供應商中立的 SASE 評估檢查表 (Vendor-Neutral SASE RFP Checklist)

導言： 真正的 SASE 應透過單一、雲端原生的平台，無縫整合網路與安全功能，而非僅將不同的安全產品打包。這份檢查表旨在幫助企業識破「假整合(拼湊式整合)」的陷阱，從架構本質、安全深度、管理體驗與支援能力四大維度，客觀評估 SASE 供應商。

評分方式： 建議以 0-3 分進行評估 (0=不支援, 1=部分支援, 2=完全支援, 3=具備差異化優勢)。

底層架構與全球網路效能 (Infrastructure & Network)

避免陷阱：宣稱雲端原生，實際上卻是將傳統虛擬化安全設備 (如虛擬機 VM) 部署於公有雲環境，而非採用具備單一通道處理 (Single-Pass) 能力的雲端原生架構，這可能導致效能瓶頸與管理複雜性。

評估項目	關鍵評估點 (廠商必須回答的問題)	權重	評分	備註/廠商回覆
1. 單一通道架構 (Single-Pass)	流量是否透過 **單一通道平行處理 (Single-Pass Parallel Processing, SPPP)** 或 **單一通道雲端引擎 (Single-Pass Cloud Engine, SPACE)** 架構，僅需解密「一次」即可同時進行 ZTNA, SWG, CASB, IPS 等所有安全檢查，從而避免多個服務節點/VM 帶來的額外延遲？	高		*檢驗真假整合的核心*
2. 全球 PoP 節點覆蓋率	在企業主要營運據點（尤其是海外工廠/辦公室）是否有供應商「自行營運與管理」的全球 PoP 節點？（而非僅依賴第三方公有雲基礎設施或轉售其服務，這可能影響服務品質與控制力。）	高		
3. 雲端原生彈性	當流量暴增或開啟 SSL 解密時，平台是否能自動且無感地橫向擴充運算資源？	中		
4. 本地網路優化能力	SD-WAN 元件是否具備前向錯誤更正 (FEC)、封包複製等技術，能有效彌補品質較差的跨國寬頻線路？	中		

零信任與安全服務深度 (Security Services - SSE)

避免陷阱：舊世代安全策略原封不動上雲，缺乏上下文情境的存取控制。

評估項目	關鍵評估點 (廠商必須回答的問題)	權重	評分	備註/廠商回覆
1. 動態與持續驗證 (ZTNA)	存取權限是否能根據 **NIST SP 800-207 零信任架構 (Zero Trust Architecture, ZTA)** 的核心原則，依據「持續變動的情境」進行動態調整？（例如：員工設備的防毒軟體狀態、地理位置、存取行為等，以決定連線是否立即中斷或降級。）	高		*符合 NIST 零信任原則*
2. 私有應用程式隱形	私有應用程式是否透過 **零信任網路存取 (ZTNA)** 機制，對外網完全隱形？使用者是否無需擁有網路層存取權 (IP 路由)，即可安全地存取特定應用程式，實現最小權限原則？	高		
3. SaaS 應用精細控制 (CASB)	是否能透過 **雲端存取安全代理 (CASB)** 功能，精細區分企業版與個人版的 SaaS 帳號，並實施差異化策略？（例如：允許使用企業版 Google Drive 上傳，但禁止個人版上傳，以防止資料外洩。）	高		
4. 統一資料外洩防護 (DLP)	**資料外洩防護 (DLP)** 策略是否能實現「定義一次，全域套用」？（確保策略能跨越網路流量 SWG、雲端應用 CASB、內部連線 ZTNA 等所有安全控制點，提供一致性的資料保護。）	中		
5. 進階威脅防護	是否內建 **雲端沙箱 (Cloud Sandbox)** 與 **遠端瀏覽器隔離 (RBI)** 技術，以有效防禦零日攻擊、惡意軟體及高風險網站，提升整體安全態勢？	中		

使用者體驗與維運管理 (UX & Operations)

避免陷阱：管理介面多頭馬車，日誌無法關聯，員工抱怨網路變慢。

評估項目	關鍵評估點 (廠商必須回答的問題)	權重	評分	備註/廠商回覆
1. 單一管理窗格 (Single Pane of Glass)	網路 (SD-WAN) 與安全 (SSE) 是否在同一個管理控制台中設定策略與檢視日誌？（需要跳轉介面即扣分）	高		
2. 數位體驗監控 (DEM)	發生連線緩慢時，平台是否具備 **數位體驗監控 (DEM)** 能力，能精確指出瓶頸所在？（例如：是端點 Wi-Fi、本地網路、ISP 寬頻、SASE 節點還是 SaaS 伺服器，從而加速故障排除。）	高		*解決 IT 抓漏痛點*
3. 統一代理程式 (Single Agent)	終端使用者是否只需安裝「一個」輕量級 Agent，即可整合 **零信任網路存取 (ZTNA)**、**安全網路閘道 (SWG)**、**數位體驗監控 (DEM)** 等所有 SASE 功能，簡化部署與管理？	高		
4. 無代理程式存取 (Agentless)	對於無法安裝 Agent 的設備（如承包商、個人設備 BYOD），是否支援透過瀏覽器提供安全的 **無代理程式 (Agentless) ZTNA 存取**，確保所有使用者和設備都能獲得一致的安全保護？	中		
5. API 與生態系整合	是否提供豐富的 API 介面，能將安全日誌與事件無縫串接至企業現有的 **安全資訊與事件管理 (SIEM)** 或 **擴展式偵測及回應 (XDR)** 平台（如 Splunk, CrowdStrike），實現集中化監控與分析？	中		

商業條件、支援與未來發展 (Commercials & Future)

避免陷阱：初期看似便宜，擴張後授權費暴增；在地支援薄弱，出事找不到人。

評估項目	關鍵評估點 (廠商必須回答的問題)	權重	評分	備註/廠商回覆
1. 定價模式透明度	計價基準為何？（基於使用者數、頻寬用量或兩者皆有？）當增加新功能時，是否需要支付額外的授權費？	高		
2. 在地化支援與原廠認證	在台灣/本地是否有具備高階除錯能力的原廠工程師？合作夥伴 (例如 **歐米英泰 (Omni Intelligent**	高		

	Services)，其為 Cloudflare 在台灣的服務交付夥伴)的認證等級與其所代理的 SASE 產品線為何？			
3. 升級與維護機制	雲端平台的升級維護是否能實現「**近乎零停機時間 (Near Zero Downtime)**」？（需確認供應商的具體承諾，並釐清是否需要客戶手動介入更新硬體/VM，以確保業務連續性。）	中		
4. 威脅情資網路	供應商是否有強大的自有威脅情資研究團隊？其情報網路的廣度如何？	中		
5. AI/AIOps 藍圖	平台未來導入生成式 AI 或 AIOps 以簡化策略管理、加速事件調查的具體發展藍圖為何？	中		

總評與建議： (在此填寫基於上述評分的最終評估結果，決定是否進入概念驗證 POC 階段。)