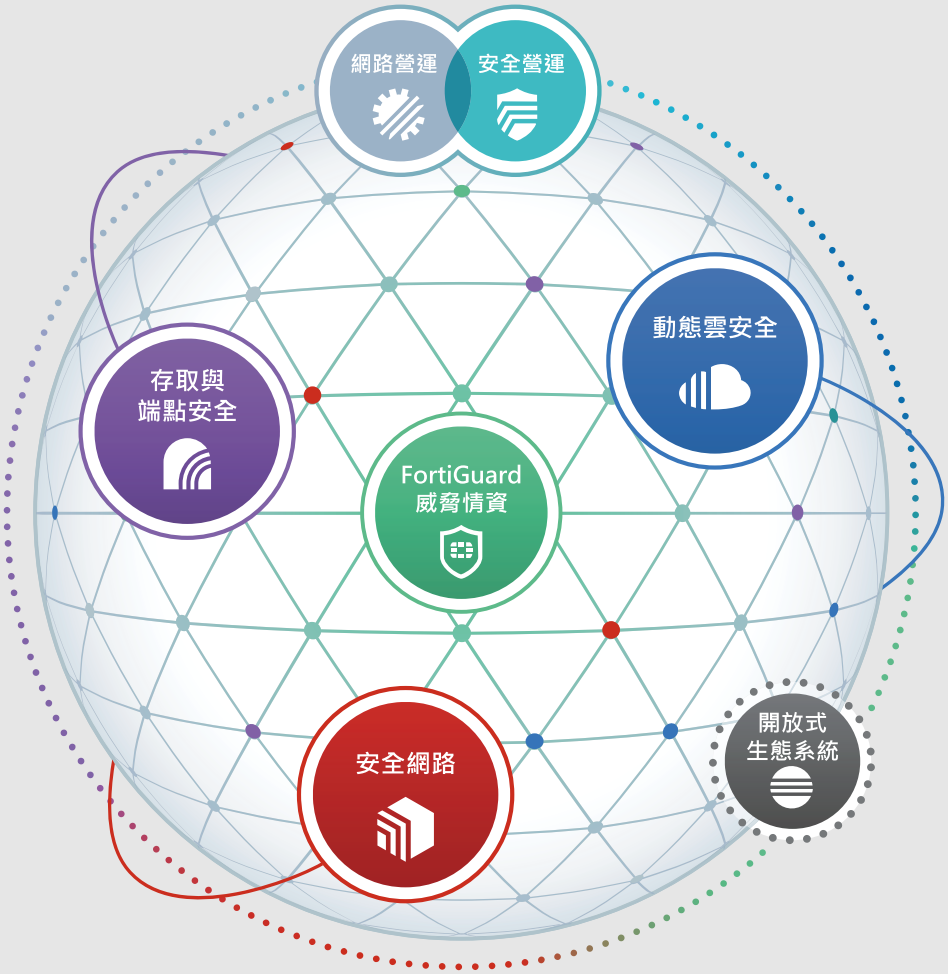
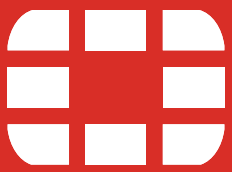
FORTINET®

公 司 介 紹



Security Fabric
安全織網網路安全網狀平台



實現足以信賴的數位世界

Fortinet 公司全景

Fortinet 是網路安全領域的全球領導者，提供全面涵蓋、深度整合與動態協作的 Security Fabric 安全織網網路安全網狀平台，使客戶能夠加速他們的數位化之旅。

