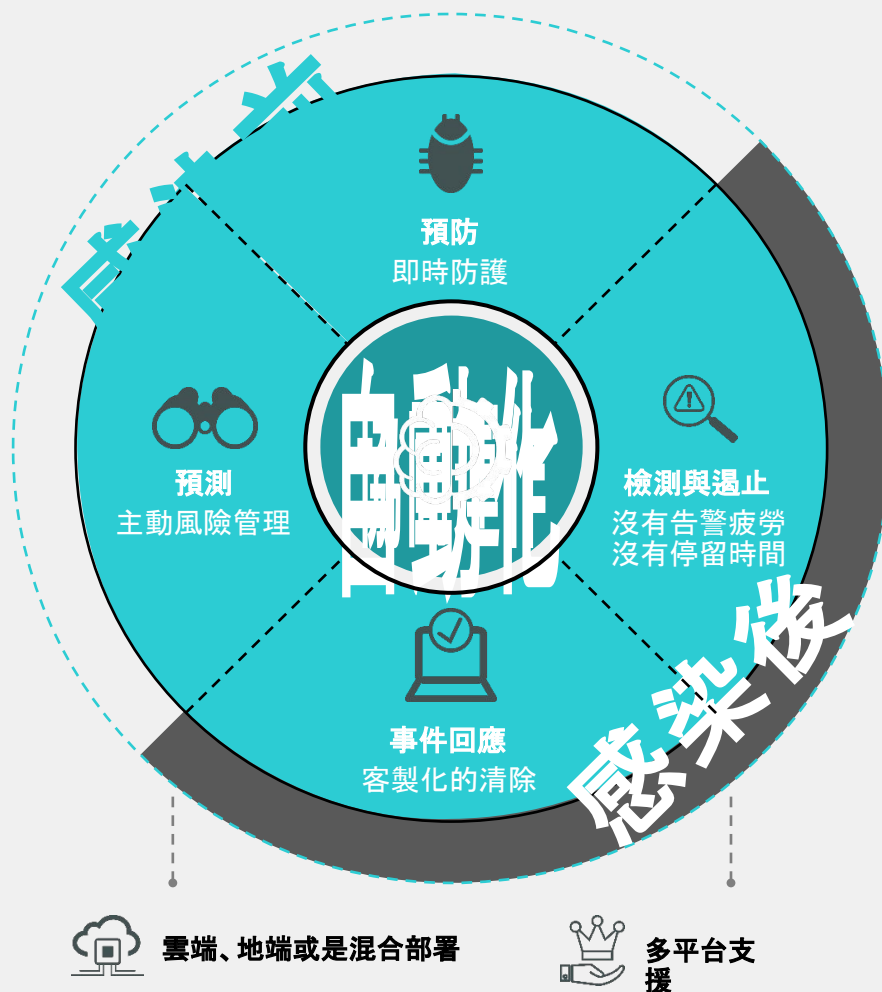
經濟損失

# FortiEDR 端點安全防護

Cloud-native Endpoint Protection, Detection & Response

FortiEDR 是一款 AI 賦能的端點安全解決方案，  
利用了 AI 技術來提供即時的偵測、分析與回應，  
包括但不限於以下幾個方面：

- 威脅檢測與分析
- 威脅情報共享
- 威脅回應與自動化



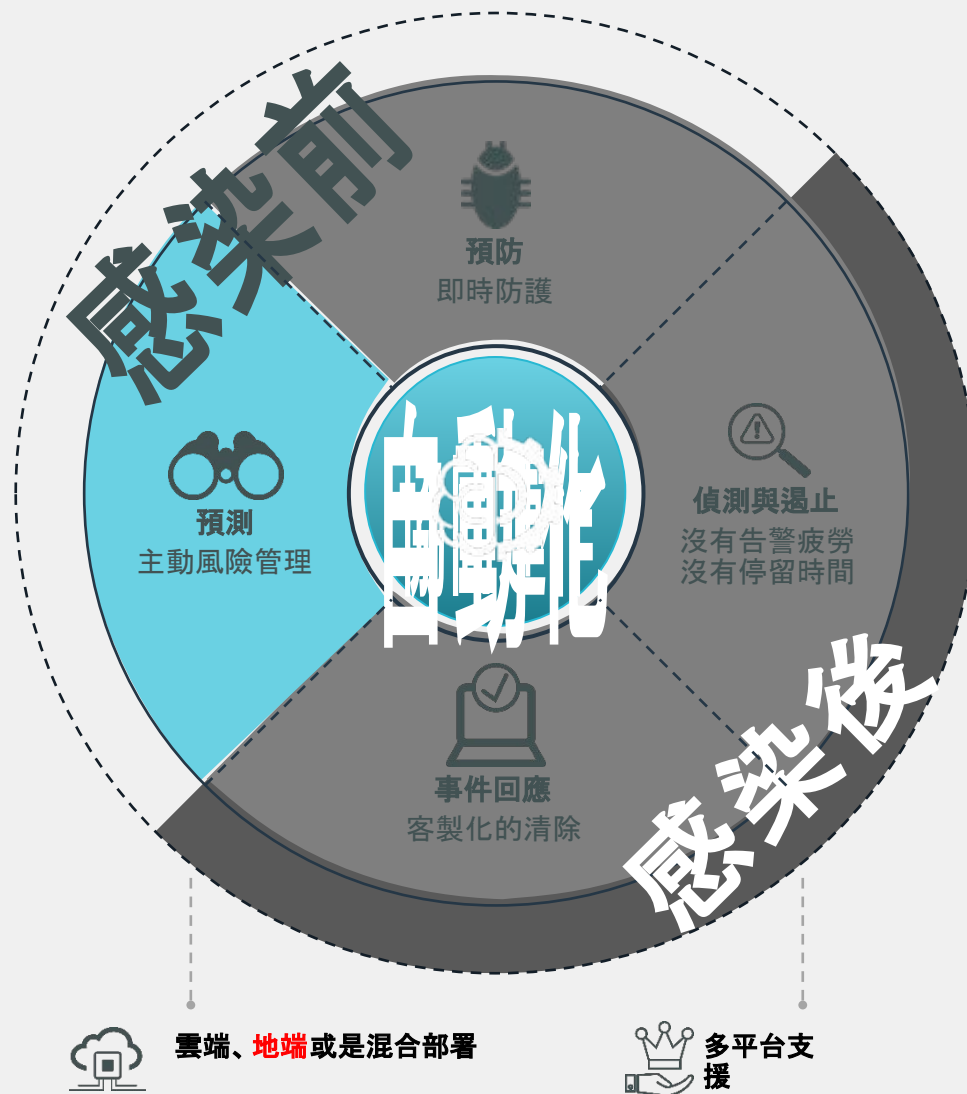
# 端點攻擊面風險控管



## 攻擊面風險控管

- 協助偵測潛在的 IOT 設備
- 連網應用程式風險評級: 漏洞、CVE 和聲譽度
- 可基於風險評級定義策略進行應用程式連線控管
- USB 設備控管

APPLICATION	VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
Google Chrome	Signed Google	Critical	Critical	15-Oct-2020	00-Mar-2021
86.0.4240.75		Critical	Critical	15-Oct-2020	15-Oct-2020
86.0.4240.103		Unknown	Critical	03-Nov-2020	03-Nov-2020
87.0.4280.66		Critical	Critical	01-Jan-2021	15-Jan-2021
88.0.4324.104		Unknown	Critical	04-Feb-2021	03-Feb-2021
87.0.4280.141		Critical	Critical	09-Feb-2021	02-Mar-2021
88.0.4324.150		Unknown	Critical	11-Feb-2021	22-Feb-2021
88.0.4324.146		Unknown	Critical	12-Feb-2021	19-Feb-2021
PasteBin Desktop	Unsigned Unknown Vendor	Unknown	Unknown	16-Oct-2020	16-Oct-2020





# 減少攻擊面 - 發現IoT設備

## IoT View

ensilofordev

DASHBOARD

EVENT VIEWER19001

FORENSICS

COMMUNICATION CONTROL1010

SECURITY SETTINGS

INVENTORY170

ADMINISTRATION12216

Protection

Galit

IOT DEVICES (170/170)

Search IOT Device

All

Create Group

Move to Group

Delete

Device Details

Export

DEVICE GROUP NAME	DEVICE NAME	CATEGORY	MODEL	INTERNAL IP	MAC ADDRESS	LOCATION	FIRST SEEN	LAST SEEN
Default IOT Group (53/53)								
Network device (6/6)								
		New Network device	HP 2530, 2920, or 5406zl...	10.51.120.1	00-FD-45-01-9C-00	Israel	Today	Today
	ens-vcsa20.ensilo.local	New Network device	HP 2530, 2920, or 5406zl switch	10.51.100.120	00-50-56-A1-AA-20	Israel	Today	Today
	ens-dgw-vl100.ensilo.local	New Network device	HP 2530, 2920, or 5406zl...	10.51.100.1	00-FD-45-01-9C-00	United States	Today	Today
	XC-6E5B97	Network device	Kemp LoadMaster LM-24...	192.168.186.2	9C-93-4E-6E-5B-97	United States	7 days ago	Today
		Network device	H3C Comware 5.20	192.168.186.1	40-B9-3C-04-A6-7C	Israel	8 days ago	Today
	ens-vcsa30.ensilo.local	Network device	OpenWrt Kamikaze 7.09 (...)	10.51.100.130	00-0C-29-A5-14-14	Israel	8 days ago	Today
Other (57/57)								
Power device (1/1)								
Printer (1/1)								
Storage (6/6)								
Unknown (46/46)								



# 減少攻擊面 - 應用程式通訊控管

## APPLICATIONS

All ▾ | Mark As... ▾ | Delete | Modify Action | Advanced Filter | Export ▾

<input type="checkbox"/>	APPLICATION	VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
<input type="checkbox"/>	Host Process for Windows Serv...	Signed	Microsoft Corporation	Unknown	09-May-2020	08-Dec-2...
<input checked="" type="checkbox"/>	Google Chrome	Signed	Google	Critical	09-May-2020	10-Nov-2...
<input type="checkbox"/>	81.0.4044.138			Critical	09-May-2020	10-May-2...
<input type="checkbox"/>	83.0.4103.106			Critical	22-Jun-2020	28-Jun-20...
<input type="checkbox"/>	83.0.4103.116			Critical	28-Jun-2020	28-Jun-20...
<input type="checkbox"/>	84.0.4147.105			Critical	05-Aug-2020	07-Aug-2...
<input type="checkbox"/>	84.0.4147.135			Critical	21-Aug-2020	27-Aug-2...
<input type="checkbox"/>	85.0.4183.83			Critical	27-Aug-2020	09-Sep-20...
<input type="checkbox"/>	85.0.4183.102			Critical	11-Sep-2020	23-Sep-20...
<input checked="" type="checkbox"/>	83.0.4103.61			Critical	17-Sep-2020	17-Sep-20...
<input type="checkbox"/>	85.0.4183.121			Critical	23-Sep-2020	19-Oct-20...

## VERSION DETAILS

Google Chrome, v. 83.0.4103.61

### Policies

Default Communication Contro...	Allow	According to policy
Servers Policy	Deny	According to policy
App Control Test	Allow	Manually
Carlos Communication Control Policy	Allow	According to policy
Carlos Servers Policy	Deny	According to policy

### Vulnerabilities

Total 105 CVEs

CVE-2020-6573	Critical	(CVSS 3.0: 9.6, CVSS 2.0: 6.8)
CVE-2020-6522	Critical	(CVSS 3.0: 9.6, CVSS 2.0: 6.8)
CVE-2020-6509	Critical	(CVSS 3.0: 9.6, CVSS 2.0: 6.8)
CVE-2020-6505	Critical	(CVSS 3.0: 9.6, CVSS 2.0: 6.8)

## ADVANCED DATA

### APPLICATION INFO

Application Description: Google Chrome

First Connection Time: 17-Sep-2020, 10:32:27

Last Connection Time: 17-Sep-2020, 10:39:11

Process Names: \Device\HarddiskVolume2\Users\admin\Desktop\Test Area\GoogleChrome...

### APPLICATION USAGE

No Collectors

### DESTINATIONS

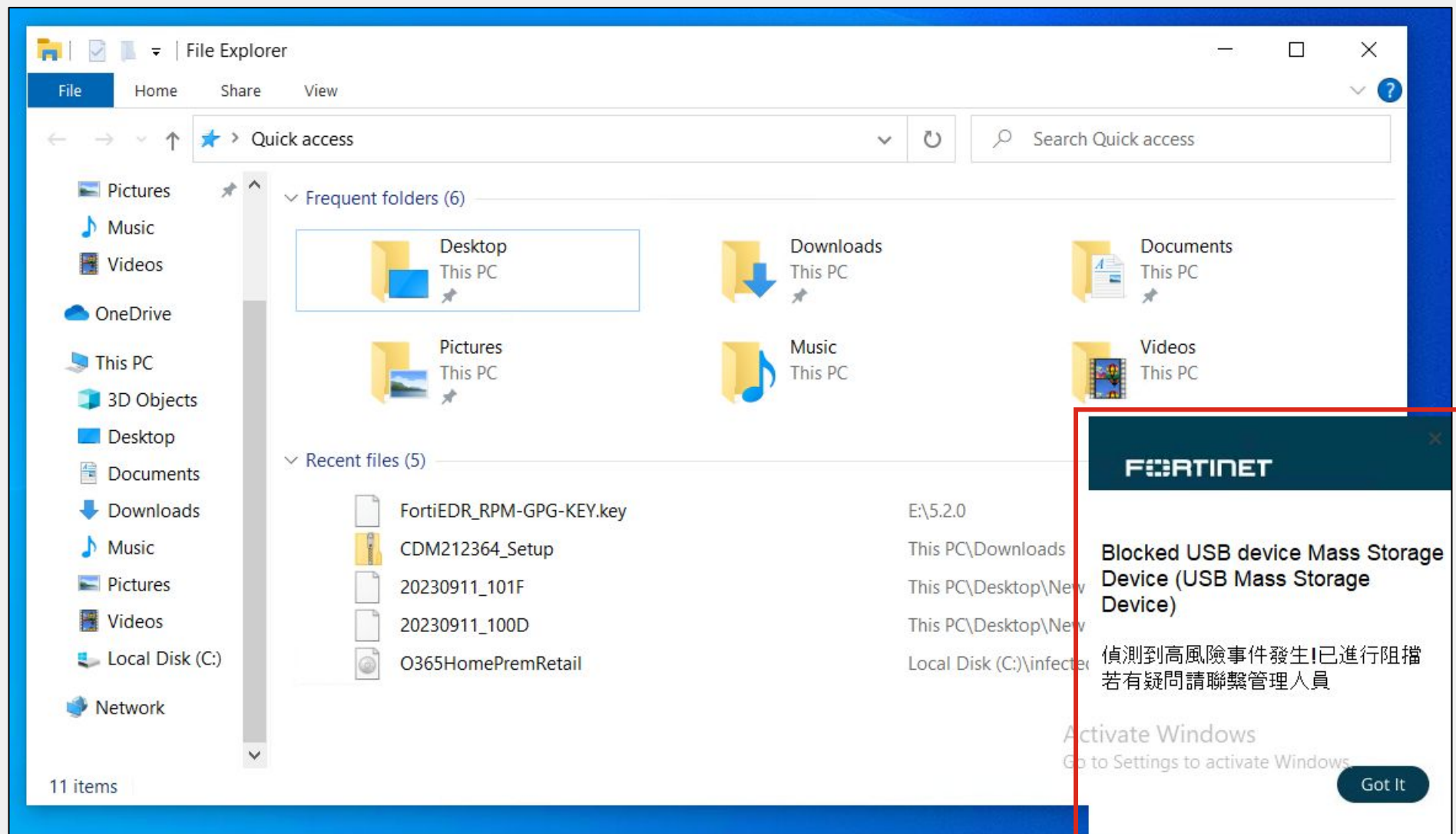
IP	CONNECTION TIME	COUNTRY
23.56.27.47	17-Sep-2020, 10:39:11	United States
172.217.160.70	17-Sep-2020, 10:38:50	United States
69.174.120.19	17-Sep-2020, 10:38:49	United States

[More...](#)



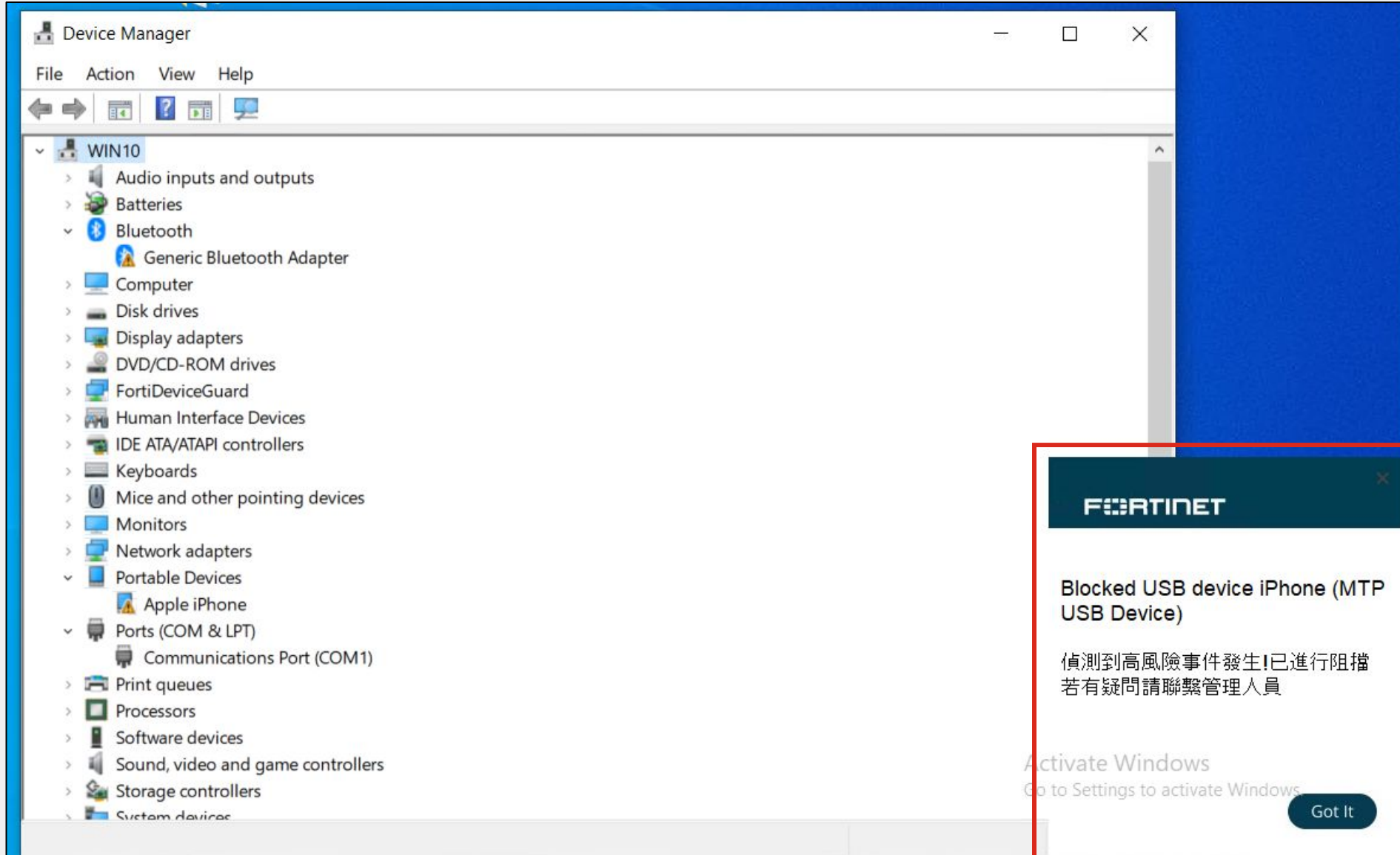
# 端點設備控管 - USB隨身碟

預設模式: 阻擋 >> 插入隨身碟時, 跳出封鎖視窗



# 端點設備控管 – 手機 iPhone

預設模式: 阻擋 >> iPhone使用USB cable插入USB時, 跳出封鎖視窗





# 機器學習強化未知威脅偵測與防護



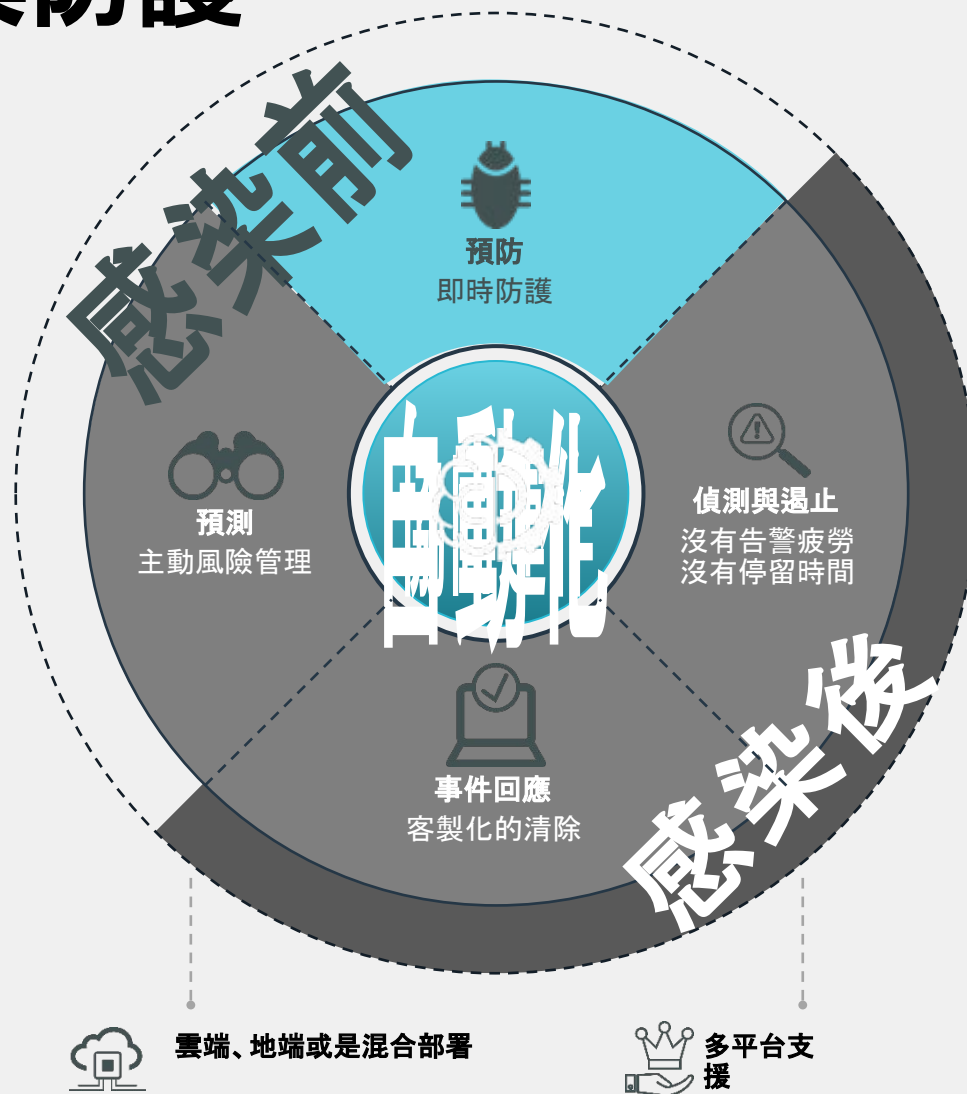
## 即時防護

- 機器學習，基於作業系統核心的 NGAV
- 持續更新的雲端資料庫
- 優秀的測試結果

POLICY NAME	RULE NAME	ACTION	STATE
Execution Prevention			
	Malicious File Detected	Block	Enabled
	Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected	Block	Enabled
	Sandbox Analysis - File was sent to the sandbox for analysis	Log	Disabled
	Stack Pivot - Stack Pointer is Out of Bounds	Block	Enabled
	Suspicious Driver Load - Attempt to load a suspicious driver	Block	Enabled
	Suspicious File Detected	Block	Enabled
	Suspicious Script Execution - A script was executed in a suspicious context	Block	Enabled
	Unconfirmed File Detected	Block	Enabled



How FortiEDR detects and blocks Revil Ransomware (aka sodinokibi) ([fortinet.com](https://www.fortinet.com))



