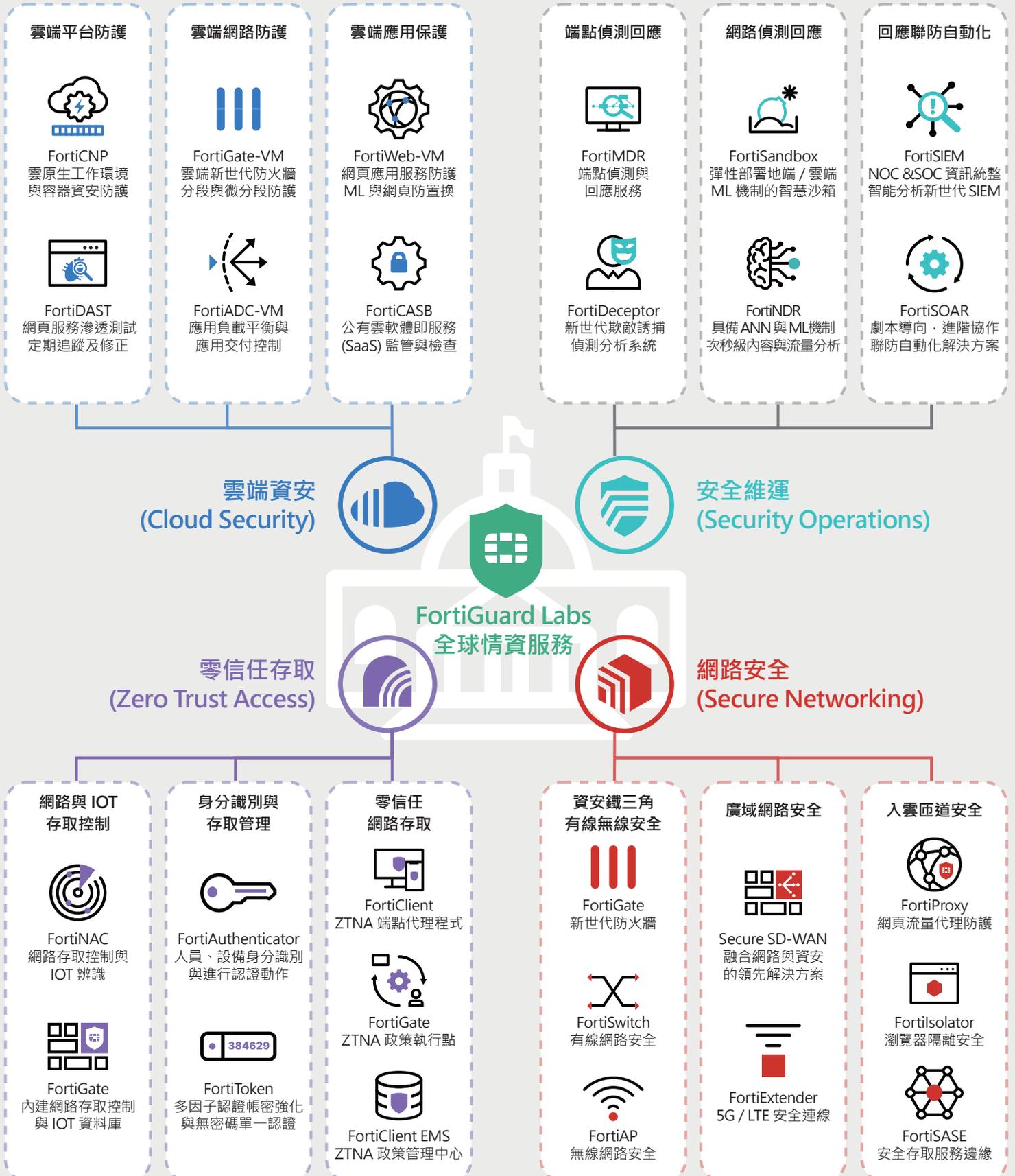


政府完整資安產業鍊

放眼過去、統領現在、展望未來

資安即國安



網路安全 (Secure Networking)



資安鐵三角 - 有線無線安全

Fortinet 資安鐵三角：業界領先將防火牆、有線無線網路統整，網路交換器 (FortiSwitch) 與無線基地台 (FortiAP) 變成防火牆 (FortiGate) 的延伸，在每一個端點前，進行內網資安控管。內建自動網路拓模圖及流量顯示，提高可視性與管理。針對有問題設備可以手動或自動快速進行隔離。



Secure SD-WAN 安全型軟體定義廣域網路

FortiGate 內建 SD-WAN 功能，整合新世代防火牆安全性，形成安全型軟體定義廣域網路解決方案 (Secure SD-WAN)，提供應用感知的動態路徑優化，廣域網路品質監督管理，線路備援與即時故障切換。整合 (FortiExtender) 支援 5G / LTE 安全連線。



FortiProxy 網頁流量代理防護

FortiProxy 為網頁應用流量提供快取與加解密分析，不但降低頻寬用量，還讓加密流量無所遁形，整合 FortiGuard 全球情資安全服務，強化上網安全。



Fortisolator 瀏覽器隔離安全

Fortisolator 可與 FortiProxy 整合，將 Internet 取得的網頁內容隔離並執行於遠端一次性的容器環境中並顯示給終端用戶，防止已知和未知的可能威脅。



FortiSASE 安全存取服務邊緣

FortiSASE 提供雲端全球性的安全加密通道連線與全套網路和安全功能，包括安全網頁閘道器 (SWG)、防火牆即服務 (FWaaS)、零信任網路存取 (ZTNA)、雲端存取安全代理 (CASB) 及 Secure SD-WAN，並做到統一的監控及管理。

安全維運 (Security Operations)