2000 年
成立時間

加利福尼亞州森尼韋爾
總部

582 億市值（截止 2021.12.31）
Nasdaq:FTNT
S&P 500

565,000+
客戶
全業界涵蓋

8M+
迄今設備銷售總量
最豐富的應用場景

1255+
全球有效的專利
頂尖的創新者

10,000+
員工人數（截止 2021.12.31）

#1 設備出貨量
（基於 2022 年 2 月
IDC 全球安全設備市場研究資料）
市場領導地位

$3.34B
2021 年營收年成長 29% (YoY)
12 億美金
自由现金流
财务摘要

數位化創新影響各行各業

許多關鍵的發展趨勢正在推動組織加速數位化創新；然而，這些重要的創新努力也使組織的數位攻擊平面成倍增長，增加了網路風險。

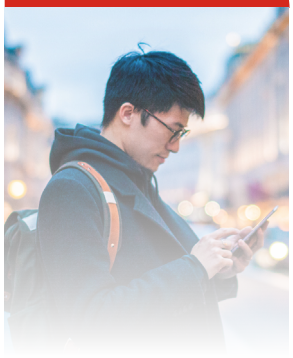
遠距辦公

大量增加的遠距辦公的存取

IoT/OT

漏洞與連網設備的大規模增加

5G/LTE

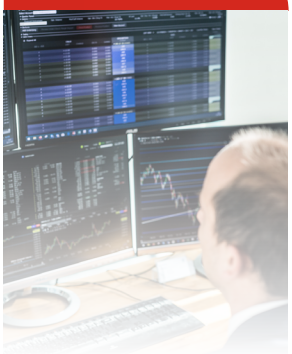


新的、且更加複雜的應用

邊緣 / 雲端運算

應用遷移到更多類型的運算平台

安全威脅態勢



零日攻擊、供應鏈攻擊、國家行為、網路漏洞與攻擊武器化

邊緣設備與網路的爆炸性成長

更多的邊緣場景出現在網路中

合規性

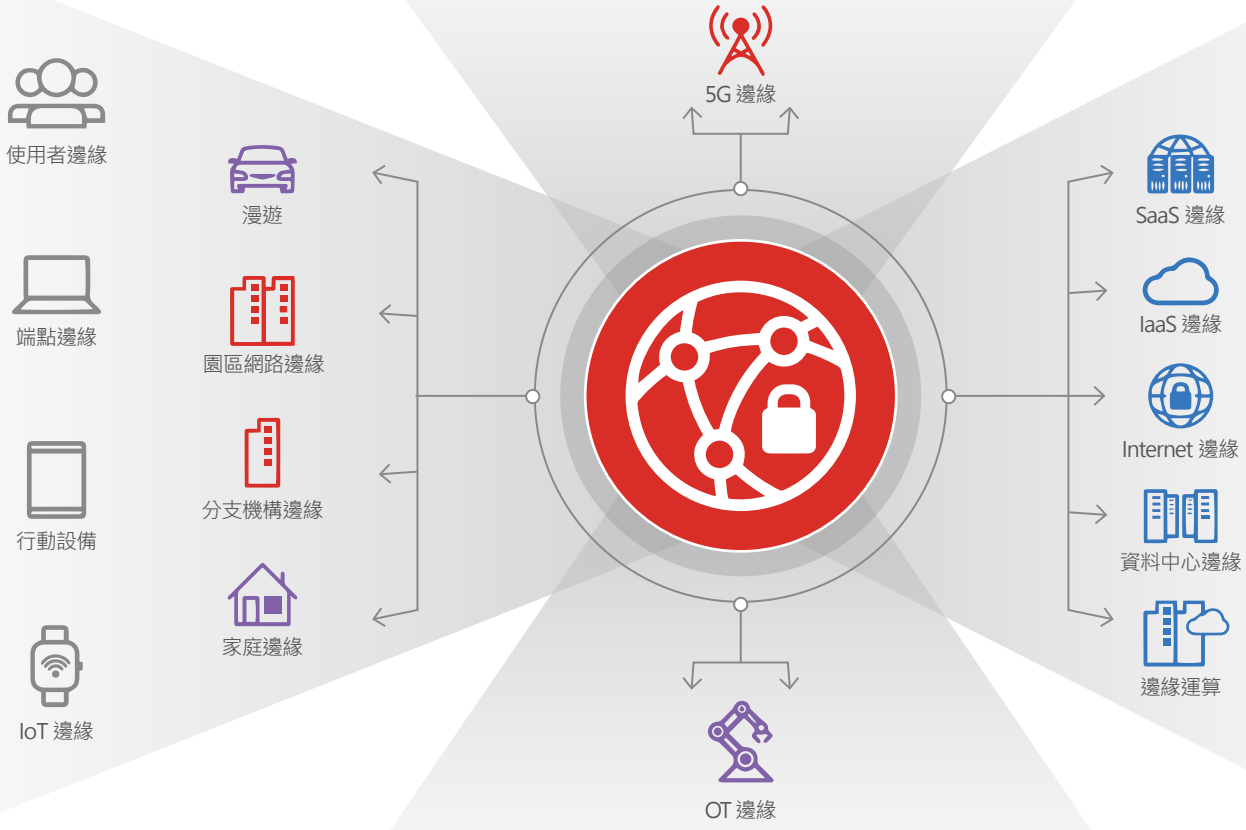
越來越多的資料隱私與監管問題，管理階層需要關注的合規報告

數位化體驗

端對端的效能與表現成為關鍵的差異化因素

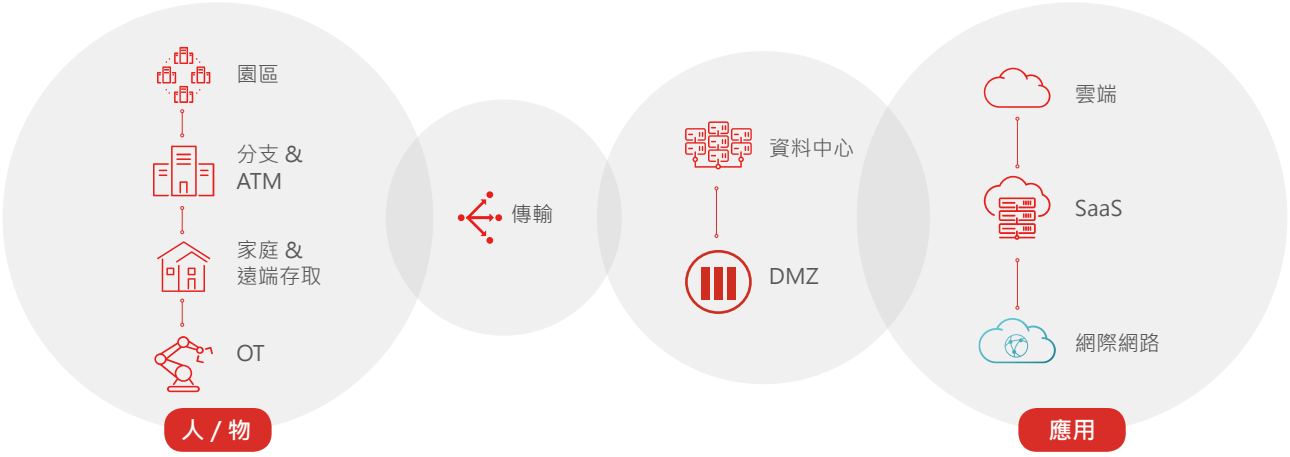
邊緣設備與場景的爆炸性增長帶來更多風險

由於邊緣無法定義，邊緣無處不在，許多組織已經部署了一系列單點安全解決方案。然而，這種方式很難提供有意義的整合與自動化協作能力，進而導致在廠商越來越多的情況下，企業不僅沒有降低財務成本與管理成本的投入，反而由於管理多種單點解決方案提升了複雜度而增加了成本。

