CLOUDFLARE

白皮書

SASE 使用案例買家指南

如何在旅程中確定優先任務並選取合適的平台

目錄

如何使用本指南

本指南的適用對象是誰？

儘管針對安全存取服務邊緣 (SASE) 進行網路和安全現代化改造最終將使整個組織中的每個人都受益，但《**SASE 使用案例買家指南**》主要面向以下人群：

CIO

負責組織的整體數位現代化策略並最佳化 IT 成本

網路主管

負責提供高效能、有韌性且安全的現代網路來支援企業目標

CISO

專注於提高網路威脅復原能力，加強整體安全狀態並減少外洩成本

無論您組織的 SASE 之旅從以安全為主導、以網路為主導的 IT 工作開始，還是從理想的完全協作的跨部門 IT 工作（跨越安全、傳統網路和現代 DevOps 團隊）開始，您選取的技術平台都必須為每個團隊服務。一個真正的 SASE 架構應該足夠靈活且可組合，以完成每個團隊的短期和長期藍圖上的優先使用案例，本指南將在您確定使用案例和縮小廠商範圍時幫您引導那些規劃談話。

如何使用本指南

您可以使用本指南做什麼？

如今，許多組織都明白採用 SASE 架構大有前景，但沒有「一體適用」的藍圖來實現。在每個組織獨特的 SASE 旅程中，會面臨各種各樣的安全和網路現代化挑戰，並且每次 SASE 實作都不一樣。

為了幫您找到獨特的 SASE 旅程的起點，請使用**《SASE 使用案例買家指南》**來：

- **確定 SASE 的開始使用案例**和「快速致勝方案」以及長期但敏捷的專案藍圖。反思內部優先任務以促進可能有助於其排名的跨部門討論。
- **安排與廠商對話**：除了「我也是」聲明和商品化功能以外，提出一些範例問題。深入瞭解廠商技術架構的核心（前端介面以及後端網路、運算和儲存）以及長期商業策略。
- **評估 SASE 選項**：利用在核心服務元件中組織的範例注意事項。瞭解廠商平台的獨特元素，以關注那些可能超越預期的基本元件的元素。

本指南假設您已熟悉 SASE 架構的主要原則和元件，但為了清楚起見，在附錄中包括了一份詳盡的「SASE 入門指南」。

找到起點：優先使用案例

Gartner®, Inc. 確定了三個單一廠商 SASE 使用案例[1]，可幫助區分組織的首要任務：

1. **基本 SASE**：本使用案例涵蓋一種易於操作的產品，通常涉及希望保護公用和私人應用程式使用者的中型企業 (MSE)。
2. **網路驅動 SASE**：本使用案例涵蓋希望部署具有進階網路功能之 SASE 的企業。
3. **具有進階安全性的 SASE**：這適用於需要最佳安全性但易用性優先順序較低的組織。

Cloudflare 還注意到，一些客戶主要關注提升終端使用者體驗，因此透過有時稱為**「咖啡店網路」**的趨勢簡化基礎架構。

雖然這個模型通常是有用的，但很多組織更願意討論範圍較窄的使用案例（類似於一個有範圍的可實現的專案），以致力於簡化旅程以及更好地闡明短期和長期目標。在 SASE 旅程中從小處著手也有助於證明功效、獲得內部動力以及增加利害關係人的支援，從而提高未來認同更大專案的可能性。