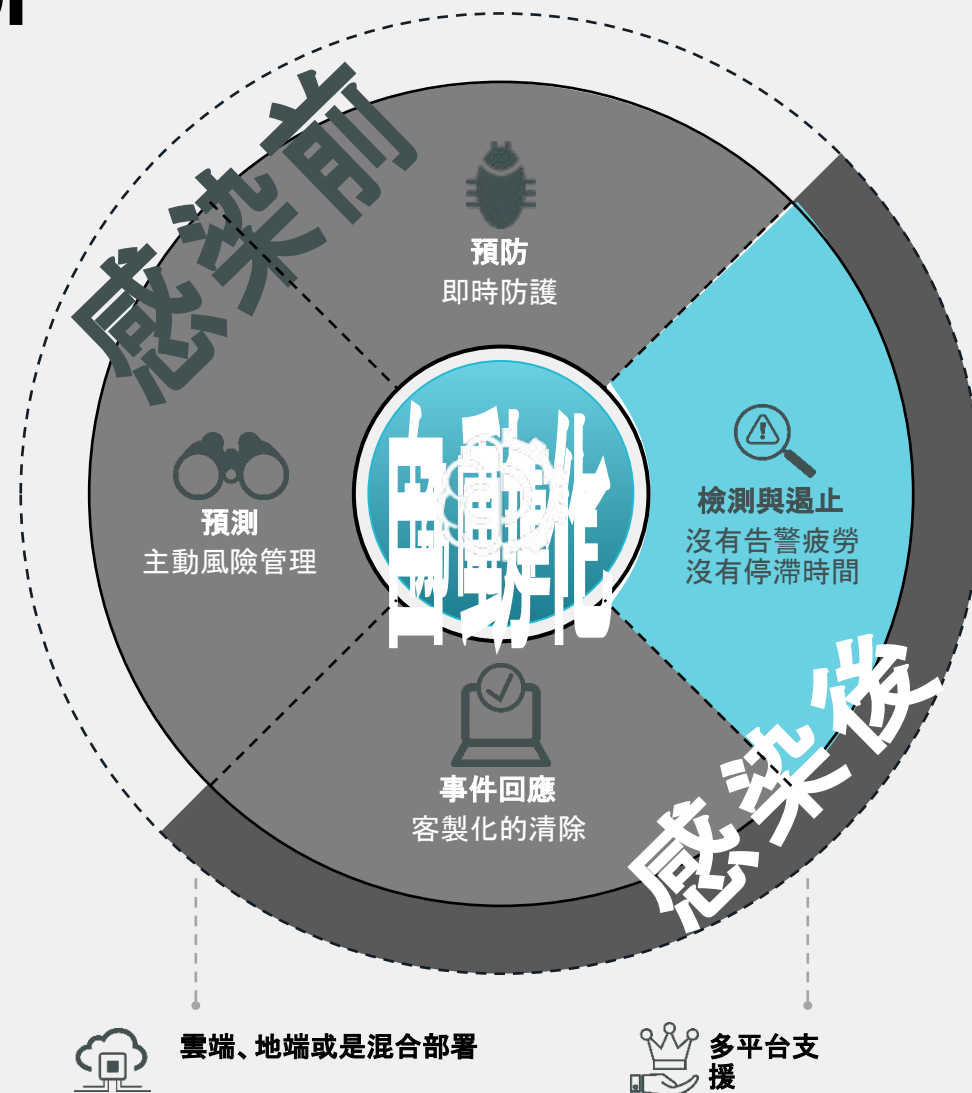
# 惡意行為分析有效偵測與阻斷



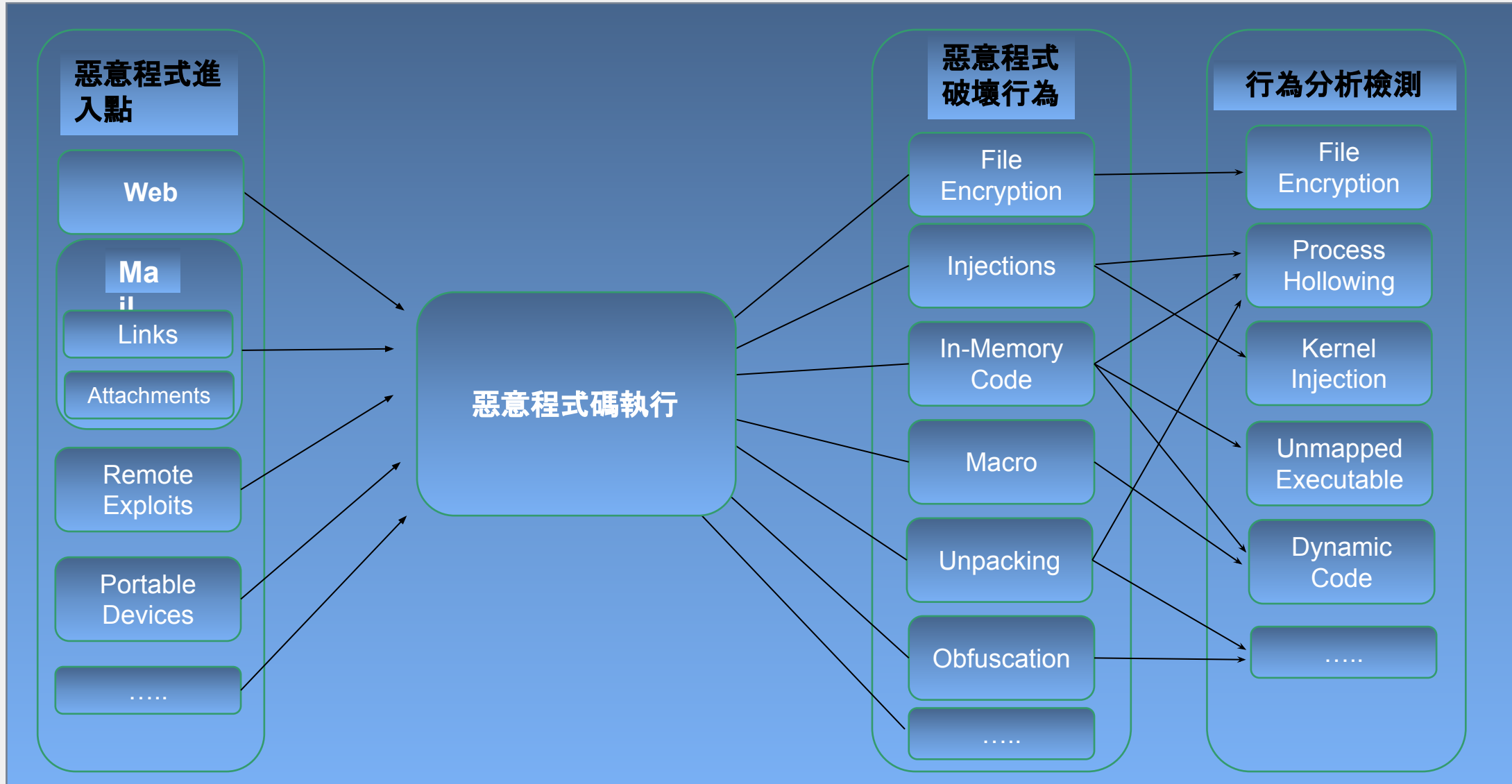
## 偵測、阻斷與稽核

專利文件號 US2016149887A1

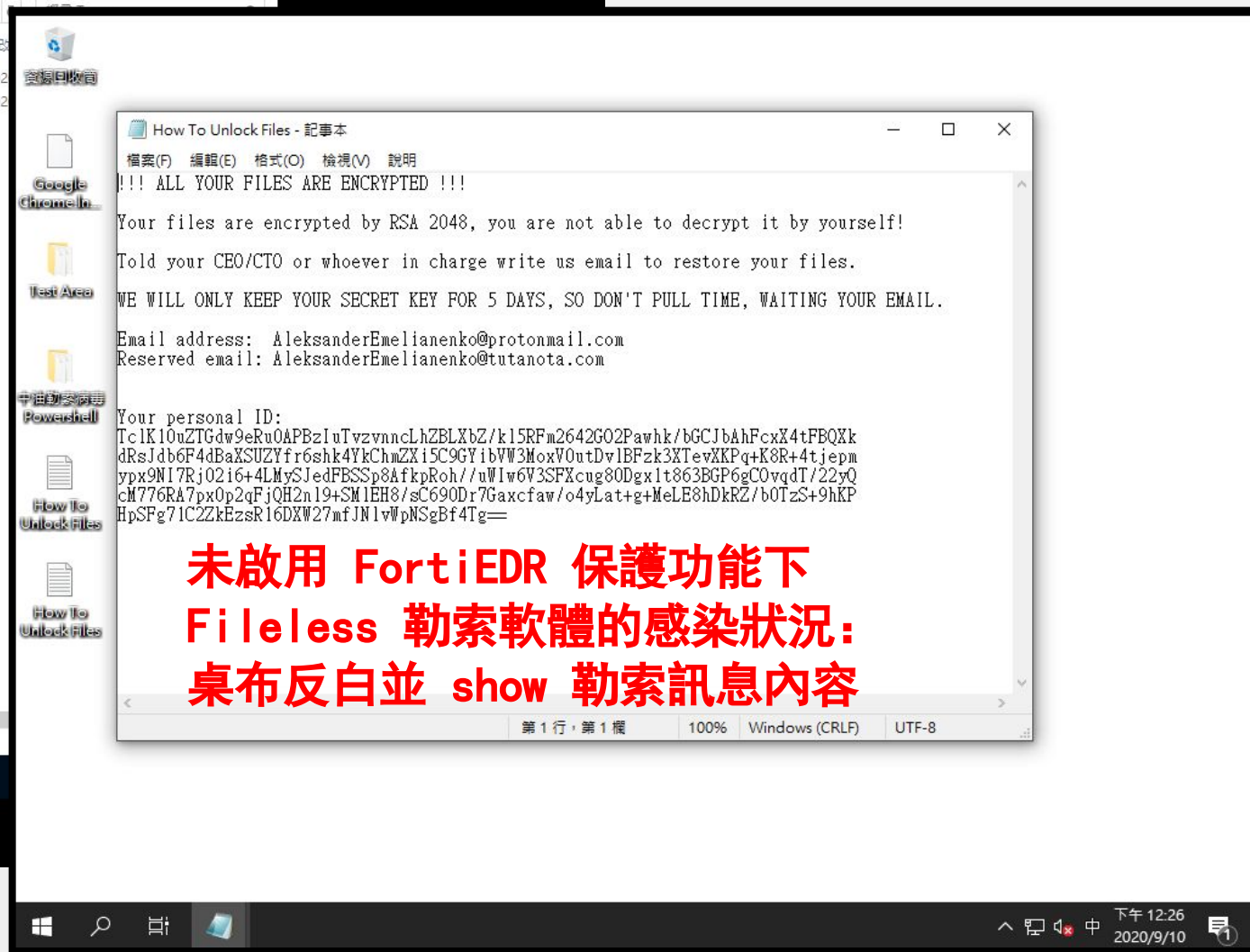
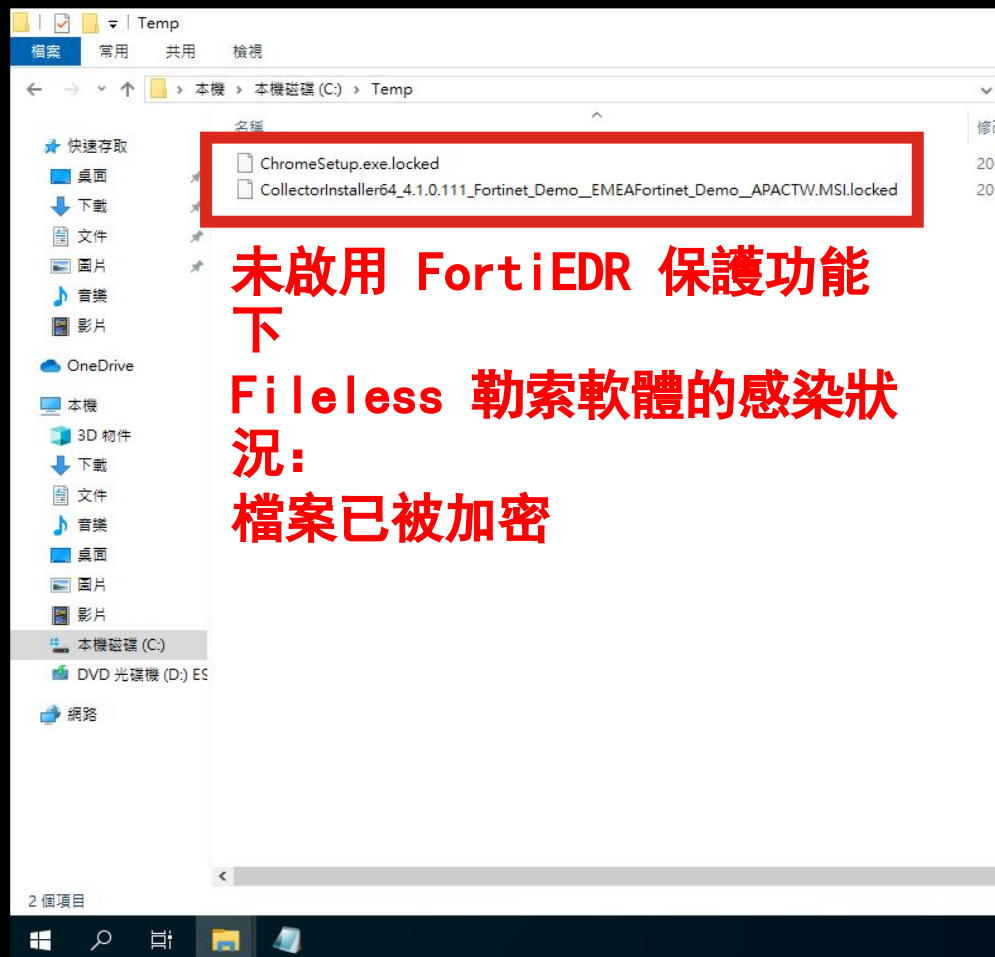
- 作業系統堆疊追蹤分析
- 即使在感染後也能即時阻斷惡意行為
- 阻擋通訊—資料外洩、橫向移動、C&C
- 檔案系統存取防護—避免檔案加密、竄改系統機碼等行為



# 端點惡意行為偵測與阻斷 - 降低損害、避免擴散



# FortiEDR 即時防護功能





# FortiEDR 即時防護功能

Windows PowerShell

– 啟用 FortiEDR 後  
– 潛藏的 Fileless 勒索軟體利用合法的 PowerShell  
– PowerShell 在執行階段就被 FortiEDR 主動阻擋

```
PS C:\Users\admin> $Assembly = [System.Reflection.Assembly]::Load($data)
以 "I" 引數呼叫 "Load" 時發生例外狀況: "陣列不能為 null。"
位於 線路:1 字元:1
+ $Assembly = [System.Reflection.Assembly]::Load($data)
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
+ FullyQualifiedErrorId : ArgumentNullException

PS C:\Users\admin> $Type = $Assembly.GetType("lc.lc")
不可在值為 Null 的運算式上呼叫方法。
位於 線路:1 字元:1
+ $Type = $Assembly.GetType("lc.lc")
+ ~~~~~
+ CategoryInfo          : InvalidOperation: (:) [], RuntimeException
+ FullyQualifiedErrorId : InvokeMethodOnNull

PS C:\Users\admin> $Type::Start()
不可在值為 Null 的運算式上呼叫方法。
位於 線路:1 字元:1
+ $Type::Start()
+ ~~~~~
+ CategoryInfo          : InvalidOperation: (:) [], RuntimeException
+ FullyQualifiedErrorId : InvokeMethodOnNull
```

**FORTINET**

Blocked process powershell.exe (PID 9060)

Contact your system administrator if a trusted application is blocked.  
如果被信任的應用程式被攔阻，請聯絡您的系統管理員。

Got It

下午 05:11  
2020/9/9



# FortiEDR 即時防護功能

The screenshot displays the Fortinet FortiEDR console interface. The top navigation bar includes links for Dashboard, Event Viewer (24), Forensics, Communication Control (137), Security Settings, Inventory (1), and Administration (33). The main content area is divided into two sections: 'EVENTS' and 'CLASSIFICATION DETAILS'.

**EVENTS Table:**

ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED	ACTION
3424973	DESKTOP-UAAD2CG	powershell.exe	Suspicious	File Write Access	09-Sep-2020, 11:25:53	09-Sep-2020, 11:26:03	[Icon]
User: DESKTOP-UAAD2CG\admin Certificate: Signed Process path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Raw data items: 1							
RAW ID	DEVICE	DESTINATION	FIRST SEEN	LAST SEEN	USERS	COUNT	
1662595536	DESKTOP-UAAD2CG	File Write Access	09-Sep-2020, 11:25:53	09-Sep-2020, 11:26:03	...TOP-UAAD2CG\admin	3	

**CLASSIFICATION DETAILS:**

**Suspicious** **FORTINET**

Threat name: Unknown  
Threat family: Unknown  
Threat type: Unknown

**History**

Suspicious, by FortinetCloudServices, on 09-Sep-2020, 11:26:02

**ADVANCED DATA**

系統啟動程序 (userinit) 帶起 explorer 執行

瀏覽器 (explorer.exe) 帶起 Powershell 執行

Process userinit.exe → 5 Create → Process explorer.exe → 6 Create → Process powershell.exe → 7 Write File Encryptor → Block FORTINET → ChromeSetup.exe

Copyright © Fortinet Version 4.2.0.83

System Time (UTC +02:00) 11:30:19

Taskbar: Fortinet, Fortinet - Fortinet..., 2020 Q3 APAC Pri..., Clean\_Win10\_EDR..., ZhongYou Virus BL...

- 已啟用 FortiEDR 保護功能下
- 當惡意軟體呼叫合法程式 (如: Powershell)
- 檔案加密程序立即被 FortiEDR 攔截阻擋

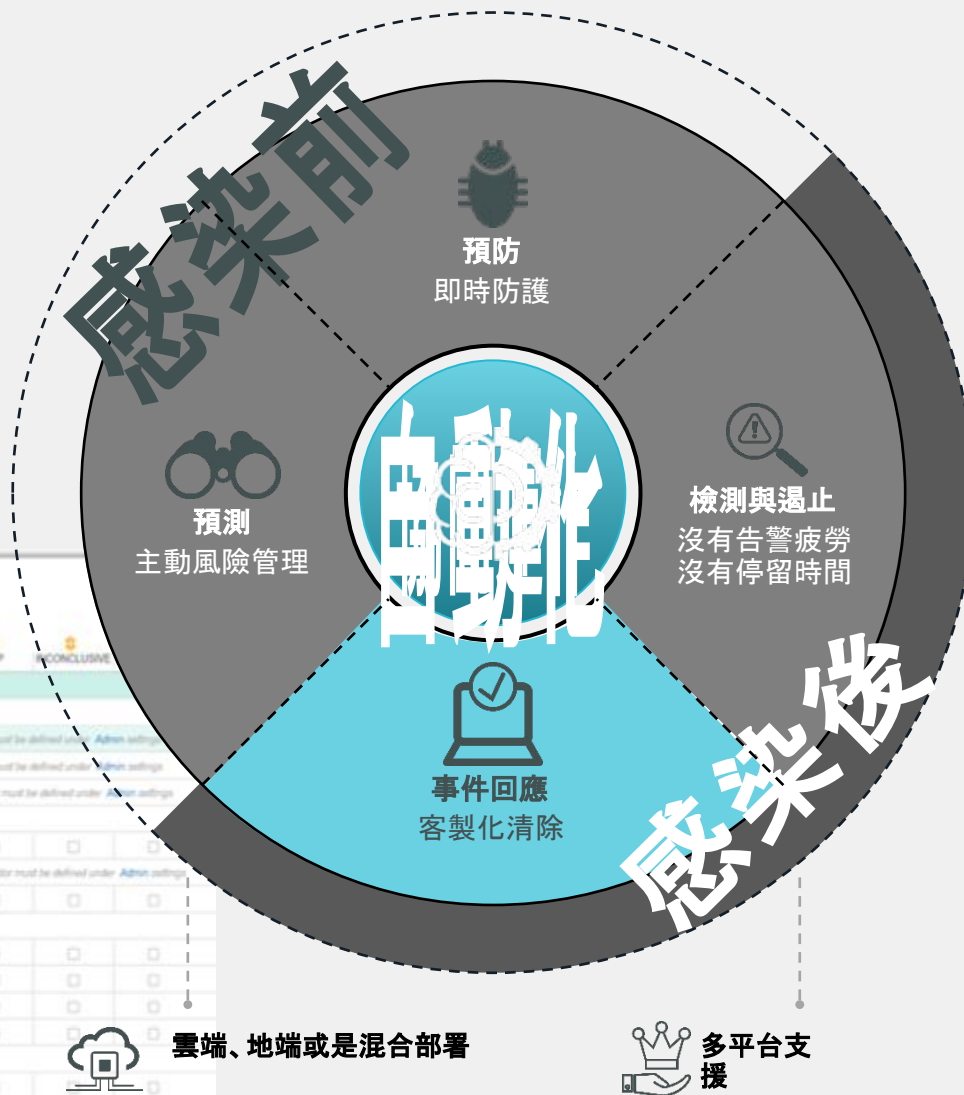
# 雲端服務提供不間斷的安全事件評估與協同響應



## 安全事件協同回應

自動的、持續的安全事件分類

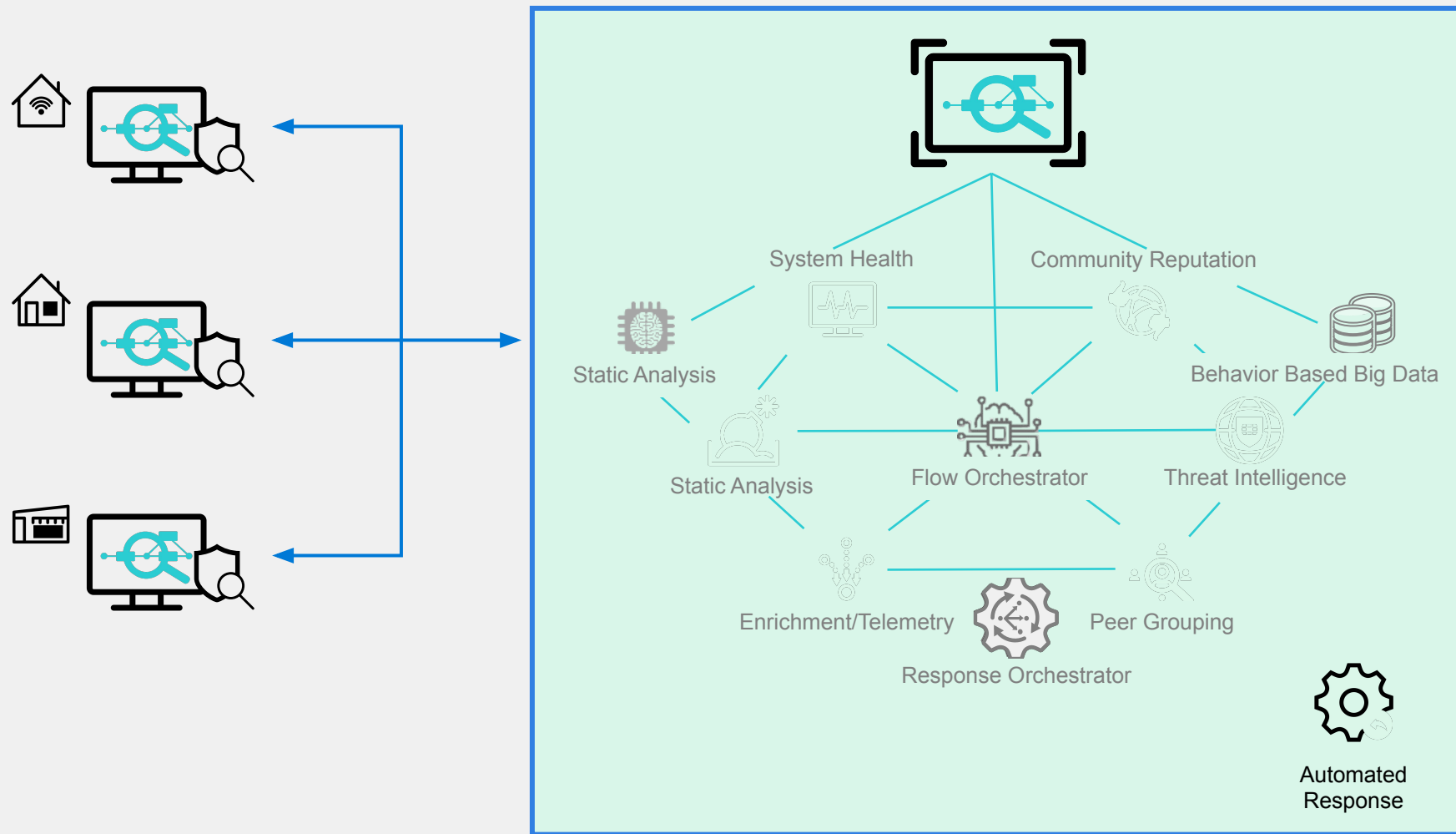
- 可基於設備組別以及威脅等級高度整合的自動處理腳本 playbooks
- 多種自動化的響應與修復動作