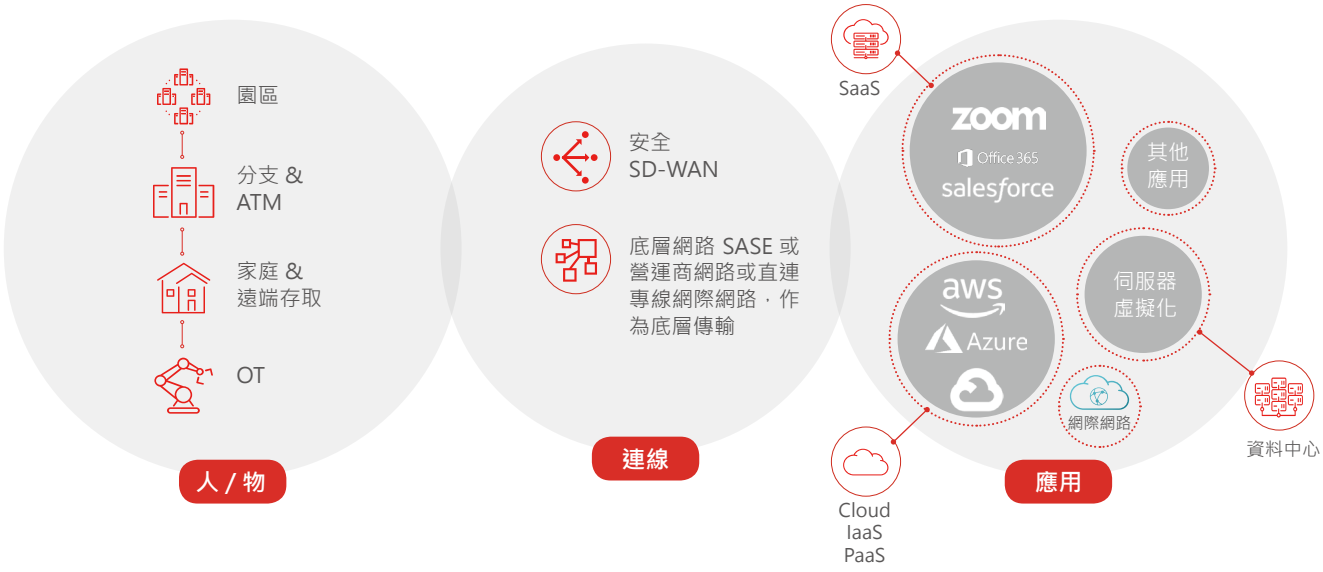


數位轉型 - 一套全新的模式

傳統架構 - **以資料中心為核心**



新架構 - **混合雲端為核心 + 行動工作**

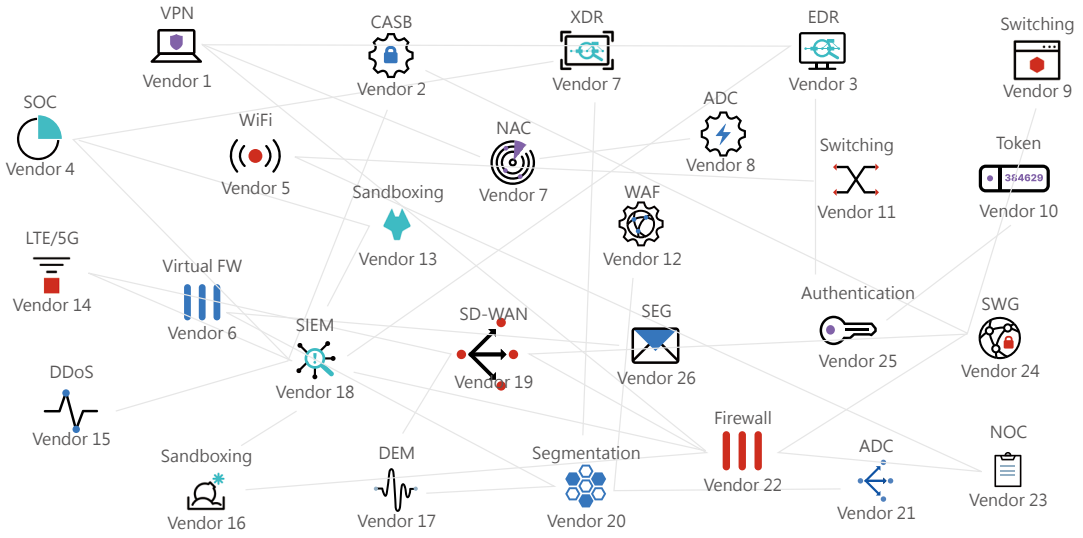


架構	以資料中心為核心，最終使用者環境偏向靜態	→	混合 IT 環境為核心，並有大量的行動工作空間
應用	部署在本地 (80%+)	→	本地 / 非本地 (50:50) 以及 SaaS
安全	建構在企業網內，並有明確的邊界 (DMZ)	→	安全無處不在
管理	手動設定 / 缺乏端對端的服務	→	端對端 自動化 / 政策 / 可視性 在一個多供應商的基礎架構環境中

