

準備



開始採用 SASE 專案 之前的 5 個考量事項

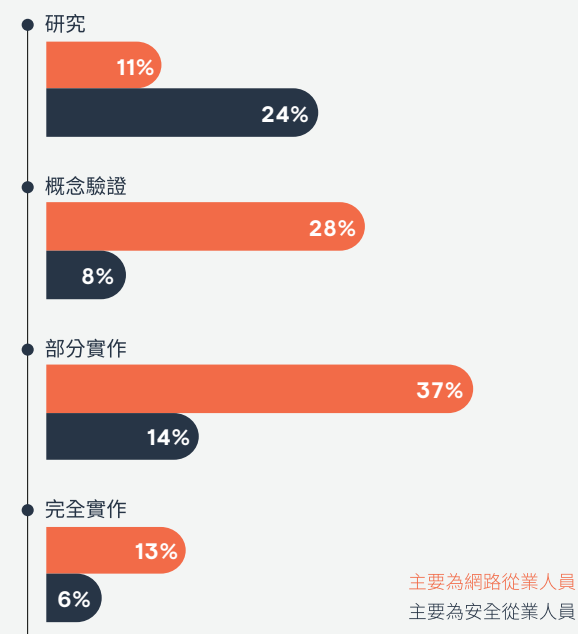
2021 年 3 月 EMA 白皮書
作者 Paula Musich

簡介

網路與安全性在雲端的融合稱為安全存取服務邊緣 (SASE)，這是一個新興市場，吸引著 IT 營運團隊尋求適應其網路與安全性架構，以求更能滿足數位轉型後企業的需求。此類數位轉型計劃在 2020 年加速發展，起因是全球疫情大流行以及讓資訊工作人員在家使用自有 Wi-Fi 與寬頻網路進行工作的需求突然增加。Enterprise Management Associates 的全新研究報告「新興 SASE 市場的可用性和採購選項」清楚指出網路專業人員主導了 SASE 的採用曲線，37% 熟悉 SASE 一詞的網路專業人員表示其企業已部分實作 SASE 專案。另外 28% 的網路專業人員表示其企業處於 SASE 評估或概念驗證實作過程中。同時，IT 安全從業人員中熟悉 SASE 者，僅 14% 表示其企業已部分實作 SASE，而另外 8% 則提到其企業實施了 POC。IT 網路專業人員最重視的 SASE 屬性包含 SD-WAN 連線能力，31% 的受訪者將其評為最重要的屬性，其次有 26% 受訪者認為最重要的是雲端多功能網路安全性，再來有 19% 受訪者將安全遠端存取評為最重要的 SASE 屬性。

無論帶動 SASE 採用的群體為何，以及最受重視的屬性為何，要確保任何 SASE 部署的成功，IT 營運團隊仍有許多需要思考的考量事項。此類考量事項可能包含 SASE 供應商是採用單一廠商還是多廠商方法、供應商是否與現有的安全性以及使用中的 SD-WAN 工具互相整合、SASE 產品的建構方式、如何讓網路與安全性團隊執行最妥善的整合部署，以及如何開始使用 SASE 專案。