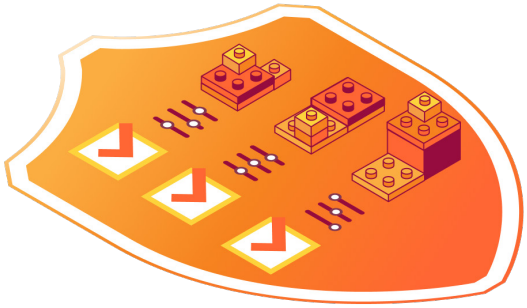
關於如何選擇起點，並不存在完美的答案，但常被提及的內部決策因素包括：

- **對變化的靈活性和開放性**——例如，如果試點專案可以更嚴格地限制範圍，並在現有基礎架構內進行，則安全團隊可能是起點 SASE 使用案例最好的首批客戶
- **實作速度**——尤其是承包商的遠端存取需求有限，可能通常無需安裝終端使用者軟體即可滿足，該軟體可以簡化專案推出並提供「快速致勝方案」來加強安全性
- **面臨更大攻擊風險的使用者/角色**——可以存取寶貴的智慧財產權的開發人員、安全/風險專業人員或高管可能是主要目標
- **面臨更大攻擊風險的應用程式**——例如，含有客戶或財務資料的敏感性內部應用程式
- **員工體驗意見反應**——考慮終端使用者投訴，以確定哪些內部工作流程可以從起點專案工作中受益，從而提高業務生產力
- **現有合約時間/組織工作**——即將為目前的單點解決方案續約可能會將您的關注轉向要解決的相關使用案例，並協助為傳統解決方案擴充或取代建立目標時間表

看看下方的使用案例，它們組織成更大的公司計畫，以反思在較長期專案藍圖的環境內，哪個使用案例可能對組織的目標產生最直接的影響。雖然您的內部優先任務和現有的 IT 堆疊最終會引導您走上最佳道路，但大多數組織都選擇了結合數個上述設定優先順序準則（如擴充 VPN、保護承包商存取、防止多通道網路釣魚、保護遠端工作者和分散式辦公室，或簡化分支機構連線）的開始使用案例。

不過，可程式設計的組合式 SASE 架構的最大好處就是沒有完美的操作順序。隨著時間的推移，不僅可以變更業務優先事項，還可以整合新技術。雖然推薦制定一份長期藍圖，不過，您應該會希望能夠靈活調整計畫。

關鍵是不要因為過度計畫，而將開始時間延遲太久。**相反，您可以將由 SASE 架構解決的數十個使用案例視為累積的：**即便實作一兩個使用案例，也會增強您組織的安全狀態，並且由於 SASE 平台上的跨服務互動，實作一個使用案例可能會讓未來實作另一個使用案例時變得更輕鬆。



計畫：採用 Zero Trust

現代工作方式（例如，混合式工作、多雲端擴張、未受管理的裝置等）帶來了新的安全性挑戰。因為依賴於傳統的基於邊界的安全性，組織不僅可見度有限、設定相互衝突，而且面臨過高的風險。

因此，組織開始轉向 Zero Trust 安全性 最佳做法，並將其作為更大規模 SASE 旅程的核心原則。這種做法基於對驗證維持精細的存取控制，依預設不信任任何人或任何物（即便位於網路週邊內亦是如此）。

使用案例：擴充或取代 VPN

基於網路週邊的控制（例如，虛擬私人網路 (VPN)）可能會擴大攻擊面、限制可見度，並讓終端使用者感到挫敗。VPN 越來越成為攻擊的目標，並且越來越容易發生外洩；它們還「拉長」了往返於中央內部部署設備的所有流量的時間，這在存取內部工具和資料時會導致延遲（並影響生產力）。

因此，遷移到 SASE 模型的一個常見驅動因素是改善資源存取和連線。在盡可能靠近使用者的全球雲端網路上路由和處理網路流量（即透過 Zero Trust 網路存取 (ZTNA) 而不是透過 VPN）可以減少終端使用者的摩擦，同時消除橫向移動的風險。開始卸載關鍵應用程式，以獲得更好的安全性和終端使用者體驗。

使用案例：保護承包商/未受管理的裝置存取

為第三方使用者（承包商、代理機構、供應商、合作夥伴等）設定安全存取可能會帶來額外的風險和管理開支。這些共同作業者通常僅需在有限的時間內存取一組有限的資源，但傳統存取控制方法可能會意外過度佈建權限。向所有人配發企業裝置通常也不可行，而且未受管理的裝置缺乏企業配發裝置的保護和可見度，從而增加風險。特別是鑒於承包和臨時工作因混合式工作仍然廣受歡迎，很多團隊選擇在 SASE 旅程的早期確保承包商的存取權。

設定 Zero Trust 原則可確保承包商僅在需要的時候存取所需的內容。特別是無用戶端 ZTNA 可以快速部署，可在沒有終端使用者軟體需求的情況下幫助承包商快速部署。承包商可以透過社交登入選項「自帶」身分識別，而 ZTNA 則充當所有身分識別的彙總層。您也可以輕鬆新增其他資料保護措施以增強安全狀態。