安全供應商整合迫在眉睫

需要將單點產品進行平台整合，以加速威脅發現與回應

單點產品十分混亂



平台架構便於安全管理與資料整合

平台 1 設備與使用者 (ZTNA)	ZTNA	EDR	NAC	Proxy	Identity
平台 2 網路 (SASE)	Home Edge	LAN Edge	WAN Edge	DC Edge	Cloud Edge
平台 3 雲端	Virtual	Microsegmentation	WAF	API	Microsoft Azure, aws
平台 4 基礎架構： ie Microsoft	Active Directory	Windows	vWAN	O365	Security Command Center

> “到 2025 年，超過四分之三的大型企業將會主動進行安全供應商整合戰略”
>
> Gartner

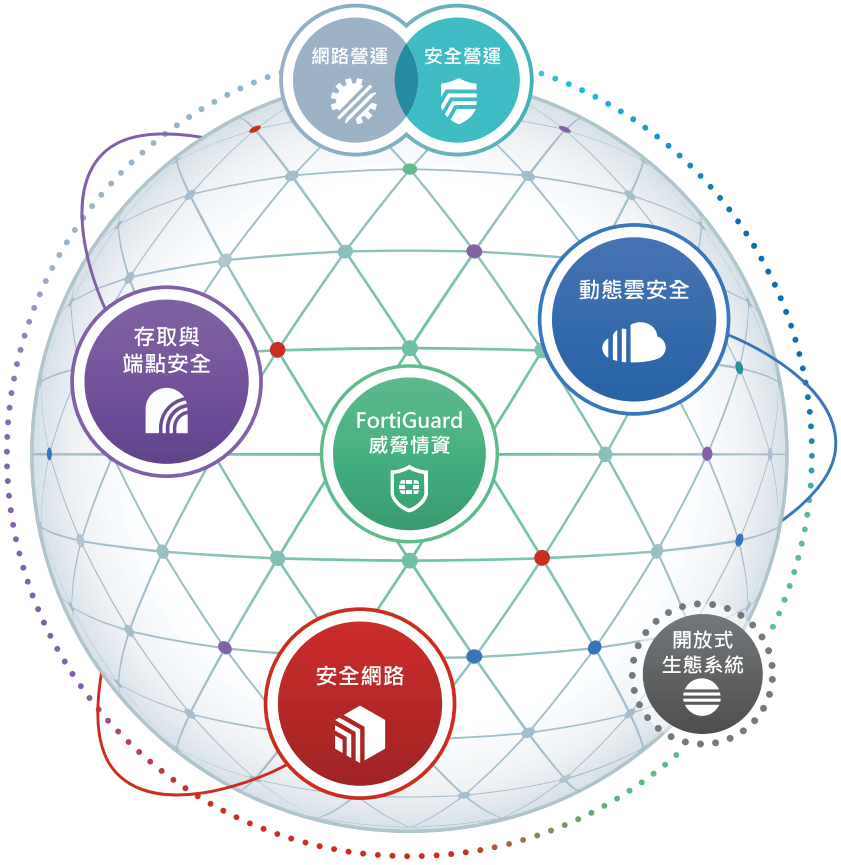
Fortinet Security Fabric 安全織網

Fortinet Security Fabric 安全織網是 Fortinet 安全創新的核心。它是一個圍繞通用作業系統與管理架構建構的一套網路安全平台， 實現了跨整個基礎架構的無縫交互運作、可視化與精細化控制。

FortiGuard Labs （FortiGuard 威脅研究與回應實驗室）提供的可操作的威脅情資進一步加強了 Security Fabric 安全織網的能力，透過與安全織網整合，提高了威脅檢測與回應的效率，簡化管理，並降低了整體複雜性。

由於 Security Fabric 安全織網基於通用標準與開放 API 建構，Fortinet Fabric-Ready 合作夥伴可以確保他們的客戶能夠將現有投資與安全織網結合並利用其能力，確保其整體網路安全狀態的一致性。

Fortinet 解決方案在橫向可以涵蓋今日大多數的分散式與需要安全處理效能提升的環境，同時也覆蓋了四大關鍵安全應用場景的基柱解決方案：安全驅動型網路，零信任存取與端點安全，動態雲安全，網路與安全營運。



全面涵蓋

數位化攻擊面的全面涵蓋， 提供全方位的可視性與防禦能力

深度整合

多點安全產品與方案的深度整合，降低管理複雜性並共享威脅情資

動態協作

搭載 AI 驅動的安全的自修復網路，提供更快更高效的營運能力

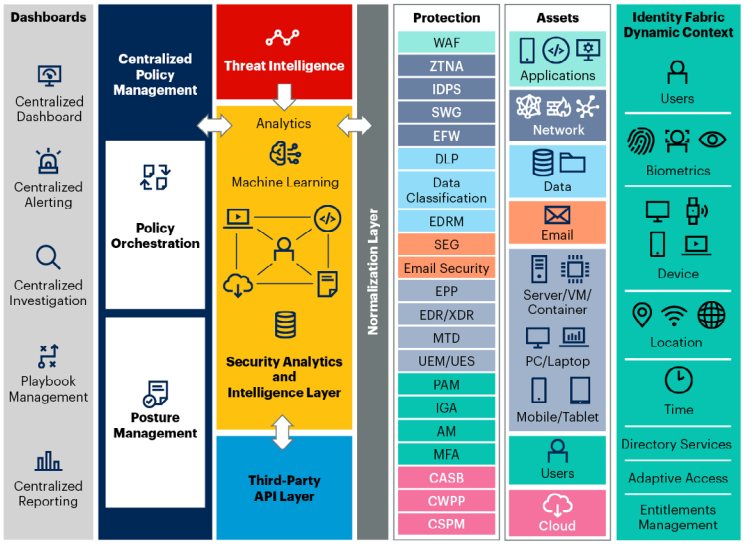
Security Fabric 安全織網是表現力最佳的網路安全網狀平台

Gartner 的網路安全網狀架構（CSMA，Cybersecurity Mesh Architecture）已被列入 2022 年網路安全主要趨勢。不謀而合，Fortinet 洞察網路安全發展趨勢提前十年佈局推出 Security Fabric 安全織網網路安全網狀平台——建設 CSMA 最佳模式。