AUTOMATED INCIDENT RESPONSE - PLAYBOOKS					
[Clone Playbook] [Go Back] [Assign Collector Group] [Delete]					
NAME		MALICIOUS	SUSPICIOUS	PUP	UNCONCLUSIVE
[Default Playbook] [Run] [Stop]					
NOTIFICATIONS (sent in protection and simulation modes)					
Send mail notification					
Send syslog notification					
Open ticket					
INVESTIGATION					
Isolate device with Collector					
Isolate device with NAC					
Move device to the High Security Group					
REMEDIATION					
Terminate process					
Delete file					
Clean persistent data					
Block address on Firewall	fortigate:forti...				
CUSTOM					
Login user	AD_FTNT				
Quarantine MAC on Firewall	fortigate:forti...				
Assign device security tag on FGT	fortigate:forti...				
Disable interface on FGT	fortigate:forti...				
Change FGT security policy	fortigate:forti...				
ADVANCED PLAYBOOKS DATA					



# Fortinet Cloud Services 動靜態分析協助事件判斷分類



## Artificial Intelligence

對於告警事件進行進階分析

## Automated Response

告警事件自動響應

**Malicious** **FORTINET**

Threat name: Kryptik.CTQltr  
Threat family: W64  
Threat type: Unknown

Automated analysis steps completed by Fortinet [Details](#)

**History**

- Malicious, by FortinetCloudServices, on 30-Mar-2022, 01:06:47
  - Device **DESKTOP-VM-BN** was isolated on NAC **TME-FortiNACz**
  - Process **...esktop\Ayfaga3.exe** with PID **2572** was terminated at device **DESKTOP-VM-BN** 4 times
  - File **...esktop\Ayfaga3.exe** was deleted on device **DESKTOP-VM-BN** 2 times
  - IP **104.168.44.45** was added to malicious IP addresses on firewall **FortiGate**

**Triggered Rules**

- G3 Exfiltration Prevention clone
  - Malicious File Detected
  - Tampered Executable - Critical Executable was Tampered With





# 資安事件自動處理與回應 —> 彈性多樣化的處理方式

ensilofordev

DASHBOARD

EVENT VIEWER196

FORENSICS

COMMUNICATION CONTROL1240

SECURITY SETTINGS

INVENTORY1

ADMINISTRATION696

Protect

AUTOMATED INCIDENT RESPONSE - PLAYBOOKS

Clone Playbook

Set Mode

Assign Collector Group

Delete

NAME

Default Playbook

FORTINET

NOTIFICATIONS (sent in protection and simulation modes)

Send mail notification

Send syslog notification

Open ticket

INVESTIGATION

Isolate device with Collector

Isolate device with NAC

Move device to the High Security Group

REMEDiation

Terminate process

Delete file

Clean persistent data

Block address on Firewall

MALICIOUS

USPICIOUS

PUP

INCONCLUSIVE

LIKELY SAFE

✓

✓

✓

✓

✓

✓

✓

✓

✓

✓

✓

✓

✓

✓

✓

✓

✓

✓

✓

✓

✓

✓

✓

✓

✓

✓

✓

✓

✓

✓

Syslog must be defined under Admin settings

A NAC connector must be defined under Admin settings

A firewall must be defined under Admin settings

ASSIGNED COLLECTOR GROUPS

Unassign Group

High Security Collector Group (0 collectors included)

Beta 4.1.0 (4 collectors included)

Cloud (2 collectors included)

Default Collector Group (8 collectors included)

edrtest (1 collector included)

emulation (0 collectors included)

emulation\_a (0 collectors included)

Eugene-emulator (0 collectors included)

Linux collectors (2 collectors included)

lior (1 collector included)

lior Testing (0 collectors included)

lior333 (1 collector included)

Nastya (0 collectors included)

oti (0 collectors included)

philip (1 collector included)

PT (0 collectors included)

ResearchTeam (1 collector included)

shanitest (0 collectors included)

© Fortinet Inc. All Rights Reserved.

25



# 資安聯防提升整體防禦能力

在 FortiEDR 中控台上設定要參與聯動防護的 FortiGate 防火牆

The screenshot displays the FortiEDR Administration console interface. The top navigation bar includes tabs for DASHBOARD, EVENT VIEWER (145), FORENSICS, COMMUNICATION CONTROL (53), SECURITY SETTINGS, INVENTORY, and ADMINISTRATION (active). The left sidebar lists various management sections: LICENSING, ORGANIZATIONS, USERS, DISTRIBUTION LISTS, EXPORT SETTINGS, TOOLS, SYSTEM EVENTS, and IP SETS. The main content area is titled 'CONNECTORS' and shows a list of connectors. One connector, 'Firewall : FG-60E\_SSL', is expanded. Below the connector name, it indicates 'Firewall Enabled' with a checkmark. The 'On-premise Core' is set to 'fedr-core: 60.250.130.70:555'. The 'Details' section is highlighted with a red box and contains the following fields: 'Name' (FG-60E\_SSL), 'Type' (FortiGate), 'Host' (60.250.130.70), 'Port' (20443), and 'API Key' (selected over 'Credentials'). The 'Actions' section, also highlighted with a red box, shows 'Block address on Firewall' with an 'Address group' of 'FEDR\_Blocking'. A red text box with white text is overlaid on the Actions section, stating: '將連線的惡意網站 IP 放入防火牆阻擋黑名單'. At the bottom of the configuration area, there are 'Save', 'Cancel', and 'Delete' buttons. Below the screenshot, the text '透過 API 聯動 FortiGate 防火牆' is displayed.

CONNECTORS

+ Add Connector

Firewall : FG-60E\_SSL

Firewall Enabled ✓

On-premise Core fedr-core: 60.250.130.70:555

Details

Name FG-60E\_SSL Type FortiGate Host 60.250.130.70 Port 20443

☒ API Key ☐ Credentials

Key .....

Actions

Block address on Firewall Address group FEDR\_Blocking

將連線的惡意網站 IP 放入防火牆阻擋黑名單

透過 API 聯動 FortiGate 防火牆

Save Cancel Delete

# 資安聯防提升整體防禦能力

## 資安事件觸發後自動啟動聯防動作

The screenshot displays the Fortinet Security Fabric interface, specifically the 'EVENT VIEWER' section. The top navigation bar includes 'DASHBOARD', 'EVENT VIEWER', 'FORENSICS', 'COMMUNICATION CONTROL', 'SECURITY SETTINGS', 'INVENTORY', and 'ADMINISTRATION'. The 'EVENTS' table lists several events, with the first event highlighted: 'powershell.exe (1 event)' with 'EVENT ID 335899'. The event details show it is 'Malicious' and occurred on '29-Mar-2021, 19:48:54'. The 'CLASSIFICATION DETAILS' panel on the right shows the threat is 'Malicious' with a 'Threat name: Unknown' and 'Threat family: Unknown'. The 'History' section indicates that 'IP 185.199.109.133 was added to malicious IP addresses on firewall FortiGate FG-SE\_Lab'.

The 'ADVANCED DATA' section at the bottom shows an 'Event Graph' with three main steps: '1 Create' (Process explorer.exe), '2 Create' (Process cmd.exe), and '3 Connect' (Process powershell.exe). The graph illustrates the flow of the attack: '瀏覽器帶起 Cmd 程序' (Browser starts Cmd process), 'Cmd 呼叫 Powershell' (Cmd calls Powershell), and 'Powershell 嘗試連線惡意網站 IP\_185.199.109.133' (Powershell attempts to connect to malicious website IP\_185.199.109.133). The '3 Connect' step is highlighted with a red box, and the 'Connection 185.199.109.133' node is also highlighted with a red box.

**FEDR 自動通知 FGT 將該惡意網站 IP 放入阻擋黑名單**



# 資安聯防提升整體防禦能力

在 FortiGate 防火牆上自動將連線的惡意網站 IP 放入防火牆阻擋黑名單

Name	Details	Interface	Fabric Sync	Type	Ref.
Bonjour	224.0.0.251 - 224.0.0.251		undefined	Multicast A...	0
EIGRP	224.0.0.10 - 224.0.0.10		undefined	Multicast A...	0
OSPF	224.0.0.5 - 224.0.0.5		undefined	Multicast A...	0
all	224.0.0.0 - 239.255.255.255		undefined	Multicast A...	0
all_hosts	224.0.0.1 - 224.0.0.255		undefined	Multicast A...	0
all_routers	224.0.0.2 - 224.0.0.255		undefined	Multicast A...	0
Address Group 5					
Demo_Malicious_IP	FortiEDR_7 FortiEDR_9 FortiEDR_5 FortiEDR_185.199.109.133		Disable	Address Gr...	1

Address: FortiEDR\_185.199.109.133

Type: IP Range

IP Range: 185.199.109.133 - 185.199.109.133

Interface: ☐ any

Fabric Sync: ☒ Disabled

Comments: FortiEDR Event ID - 335899

References: 1

Edit

- ✓ 有裝 FortiEDR 的電腦保護了自己
- ✓ 沒裝 FortiEDR 的電腦或 IOT/OT 設備受到了防火牆自動聯防機制的保護



# 整合 FortiSIEM 使用情境與技術

AI/ML 關聯分析產生告警，對應 MITRE ATT&CK 資安框架，顯示主機在資安攻擊鏈所處的狀態

FortiSIEM

儀表板關聯分析告警事故派工管理CMDB資源庫工作系統管理

告警總覽List風險分析探索分析

Tactics: 全部搜尋設備... (10/10)

Status: 已啟用時間範圍: Last 2 Hours

1 分鐘

設備	Reconnaissance	Resource Development	Initial Access	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
w2k12r2-ad			1	12	5	11	3		1	2	3	7
laba	1		2	6	2	1	4	3	1			
FDC-Decoy-WIN7	1						1	4				
WIN10-LoCo	1						1	4				
211.141.78.56			1		1			1		1		
195.211.29.229											3	
www.abcd.z2.dca1.com										1		
www.xyz.z1.dca0.com										1		
224.229.172.66												

Execution Incidents for laba: 6

嚴重性類別	最後一次發生	告警事故	戰術	技術	來源	目標	詳細資訊	告警事故狀態	解決處理狀態
HIGH	Jul 02 2023, 03:21:00 PM	Backdoor Found	Execution	User Execution: Malicious Link	192.168.68.74		Component Event Type: FortiGate-ips-signature-23098 Signature Id: 23098	Active	Open
MEDIUM	Jul 02 2023, 03:21:00 PM	FortiEDR-Security-Malicious-Logged	Execution,Defense Evasion	Signed Binary Proxy Execution: CMSTP, Signe...	192.168.68.74	User: admin	Process Name: powershell.exe	Active	Open
MEDIUM	Jul 02 2023, 03:21:00 PM	FortiEDR-Security-Malicious-Logged	Execution,Defense Evasion	Signed Binary Proxy Execution: CMSTP, Signe...	192.168.68.74	User: admin	Process Name: net1.exe	Active	Open
MEDIUM	Jul 02 2023, 03:21:00 PM	FortiEDR-Security-Malicious-Logged	Execution,Defense Evasion	Signed Binary Proxy Execution: CMSTP, Signe...	192.168.68.74	User: admin	Process Name: net.exe	Active	Open

Copyright © 2022 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Global FortiSIEM 6.6.2.1637

執行運作  
FortiEDR 偵測到利用 Powershell 執行的異常行為並建立後門

# EDR告警分析需要更多的資料 - 看一下AI怎麼說？

資安專家：當在 EDR (Endpoint Detection and Response) 上接收到告警事件時，我們需要進行一系列的分析步驟來確定該事件的性質、風險程度以及需要採取的應對措施。以下是一個分析過程的概要：

1. **\*\*收集信息\*\***: 首先，收集 EDR 告警事件的詳細信息，包括事件類型、時間、源和目標端點、網絡流量等相關數據。
  2. **\*\*初步判定\*\***: 根據告警信息，對事件進行初步判定。判斷事件是否是誤報、已知的安全風險或可能的新型攻擊。
  3. **\*\*深入調查\*\***: 對疑似具有安全風險的事件進行深入調查，這可能包括：
    - 分析網絡流量，尋找可疑的通信模式或命令
    - **檢查相關端點的系統日誌，尋找可疑的行為或變更**
    - 搜索已知的漏洞數據庫，了解此類事件可能與已知漏洞的關聯
    - **檢查端點的文件和註冊表，尋找可疑的修改或新增**
    - 與其他安全產品（如IDS、IPS、SIEM等）進行數據整合，分析事件的整體情況
  4. **\*\*風險評估\*\***: 基於調查結果，評估事件的嚴重性和對業務的影響。風險評估應包括以下因素：
    - 攻擊的目的（例如：網絡入侵、數據竊取、勒索軟件等）
    - 受影響的資產類型（例如：敏感數據、關鍵基礎設施、業務流程等）
    - 可能的損失範圍（例如：數據洩露、系統停機、法律責任等）
  5. **\*\*制定應對措施\*\***: 根據風險評估結果，制定相應的應對措施。這可能包括：
    - 即時隔離受影響的端點，阻止攻擊者進一步擴散
    - 更新防火牆、IDS/IPS等安全設備的策略，以阻止相關攻擊
    - 應用安全補丁，修復已知的漏洞
    - 恢復受影響系統的正常運行
    - 提高安全意識培訓，降低人為風險
  6. **\*\*後續監控\*\***: 在事件解決後，持續監控網絡和端點的狀態，以防止類似事件的再次發生。此外，定期進行安全審計和風險評估，不斷完善企業的安全防護能力。
- 通過以上分析過程，資安專家可以對 EDR 告警事件進行有效的處理，確保企業網絡和資產的安全。



# FortiEDR 深度端點軌跡記錄，強化資安鑑識能力

- 程序、檔案、機碼、網路、事件紀錄

### Event Collection And Storage

Collect and store Activity Events of the following categories and Types

Inventory

Enabled

☒ File Detected

Process

Enabled

☒ Screen Capture

☒ Process Termination

☒ Process Creation

☒ Process Start

☒ Thread Created

☒ Executable Loaded

☒ Driver Loaded

☒ Library Loaded

☒ Keystroke Consumption

File

Enabled

☒ File Created

☒ File Write

☒ File Read

☒ File Rename

☒ File Delete

☒ File Time Set

☒ Direct Volume Access

☒ Direct Volume Write

Network

Enabled

☒ HTTP Request

☒ Socket Network Statistics

☒ Socket Connect

☒ DNS Query

☒ Socket Listen

☒ Socket Close

☒ Socket Accept

Registry

Enabled

☒ Key Created

☒ Key Deleted

☒ Key Renamed

☒ Key Loaded

☒ Key Saved

☒ Key Replaced

☒ Key Restored

☒ Value Created

☒ Value Read

☒ Value Deleted

☒ Value Set

Log

Enabled

☒ Event Log Entry Created

☒ Trace Entry Created

☒ Log Entry Created



# 主動式威脅捕獵 – 快速搜尋與定位關鍵記錄！

The screenshot displays the Fortinet Security Fabric interface, specifically the Threat Hunting section. The top navigation bar includes links to DASHBOARD, EVENT VIEWER (197), FORENSICS, COMMUNICATION CONTROL (1240), SECURITY SETTINGS, INVENTORY (1), and ADMINISTRATION (696). The Threat Hunting section features a search bar with a Lucene-like syntax and filters for CATEGORY (All Categories) and DEVICE (Choose). A table of results is shown, with columns for Behavior, Type, Device Name, Target Process, Protocol, Remote IP, Remote Port, Target Process Signed, and Signed By. The Behavior column is highlighted with a red box, showing 'credential access' (3052) and 'discovery' (855). Below the table, a list of EDR Events (2.16M) is displayed, with columns for Category, Time, OS, Device Name, Type, Behavior, Process And Attributes, Target, and Event Attributes. One event is highlighted with a red box: a File Read event on 2020-Sep-16 at 13:05:13 on device LIOR-NewPC, involving chrome.exe (PID 53584) reading a file (f\_005f5b) from the path Users\lior\AppData\Local\Google\Chrome\Application\chrome.exe. A detailed view of this event is shown on the right, including a Summary tab, Status (Disconnected), Internal IP (10.51.121.49), and a list of attributes such as Path, Executing user, Product, SHA1, and Command line.

Behavior	Type	Device Name	Target Process	Protocol	Remote IP	Remote Port	Target Process Signed	Signed By
credential access (3907)	File Read (2161981)	lior-newpc (2161981)	chrome.exe (33395)	tcp (21152)	3.222.249.36 (21152)	636 (21152)	Signed (33075)	engineering (32196)
discovery (855)	Executable Loaded (735967)	ensw-lap153 (350083)	proxyhost.exe (3927)	udp (2885)	8.241.17.254 (21152)	993 (21152)	Unsigned (320)	empty (320)
	File Write (259258)	ensw-lap149 (97660)	teams.exe (2398)		10.0.0.30 (21152)	5000 (21152)		information technology (78)
	File Create (136152)	ensw-lap119 (37322)	svchost.exe (1715)		10.0.0.138 (21152)	5353 (21152)		acrobat dc (75)
	File Delete (105581)	einat-pc (10816)	backgroundtaskhost.exe (1509)		10.51.102.170 (21152)	10443 (21152)		

Category	Time	OS	Device Name	Type	Behavior	Process And Attributes	Target	Event Attributes
2020-Sep-16...	2020-Sep-16...	Windows	ENSW-LAP119	Socket Conn...	chrome.exe	chrome.exe	2001:4860:4...	Source PID 13284, Local Address 0:0:0:0:0:0:64983, Remote Address 2001:4860:4860:0:...
2020-Sep-16...	2020-Sep-16...	Windows	LIOR-NewPC	File Read	chrome.exe	chrome.exe	f_000474	Source PID 53584, Path Users\lior\AppData\Local\Google\Chrome\Application\chrome.exe, Hash
2020-Sep-16...	2020-Sep-16...	Windows	ENSW-LAP119	File Read	SelfElectController.exe	SelfElectController.exe	download...	Source PID 8696, Path ProgramData\LAN..., Hash
2020-Sep-16...	2020-Sep-16...	Windows	LIOR-NewPC	File Read	chrome.exe	chrome.exe	f_005f5b	Source PID 53584, Path Users\lior\AppData\Local\Google\Chrome\Application\chrome.exe, Hash
2020-Sep-16...	2020-Sep-16...	Windows	LIOR-NewPC	Socket Close	chrome.exe	chrome.exe	0:0:0:0:0:0:...	Source PID 53584, Local Address 10.51.121.49/56718, Remote Address 0:0:0:0:0:0:0/0

### File Read

Summary → chrome.exe 2020-Sep-16, 13:05:13 UTC

LIOR-NewPC Status: Disconnected Internal IP: 10.51.121.49, 192.168.116.100 Up time: 3d, 3h, 49min, 38sec

chrome.exe PID: 53584

Path: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

Executing user: ENSILO\lior

Product: Google Chrome

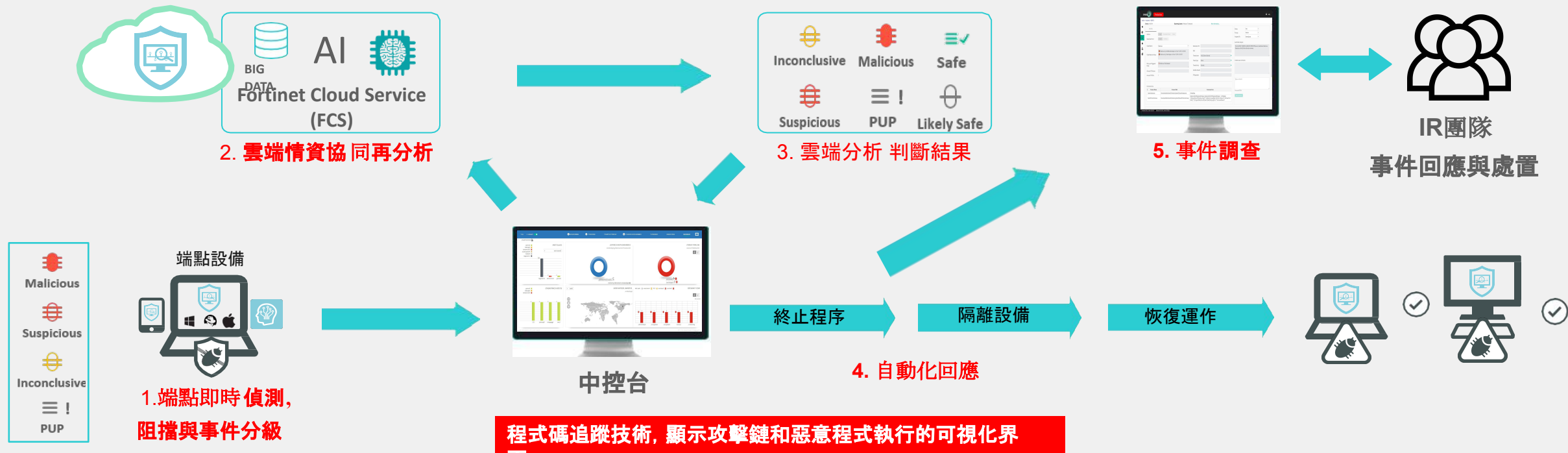
SHA1: 943A2D62A7AB288B239DC690AEAF75A67155C642

Command line: --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1632,5379426322936354670,3234879161765688624,131072 --

System Time (UTC): 2020-09-16 11:47:00

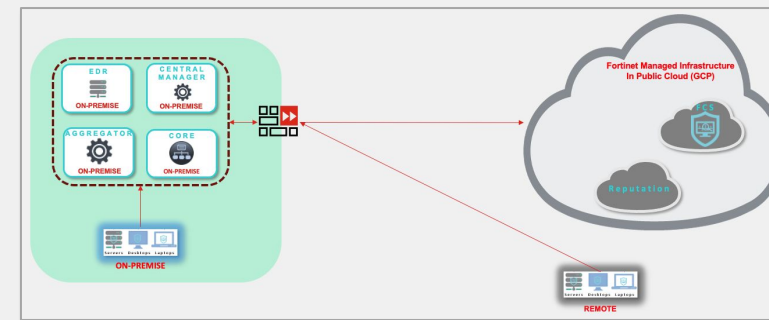
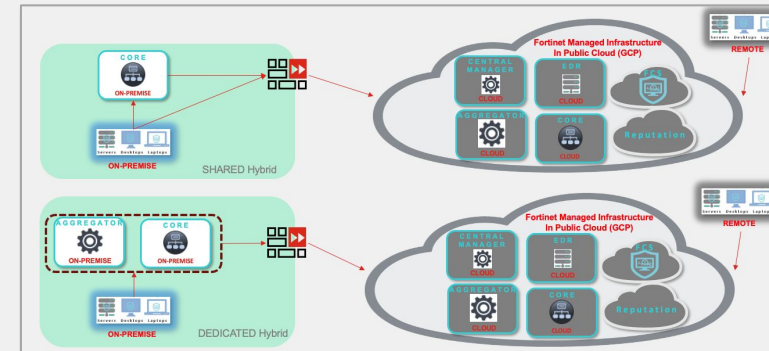
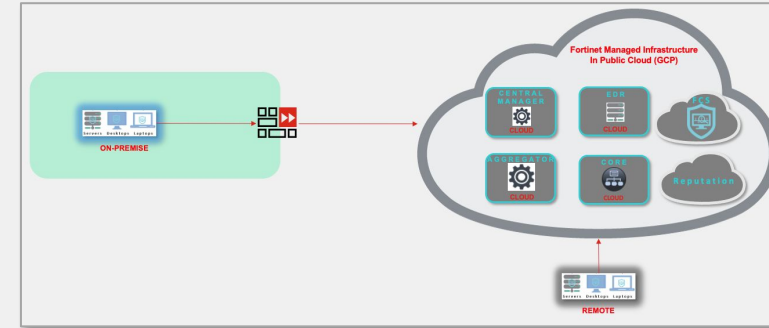


# 快速有效的端點資安防護



# 彈性部署架構

1. 雲端 = All components in the Cloud
2. 混合 = On Premise and in the Cloud
3. 地端 = All components on-prem (with FCS connection).