使用案例：緩解勒索軟體攻擊

由於 Zero Trust 會持續監控並定期重新驗證使用者和裝置，因此一旦偵測到感染，它就可以透過撤銷網路和應用程式存取權來防止勒索軟體攻擊的傳播。Zero Trust 還遵循「最低權限」原則進行存取控制，使勒索軟體難以提升其權限並獲得對網路的控制權。

使用案例：檢視並減少資料暴露

使用 Zero Trust 原則限制哪些人員可以存取哪些應用程式有助於防止資料外流，但您可以採取進一步措施，使用資料保護策略來偵測潛在的暴露並強化安全狀態，從而緩解資料外洩的風險。這可能包括掃描熱門 SaaS 套件（如 Google Workspace、GitHub 和 Salesforce），來尋找存在外洩風險的敏感性資料和設定錯誤，然後根據規範指導來透過封鎖或其他管理員行動進行補救。

案例研究：採用 Zero Trust

《財富》雜誌前 500 大電信服務提供者使用 Cloudflare 確保 100,000 多名混合工作者的安全

- 資訊、電信和技術 (ICT) 解決方案的全球領導者
- 5G 網路基礎架構的主要提供者之一
- 在歐洲、印度和美國擁有 100,000 多名員工

挑戰：

擴展部門和地區間的存取控制

經過數十年的技術創新和發展，一家《財富》雜誌前 500 大電信服務提供者開發了一個複雜的 IT 和安全性架構，可涵蓋數百種舊版應用程式。

內部部署基礎架構變得難以維持。IT 複雜性降低了他們加強安全性和實作 Zero Trust 最佳做法的能力。而依賴 Cisco Umbrella 成為一種負擔——原則很難針對特定的使用者群組進行調整；基本網路存取需要廣泛的管理監督；它所提供的威脅防護在公司的架構中留下了漏洞。

公司開始尋找轉移到更敏捷的雲端環境的方法。這包括：

- 選擇一個安全合作夥伴以支援將應用程式從內部部署環境遷移至 AWS、Azure 和其他雲端環境
- 用更簡單、更具成本效益的 DNS 篩選取代 Cisco Umbrella

主要成效

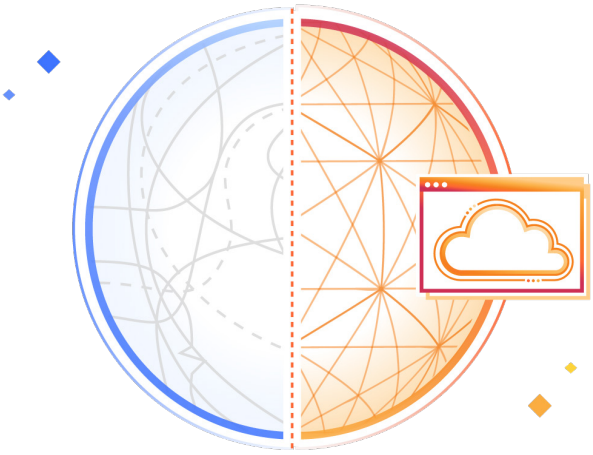
採用 Cloudflare 的 ZTNA 和 SWG 服務：

公司意識到，支援混合員工和數位化轉型的雄心需要將安全性整合到基於雲端的單一平台上。

在部署 Cloudflare 的 ZTNA 和安全 Web 閘道 (SWG) 服務（分別為 Cloudflare Access 和 Cloudflare Gateway）之後，公司：

- **保護了混合式工作**：針對 100,000 多名員工的應用程式和網際網路存取採取統一控制
- **取代了 Cisco Umbrella**：使用 Cloudflare 來防範惡意程式碼、網路釣魚和其他威脅
- 針對 AWS、Azure 和其他雲端環境中的數百種應用程式**實作了基於身分識別的 Zero Trust 原則**
- **無需再使用多個原則構建介面**來處理不同的 VPN 和網際網路篩選服務
- **集中進行記錄**，簡化了 SOC 事件回應和所有合規性稽核

計畫：實現網路現代化



組織可以利用分散式的動態雲端原生 SASE 服務來實現網路現代化，而不是在當今的分散式環境中盡可能長久地維護傳統企業網路。

整合網路和安全服務降低了複雜性和風險，進而幫助企業變得更敏捷，更有競爭力。

使用案例：簡化分支機構連線/從 MPLS 或傳統 SD-WAN 轉換

高效連接分支機構是一種挑戰。多通訊協定標籤交換 (MPLS) 佈建和調整單點解決方案花費了太長時間；透過拼湊的網路安全設備回傳流量提供了一種糟糕的不安全體驗；大量低效情況迅速翻倍。同時，如果傳統的 SD-WAN 實作針對分支機構之間的流量繞過雲端安全性，則可能會增加風險