Gartner

Cybersecurity Mesh Architecture

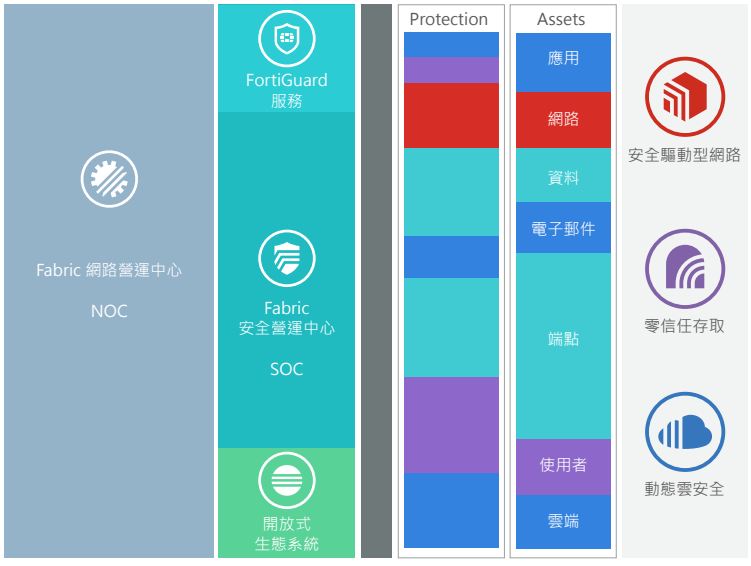
Fortinet Security Fabric 安全織網網路安全網狀平台已經成為業界“網路安全網狀架構 (CSMA)”理念最佳落地實踐



FORTINET

Fortinet Security Fabric

Fortinet 使網路安全網狀架構成為可能



網路安全網狀架構

- 透過提供支援服務層（整合政策管理，整合控制台，安全情資與身份矩陣）來讓安全工具之間能夠協作，而不是各自為戰。
- 能夠讓任何使用者與設備可以安全地存取或使用數位化資產，無關乎其所在的實體位置。

Security Fabric 安全織網開放的生態系統

400+ 一流的綜合解決方案，提供全面防護

Fabric Connector
Fortinet 研發的深度整合解決方案，安全協作與政策自動化

aws · aruba a Hewlett Packard Enterprise company · cisco · Microsoft Azure · IBM Cloud · Google Cloud · ORACLE · servicenow · Symantec.