# FortiEDR – 優秀的端點安全防護方案

## 01 主動防護

### 強化端點安全能力

降低端點攻擊面風險+NGAV 機器學習  
強化端點安全防護能力以對抗新型態惡  
意程式與攻擊手法。

## 02 即時偵測

### 保持營運不中斷

通過端點系統即時監控、快速回應與恢  
復以降低突破性感染攻擊事件帶來的衝  
擊。

## 03 安全聯防

### 簡化安全維運

提供地端部署彈性選項！多樣的自動化  
回應動作，豐富的軌跡鑑識資訊以應對  
資安事件的調查與處理。

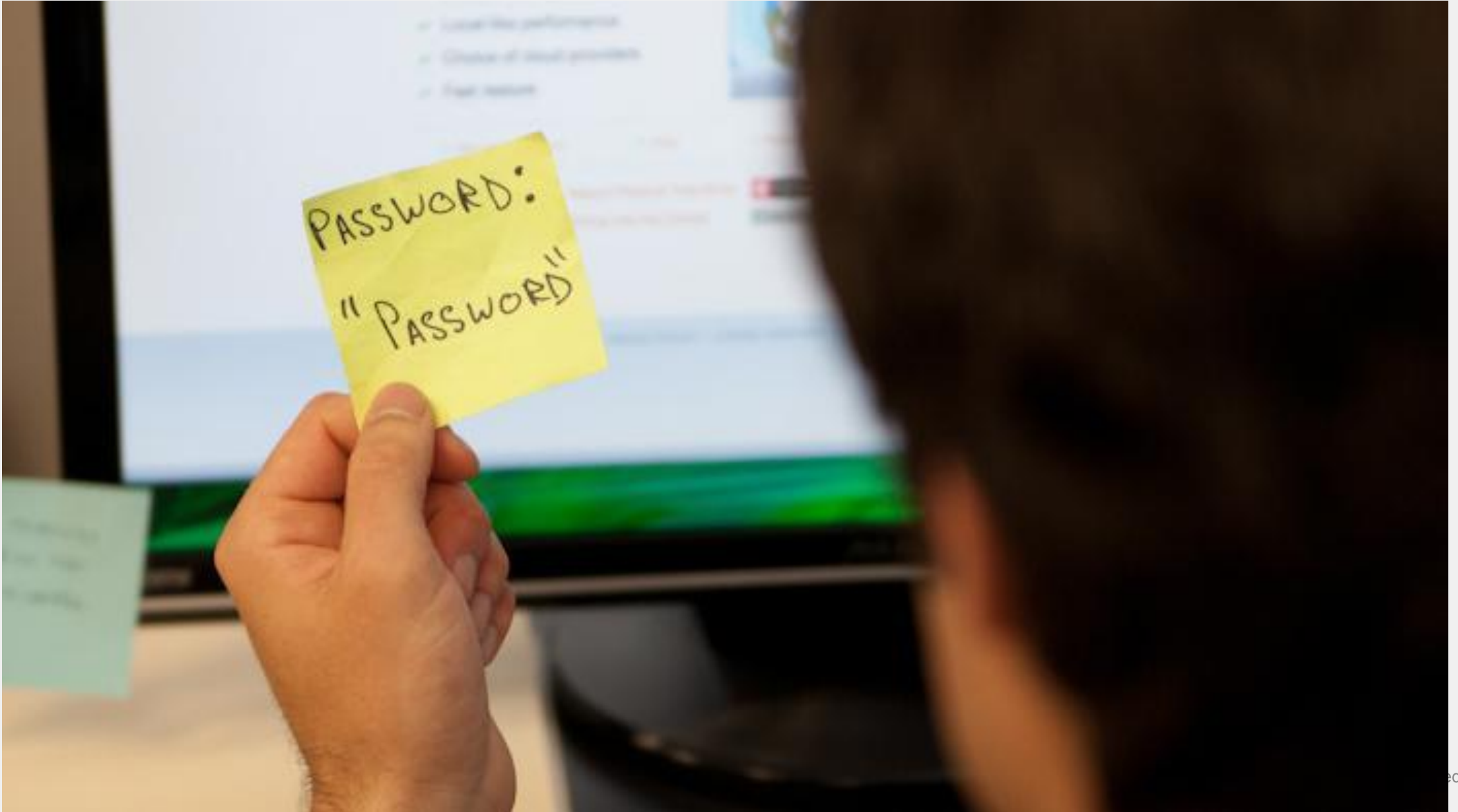




# 密碼小偷哭哭了



# 用戶的密碼強度.....？





# 密碼災難 ...

iThome 新聞 產品&技術 專題

IT EXPLAINED 全新企劃 Webinar

## 網釣

### Delivering origin-bound one-time codes over SMS Proposal

To address this, we propose a lightweight text format that services may adopt for such gets. It begins with (optional) human-readable text. After the human-readable text both single line, with sigils denoting which is which. This is the last line of the text. Here's an e

747723 is your FooBar authentication code.  
#fooBar.com #747723

| 雙因素驗證 | 動態密碼 | 2FA | 一次性密碼 |  
OTP | OTP簡訊 | 網釣 | 資安 | 身分驗證 | 身分  
認證

### 蘋果提出OTP簡訊格式草案，獲Google支持

為了提高以簡訊傳送動態密碼的安全性，蘋果提出改良版一次性密碼（OTP）簡訊格式，以避免使用者遭遇網釣攻擊

2020-02-04

### CISA STATEMENT ON IRANIAN THREATS



| 資安 | 伊朗 | 網軍 | 網路攻擊 | 關鍵基礎設施  
網釣 | 工控

### 美國土安全部警告企業， 伊朗可能發動網路攻擊

因美國在中東發動空襲炸死伊朗重要軍事將領，美方對內發出警告，留意伊朗網軍針對關鍵基礎設施業者以及各類組織發動

iThome 新聞 產品&技術 專題

IT EXPLAINED 全新企劃 Webinar

新聞

## 國發基金系統遭中國駭客

國發基金執行秘書蘇來守表示，遭駭創業投資電腦系統於6月28備份，沒有企業營運機敏資料；經數位遠端發現3個惡意程式和3階段，沒有發現資料竄改、外洩的跡象

文/黃彥霖 | 2021-07-23 發表



行政院國家發展基金管理會

關於本會 主要

## 假冒國泰世華網路銀行傳簡訊盜

2021-07-23 14:47 中央社台北電



刑事局今天表示，有民眾接獲「假冒國等字詞，經統計，3天內21人帳戶遭盜求證。



警政署刑事警察局透過新聞資料指出「假冒國泰世華網路銀行」詐騙簡訊，騙簡訊內的連結網址，恐被盜領。

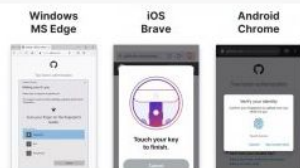


刑事局表示，詐騙簡訊內容為「您的銀則帳戶會被凍結無法使用」，若被害人網路銀行。

iThome 新聞 產品&技術 專題

IT EXPLAINED 全新企劃 Webinar

## 雙因素驗證



| GitHub | WebAuthn | 雙因素驗證

### GitHub使用者現可在更多 平臺使用實體安全金鑰， 作為第二身份驗證因素

GitHub服務擴大實體安全金鑰支援，在Windows、macOS和Linux上的Firefox和Chrome瀏覽器都能使用

2019-08-22

### How Android phone's security key works with iOS devices

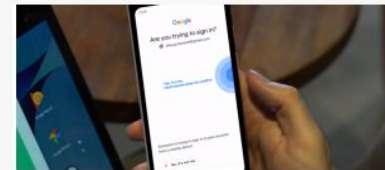


| Android手機 | 雙因素驗證 | iPhone | 2FA |  
2SV

### Android的2FA金鑰功能 延伸到iOS裝置

Android 7以上手機也可用來驗證用戶在iPhone、iPad上的Google帳號登入，只要使用者同時擁有Android手機和

2019-06-13



| 雙因素驗證 | 2FA | 安全金鑰 | google | 身分  
驗證

### Google將讓Android 7以 上手機當2FA安全金鑰

搭載Android 7.0以上系統的手機，在更新後都可當成FIDO 2/WebAuthn標準的安全金鑰，不再需要額外購買硬體金鑰

2019-04-11



| 臉書 | 雙因素驗證 | 2FA | 個資

### 臉書2fa手機號碼可能讓用 戶被任何人搜出來，而且 關不掉

繼去年被發現將用戶在雙因素驗證頁面（2fa）輸入的電話號碼，提供給外部廣告主之後，又有研究人員揭發臉書用戶在



| 釣魚郵件 | 駭客 | 2FA | 雙因素驗證 | Gmail |  
Yahoo

### 中東、北非人權人士也遭 駭客網釣信件鎖定，連雙 因素驗證機制也被突破

駭客用兩種方法繞過驗證，第一種是偷App密碼。某些信箱服務提供app密碼，可透過手機驗證登入，第二種是



| 釣魚郵件 | 雙因素驗證 | 2FA

### 伊朗駭客假冒Gmail和 Yahoo Mail遭駭通知信來 發送釣魚郵件，專門鎖定 記者、社運人士和官員

釣魚信件會將受害者導向假的Gmail或Yahoo Mail網頁，要求用戶驗證帳號、





# 強化帳號密碼安全的必要性

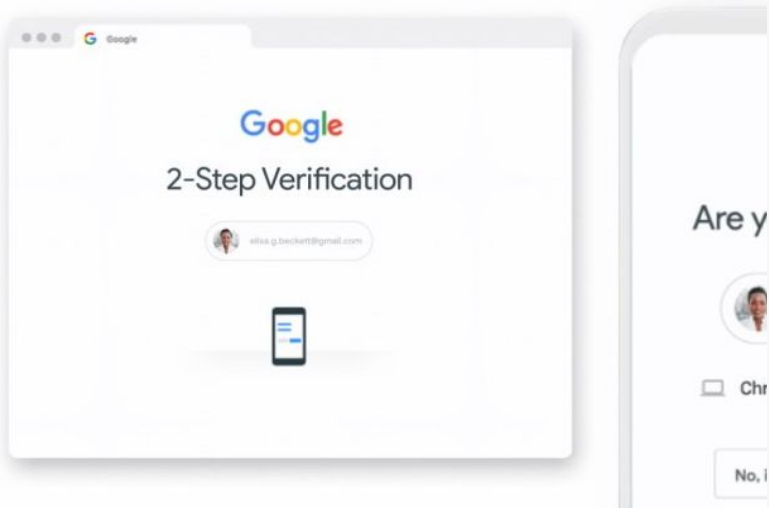
新聞

## Google將強制用戶啟動帳號雙因素驗證

Google將全面要求所有用戶透過Authenticator App、Google Titan以及Google Smart Lock登入Google帳號的第二層驗證機制

文/ 林妍臻 | 2021-05-07 發表

✓ 讀 6.6 萬



新聞

## 金融FIDO今年Q4啟動試辦，先從銀行業跨機構身分識別開始

金融行動身分識別標準化機制（金融FIDO）在今年Q4要啟動試辦，將採取集中式開發手機身分識別App，導入FIDO標準，綁定實體卡片，以提供跨機構身分識別功能。金管會也表示，要採用哪種實體卡片如自然人憑證、晶片金融卡等來開通金融FIDO，則還在討論中。

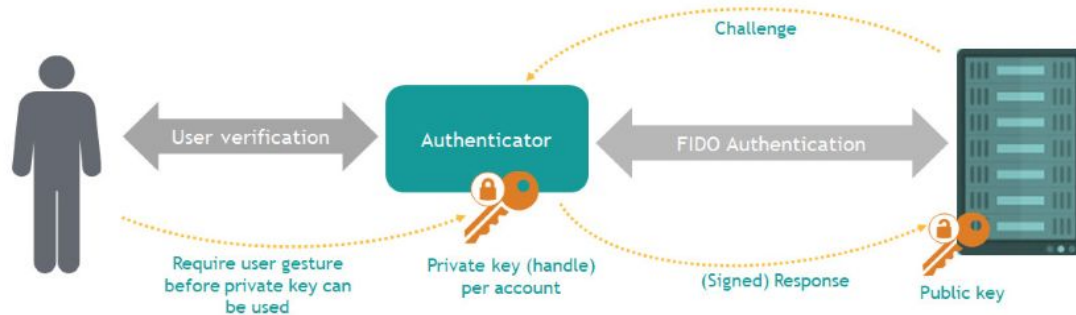
文/ 李靜宜 | 2021-06-15 發表

✓ 讀 6.6 萬 按讚加入iThome粉絲團

👍 讚 180

分享

### FIDO AUTHENTICATION



(示意圖，圖片來源 / FIDO Alliance)

### 迎向任何挑戰

Business security to meet any challenge

kaspersky

去年8月，金管會所發布的金融科技發展路徑圖中，有一大重點是要研究發展金融行動身分識別標準化機制（簡稱金融FIDO）。金管會在今天（6/15）宣布金融FIDO最新進展。

COMMScope RUCKUS

立即下載閱讀

抽 Häagen-Dazs 雪糕即享券 限外帶

雖然Google提供雙因素驗證（2-Step Verification），但目前仍允許用戶自行選擇，不強制Google帳號用戶啟用2SV。

Google身份與用戶安全產品管理

aws SUMMIT ONLINE TAIWAN

2021 AWS 台灣雲端高峰會

雲隨商轉 建構由我

9月2日 線上登場

iThome Weekly 電腦報

按讚追蹤 iThome 最新報導

✓ 讀 6.6 萬

第12屆iT邦幫忙鐵人賽獲獎主題

- Scrum Master使用Coaching的這回事
- 我說那個手機版
- 網頁阿尼翁，到底是在幹啥？
- 擁抱「資料結構」的「演算法」
- 看完眼眶濕濕的App開發者慘烈對抗險惡資安環境血與淚的控訴！



# 微軟/Google宣布啟動「無密碼登入」加速全球邁向無密碼時代

safety.google/intl/zh-TW\_tw/authentication/passkey/

Google 安全中心

總覽

Google 產品採用的防護機制

安全性與隱私權

內容安全

家庭安全

網路安全

安全性與隱私權 > 內建安全防護機制 > 驗證 > 密碼金鑰



## 無密碼登入 Google 帳戶，安全 又簡便

[https://safety.google/intl/zh-TW\\_tw/authentication/passkey/](https://safety.google/intl/zh-TW_tw/authentication/passkey/)

密碼金鑰可取代密碼，帶來更簡單安全的登入體驗。只要掃描指紋/臉孔或使用螢幕解鎖機制即可輕鬆登入。歡迎下載單頁簡介 PDF 瞭解詳



# 何謂無密碼身分驗證

## FIDO

FIDO (Fast IDentity Online) 聯盟[7]其使命為「身份驗證標準」，以幫助人們減少對密碼的過度依賴。FIDO聯盟促進認證和設備認證標準的開發、使用和遵守。FIDO協議為FIDO聯盟[8]所制定的一套網路識別標準，意在確保登入流程中伺服器及終端裝置協定的安全性。FIDO協議使用公開金鑰加密技術、多重要素認證與生物辨識特性進行認證，來提供更強的身份驗證。同時FIDO聯盟也確保所有利用FIDO核心規範的產品能夠協同工作，以提升全球無密碼身分驗證的兼容性和標準化。

## FIDO UAF

用戶安裝FIDO UAF 堆疊(Stack)設備後，可以選擇在終端裝置上透過各種生物辨識等方式，例如：輸入PIN、聲音辨識、指紋辨識，即可進行線上登入。結合生物辨識等認證途徑，提供使用者順暢的無密碼登入體驗。

## FIDO U2F

FIDO U2F允許雙因素驗證，用戶登入時需添加第二個驗證因素，以證明是否為本人，增強現有密碼基礎設施的安全性。該服務還可以在其選擇的任何時間提示用戶提供第二因素設備，例如：FIDO安全密鑰。

## FIDO2

FIDO2由WebAuthn規範和Client to Authenticator Protocol (CTAP) 組成。FIDO2通過嵌入式身份驗證，例如：生物識別或PIN，或用外部身份驗證，例如：FIDO安全密鑰、行動設備、可穿戴設備等，以支持無密碼、第二因素和多因素用戶體驗。



# 降低人性弱點的風險



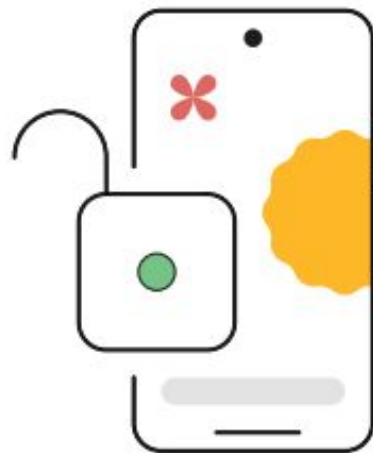
# 葫蘆裡賣什麼藥？



密碼金鑰由兩部分組成：  
您正在登入的網站的伺服器上的公開金鑰和裝置上對應的私密金鑰。



當您登入時，網站會檢查  
您的公開金鑰是否與您的  
私密金鑰相符。



若要驗證它是否相符，只  
需要求您解鎖裝置即可。



您將登入您的帳戶，您的  
私密金鑰和生物識別資訊  
將安全地保存在您的裝置  
上，並且永遠不會被 共享。

# 優點和缺點

## 優點:

1. 更高的安全性
2. 更好的使用者體驗
3. 降低 IT 成本
4. 更了解憑證的使用情況
5. 可擴展性

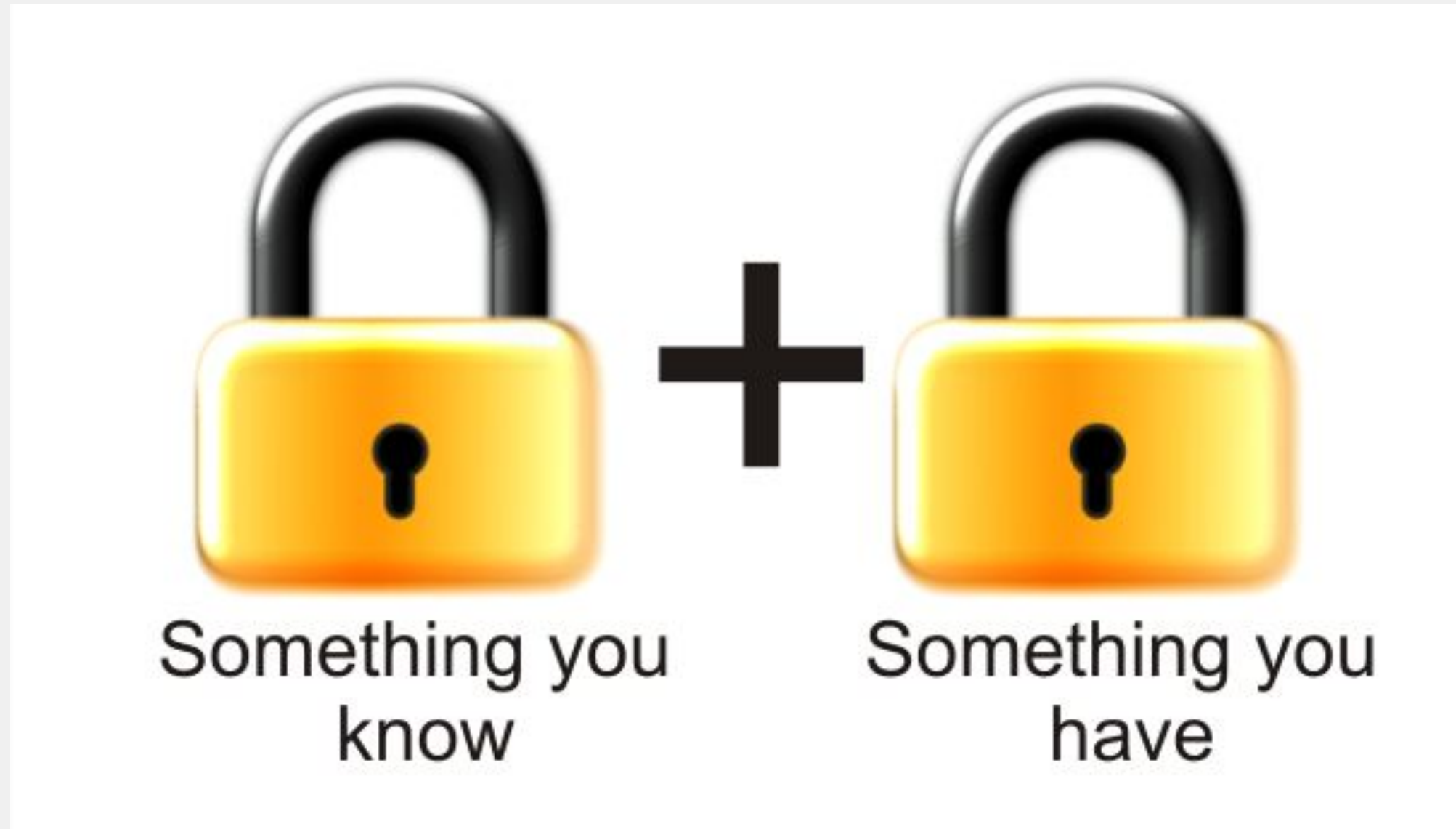
## 缺點:

1. 實施成本
2. 需要培訓和專業知識
3. 單點故障





# 何謂 雙因子認證 (Two factor Authentication)

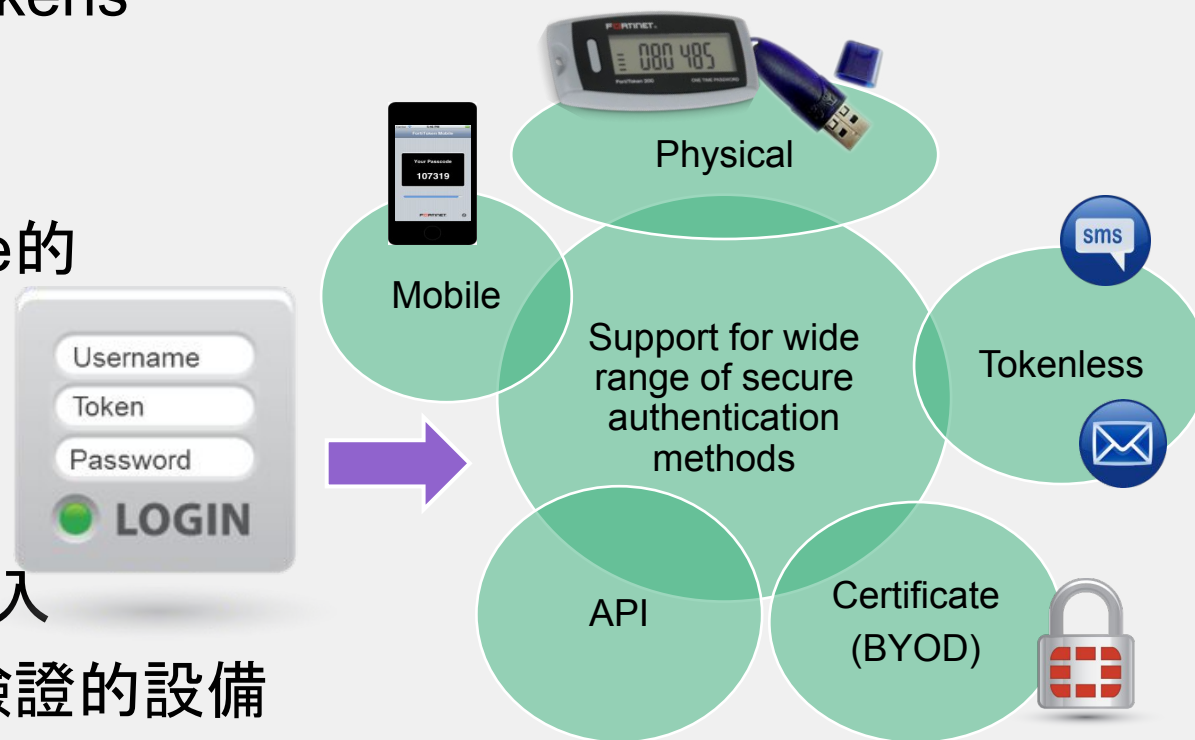


# 雙因子認證應用介紹

- 多樣化的 token 種類, 適應不同的應用需求
  - 相容 OATH 協定 TOTP (time) based tokens (FTK200)
  - USB certificate tokens (FTK300)
  - 適用 Android, iOS and Windows Mobile的 FortiToken Mobile
  - SMS 與 Email 動態密碼.