採用 SASE 架構，您可以擴充或取代 MPLS 電路和傳統網路設備拼湊而成的方案，以便更輕鬆地在分支機構之間路由流量，並促進不同位置之間的網站到網站連線。在實體位置內部署所需的最少硬體，並使用低成本網際網路連線到達最近的「服務邊緣」位置。

使用案例：減少/消除 DMZ

組織使用 DMZ（非保護區網路）在與企業防火牆隔開的網路區段中託管公用或私人應用程式，旨在防止暴露企業網路的其餘部分。然而，DMZ 作為一種網路建構的重要性不斷下降，因為可以採取替代方式來構建和託管應用程式且不會暴露。

除了利用現代應用程式和網路服務將 DMZ 安全性轉移至雲端以外，組織還可以開始減少或完全消除對 DMZ（和 VPN）的需求。透過採用 Zero Trust 方法，組織可以在不允許輸入流量的情況下提供簡單、安全的存取。這可大大縮小攻擊面，提高對哪些人員可以存取哪些內容的可見度，而無需稽核防火牆或網路。

設定 Zero Trust 原則可確保承包商僅在需要的時候存取所需的內容。特別是無用戶端 ZTNA 可以快速部署，可在沒有終端使用者軟體需求的情況下幫助承包商快速部署。承包商可以透過社交登入選項「自帶」身分識別，而 ZTNA 則充當所有身分識別的彙總層。您也可以輕鬆新增其他資料保護措施以增強安全狀態。

使用案例：緩解勒索軟體攻擊

由於 Zero Trust 會持續監控並定期重新驗證使用者和裝置，因此一旦偵測到感染，它就可以透過撤銷網路和應用程式存取權來防止勒索軟體攻擊的傳播。Zero Trust 還遵循「最低權限」原則進行存取控制，使勒索軟體難以提升其權限並獲得對網路的控制權。

使用案例：檢視並減少資料暴露

使用 Zero Trust 原則限制哪些人員可以存取哪些應用程式有助於防止資料外流，但您可以採取進一步措施，使用資料保護策略來偵測潛在的暴露並強化安全狀態，從而緩解資料外洩的風險。這可能包括掃描熱門 SaaS 套件（如 Google Workspace、GitHub 和 Salesforce），來尋找存在外洩風險的敏感性資料和設定錯誤，然後根據規範指導來透過封鎖或其他管理員行動進行補救。

案例研究：實現網路現代化

網路即服務讓鞋類零售商 DTLR 走向 Zero Trust

- 成立於 1982 年
- 總部位於美國的鞋類和休閒服飾零售商，擁有將近 250 間分店
- 僱用了 3,000 多名店員

挑戰：

提高網路邊緣安全性

生活方式零售商 DTLR 正在大力推進數位化轉型。店長尋求更好的資料分析，企業希望客戶的線上訂單能夠在兩個小時內從實體店提貨。

然而，他們的 IT 基礎架構很難同步發展。例如，其安全架構所包括的 IPSec VPN 可將店鋪連線至集中位置，這「從 IT 的角度看完全缺乏控制。」

DTLR 也面臨著獨特的安全性挑戰（例如，將 DTLR Radio 內容安全地廣播到所有門店）。

其 IT 總監 Nigel Williams-Lucas 對 Network World 表示，「...我們需要一個單一視角，讓我們無需挨個走訪每家店，就能讓變更在所有零售店內生效。我們希望能夠對事情進行稽核來確保其正確。而為了網路安全，我需要能夠看到流量輸入和輸出。」

DTLR®

主要成效

使用 Cloudflare 的 Zero Trust 和網路服務：

DTLR 需要循序漸進、有條不紊地向雲端遷移，同時保持可預測的成本。

該公司（已經在使用 Cloudflare 的 DNS 服務）選擇了 Cloudflare 的網路即服務 (NaaS) 來開啟通往 Zero Trust 的分階段旅程。

