

解決方案簡報

FortiSASE：全面性的 SASE 解決方案 讓遠端使用者獲得雲端提供的 資安和網路功能

執行摘要

現今大多數企業使用混合的工作方式，每週會有一部分的時間不在公司辦公室內工作。這會導致攻擊面擴大（因為納入了居家辦公室和行動工作的員工），並讓網路、應用程式和數位資源的防護更具挑戰性。擁有大量遠端辦公室和混合工作模式員工的企業組織，經常因為要確認資安政策是否一致性套用與執行而感到困擾，同時還要確保無論使用者是否在網路中，都要有最佳的工作體驗。

有部分的挑戰源自於這些變動都是自然發生的，而不是精心安排的策略環節。新的網路邊緣和遠端使用者數量快速成長，但解決方案通常都以獨立的形式部署，如此一來會留下資安破口，讓網路犯罪者巴不得快點暴露這個漏洞。

安全存取服務邊緣（Secure Access Service Edge，SASE）架構可以協助解決這些問題。只要透過將安全存取和高效能連線能力延伸至任何位置的使用者，就能辦到。然而，許多 SASE 解決方案只能應對部分的問題，不是無法為遠端使用者提供企業級的資安能力，就是沒辦法無縫整合實體和雲端網路，以及部署在網路邊緣的資安工具。甚至是都辦不到。最終導致無法提供一致的安全狀態，也不能在各個位置維持良好的使用者體驗。

FortiSASE 採用 Fortinet 的單一廠商 SASE 做法，並能提供全面的 SASE 解決方案。方法是將雲端提供的軟體定義廣域網路（SD-WAN）連線能力，與雲端提供的安全服務邊緣（SSE）進行整合，並將此整合的網路與資安功能從網路邊緣延伸到遠端使用者身上。

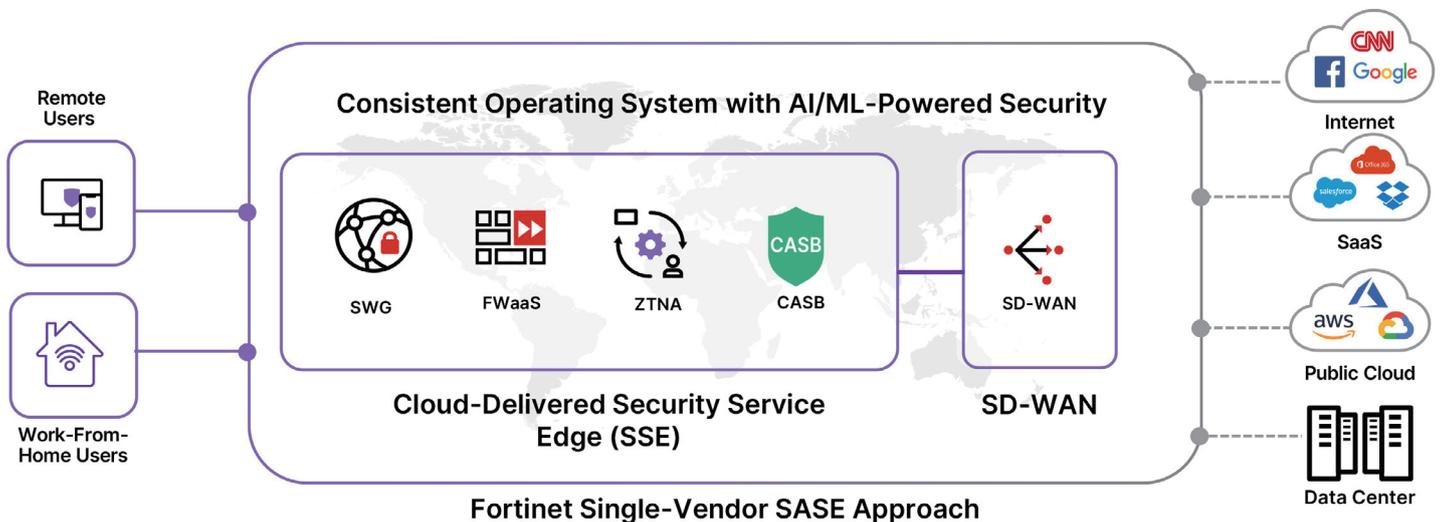
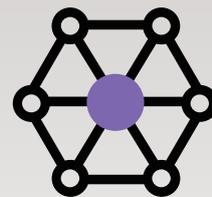


圖 1：透過 FortiOS 確保安全狀態能維持一致，並為位於各地的使用者帶來卓越的使用者體驗

FortiSASE 是經過精心打造的服務，它可以將網路與資安功能合併至整合式的適應性解決方案當中，以確保網路邊緣至遠端使用者之間的連線不僅安全，且傳輸最佳化。累積了 20 多年以來的活躍創新，FortiSASE 能提供安全網頁閘道 (SWG)、零信任網路存取 (ZTNA)、次世代雲端存取安全代理 (CASB)、以雲端提供的防火牆即服務 (FWaaS)，以及安全 SD-WAN，讓企業組織可以從資本支出模型轉換為營運支出模型。