## 應用範圍

- Windows/Linux 伺服器或個人電腦的登入
- 任何可以透過Radius 通訊協定做身分驗證的設備
- Fortinet設備的管理登入驗證
- VPN連線的使用者登入驗證



# FortiToken Current Portfolio

## FortiToken Mobile



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

## FortiToken 210



Integrated with FortiClient™ and protected by FortiGuard • OATH TOTP compliant • OTP Timer • FTK-210 is FIPS 140-2 compliant

## FortiToken 310



Driverless USB device n High-performance smart card chip n FIPS140-2 Level 3 Certified n Windows, Linux, and MacOS supported

## FortiToken 410

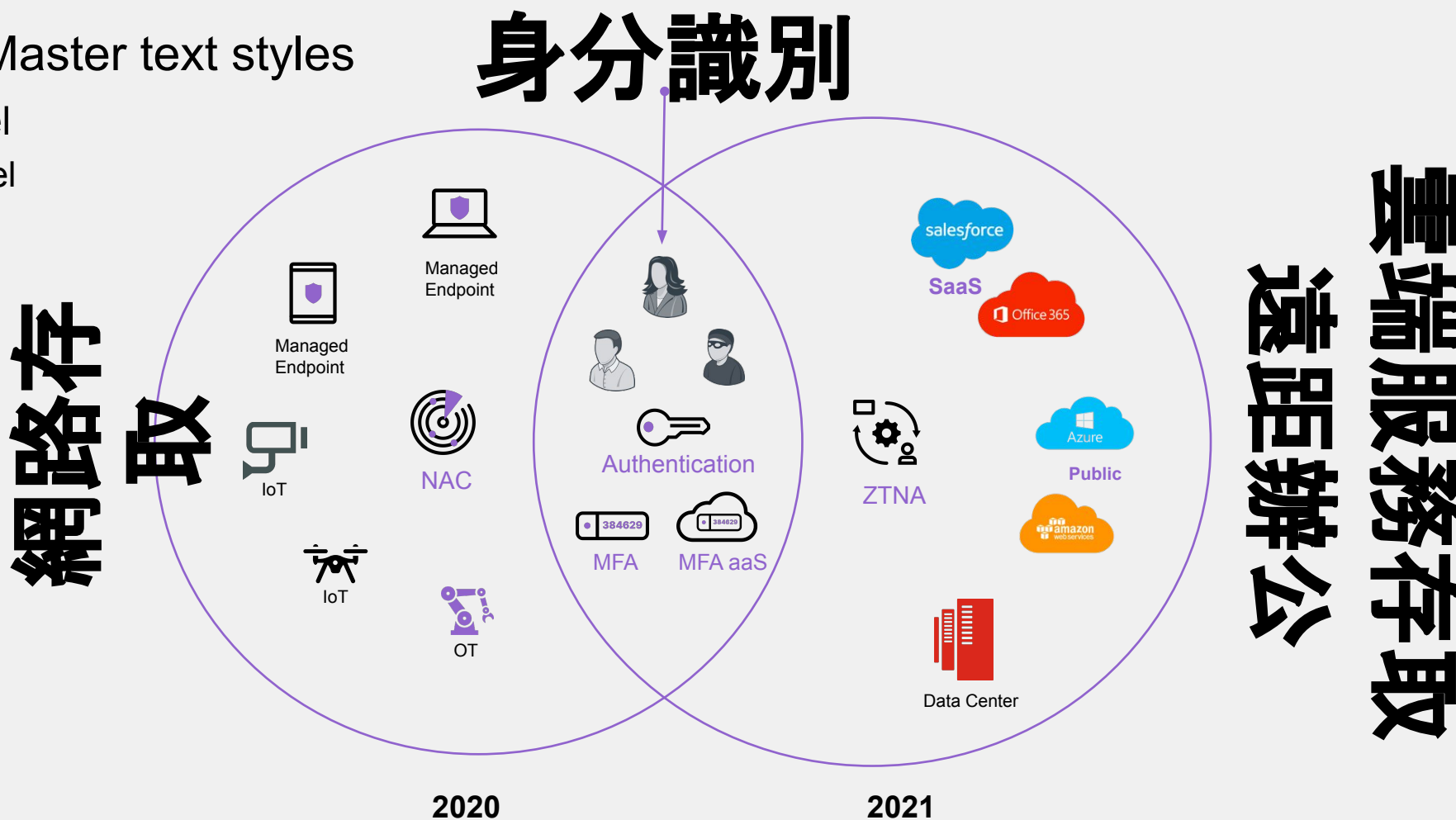


FIDO-enabled client (FortiClient) and browsers, or captive portal with FIDOenabled browsers n Protects users from phishing, password theft, and replay attacks



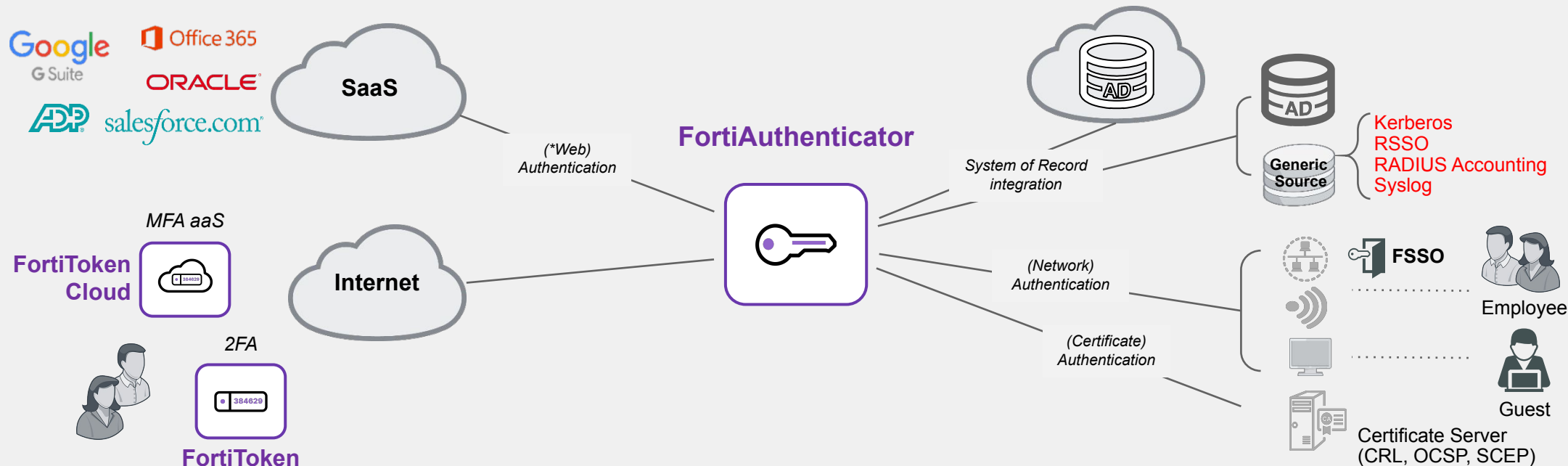
# 零信任的存取

- Click to edit Master text styles
  - Second level
  - Third level





# 集中管理、安全存取



## 帳號密碼強化

Establish identity through user log-in, adaptive, certificate, and/or multifactor input

## 權限控管

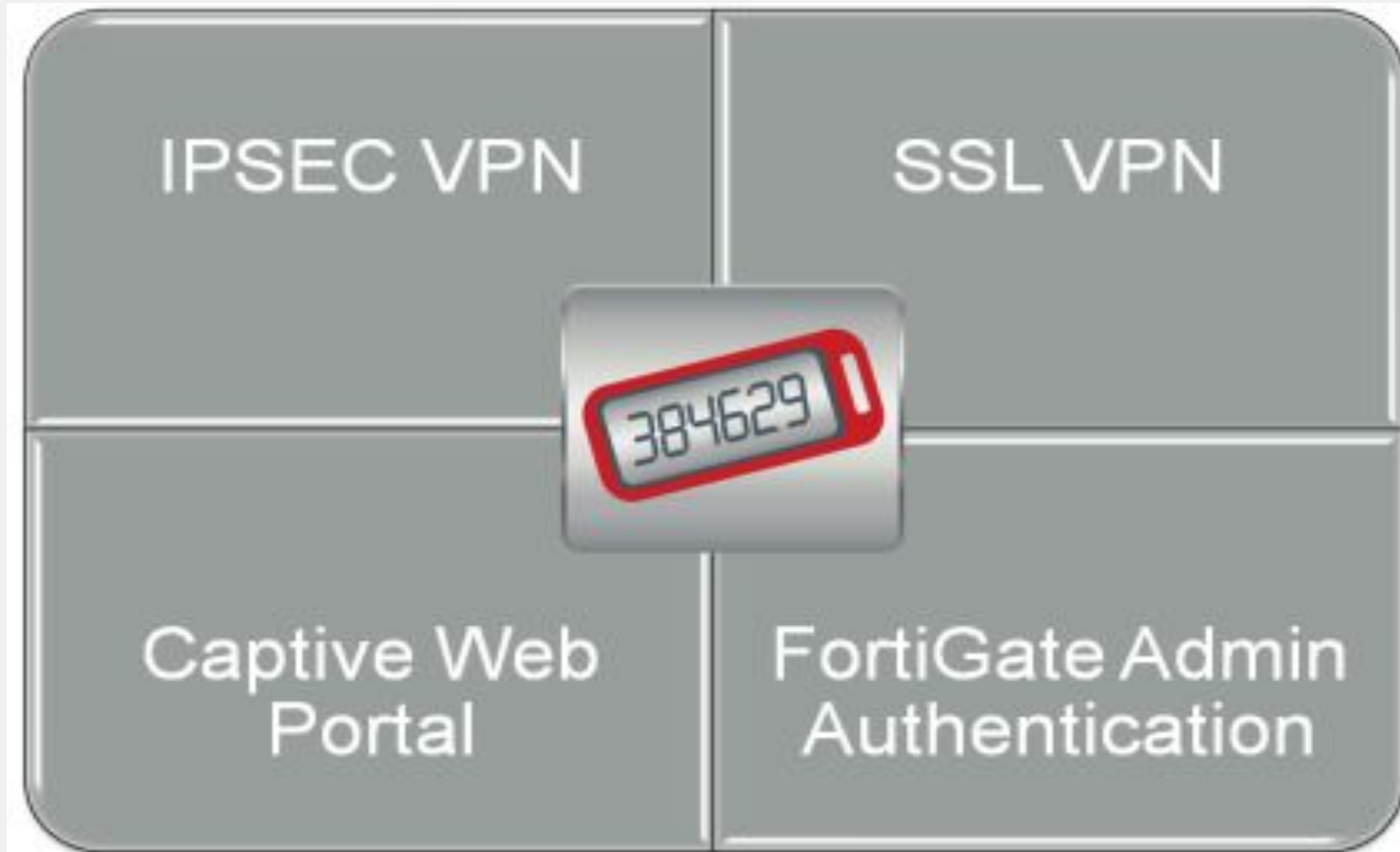
Provide information from authentication source for use in privileged access

## 單一登入

Improve security with improved user experience, i.e. reduce user login fatigue

\*(Web) Authentication: SAML2, oAUTH2, OIDC, RestAPI

# 2FA Native Authentication in FOS for:



FortiToken Common Use Cases

# 強化微軟作業系統的身分驗證

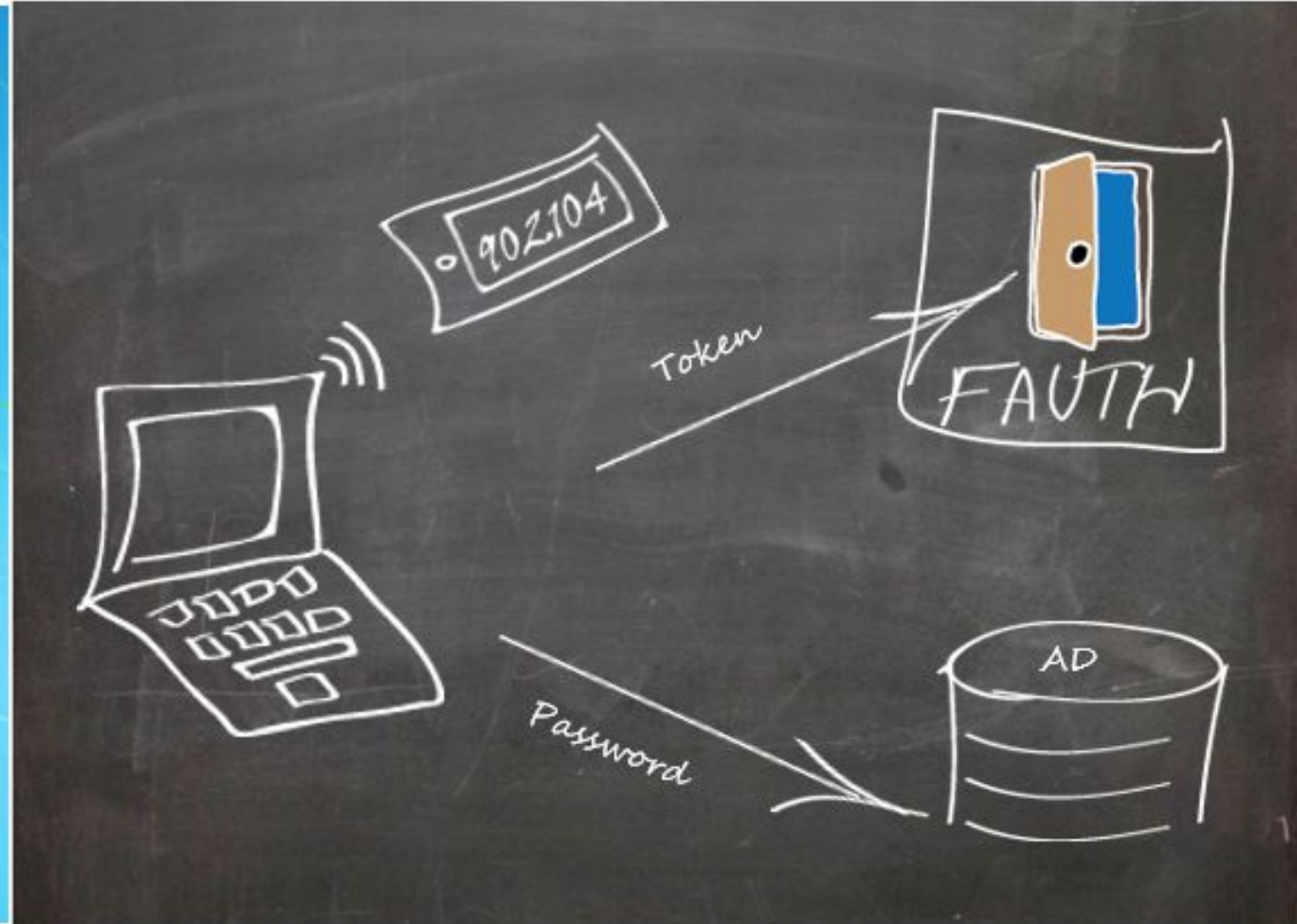
- Click to edit Master text styles

- » Second level

- Third level

- » Fourth level

- Fifth level



**FORTINET**

**SAML**



**CONFIDENTIAL**

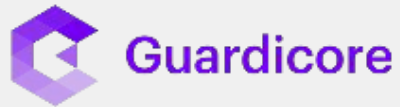
Access Limited to Authorized Personnel



# 開放式的整合生態 – 單一身分識別

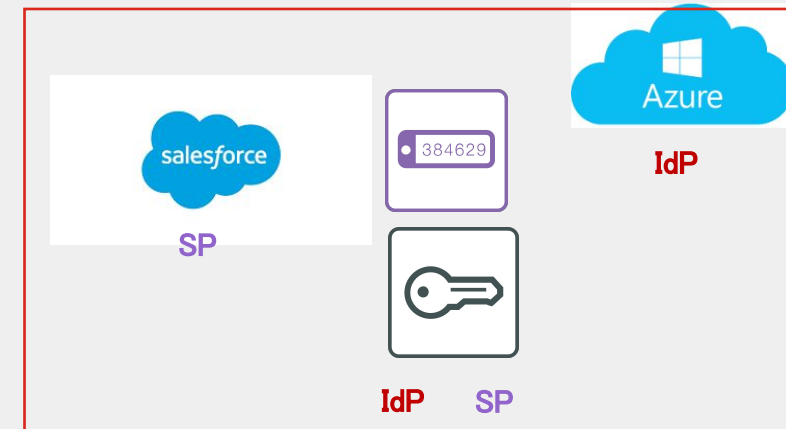
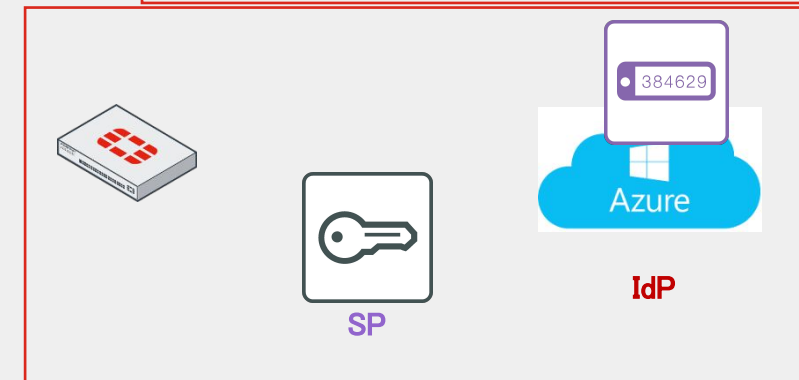
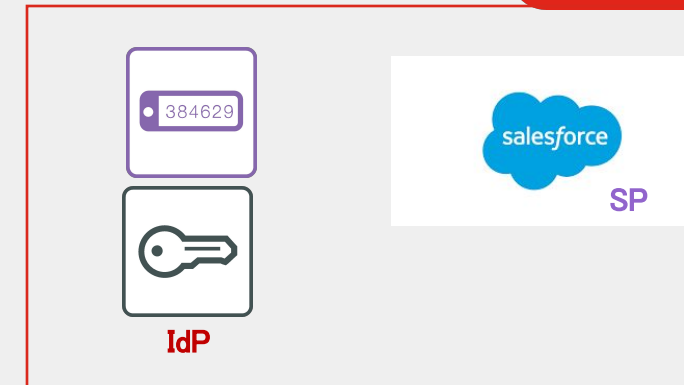
Technology Partners

PRE-VALIDATED. DOCUMENTED.

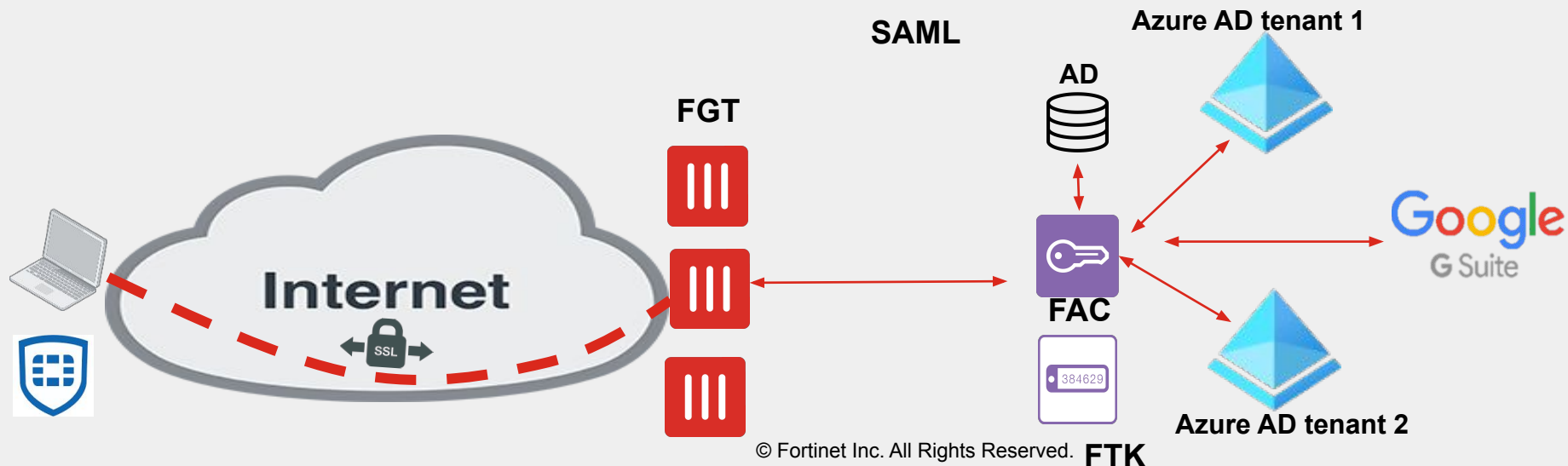
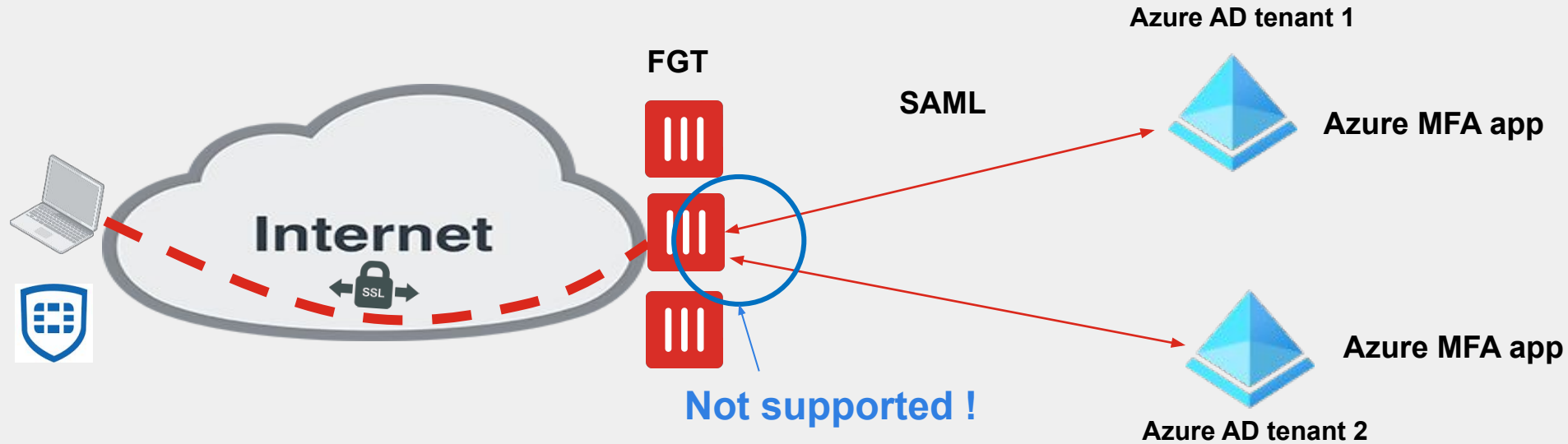


# FAC SAML roles and Use Cases

- FAC IdP
  - Identity centralized and stored on-prem on FAC (1<sup>st</sup> factor)
  - FAC 2FA with single Fortitoken and single app (2<sup>nd</sup> factor)
  - SSO to multiple internal and external services/applications
- FAC SP
  - Identity centralized and stored at cloud identity providers (1<sup>st</sup> factor)
  - Cloud IdP 2FA with single Fortitoken and single app (2<sup>nd</sup> factor)
  - Push user + group membership + IP via FSSO to Fortigate
- FAC “IdP Proxy”
  - Identity centralized and stored at cloud identity providers (1<sup>st</sup> factor)
  - FAC 2FA with single Fortitoken and single app (2<sup>nd</sup> factor)
  - Customer using FAC and Fortitoken already for other use case (e.g. hybrid on-prem and cloud users)
  - SSO to multiple internal and external services/applications