使用 Cloudflare，DTLR：

- 使用 Cloudflare Tunnel **在 Zero Trust 模型中部署了應用程式**，而不必變更防火牆
- **提升了網路效能**，每個店鋪現在都連接到了最近的 Cloudflare 網路連接點 (PoP)
- **取得了對端點流量流程的可見度**，並關閉了不再使用的傳統端點
- **強化整體安全狀態**：「我們現在瞭解網路中的流量情況，因此，應該能夠構建適用於未來的更好、更強大的安全狀態。」

計畫：保護您的攻擊面

隨著企業不斷創新、擴展，以及數位足跡越來越多元化（從雲端遷移到增強 API 驅動的功能），他們無意間創造了更多的進入點和媒介以供對手利用。

隨著組織採用分散式/混合式工作、加速雲端遷移並投資於數位化轉型，SASE 方法可提供保護以防攻擊面不斷擴大。

使用案例：防止多通道網路釣魚和商業電子郵件入侵

攻擊者越來越多地將網路釣魚誘餌投放於使用者對點擊位置不太謹慎的通道。在「多通道」網路釣魚中，攻擊可能源於電子郵件之外，如 SMS/文字簡訊、IM、社交媒體、雲端協作/生產力服務以及通常不受電子郵件安全控制保護的其他工具。SASE 從單一平台實現了對以上所有環境的全面保護，從而緩解了透過進階網路釣魚策略進行認證盜竊、帳戶盜用或資料外流的風險。

使用案例：保護遠端工作者

遠端工作擴大了攻擊面，因為更多分散的使用者和未受管理的裝置都需要存取內部資源。採用 SASE 架構擴展了可見度和控制來支援「無周邊」模型，讓您能夠透過單一的統一平台，針對網路內外的威脅強制執行一致的防禦。擴大安全周邊以適應「隨處辦公」的方法也可確保高效的使用者體驗，並幫助從任何地方留住最優秀的人才。

使用案例：保護分散式辦公室

清理辦公室流量的傳統方法包括將流量回傳至集中式企業資料中心，這可能會增加延遲並損害生產力。同時，允許員工直接存取網際網路會導致每個地點的保護措施不一致、低效甚至無效。相較之下，SASE 方法透過在不同的辦公室提供一致的高效能安全性實現了混合式工作，同時降低了管理網站特定防火牆或其他內部部署設備的開支。

使用案例：保護 WAN

透過 SASE，組織簡化了連接和保護辦公室、資料中心和雲端的方式。這意味著，透過為廣域網路 (WAN) 新增防火牆和基於代理的 SWG 控制，針對位置（分支機構、資料中心等）之間的流量以及進出這些位置（進出更廣泛的網際網路）的流量套用篩選和檢查。一些 WAN 解決方案針對分支機構之間的流量繞過了雲端安全性，因此，安全服務和 SD-WAN 之間的整合理念可能不像最初看起來的那樣，具體取決於廠商。

案例研究：保護您的攻擊面

Werner Enterprises 與 Cloudflare 合作，整合電子郵件、應用程式和網路安全解決方案

- 成立於 1956 年
- 北美最大的整車運輸公司之一
- 使用一流的技術為客戶提供最佳化的路上貨物管理服務和資源

挑戰：

阻止網路釣魚和 BEC 攻擊，並確保內部部署/雲端混合基礎架構的安全

由於其員工的規模和地理多樣性，以及廣泛使用電子郵件進行通訊，Werner Enterprises 對網路釣魚和商業電子郵件入侵 (BEC) 攻擊感到擔憂。隨著從電子郵件產生的威脅不斷增加，該公司以前的電子郵件安全系統已經無法應對了。