我們獨特的資安驅動網路策略會借助於單一的 FortiOS 作業系統，並透過 FortiGuard 的 AI 技術資安服務強化，讓我們可以將資安與網路功能融合成一個單一且整合的系統，以提供一致的資安服務與使用者體驗給任何地點的使用者。FortiSASE 以獨特的方式協助組織，讓他們可以在任何位置安全地存取網路、雲端，和應用程式，並擁有企業級的安全性與卓越的使用者體驗。



FortiSASE 藉助於 FortiOS 和 FortiGuard 的 AI 強化資安服務，提供簡單又可擴充的雲端資安工具。讓各地的使用者均擁有一致的安全性和卓越的使用者體驗。

FortiSASE：由雲端提供的簡單、無縫、可擴充的資安工具

FortiSASE 提供簡單且以雲端為基礎的管理方式，並使用自助服務設計，讓使用者可以輕鬆進駐。FortiSASE 也擁有業界最具彈性，以使用者為本的層級式授權模式。這能讓企業組織的商業模式由資本支出的轉換為營運支出，並將建置當今高度變動的網路和基礎架構的成本保持在預期範圍之內。

FortiSASE 同時也獲得服務組織控制 (SOC 2) 的認證。此組織會進行獨立驗證，確保解決方案安全性控制的運作依照美國註冊會計師協會 (AICPA) 所適用的信任服務方式原則與標準。獲得 SOC 2 Type II 標準認證，彰顯了 Fortinet 對客戶堅定的承諾，確保客戶能夠符合各類法規的需求。FortiSASE 同時也提供了全面的企業等級資安功能，並已完整整合至解決方案當中，包括 SWG、ZTNA、次世代雙重配置模式 CASB、FWaaS，以及先進的威脅防護功能。可運用於下面三種重要的使用案例：

■ 確保網際網路存取安全：

對在企業邊界以外運作的遠端使用者來說，直接存取網際網路會讓他們的攻擊面變大，同時提高連線風險。FortiSASE 提供完整的 SWG 與 FWaaS 功能，並支援代理程式和無代理程式的方式，同時為受管理和未受管理的裝置提供防護。

■ 確保私人存取安全：

隨著混合工作模式成為新的標準，傳統 VPN 在擴充上也面臨了困境。因為 VPN 並沒有包含整合式檢查或先進的防護功能，一旦 VPN 連線被挾持便會被用來存取所有應用程式，讓攻擊面擴大，提高受到橫向移動威脅的風險。FortiSASE Secure Private Access 為企業應用程式提供業界最靈活且安全的連線能力。企業組織可以使用 ZTNA 的做法來實現細緻的應用程式存取功能。啟用最小授權且明確應用程式的存取方式，可以協助將資安策略從隱性信任模型轉換為更為安全的顯性信任策略。FortiSASE Secure Private Access 現在也無縫整合了 SD-WAN 網路。只要透過 FortiSASE 的智慧操作與動態路由功能，就可自動找出抵達企業應用程式的最短路徑。

■ 確保 SaaS 存取安全：

隨著採用 SaaS 模式的比例快速提升，企業組織也會持續面臨影子 IT 的挑戰，以及如何阻止資料外洩的問題。FortiSASE Secure SaaS Access 擁有次世代雙重配置模式 CASB，同時使用 In-Line 與以 API 為基礎的支援，藉由識別關鍵 SaaS 應用程式與回報高風險應用程式，來提供完整的可視性，即可克服影子 IT 的挑戰。次世代的 CASB 也會針對應用程式提供細緻控制，以確保敏感資料的安全，同時能偵測和修復受管理與未受管理裝置應用程式中的惡意軟體。