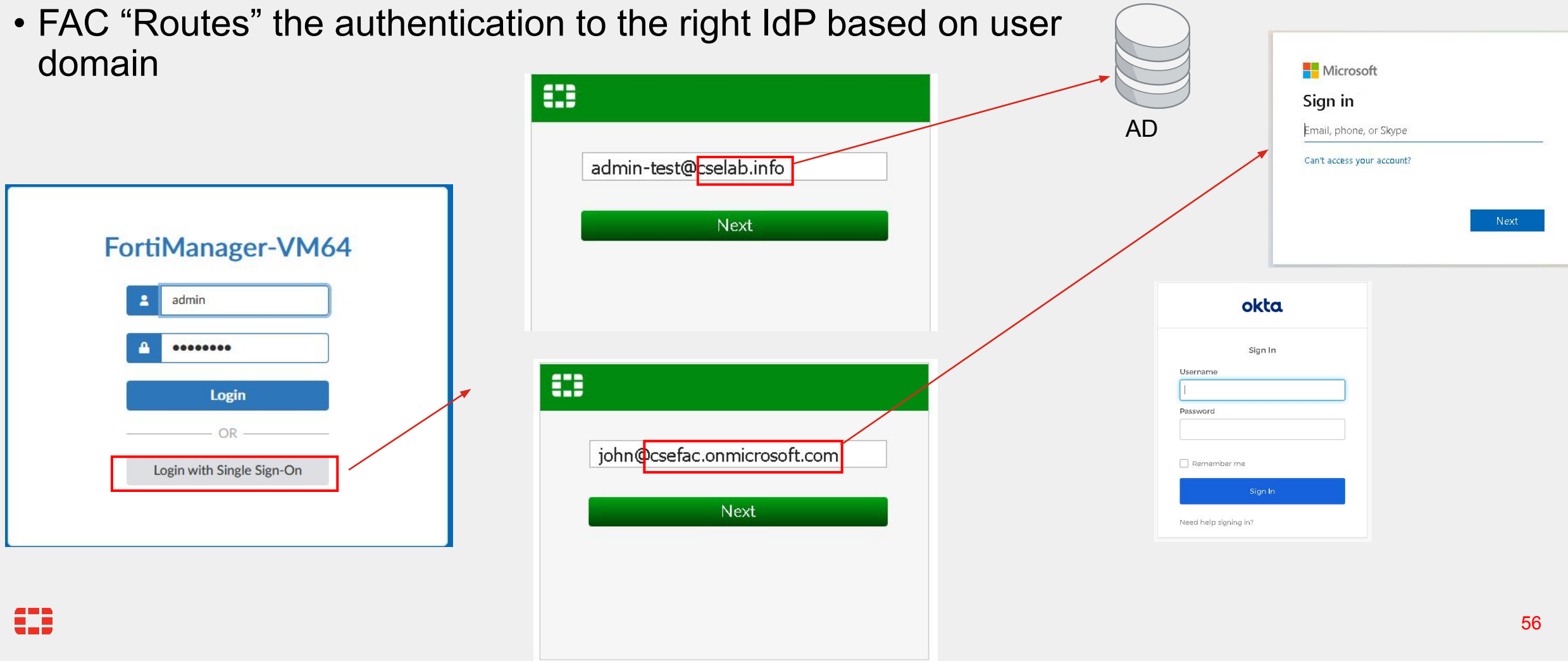


# Why do we need FAC IdP proxy ?



# SAML IdP Resolution for IdP Proxy with multiple external IdPs

- SAML authentication – users belong to multiple IdPs databases
- FAC “Routes” the authentication to the right IdP based on user domain



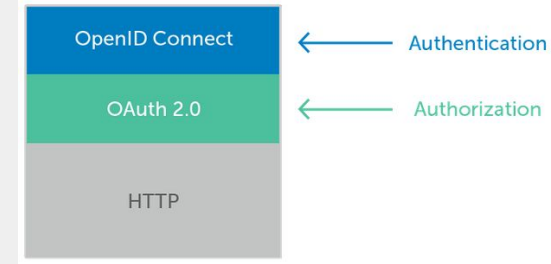




OAuth / OIDC



# OpenID Connect (OIDC) introduction



- Standard used for user-authentication ([https://openid.net/specs/openid-connect-core-1\\_0-final.html](https://openid.net/specs/openid-connect-core-1_0-final.html))
- Based on OAuth 2.0 framework (RFC 6749)
  - Uses REST/JSON
  - Issues Access Token
  - Authorization code flow
- OIDC
  - Specifies authentication flows
  - Issues **ID Token** which contains **Claims** which are used to communicate information about the End-user (similar in concept to SAML “attributes”)
  - Used for SSO - similar to SAML which uses XML instead of REST/JSON – but not limited to web browsers

# OIDC - details

- Concepts

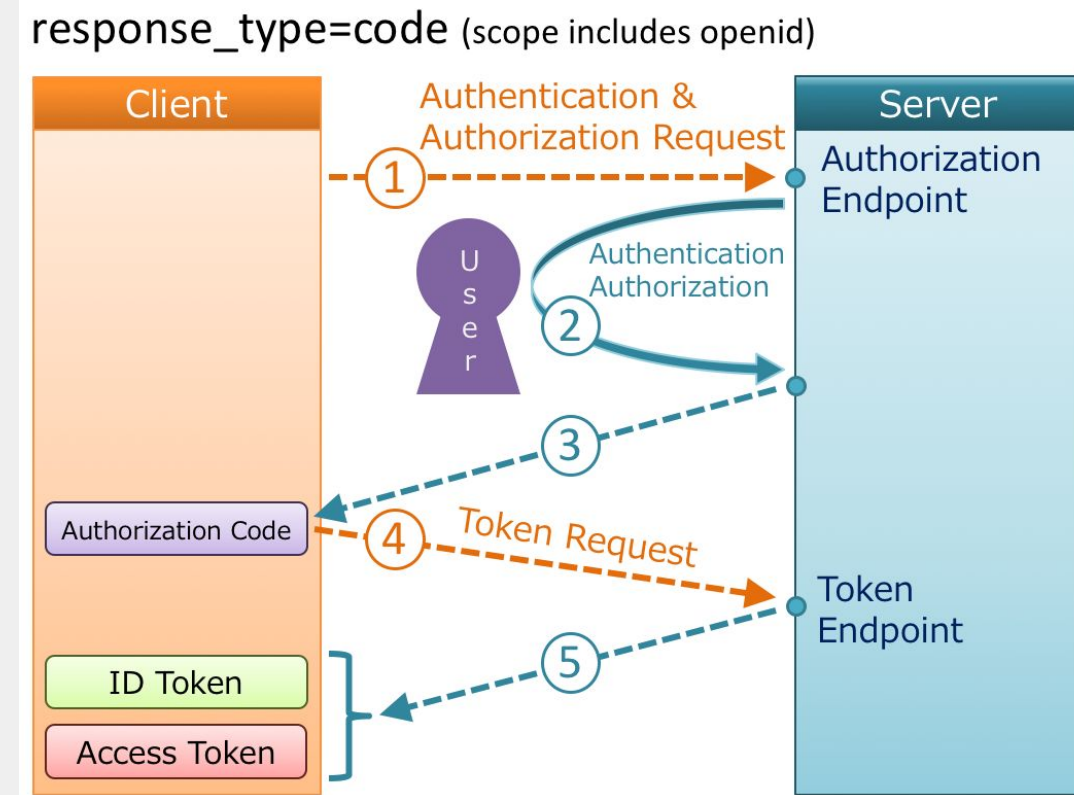
- OP (OpenID Provider) is the server - user repository and “authorization server” (IdP equivalent i.e. FAC)
- RP (Relying Party) is the “client” – application (SP equivalent)
- End User is the equivalent of OAuth “Resource owner” – smartphone app or web browser

- 3 flows

- **Authorization Code Flow with optional PKCE**
- Implicit Flow
- Hybrid flow

# OIDC “Authorization Code” flow

- Uses OAuth 2.0 “Authorization code” grant type flow
- Steps (as per OIDC standard 3.1.1)
  1. Client prepares an Authentication Request containing the desired request parameters.
  2. Client sends the request to the Authorization Server.
  3. Authorization Server Authenticates the End-User.
  4. Authorization Server obtains End-User Consent/Authorization.
  5. Authorization Server sends the End-User back to the Client with an Authorization Code.
  6. Client requests a response using the Authorization Code at the Token Endpoint.
  7. Client receives a response that contains an ID Token and Access Token in the response body.
  8. Client validates the ID token and retrieves the End-User's Subject Identifier.
  9. RP can use Access Token with the /oauth//userinfo/ endpoint to retrieve more info about user





# Key Differences Summarized:

Feature	OAuth 2.0	OpenID Connect (OIDC)
Primary Goal	Authorization	Authentication
Focus	Access to resources	User identity verification
Token Type	Access token, Refresh token	ID token, Access token, Refresh token
Relationship	Foundation for OIDC	Built on top of OAuth 2.0
Use Cases	Accessing APIs, authorizing apps to use resources	Logging in users, verifying identity



# Identity and Access Management Use-Cases

## SSO Cloud Apps Two-Factor Authentication Using SAML 2.0

### Standardization

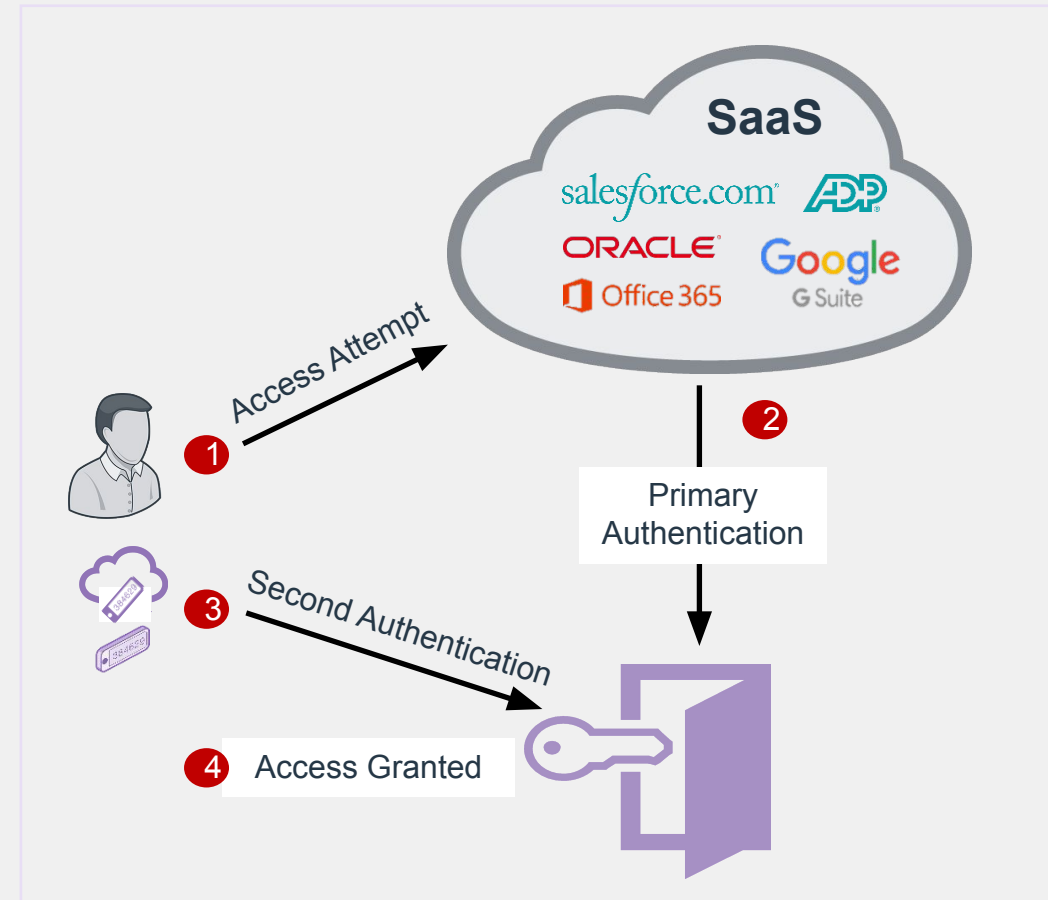
Provides Seamless Cloud Authentication.  
Supports SAML 2.0 IdP-Initiated,  
SP-Initiated and IdP Proxy flows

### Improved User Experience

Users sign-in Once, No further  
Authentication to Use other Cloud Apps

### Increased Security

A Single Point of Authentication with  
Two-Factor



# 使用情境 – 單一登入加上雙因子驗證

## 標準化的單一登入機制

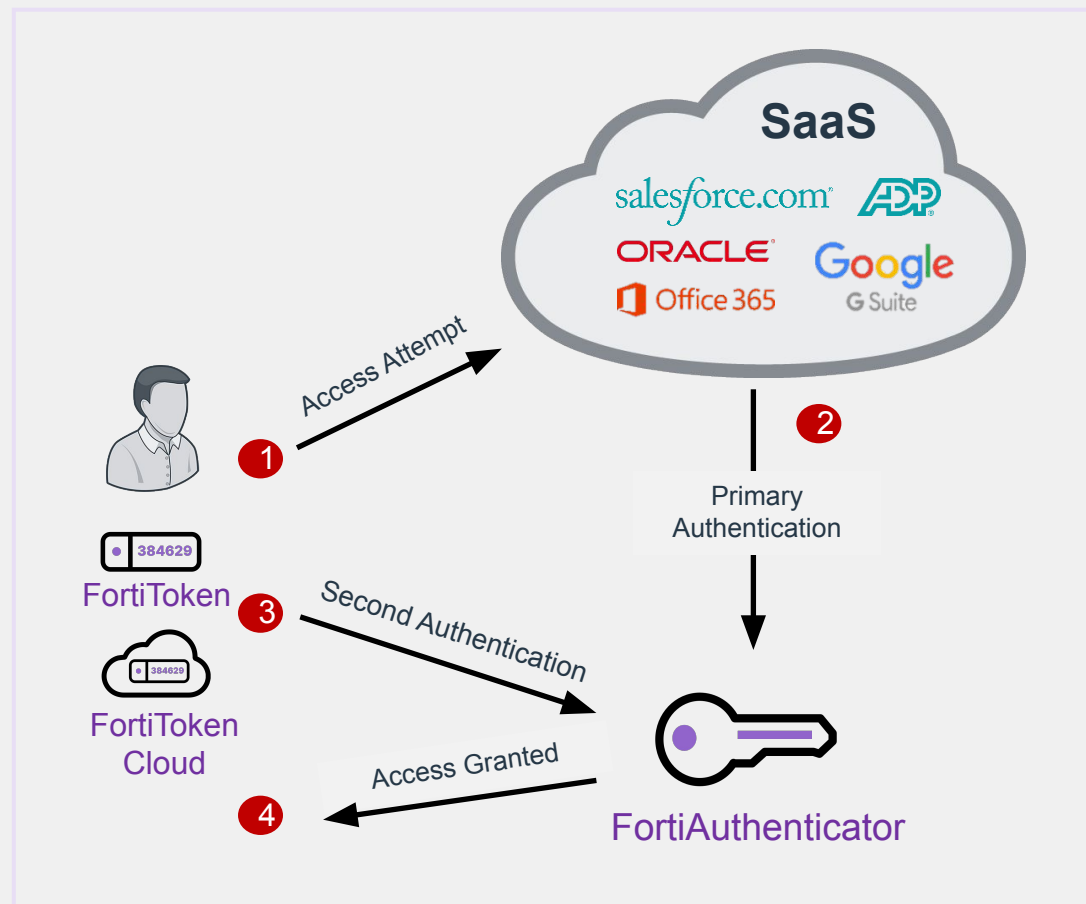
Provides Seamless Cloud Authentication.  
Supports SAML 2.0 IdP-Initiated, SP-Initiated and  
IdP Proxy flows

## 提供使用者方便性

Users sign-in Once, No further Authentication  
required to use other cloud apps

## 增加安全性 – 降低密碼被竊的機率

A single point of strong authentication, minimizing  
the overwhelming password syndrome



# 迎接WiFi 7的到來!



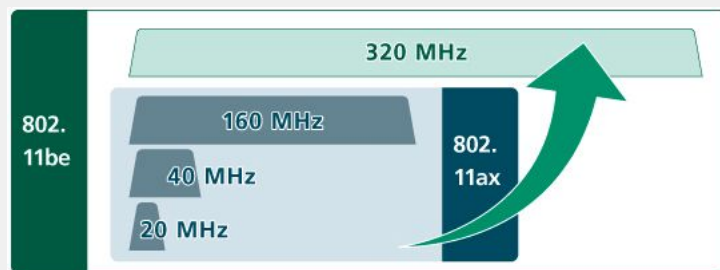
This content is shared exclusively with the **CTO Office** and **Product Management** teams and is considered void if transferred to (or presented by) anyone outside of this group. The contents are for individual use and should not be copied, transferred, uploaded or shared to anyone without written consent. © Fortinet Inc. All Rights Reserved.

**CONFIDENTIAL**

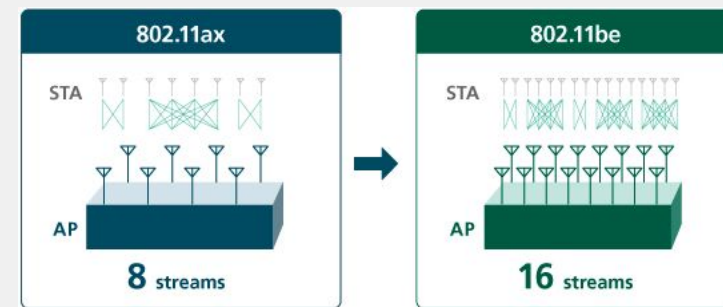
Access Limited to Authorized Personnel

# 802.11be – Extremely High Throughput (ETH)

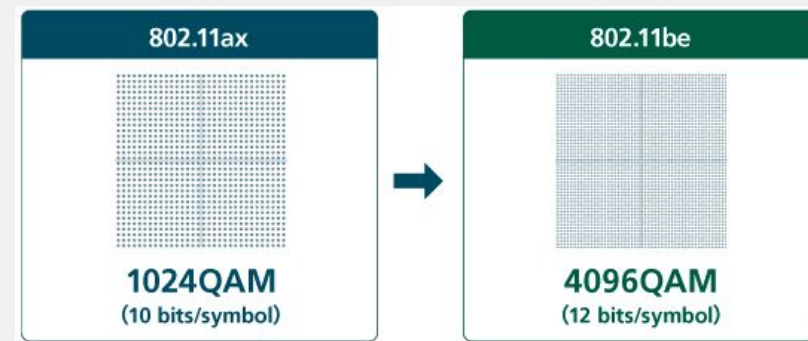
IEEE802.11		11b	11g	11n	11ac	11ax	11be
Transmission Vector Format		Non-HT (Non-High Throughput)	Non-HT (Non-High Throughput)	HT (High Throughput)	VHT (Very High Throughput)	HE (High Efficiency)	EHT (Extreme High Throughput)
Definition		1999	2003	2009	2014	2021	Planned in 2024
Freq.	2.4 GHz	✓	✓	✓		✓	✓
	5 GHz			✓	✓	✓	✓
	6 GHz					✓	✓
Bandwidth [MHz]		22	20	20/40	20/40/80/160/80+80	20/40/80/160/80+80	20/40/80/160/320
Maximum throughput rate [bps]		11M	54M	540M	6.93G	9.6G	30G~
Modulation scheme		DBPSK DQPSK	BPSK QPSK 16QAM 64QAM	BPSK QPSK 16QAM 64QAM	BPSK QPSK 16QAM 64QAM 256QAM	BPSK QPSK 16QAM 64QAM 256QAM 1024QAM	BPSK QPSK 16QAM 64QAM 256QAM 1024QAM 4096QAM
Stream				4x4	8x8	8 Steam OFDMA	16 Stream OFDMA



Wider Channels



More Special Streams



More Symbols



# Need for Speed

		x 11.5	x 1.3	x 4.8
	<b>Wi-Fi 4</b>	<b>Wi-Fi 5</b>	<b>Wi-Fi 6/6E</b>	<b>Wi-Fi 7</b>
Standard	802.11n	802.11ac	802.11ax	802.11be
Max Speed with 1 Spatial Stream	150 Mbps	866.7 Mbps	1.2 Gbps	2.9 Gbps
Max Speed with 2 Spatial Streams	300 Mbps	1.73 Gbps	2.5 Gbps	5.8 Gbps
Max Speed with Max # Spatial Streams	600 Mbps	6.92 Gbps	9.6 Gbps	46.4 Gbps





# FortiAP Series

Protected by FortiGuard



Protected by FortiGuard

802.11ac  
**w1**

802.11ac  
**w2**

802.11ax  
**Wi-Fi 6**

802.11ax  
**Wi-Fi 6E**

802.11be  
**Wi-Fi 7**

FAP SUFFIX

**C**

**SUNSET**

FAP SUFFIX

**E**

**SUNSET**

FAP SUFFIX

**F**

**SUNSET**

FAP SUFFIX

**G**

**SUNSET**

FAP SUFFIX

**K**

**SHIPPING  
NOW**



This content is shared exclusively with the **CTO Office** and **Product Management** teams and is considered void if transferred to (or presented by) anyone outside of this group. The contents are for individual use and should not be copied, transferred, uploaded or shared to anyone without written consent. © Fortinet Inc. All Rights Reserved.