FortiMDR 端點偵測與回應服務

FortiMDR 透過機器學習的智能分析偵測與回應端點上的異常行為與潛在威脅，提供 7x24 隨時監控及防護，並且提供 IR 無限次數使用之服務。



FortiDeceptor 新世代的欺敵誘捕偵測分析系統

FortiDeceptor 可模擬 Windows、Linux、SSLVPN、IP cam 等 IoT 設備，誘騙駭客露出馬腳，做到第一時間的反應及防禦。



FortiSandbox 彈性部署地端 / 雲端 ML 機制的智慧沙箱

FortiSandbox 具備機器學習智能分析可疑與未知威脅，提供硬體、軟體、雲端及地端的彈性部署，並能整合眾多 Fortinet 產品及第三方軟硬體。



FortiNDR 具備 ANN 與 ML 機制次秒級內容與流量分析

FortiNDR 透過人工神經網路 (ANN) 分析流量內容，機器學習分析網路流量動態，追蹤異常行為，並且能與 Fortinet Security Fabric 安全織網連動協防，次秒級超高速偵測與回應未知與新形態資安威脅。



FortiSIEM NOC & SOC 資訊統整智能分析新世代 SIEM

FortiSIEM 為新世代 SIEM 平台，不僅滿足日誌稽核，合規報表管理，還能協助資安與維運管理優化，內建 AI & ML 關聯分析，對應 MITRE 資安框架，提供先期預警能力。內建派工管理，連動跨品牌設備，滿足協作與自動化回應 (SOAR) 需求。



FortiSOAR 劇本導向，進階協作聯防自動化解決方案

FortiSOAR 為進階資安協作與自動化回應 (SOAR) 工具，經 SIEM 導入資安告警，藉由豐富的劇本 (Playbooks) 與客製化能力，完成複雜回應流程。內建連接器，可整合 400+ 跨品牌的各類產品。

零信任存取 (Zero Trust Access)



FortiClient ZTNA 端點代理程式

FortiClient 除了作為 ZTNA 端點上的代理程式，也提供 SSL-VPN / IPsec VPN 的連線能力，方便用戶從 VPN 進展到 ZTNA 的連線環境，本身還提供 NGAV、網頁過濾、應用程式防火牆等豐富的端點防護能力。



FortiGate ZTNA 政策執行點

FortiGate 作為 ZTNA 的政策執行點，接受來自 FortiClient 的安全加密連線整合中央 ZTNA 政策管理中心，提供業界驗證最高等級新世代防火牆資安防護能力。



FortiClient EMS ZTNA 政策管理中心

FortiClient EMS 作為 ZTNA 的政策管理中心，集中管理所有的 FortiClient ZTNA 端點代理程式，並將 ZTNA 政策透過標籤與 ZTNA 政策執行點 FortiGate 進行同步，建構一個隨處辦公的零信任安全環境，無論是在內網或外網。



FortiAuthenticator 人員、設備身分識別與進行認證動作

FortiAuthenticator 提供集中式身份認證管理，包括單點登錄服務、憑證管理和來賓訪問管理，防止未經授權存取組織或企業資源。



FortiToken 多因子認證帳密強化與無密碼單一認證

FortiToken 提供硬體式、行動裝置軟體式 Token，在身分驗證過程中添加第二個驗證因素來強化帳密的安全性，通過主動推送 (PUSH) 方式，方便用戶接受/拒絕憑證，進一步確認使用者身分。支援 FIDO 無密碼登入模式。



FortiNAC 網路存取控制與 IOT 辨識

FortiNAC 可整合第三方網路設備，在無安裝代理程式情況之下，做到 IOT 辨識，並且做到內網零信任存取以及訪客系統。



FortiGate 內建網路存取控制與 IOT 資料庫

FortiGate 內建網路存取控制，能與 FortiSwitch 整合，結合 FortiGuard IOT 資料庫，提供設備識別、網路存取控制能力與新世代防火牆等級資安防護能力。

雲端安全 (Cloud Security)



FortiWeb 網頁應用服務防護 ML 與網頁防置換

FortiWeb 為具備機器學習 (Machine Learning) 機制的網頁應用防火牆 (WAF: Web Application Firewall)，並能提供網頁防置換功能，為阻擋層出不窮的大陸網軍攻擊，多一層保障。



FortiCASB 公有雲的檢查及防禦

FortiCASB 為雲端軟體即服務 (SaaS)，例如：Office365、Google Drive 等，提供雲端 SaaS 資安更好可視性、合規性、以及防止影子 IT (Shadow IT) 行為，避免資料外洩及可能的資安風險。



FortiGate-VM 雲端新世代防火牆分段與微分段防護

FortiGate-VM 將防火牆虛擬化，為私有雲與公有雲環境提供 VPN、網路分段與微分段解決方案，整合 FortiGuard 全球情資與安全服務，提供業界與全球用戶驗證，雲端新世代防火牆資安防禦能力。



FortiADC-VM 應用負載平衡與應用交付控制

FortiADC-VM 透過伺服器負載平衡功能達到 99.999% 應用服務可用度，加速與優化應用服務交付與智能流量管理。



FortiCNP 雲原生工作環境與容器資安防護

FortiCNP 為多個公有雲平台提供一致性的風險監控。能夠快速定位雲平台設置問題、偵測惡意檔案 (Malware、Ransomware) 與機敏資料，偵測漏洞與威脅活動的資源關聯性，簡化雲平台配置的合規性檢查、追蹤並產生報告。



FortiDAST 網頁服務滲透測試定期追蹤及修正

FortiDAST 提供資安領先廠商的網頁應用滲透測試服務，並且在一年內無次數限制，可偵測掃描 OWASP Top 10 及其他弱點及漏洞，並提供風險緩解建議。