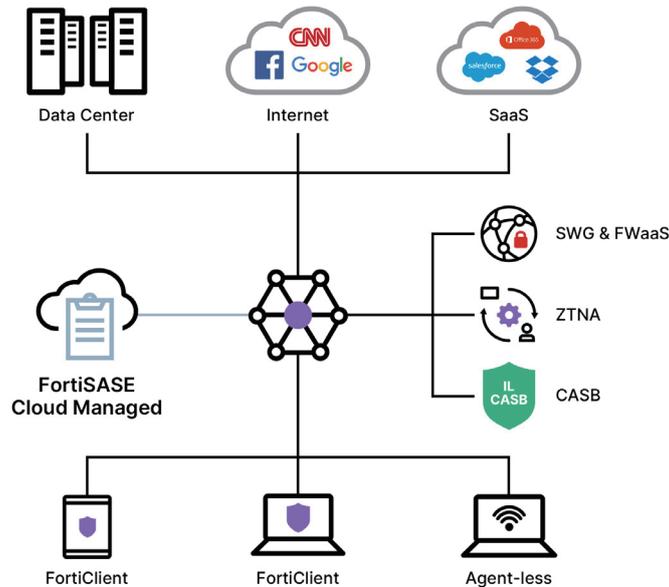


圖 2：FortiSASE 為所有應用程式提供安全且可信賴的雲端連線能力

大規模提供廣泛的資安功能

FortiSASE 提供一系列廣泛的資安功能，為的是保護前往網際網路、私人資料中心，以及 SaaS 應用程式的流量：

安全網路閘道：透過一系列功能來保護網路流量（包括加密流量），來對抗最先進的網路威脅。它的網路過濾、防毒軟體、檔案過濾、防資料洩漏等功能，可以彼此合作組成深度防禦策略，保護受管理與未受管理的裝置。

防火牆即服務：利用 FortiOS 進行獨立驗證的能力（這同時也是 Fortinet 領先業界的 Security Fabric 策略的核心），讓高效能 SSL 檢查和針對雲端流量、應用程式與服務的進階威脅偵測技術得以實現。Fortinet 的 FWaaS 解決方案可以為遠端使用者建立並維持安全連線，同時在不影響使用者體驗的情況下，分析往內與往外的流量。

ZTNA：ZTNA 讓 IT 團隊可以依照使用者和工作階段，在存取企業關鍵應用程式時，對其持續進行驗證、保護與監控。ZTNA 讓這個功能可以適用在各處的使用者和裝置上，無論其確切位置。同時以持續驗證身分與情境為底，依據應用程式將資安策略從隱性存取轉變為更加安全的顯性存取策略。

次世代雙重配置模式 CASB：透過同時支援 In-Line 與以 API 為基礎的模式，FortiSASE 可以辨識關鍵 SaaS 應用程式、回報影子 IT 應用程式、保護存取獲批准的 SaaS 應用程式，以及限制信任的端點存取 SaaS 應用程式。一旦啟用 ZTNA 應用程式存取狀態檢查，即可享有這些功能。



網域名稱系統 (DNS): 可以為針對 DNS 的複雜威脅提供防護，包括 DNS 通道攻擊、DNS 協定濫用、DNS 入侵、C2 伺服器識別，以及網域生成演算法 (DGAs)。在取得 DNS 流量完整可視性的同時，阻擋高風險網域，包括惡意的新註冊網域 (NRDs)、網域寄放等等。

入侵偵測 (IPS): 透過即時威脅情資，即可對全新或現存的漏洞進行防護，並將效能的影響降至最低。

沙箱: 透過對威脅進行安全的辨識、觸發和分析，達成即時預防和偵測的目的，以確保檔案在未知的先進威脅下保持安全。

大規模提供廣泛的資安功能

相較於提供獨立又僅限於雲端的方案，FortiSASE 可以與 Fortinet Security Fabric 進行協同合作。將 FortiOS 的優勢加以延伸利用之後，Fortinet Security Fabric 可以為任何位置提供寬闊的可視性、細緻的控制能力，以及一致且主動式的防護。

無論使用者是否在內部網路，皆能提供一致的安全性：FortiSASE 提供廣泛的雲端資安工具，且原生整合了 ZTNA，以對本地與遠端的使用者提供一致的防護。

單一代理程式：FortiClient 是我們的唯一的代理程式，可支援多種使用案例，包括 ZTNA、流量導向至 SASE、次世代 CASB、以及強大的端點防護，如此便不需要針對各種防護需求而使用不同的代理程式。

簡易的管理和消費模式：藉由自助式服務設計，讓解決方案易於部署、連入網路和管理，且擁有業界最具彈性，以使用者為出發點的層級式授權模式，讓 IT 團隊可以為混合工作模式員工實現全面且一致的安全防護。而且不需要費盡心思就能管理、監控、協作，以及對部署在不同網路生態系的系統進行最佳化，幫助焦頭爛額的 IT 團隊減輕負擔。

這些技術都源自於單一的 FortiOS 作業系統，它可以提供整合式，以雲端為基礎的 SASE 解決方案，可保護使用者、應用程式和端點設備，同時與其他的分散式網路無縫連動。這種無縫的點對點解決方案整合了網路和資安功能，讓企業可以採用更具彈性的策略，在現今快速演變的數位市場中取得強大的競爭力。



Fortinet (NASDAQ : FTNT) 致力保護全球大型企業、服務供應商和政府組織的資安防禦。唯有 Fortinet 安全織網 (Security Fabric) 能解決最嚴苛的資安挑戰，為網路、應用程式、多雲或邊緣環境中的數位基礎架構提供滴水不漏的資安防護。Fortinet 的資安設備出貨量在全球排名第一，深受全球超過 50 萬客戶的信任。



官方網站



LINE@



Facebook



YouTube



與我們聯絡