**CONFIDENTIAL**

Access Limited to Authorized Personnel

# Wi-Fi Evolution

## Standards Evolution

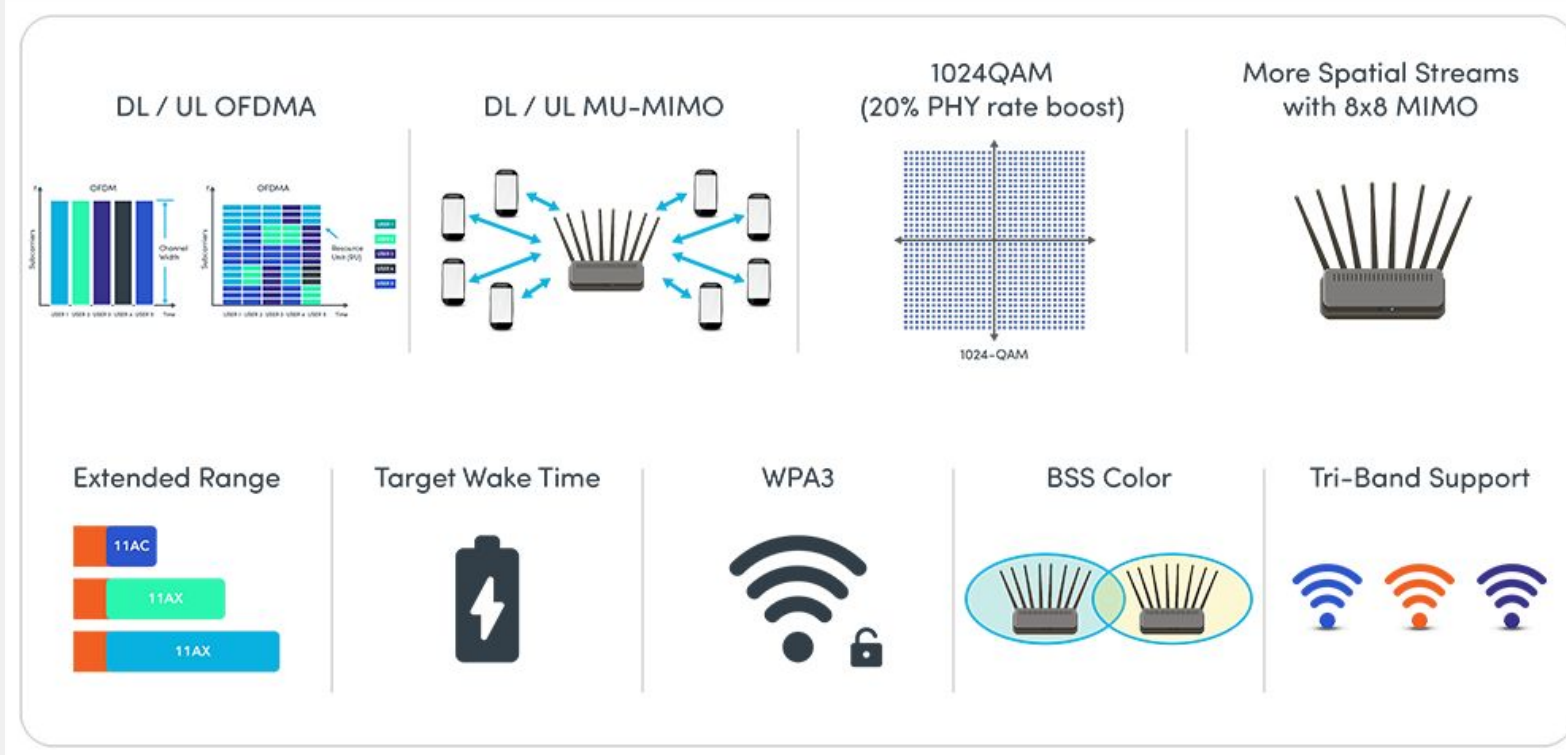


## Spectrum Evolution



# Key Technology Advancements

## Wi-Fi 6/6E Improvements Over Wi-Fi 5



### Better Performance

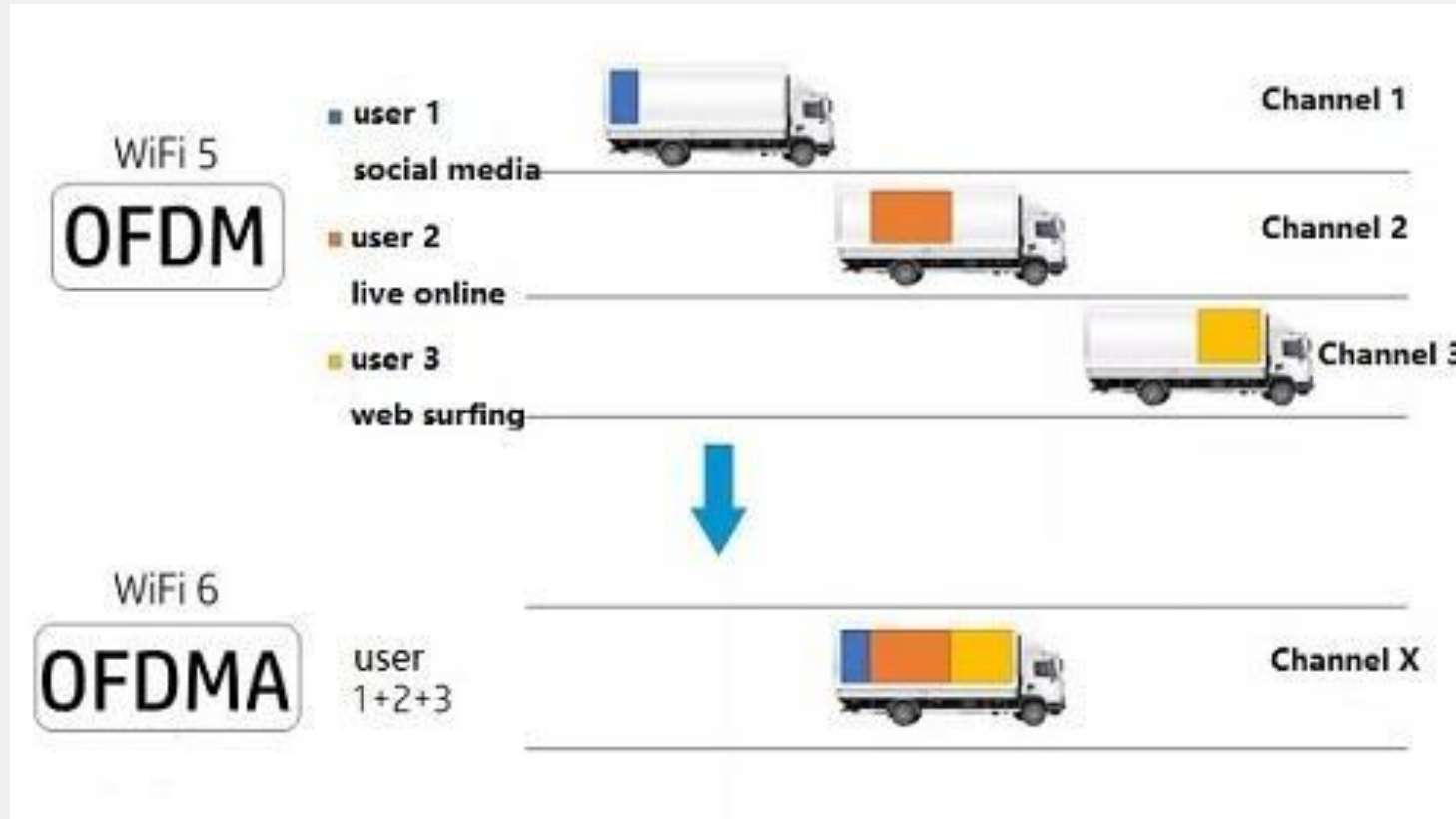
- Multiuser, multiple input, multiple output (**MU-MIMO**)
- Orthogonal frequency division multiple access (**OFDMA**)
- 1024-quadrature amplitude modulation (**QAM**)

### Better Security

- Wi-Fi Protected Access 3 (**WPA3**)
- Simultaneous Authentication of Equals (**SAE**)
- Protected Management Frames (**PMF**)

# Wi-Fi 6/6E/7 Advancements

## OFDMA



**Orthogonal frequency division multiple access (OFDMA):** Divides a Wi-Fi channel into smaller frequency allocations known as resource units. This allows an AP to communicate with multiple clients by assigning them to specific resource units.



# Wi-Fi 6/6E/7 Advancements

## MU-MIMO



### OFDMA

- Improves performance & efficiency
- Reduces latency
- Suits low BW applications

### MU-MIMO

- Boost capacity
- Provide High speed connectivity
- Suits High BW applications

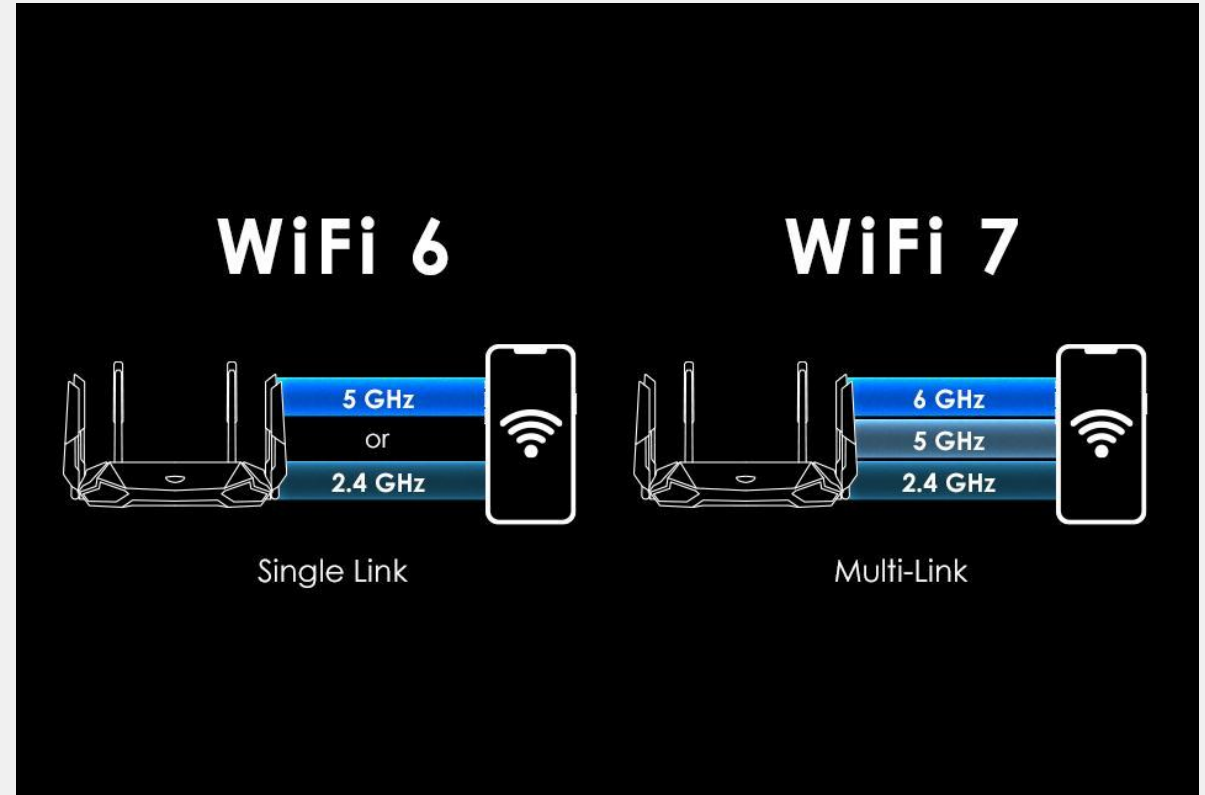
### Multiuser, multiple input, multiple output (MU-MIMO):

Allows a Wi-Fi AP to communicate with multiple devices simultaneously, improving the overall Wi-Fi experience. MU-MIMO can significantly improve throughput in high-density networks, even in those that use bandwidth-intensive services.



# Wi-Fi 7 – Multi Link Operation

- Wi-Fi 7 can deliver massive throughput gains
- Thanks to a wider channel and capacity gains from 6GHz spectrum.
- Wi-Fi 7 can deliver peak rates of over 40 Gbps, a 4X increase over Wi-Fi 6/6E.
- Wi-Fi 7 introduces multiple combinations of multi-link options that can significantly increase throughput and reduce latency.



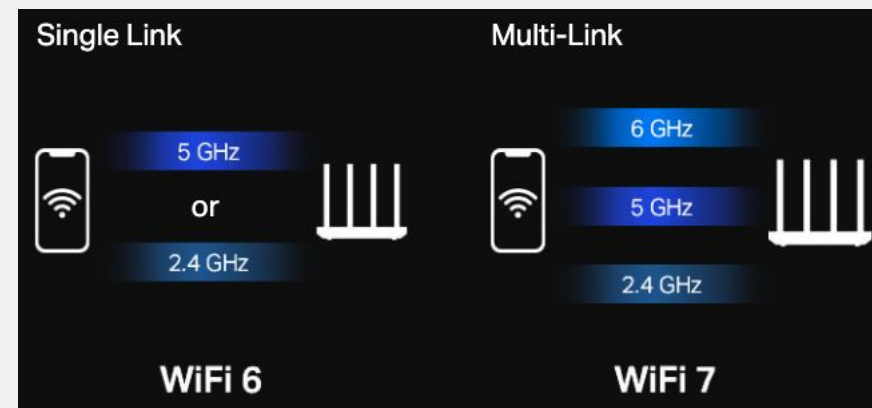
# MLO - Multi-Link Operation Goals

Higher Speed, Lower Latency, More Reliable  
Multi-Link Operation.

Traditional Wi-Fi devices use a single link to  
transmit data.

With Multi-Link Operation (MLO), Wi-Fi 7  
enables devices to simultaneously send and  
receive data across different frequency bands  
and channels to increase throughput, reduce  
latency, and improve reliability.

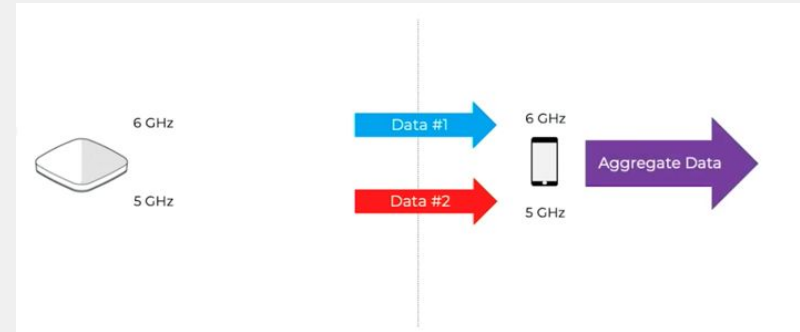
Beneficial for emerging applications like  
VR/AR, online gaming, remote offices, and  
cloud computing.



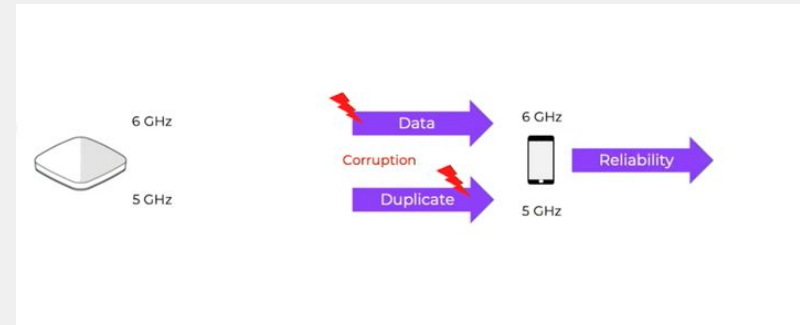
Goal	MLO method
Higher Throughput	Link aggregation
Lower Latency	Link steering
Increases Reliability	Link redundancy

# Multi-Link Modes

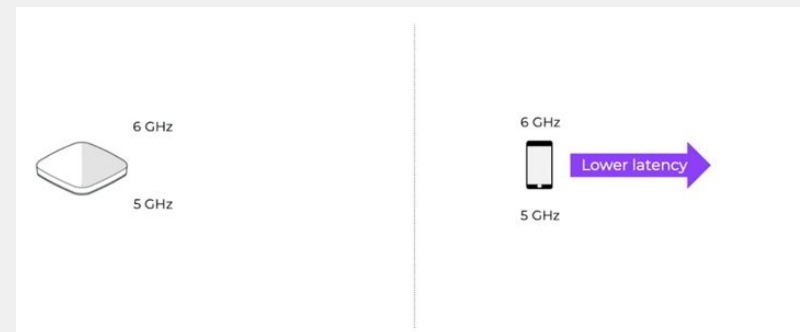
## Data Aggregation



## Data Redundancy



## Link Steering



# 6 GHz Support WPA3 only

No more “open” unencrypted SSIDs – They will be replaced with (OWE) Opportunistic Wireless Encryption

No more PSK security – Replaced entirely with (SAE) Simultaneous Authentication of Equals

Also will be required (MFP) Management Frame Protection

No backwards compatibility with WPA2 or OPEN – NO transition modes





# WPA3 - Highlights



- Next Gen Wi-Fi security from WFA, simplifies and enhances Wireless security
- Robust Authentication, greater cryptographic strength – more protection regardless of password complexity
- Disallows legacy protocols (TKIP)
- Requires PMF
- Transition mode with WPA2 (same SSID with same PSK WPA2 and WPA3)
- Forward secrecy – SAE handshake means PMK cannot be recovered if password becomes known
- Easier, secure onboarding of IoT and Wi-Fi networks
- Higher level of protection in Open Networks (OWE)
- Optional min 192-bit security for sensitive environments
- No susceptible to KRACK (replay attack) vulns



# Wi-Fi 6E/7 Different Securities on Different SSIDs

**No backwards  
compatibility  
legacy support**

**WPA-3 on 6 GHz  
and WPA-2 on  
5GHz**

5 GHz Channel (32)

SSID: **Employee**  
WPA2-Enterprise (802.1x)

SSID: **BYOD**  
WPA2-Personal (PSK)

SSID: **Guest**  
Open

SSID: **IoT**  
WPA2-Personal (PSK)



6 GHz Channel (101)

SSID: **Employee**  
WPA-3-Enterprise (802.1x)

SSID: **BYOD**  
WPA3-Personal (SAE)

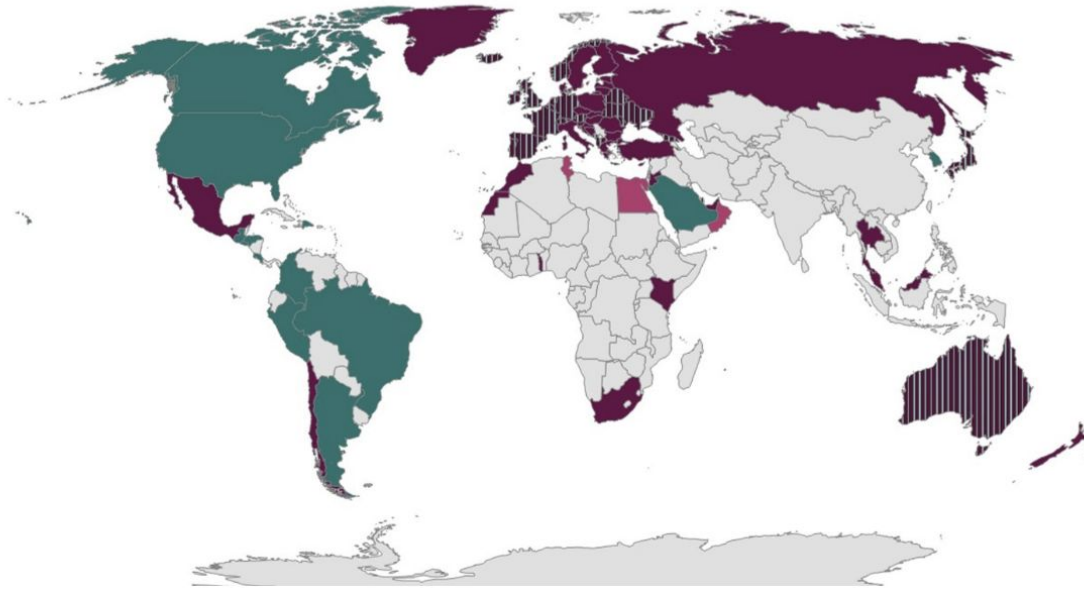
SSID: **Guest**  
Enhanced Open (OWE)



# Countries Enabling Wi-Fi in 6GHz(Wi-Fi 6E/7)

## Countries Enabling Wi-Fi in 6 GHz (Wi-Fi 6E)

- Adopted 5925-6425 MHz
- Adopted 5925-7125 MHz
- ▨ Adopted 5925-6425 MHz, Considering 6425-7125 MHz
- Considering 5925-6425 MHz



Most recent updated information on countries adopting to Wi-Fi 6E around the world.

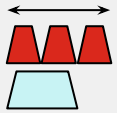
<https://www.wi-fi.org/countries-enabling-wi-fi-in-6-ghz-wi-fi-6e>

# Wi-Fi 6E / 7 – 6 GHz Frequency / More Channels!

2.4 GHz

3 x 20 MHz  
1 x 40 MHz

60 MHz of Spectrum

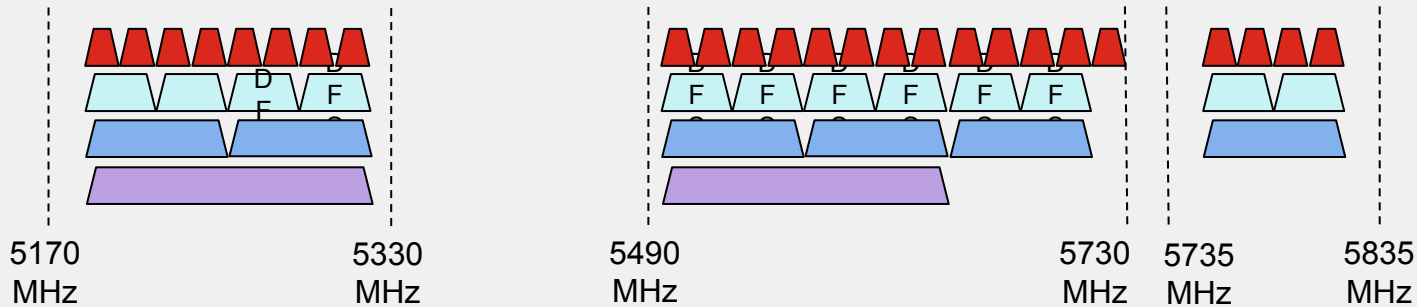


More than 2X channels!  
Fourteen 80MHz  
channels!