Fabric API
合作夥伴研發整合，透過 Fabric API 提供端到端解決方案與廣泛可視性

EQUINIX · Guardicore · DELL · DRAGOS · ordr · ARISTA · SIEMENS · NVIDIA · tufin

Fabric DevOps
社群驅動的 DevOps 腳本，實現網路與安全部署、配置與協作自動化

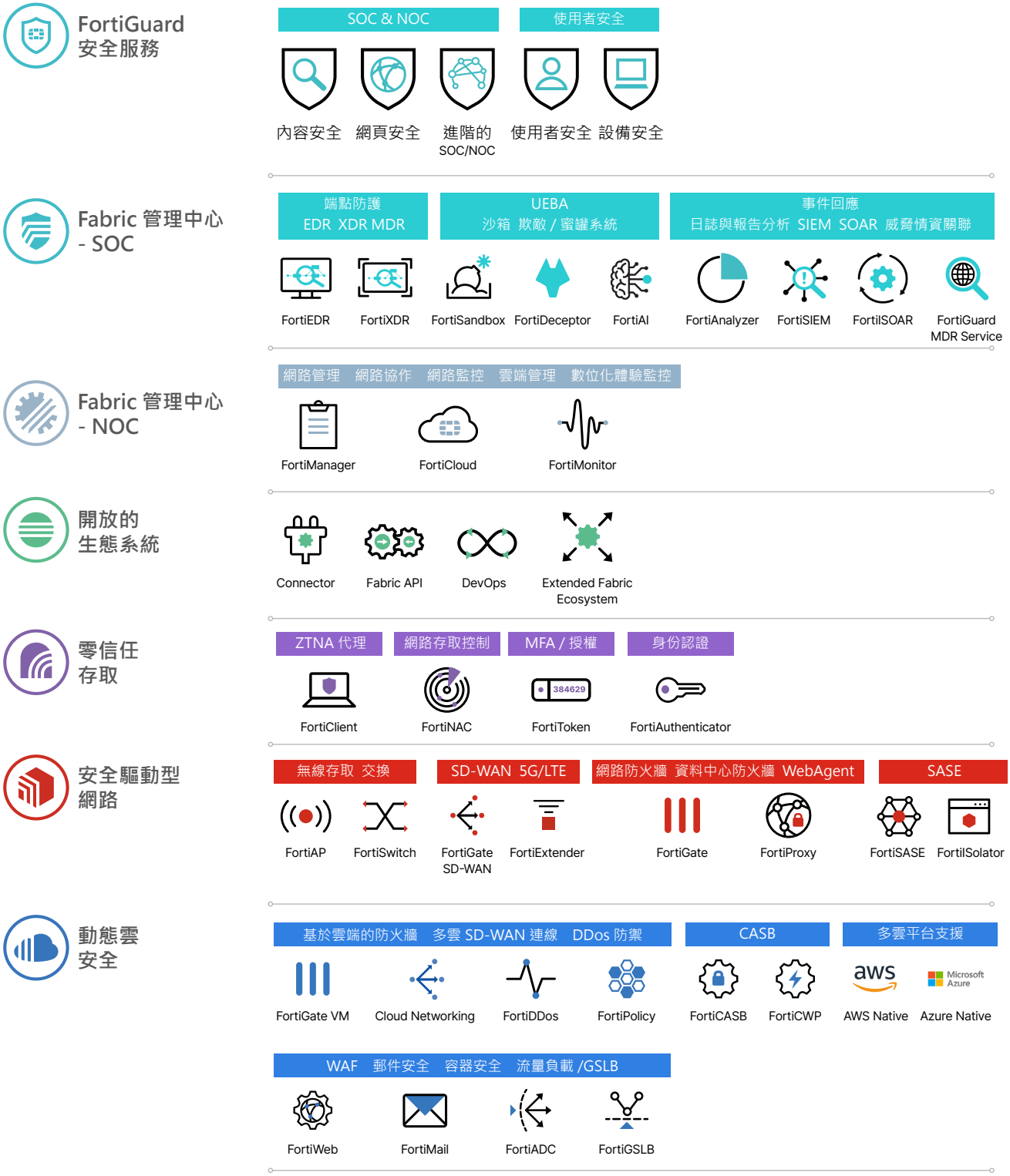
aws · Google Cloud · HashiCorp · Microsoft Azure · RED HAT ANSIBLE Automation · openstack. · ORACLE · TIGERA · vmware

可擴充的生態系統
威脅情資共享計劃與其他供應商技術整合

MITRE · STIX · CYBER THREAT ALLIANCE · INTERPOL · OT CSA

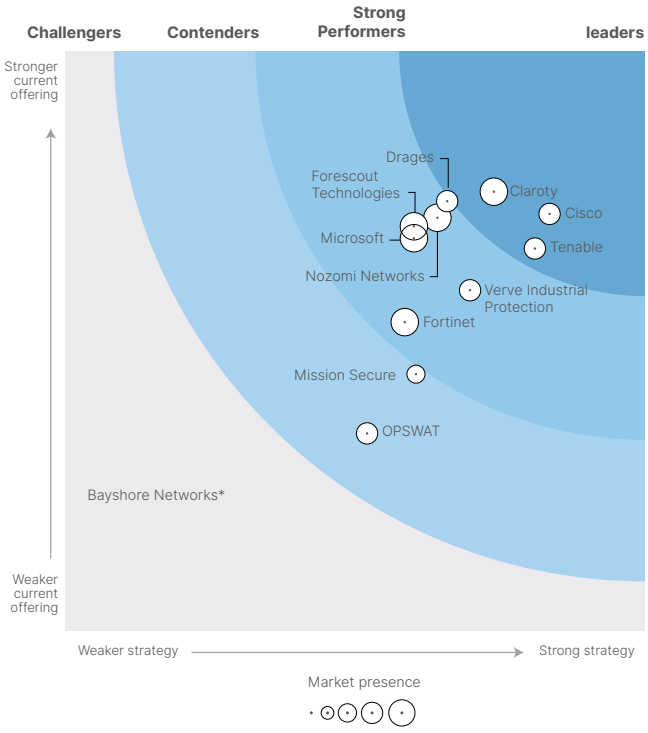
Firewalls · Switching · Wireless · Endpoint Security

Fortinet 建構數位安全 - 在您需要的任何地方



Fortinet 屢獲分析機構認可及第三方測試認證

THE FORRESTER WAVE
Industrial Control Systems (ICS) security Solutions

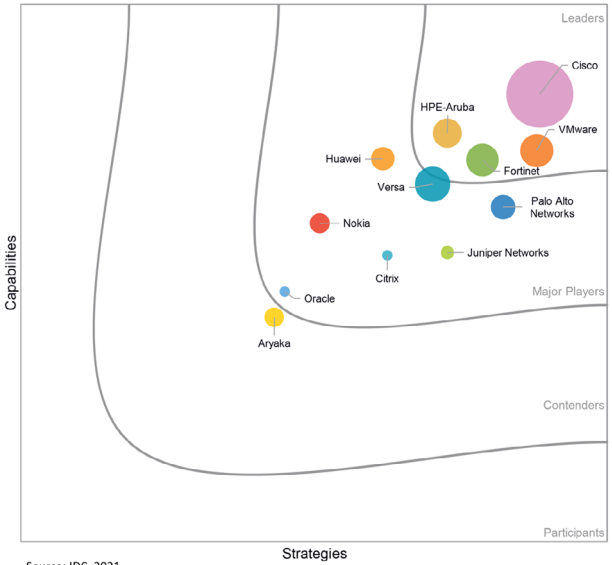


Fortinet 榮獲《 Forrester Wave：2021 年工業控制系統（ICS）安全解決方案報告》強勁表現者

Fortinet 在 Forrester Wave 等第三方權威報告中的優秀排名，再次凸顯了 Fortinet 的企業規模且龐大的使用者基礎所帶來的卓越優勢，且在全球市場久經考驗的吸引力。