此外，Werner 還系統地將舊版內部部署應用程式遷移至雲端，以便北美資源能夠在不受傳統 VPN 限制的情況下工作。

在轉換期間保持這些核心系統的可用性至關重要，保護客戶的商業歷程記錄及其員工的個人識別資訊 (PII) 亦是如此。

該公司還尋求最大限度減少工具氾濫，並減少管理多個廠商安全解決方案的複雜性。

主要成效

使用 Cloudflare 的電子郵件安全和網路安全服務：

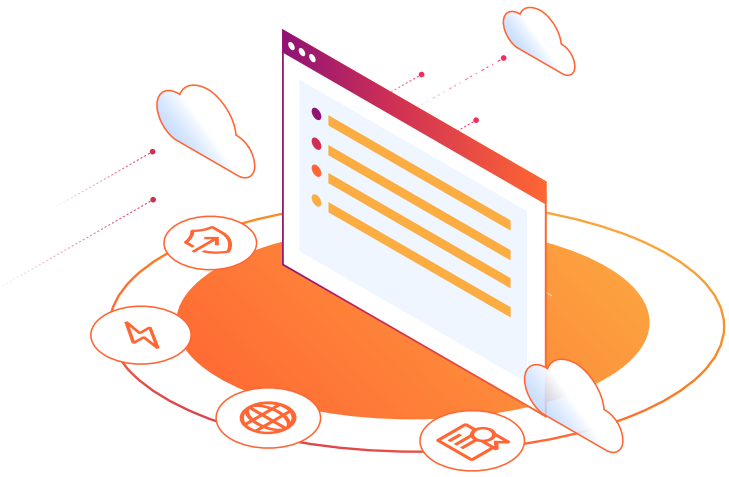
Werner 想要一套統一的工具，幫助他們遷移到雲端，以緩解威脅、提高效能，並為客戶及使用者提供與他們實際在大樓中一樣的安全性。使用 Cloudflare 的電子郵件安全和網路安全服務，該公司：

- **將使用者收件匣中的惡意電子郵件減少了** 50% 以上
- **每天減少了數小時的手動電子郵件分類工作**，讓團隊重新投入到實現策略業務目標的工作中
- **將核心傳統服務遷移**至雲端，且沒有中斷關鍵業務或客戶服務

透過整合到單一廠商、單一介面的解決方案，Werner 降低了系統複雜性，促進了自動化並提高了資料可見度。

WERNER ENTERPRISES

計畫：實現應用程式現代化



現在，從點早餐到處理工資，所有事情都可以透過應用程式完成。然而，舊版應用程式（無論是面向消費者還是用於後台功能）需要實現現代化，以便進一步支援資料驅動或採用 AI 技術。

應用程式還需要對終端使用者保持安全、彈性和高效能，並提供可擴展性來處理資料增長，同時仍然滿足資料控管要求。SASE 架構可以幫助開發人員及其關鍵共同作業者簡化應用程式現代化程序的數個階段，同時確保其安全。

使用案例：確保應用程式存取和雲端遷移的安全

開發人員應該能夠專注於透過他們旨在提供的商業價值視角構建新的應用程式，而無需擔憂從零開始建立自訂安全存取機制。ZTNA 充當一個組織所有資源的存取彙總層，與所有現代身分識別通訊協定整合，從而在企業中以一致的方式簡化對新應用程式的安全存取。

對於那些對舊版內部部署應用程式進行現代化改造和將其遷移至雲端的團隊而言，現代化的存取解決方案還可以透過相同的 ZTNA 解決方案連接內部部署和雲端執行個體，從而實現輕鬆轉換並確保終端使用者存取體驗在整個遷移過程中的連續性。

使用案例：保護特殊權限（開發人員/IT）存取

開發人員需要對關鍵基礎架構的特殊存取權限，這讓他們成為了有吸引力的攻擊目標。他們需要能夠存取多個不同的資源類型（SaaS、自託管、SSH/VNC/RDP 等），但不會感覺被過於嚴格的安全性所束縛。Zero Trust 方法可透過流暢的低延遲使用者體驗，幫助特殊權限使用者保持高效，同時保持最低權限存取。透過工作階段記錄，可以進一步瞭解特殊權限使用者工作階段，從而加強對更高風險工作流程的可見度。

使用案例：防止洩漏和竊取開發人員程式碼

程式碼資料快速增長。開發人員程式碼推動了數位業務，但這些高價值原始程式碼也可能會在許多開發人員工具中暴露或成為竊取目標。保護在 SaaS 資料存放庫（如 GitHub Copilot）中儲存和共用的程式碼，並使用 SASE 查看暴露的程式碼並控制其去向。

使用案例：確保 DevOps 工作流程安全

DevOps 團隊希望能夠更輕鬆地建立安全的 Zero Trust 連線以加速測試。一些 SASE 解決方案將其覆蓋範圍延伸至使用者到應用程式使用案例以外，以覆蓋網狀和點對點安全網路，並支援服務到服務工作流程和雙向流量。實現真正的任意連線現代化有助於簡化持續整合和持續交付 (CI/CD) 管道及其相關聯的流量流程。