5 GHz

25 x 20 MHz  
12 x 40 MHz  
6 x 80 MHz  
2 x 160 MHz

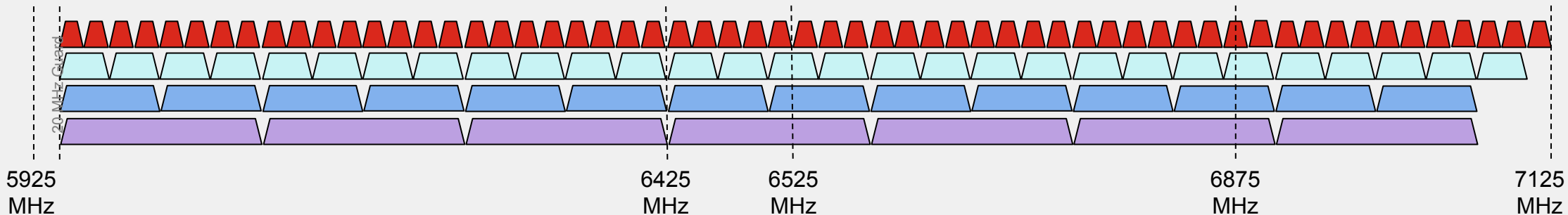
500 MHz of Spectrum



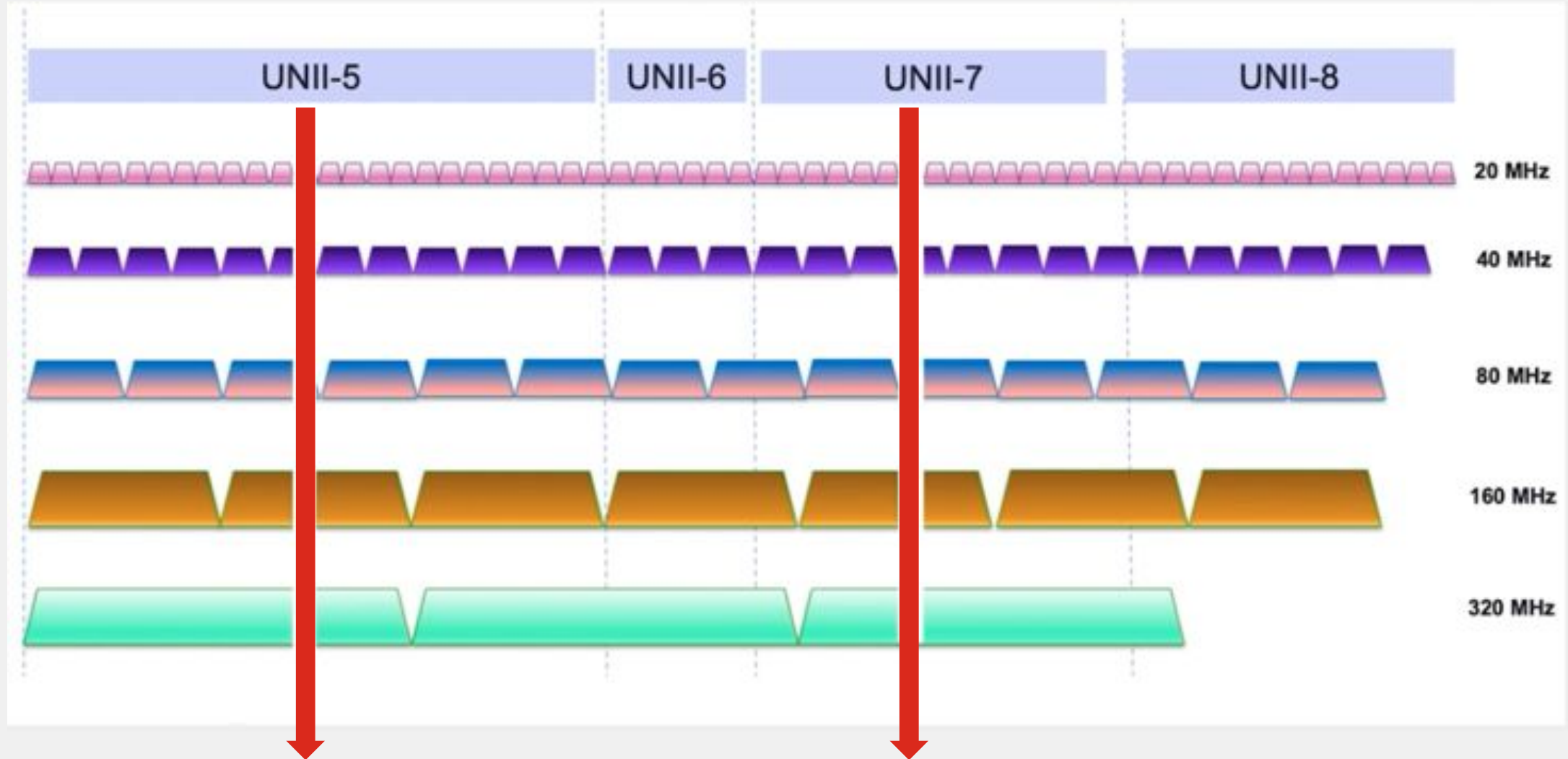
6 GHz

59 x 20 MHz  
29 x 40 MHz  
14 x 80 MHz  
7 x 160 MHz

1,200 MHz of Spectrum



# Puncturing in 6GHz







# 6 GHz AFC ( Unlicensed band )

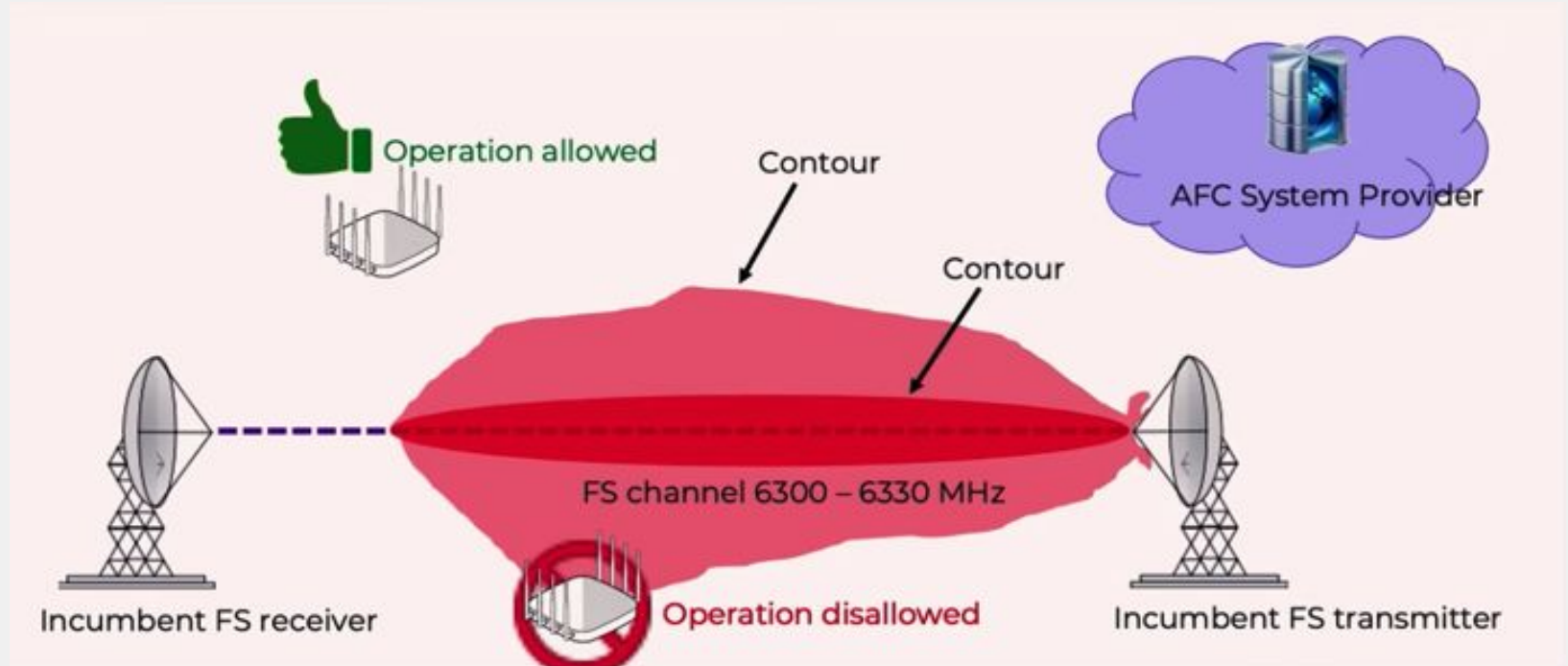
## Evolution

- The 6 GHz band has been traditionally licensed for reliable Point-to-Point microwave communications.
- In 2020, due to increasing demand for high-speed, reliable internet access,
  - FCC enabled unlicensed use of the 6 GHz band, significantly increasing the available spectrum for Wi-Fi and other applications.
- Only a **Low Power operating mode** for Indoor-only (**LPI**) use was authorized without any specific interference analysis requirements due to heavy usage of P2P microwave communications.
- FCC also specified a **Standard Power (SP)** mode that can be used for **indoor and outdoor** applications, as long as the system is **under the control of an automated frequency coordination (AFC)** system.
- Where an access point must register its location to a central database, which looks at nearby licensed usage and returns allowed frequencies and output power to the APs



# AFC – Automatic Frequency Coordination

- AP checks-in to AFC provider
- Reports coordinate
- Request a channel
- Check with list of channels already incumbent
- Make sure it doesn't interfere with incumbent
- Check in once a day





# 6 GHz AFC

QCA Partnership



Enabling 6GHz standard power indoor and outdoor operation for superior customer experience

## QCOM 6GHz AFC Solution



### End-to-end Solution

Turnkey implementation of Cloud Service and AP Agent with end-to-end validation and certification



### Standards Based

Enabling interoperability across devices complying to standard defined interfaces



### Cost Effective

Accelerating 6GHz adoption to drive cost lower with economies of scale



### Scalable

Designed to scale to millions of units meeting local regulatory requirements



# AFC Providers

Open AFC, same as open wi-fi <https://telecominfraproject.com/open-afc/> .

Growing around the globe.

Broadcom, google, Wi-Fi Alliance are all looking into it as becoming an AFC Provider.

**Fortinet using Qualcomm Worldwide as AFC Provider.**

Technology already used in cellular, just extending into Wi-Fi.

AFC takes a proactive approach, compared to DFS, more of a reactive approach.

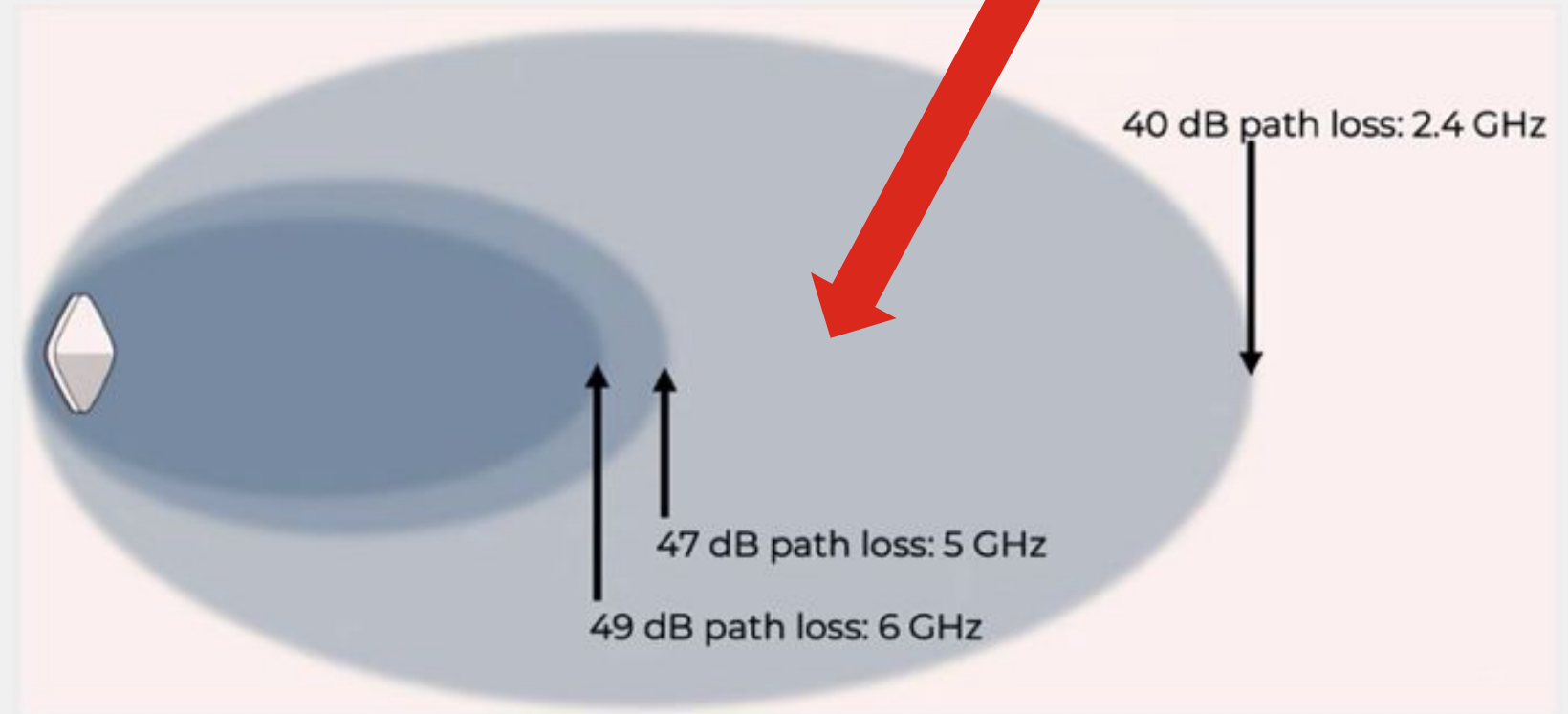


# Range Differences Between 5 GHz & 6GHz

Is one to one replacement recommended?

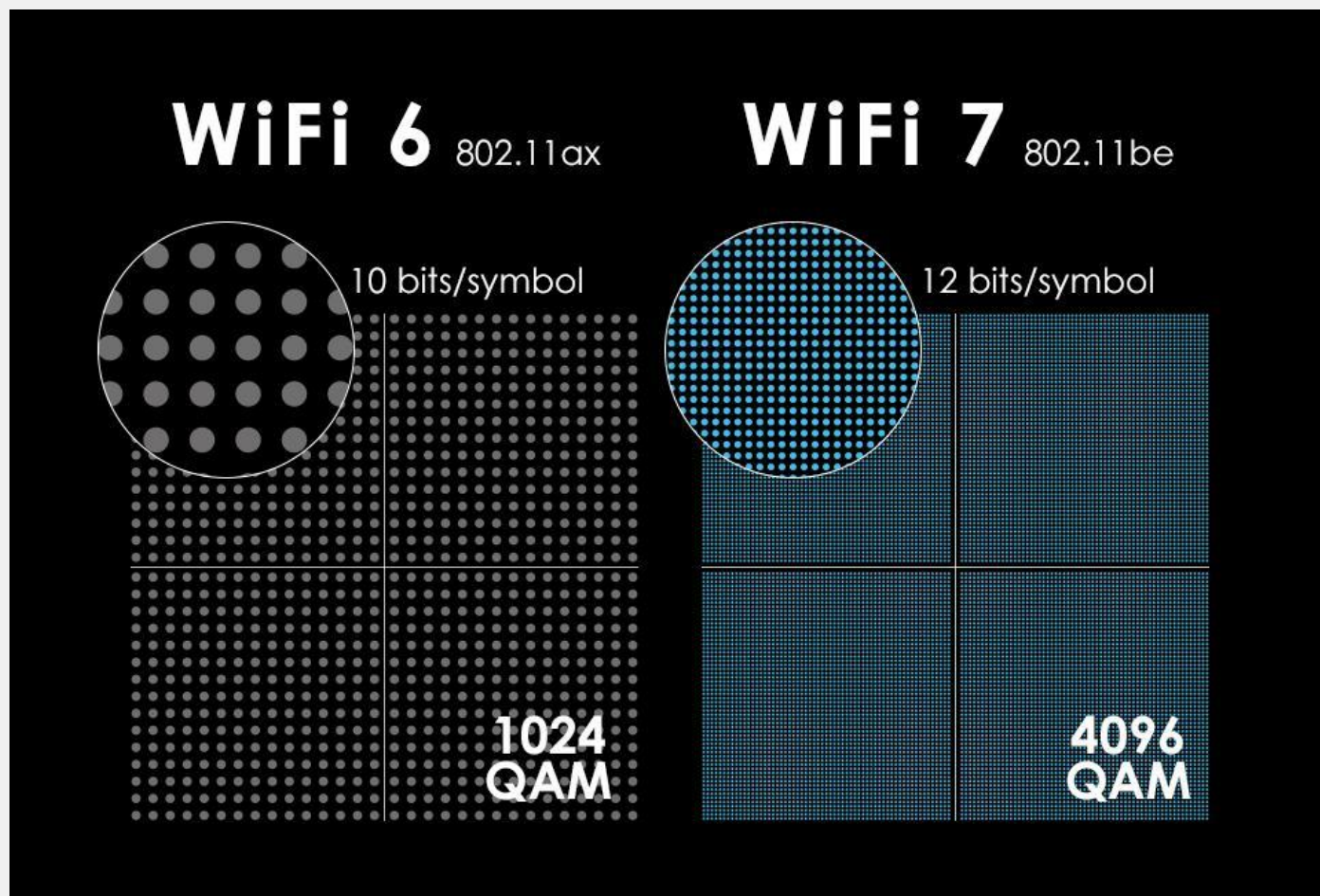
- One AP per room in hotel deployments may be acceptable.
- Home deployments may be acceptable
- Enterprise and High density deployments planning is needed

**However MU-MIMO will help make up for some range loss!!!**



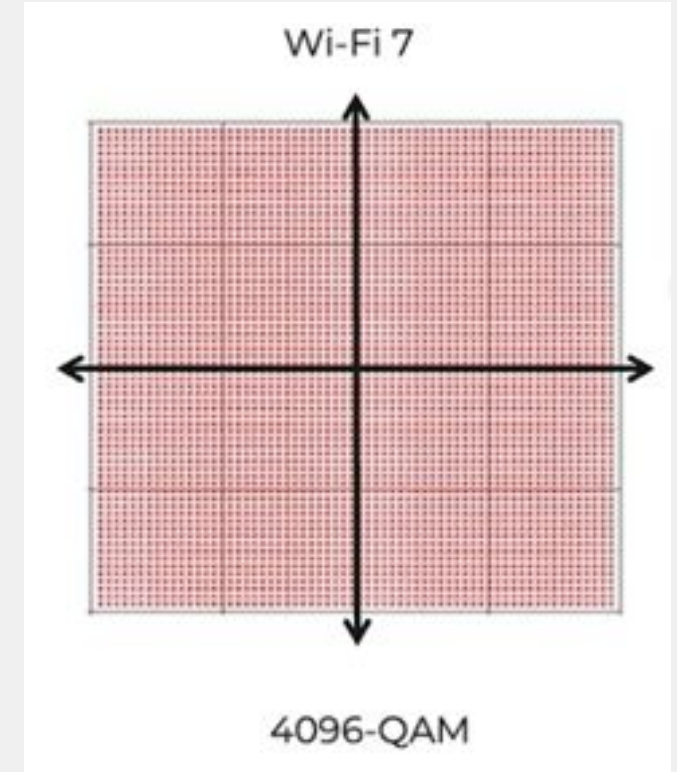
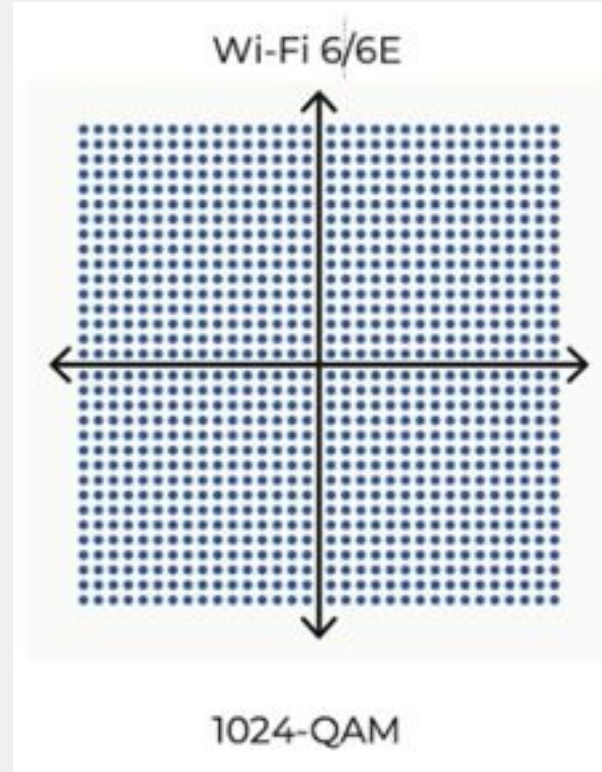
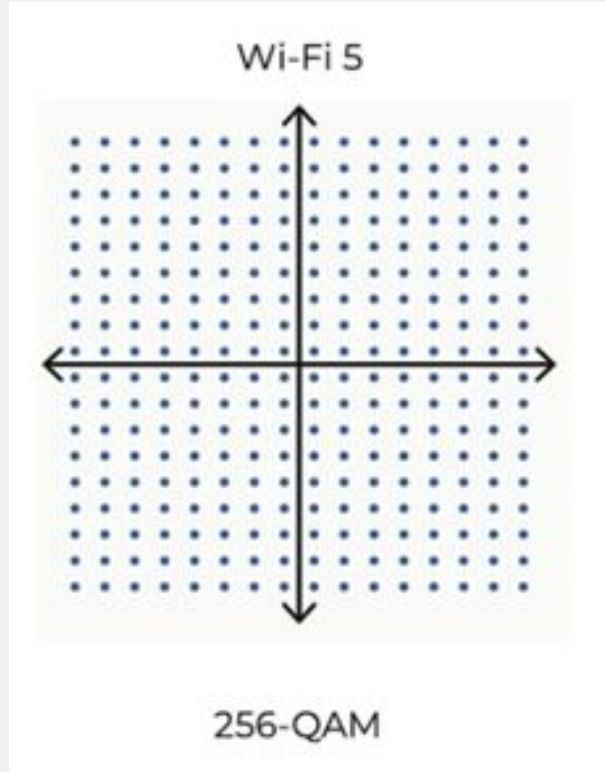


# Wi-Fi 7 – Higher Modulation



- Wi-Fi 7 will support Advanced modulation scheme called 4K QAM.
- Increases throughput and capacity.
- Transmitter should be more linear in amplifying power.
- it requires high SNR in order to decode the bits at the receiver.

# Wi-Fi 7 4K QAM Reality



**256-QAM – SNR of +/- 25dB**

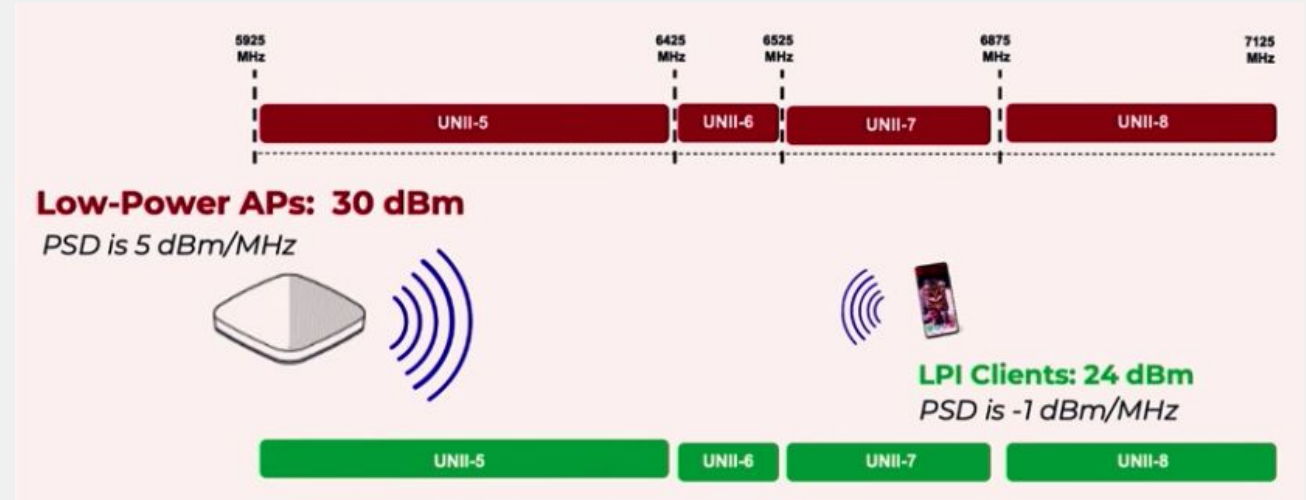
**1024-QAM – SNR of +/- 32dB**

**4096-QAM – SNR of +/- 41dB**

# LPI – Low Power Indoor

## Wi-Fi 6e 6 GHz does come with it's contains

- Aside of higher band spectrum and higher path loss.
- AP and clients are put in an asymmetrical power level.
  - Max EIRP for indoor AP's is 30 dBm.
  - Max EIRP for outdoor AP's is 36 dBm.
  - Yet clients are only allowed to have a max EIRP of 24 dBm.



## Wi-Fi 7 Into Reality

There was noise of 802.11ax Draft back in 2018.

However, 11ax didn't really mature until about 3 years ago.



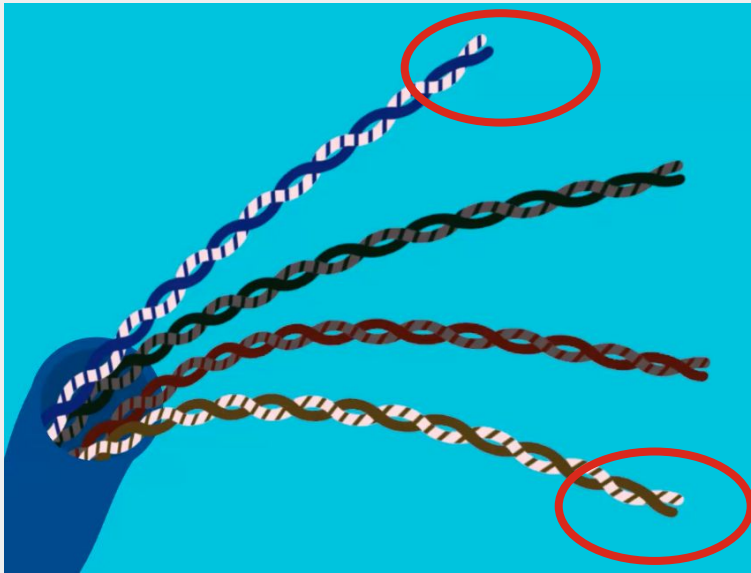




# 802.3at vs. 802.3bt

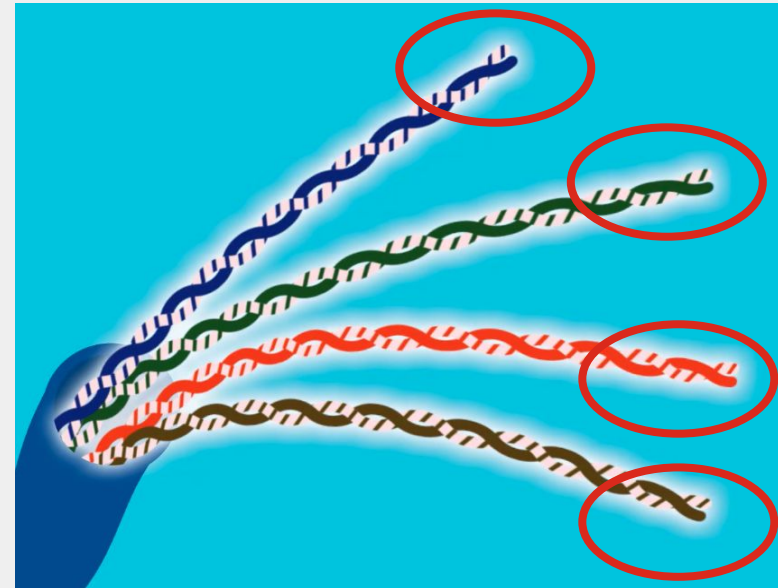
## 802.3at

30 watts PSE - Power Source Equipment  
25.5 watts PD – Power Device  
Uses 2 pairs out of 4 pairs to transmit power



## 802.3bt

99 watts PSE - Power Source Equipment  
71 watts PD – Power Device  
Uses all 4 pairs for power transmission



**802.3af – 15 watts PSE w/ 13 watts PD\***







FORTINET