除了在“使用者數量”評估中獲得最高分之外， Fortinet 還在另外六項評估範疇中獲得最高分，包括政策與規則管理、微隔離、API 與整合、產品安全性、合作夥伴生態系統與產品投資回報率。

IDC MarketScape: Worldwide SD-WAN Infrastructure · 2021



Source: IDC, 2021

IDC MarketScape 報告：Fortinet 榮膺 SD-WAN 基礎架構業界領導者

2021 年度 IDC MarketScape 報告採用一套綜合評估架構與一系列評估參數， 從多個維度對 12 家 SD-WAN 基礎架構廠商全面客觀的評估，判斷其是否具備為客戶提供高效 SD-WAN 解決方案的能力與戰略。

作為業界首屈一指的 SD-WAN 基礎架構廠商，Fortinet 推出一套統一的高效運作平台，為使用者打造一整套企業級安全解決方案，並首次在該領域提出整合進階網路技術與連線功能的創新型網路部署方案。

Virus Bulletin (VB)

唯一榮獲涵蓋 VB100,VBSpam 及 VBweb 三項認證的廠商

獲得最高 VBSpam 評選

獲 4 個技術領域認證

反惡意軟體
網路防火牆
IPsec VPN
Web 應用防火牆

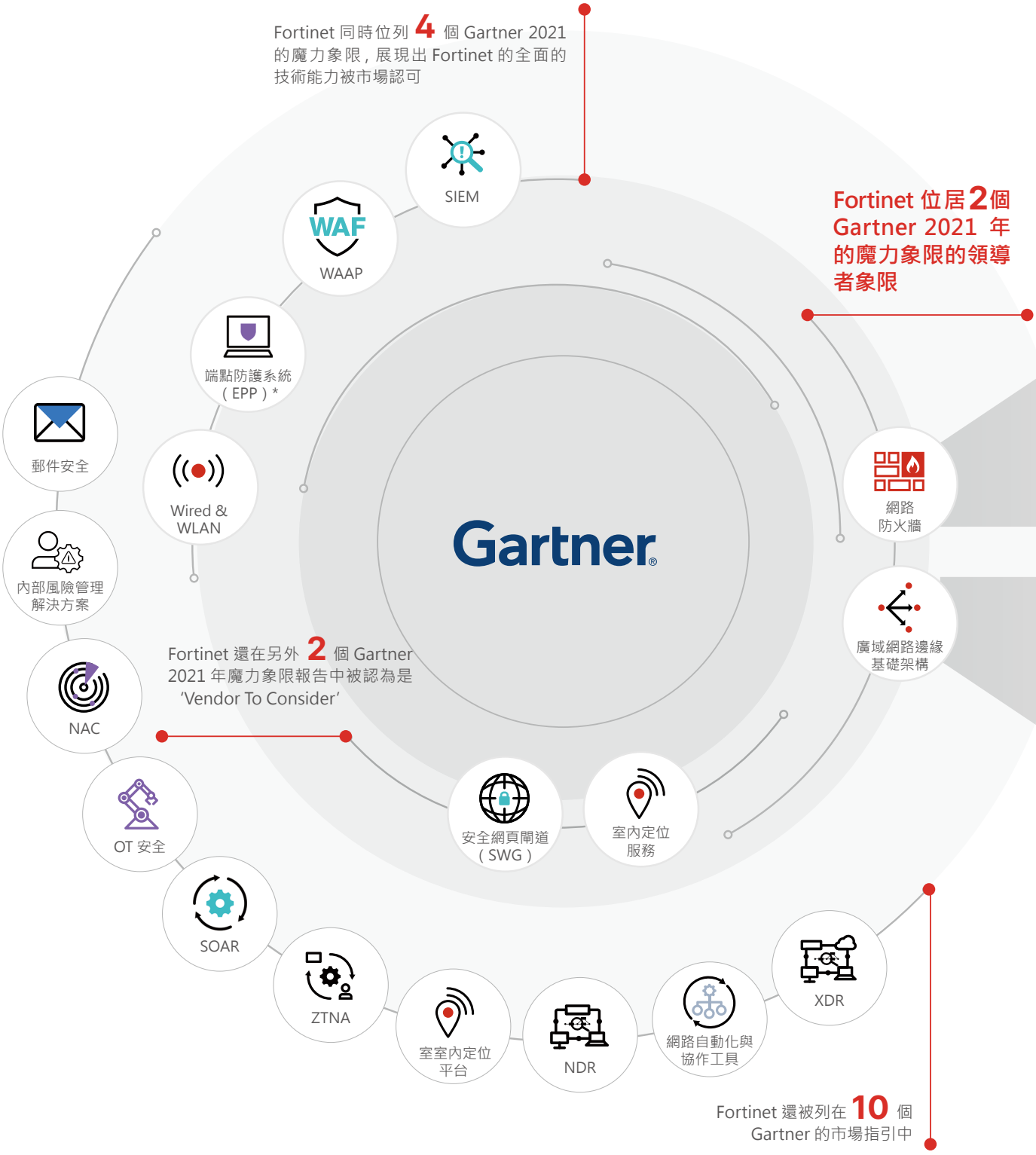
AV Comparatives 真實場景測試

Fortinet 終端威脅防禦能力在兩個類別通過測試
業務安全類別
反釣魚類別

MITRE Engenuity ATT&CK 評估

100% 防禦評級
優異的偵測與情資提供
全部機器學習智能防禦

Fortinet 獲 18 份 Gartner 報告提名



2021 年網路防火牆魔力象限

2021 MQ for network firewall

2021 年廣域網路邊緣基礎架構魔力象限

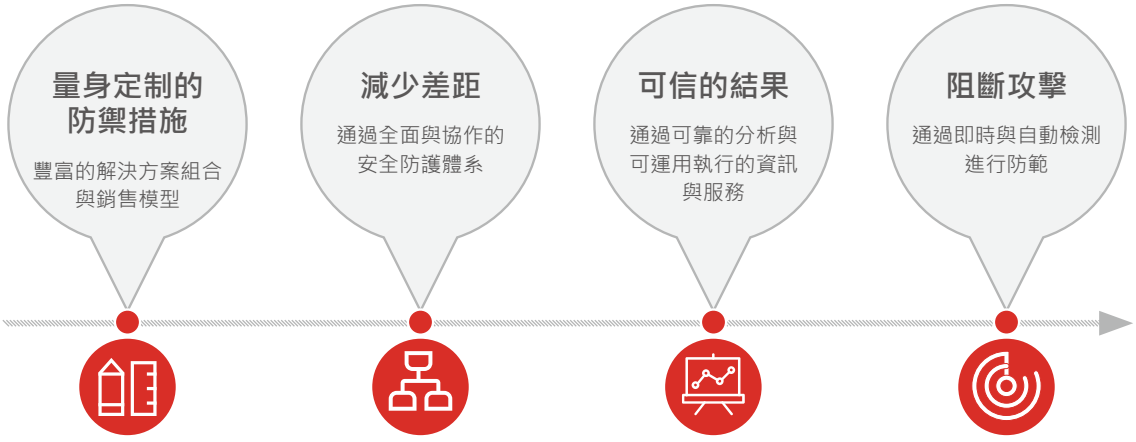
2021 Magic Quadrant

FortiGuard 實驗室

FortiGuard Labs（FortiGuard 威脅研究與回應實驗室）—— 威脅情資業界領導者

Fortinet 的 FortiGuard Labs 實驗室成立於 2002 年，是全球網路安全威脅資報研究實驗室的業界翹楚，持續引領全球威脅情資領域新進程。

作為推動全球安全業界持續發展的先驅者及創新者，FortiGuard Labs 率先開發利用機器學習與人工智慧（AI）先進技術，為全球使用者提供全方位威脅情資，支援使用者實現即時回應、一致的頂級防護及最佳落地實踐。 FortiGuard Labs 始終致力於推動業界高效協作，攜手世界各地機構、組織且業界優秀安全聯盟廠商，共同應對全球新興安全風險挑戰。



FortiGuard 實驗室的主動性研究