受訪者企業的 SASE 執行過程



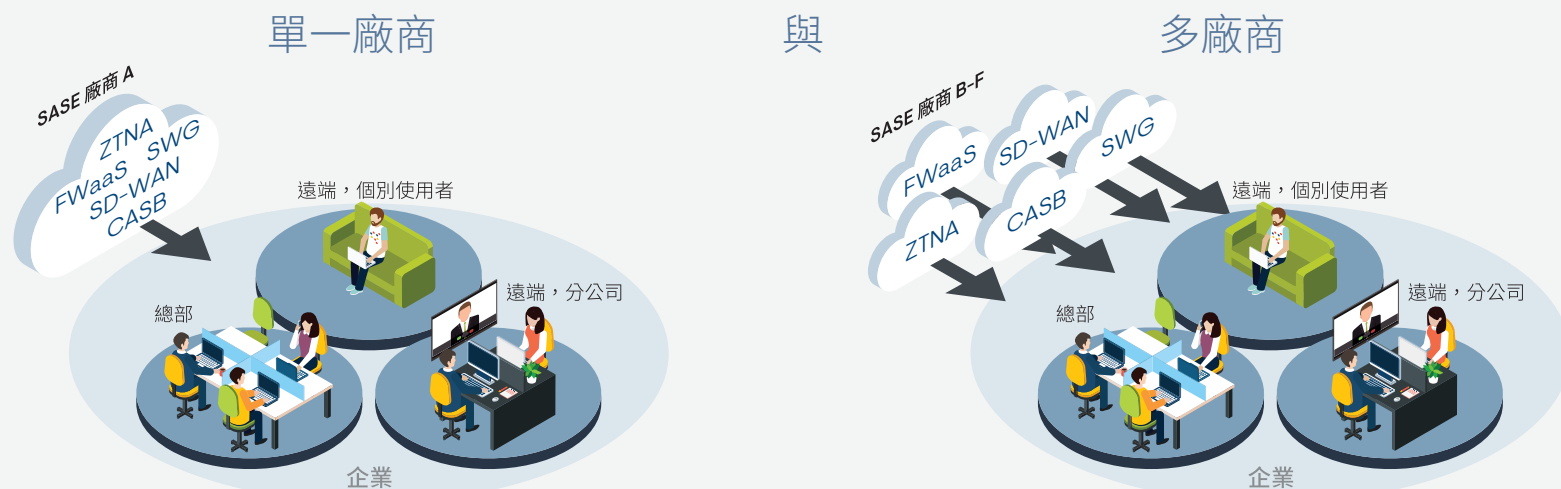
在 2020 年底實施的這兩項個別研究專案主要是以網路和安全從業人員為調查對象

01. 單一與多廠商 SASE

單一廠商 SASE 供應商致力於透過其本身的產品組合傳遞所有需要的 SD-WAN 與安全性功能，並為客戶提供單一的整合平台。而多廠商 SASE 供應商與廣泛的技術整合合作夥伴攜手合作，以提供一系列的 SD-WAN 與安全性功能。兩者各自有其優劣勢。

單一廠商 SASE 供應商在發生支援問題時容易找出癥結、更加簡化且一致的定價，以及對客戶而言整合度與一致性可能更高的政策管理體驗。然而，多數供應商難以提供客戶可能需要的全部網路與安全性功能。要達成這種廣泛的權衡可能會以個人功能的深度為代價。這可能會限制潛在客戶考量可靠廠商的範圍。

多廠商 SASE 方法則為客戶提供建立 SASE 部署的選項，並針對客戶的特定需求量身打造，以在多家供應商之間提供整合的最佳功能。這種方法也會引起一系列的問題，包含：合作夥伴解決方案的整合程度為何？整合合作夥伴是否已簽訂協議並妥善定義了工作流程，以在發生問題時順暢地提供支援，使客戶不必忙於究責？與此同時，多廠商 SASE 部署可能會讓 SASE 收購更加複雜且難以負擔，因為定價模型與單一合作夥伴全然不同。



02. 支援現有的安全性與網路管理工具

由於企業針對特定使用案例開始採用 SASE，而且企業將其新的 SASE 部署擴充至其他領域，IT 安全團隊與網路團隊將需要隨著新 SASE 的部署持續保護和管理現有的內部部署基礎結構。特別是 IT 安全團隊苦惱於如何整合目前使用的大量安全工具以實現合理化。這些團隊的當務之急是能夠將其 SASE 部署整合至企業內已使用的政策引擎與安全管理介面，以便降低操作複雜度並確保一致的政策執行，無論使用者位於何處或使用者以何種方式連線至整合網路。在此同時，一直會有 SASE 供應商未能提供的安全功能或服務，且 SASE 供應商必須提供一種方式，讓客戶在發生任何技術問題時能夠透過簡化的 API 自行啟用特定整合。

03. SASE 架構：輕型分支？重型分支？

SASE 供應商通常將其架構描述為輕型分支、重型分支或二者兼而有之。實質上，輕型分支是指從雲端交付的安全性，重型分支則會在本機執行安全任務。儘管需要深入封包檢驗以確保本機東西向流量安全時傾向於後者，卻會減損 SASE 降低操作複雜度與開支，以及改善部署靈活度的優勢。重點在於佈建、管理與政策決策都是在雲端進行，而 SASE 服務可以擴大利用規模與彈性，同時政策執行會在本機的代理程式、虛擬設備或更小佔用空間的裝置中發生。