案例研究：實現應用程式現代化

Cloudflare Zero Trust 為 5,000 多名 Creditas 員工居家辦公存取提供安全保障

- 巴西最大的貸款金融科技平台
- 47 億美元估值
- 在拉丁美洲、歐洲和墨西哥提供房屋淨值、汽車和擔保貸款以及其他服務

挑戰：

在夜間為 5,000 名員工提供對內部工具和應用程式的安全存取

當 COVID-19 襲擊巴西時，巴西政府指示 Creditas 讓所有人回家。Creditas 有 48 小時的時間來變更整個工作模式，從 100% 現場辦公轉變為幾乎完全遠端辦公。

在為了滿足這一要求做準備時，工程團隊面臨著多個挑戰，包括：

- 維護傳統 VPN，它需要複雜的設定才能在不同的作業系統上執行，並且只能支援一小部分員工
- Creditas 團隊與其協力廠商共同作業，花費了大量時間來修改新的 VPN 工具，然後才能安全使用
- 維護安全和資料保護標準以及監管合規性

主要成效

採用 Cloudflare 的 ZTNA 服務：

Creditas（最初是 Cloudflare 核心應用程式安全套件的客戶）改為簡化員工連線以及保護內部資源存取，來滿足政府保護遠端工作的高壓期限。

Creditas 迅速部署了 Cloudflare 的 ZTNA 服務 (Cloudflare Access)，強制在員工中針對每個應用程式執行基於身分識別的驗證。

主要成果包括：

- 將應用程式委託和實作所花費的時間從 2-4 週減少到兩天，**提高了開發營運生產力**
- **簡化了員工連線**並確保了 45 款易受攻擊的應用程式和內部資源的安全
- **員工增長了一倍**，而工程支援員工只增加不到 30%

creditas

計畫：隨時隨地保護您的資料

資料跨越的環境超出了大多數組織所能追蹤的範圍；例如，敏感性資料可能會因未經批准使用產生型 AI (GenAI) 和影子 IT 而暴露。這些不斷擴張的雲端和 SaaS 環境帶來了更多的風險。

因為 SASE 將 Web、SaaS 和私人應用程式環境中的資料可見度和控制融合到一個架構中，所以它有助於簡化組織滿足監管要求的方式並提前應對現代資料風險。

使用案例：簡化資料隱私法規合規性

資料隱私從未像現在這樣成為人們的頭等大事；例如，2023 年，立法者開出了一張破紀錄的價值 12 億歐元的罰單，原因是 GDPR 違規。預計將會出台更嚴格的要求來保護使用者資料，特別是隨著大型語言模型 GenAI 以及其他 AI 工具的使用不斷增加。

SASE 幫助組織努力確保資料安全和私密：透過統一所有環境中的控制和可見度可以封鎖受監管資料類別、透過記錄維護詳細的稽核追蹤，並加強安全狀態來降低外洩風險。

使用案例：管理影子 IT

SASE 可幫助組織重新獲得對影子 IT 的控制並緩解其帶來的風險。透過內嵌式雲端存取安全性代理程式 (CASB) 代理流量會記錄每一個連線和請求，以顯示未經批准的 SaaS 應用程式，以及使用者在其中所採取的動作。然後，管理員可審查這些應用程式、核准/封鎖它們，並相應地套用身分識別和裝置驅動的原則。

使用案例：安全使用產生型 AI

SASE 服務可幫助組織安全而高效地使用產生型 AI，從流量來源（無論是來自員工還是自動化服務）到流量目的地（例如，ChatGPT 等公用應用程式或私人 AI 應用程式），均會套用控制和可見度。

例如，使用 SASE 平台的安全 Web 閘道 (SWG)/內嵌 CASB 服務，安全團隊可以偵測並核准 AI 應用程式使用，掃描設定錯誤（這些錯誤會透過 API 驅動的 CASB 帶來資料外洩風險），或在隔離的 Web 瀏覽器中執行 AI 應用程式以限制資料輸入和輸出。