Fortinet 菁英匯集的網路安全威脅情資和研究機構

全球領導力與協作
共同創辦 CTA
共同創辦世界經濟論壇網路安全中心

可運用執行的資訊與服務
零日攻擊研究
回應流程與劇本
通訊郵件、部落格、部落客

採用機器學習與人工智慧的研發與訓練
優化跨網路、端點與雲端的
全球統一資料庫
利用 AI/ML 提供即時與一致的頂級防護

FortiGuard 安全服務

跨越攻擊生命週期與攻擊平面的市場領先的安全性

協同工作
跨網路、端點與雲端的情境感知安全

AI/ ML
由專業人員對統一資料集進行教育訓練

即時
自動更新整個生態系統的
安全規則與檢測能力

內容安全　網頁安全　使用者安全
設備安全　SOC/NOC 工具

FortiGuard 實驗室諮詢服務

提高您的安全規則與技能的工具與服務

攻擊開始前
滲透測試，焦點威脅分析，威脅分析，反釣魚服務，安全架構評估

攻擊發生時
即時的安全防護更新，外部
威脅情資

攻擊結束後
告警事故回應

資安教育訓練
縮小技能差距的網路安全訓練課程

技術與學習夥伴

培養合格的專業人員，彌補網路技能的不足

770,000+
認證

400+
安全學院

90+
具備教育訓練機構與認證中心的國家與地區

網路安全技能合作夥伴

IBM　salesforce　WORLD ECONOMIC FORUM

步驟	等級目標
NSE 1	Foundation - Public
NSE 2	Solutions - Public
NSE 3	Products
NSE 4	Professional
NSE 5	Analyst
NSE 6	Specialist
NSE 7	Architect
NSE 8	Expert

Fortinet 公司的社會責任

為我們的利益相關者、員工與社群建立可持續的長期價值。

具體的事項

200 萬美元

COVID-19 相關的捐贈

3-16 倍

產品的節能效率比競爭對手高

TOP25

躋身董事會性別多元化程度最高的 25 家科技公司之一

770,000+

NSE 認證授予 Fortinet 網路安全專家認證（Network Security Expert）

90+ 國家
400+ 學院

Fortinet 網路安全學院項目（Network Security Academy）

1255 個

專利

IBM SkillsBuild 項目

符合 LEED Gold 環境標準的總部大樓

為您實現
足以信賴的數位世界

Fortinet 是網路安全防護市場的領導者
提供最先進可靠的網路系統安全整合平台

我們致力於建造安全的網路世界
並持續投資於技術與服務

無論是現在還是將來
都是您值得信賴的合作夥伴。

FORTINET

台灣分公司 | 免付費技術服務電話：0809-089-210

官方網站 LINE@ Facebook YouTube