04. 成功的 SASE 部署：需要同心協力

對於多數的大型企業而言，成功的整合網路與安全基礎結構需要網路與安全團隊之間的緊密協作，然而兩個 IT 營運團隊往往無法彼此緊密配合。若要達成此類協作，將需要大型企業的文化轉型，而他們將必須重新評估其建構的方式、仔細檢驗採用 SASE 方法的方式，以及決定預算從何而來。重點在於確保 IT 管理最高層（特別是 CIO 與 CISO）對於任何 SASE 專案的支持，透過建立虛擬 SASE 團隊並同時納入網路與安全架構師以主導部署，藉以協助促進文化轉型。這些 IT 與安全執行主管將需要同心協力建立更嚴謹的新目標與誘因，確保這些團隊有效率地共同保障部署後的操作能夠順暢執行。

05. 如何開始

已開始使用 SASE 的人員通常會建議其同行尋求 SASE 部署，從少量特定使用案例開始，然後隨時間在新的專案商機出現時擴充至其他使用案例。使用案例的範例包含行動使用者的遠端存取安全、MPLS 更換專案，或將邊緣防火牆取代為雲端安全的計劃。較小的網站可以作為新 SASE 部署的實驗場所。由於現有防火牆或網路篩選的合約需要更新，SASE 應視為一種替代方案。在早期率先採用的 SASE 客戶之間，典型的部署取決於三種迥異的情境。第一種涉及將遠端存取安全從內部部署裝置移至 SASE 雲端，搭配規劃用於後續部署階段的 SD-WAN 整合。第二種以 MPLS 到 SD-WAN 的移轉作為主軸，搭配規劃用於後續部署階段的雲端安全整合。第三種也是最具變革性的一種方法，也就是一併將安全與 SD-WAN 直接移至雲端。後者需要縝密的規劃以確保成功，但如此可以立即帶來更大的優勢。

關於 Palo Alto Networks

Palo Alto Networks 是全球網路安全產業的領導廠商，我們的技術不斷改變人員與企業的工作方式，打造以雲端為中心的未來格局。我們的目標是成為您網路安全合作夥伴的首選，為人們的數位生活方式提供安全保護。我們協助處理世界上最艱鉅的安全性挑戰，在持續的創新之中不斷掌握人工智慧、分析技術、自動化和協調技術上的最新突破。我們提供整合式平台，培養日益壯大的合作夥伴生態系統，因此始終能夠站在安全產業的最前線，為成千上萬企業的雲端、網路與行動裝置提供安全保護。我們的願景是讓世界一天比一天更加安全。如需瞭解更多資訊，請造訪 www.paloaltonetworks.com。

Palo Alto Networks、Prisma 和 Palo Alto Networks 標誌是 Palo Alto Networks, Inc. 在美國與全球各個司法管轄區的註冊商標。本文使用或提及的所有其他商標、商品名稱或服務標識皆屬於其各自的擁有者。



關於 Enterprise Management Associates, Inc.

Enterprise Management Associates (EMA) 成立於 1996 年，是一家業界領先的分析公司，針對 IT 與數據管理技術提供全方位的深入見解。EMA 分析人員利用了獨特的實務經驗組合、對業界最佳實務的見解，以及目前與規劃中廠商解決方案的深度知識，協助 EMA 的客戶達成其目標。深入瞭解適用於企業業務單位使用者、IT 專業人員以及 IT 廠商的 EMA 研究、分析以及諮詢服務，網址為 www.enterprisemanagement.com。您也可以在 [Twitter](#) 或 [LinkedIn](#) 上關注 EMA。

未經 Enterprise Management Associates, Inc 事前書面許可，不得複製、重製、儲存於檢索系統，或轉發此報告的全部或部分內容。本文中所有意見和預估皆僅構成當時的評論，內容如有變動，恕不另行通知。本文提及的產品名稱皆為其各自公司所擁有之商標和/或註冊商標。「EMA」與「Enterprise Management Associates」為 Enterprise Management Associates, Inc. 在美國與其他國家/地區的商標。

©2021 Enterprise Management Associates, Inc. 保留所有權利。EMA™、ENTERPRISE MANAGEMENT ASSOCIATES® 與 Mobius 符號為 Enterprise Management Associates, Inc. 的註冊商標或普通法商標。