使用案例：保護敏感性資料

採用 SASE 服務，組織可以偵測並控制敏感性資料進出其 IT 環境以及在其中移動的方式。這包括掃描應用程式和檢查流量以尋找敏感性資料，這些資料可能是受監管資料（如 PII、健康、財務資訊），也可能是高價值資料（如開發人員程式碼或智慧財產權）。針對資料竊取或無意外洩的其他 SASE 保護措施包括使用 Zero Trust 最佳做法確保資料存取安全、封鎖網際網路威脅（如網路釣魚和勒索軟體）。

案例研究：隨時隨地保護您的資料

Applied Systems 整合員工、應用程式和網路的安全性，加速數位化轉型

- 創立於 1983 年
- 為保險業構建 SaaS 解決方案
- 在美國、英國、加拿大、西歐和印度擁有 2,500 多名員工

挑戰：

加速數位化轉型

網路安全對 Applied Systems 而言至關重要，該公司必須為其保險客戶的大量財務資料、付款記錄、PII，以及其他受監管和敏感類別的資訊提供安全保障。

Applied Systems 在迎來一個全新的執行團隊之後，開始尋找機會，以不斷增強敏捷性、高效性和安全性。他們擁有不同廠商的元件，但也有怨言；例如，開發人員抱怨 Zscaler 封鎖了工作關鍵型網站並損害了生產力。

Applied Systems 專注於整合大量的安全和網路功能，包括：

- 增強面向公眾的網站和應用程式的保護和效能
- 在整個網路基礎架構中提供安全且可擴展的連線
- 為員工和內部資源提供 Zero Trust 安全狀態

APPLIED

主要成效

採用 Cloudflare 的應用程式服務和 Zero Trust 產品組合：

Applied Systems 希望與瞭解雲端原生客戶預期的雲端原生廠商建立合作夥伴關係。為了提高技術效率並支援業務發展和抱負，Applied Systems 部署了大量的 Cloudflare 應用程式服務、Zero Trust 和網路連線服務。

主要成果包括：

- **保護存取**：2500 多名員工可安全存取自託管應用程式和基礎架構，取代了 Zscaler 和 Cisco
- **靈活性**：可調整控制的嚴格程度，以滿足不同的使用者需求
- **資料受到保護**：在新興 AI 工具（包括 ChatGPT 和 Bard）內保護資料

Applied Systems 的 CISO 表示：「當客戶問及我們的監管合規性時，我們可以告訴另一方的 CISO，我們是 Cloudflare 的客戶，並對我們正在使用的產品進行說明。」

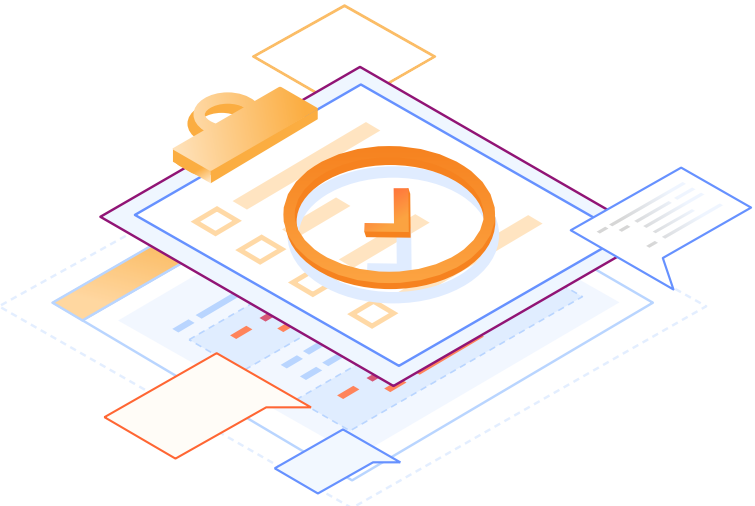
執行廠商評估

在全面瞭解您組織的需求之後，**尋找一個可以滿足您 SASE 之旅任何階段需求的廠商**，並與您用於網路入口、身分管理、端點安全、記錄儲存以及網路安全局勢其他部分的現有工具整合。

許多廠商都擁護一體化平台，但實際上，它需要組織整合幾個不同的單點產品。

基於角色的開場白

雖然傳統的廠商「並排」比較仍然是有價值的，但人們往往會更關注功能檢查清單，而在市場發展如此迅速的情況下，後者很難客觀執行。新的小工具可能明天就會出現在任何給定廠商的解決方案中，但深層的基礎架構優勢（或瑕疵）會持續更長時間。



一些 SASE 提供者也在十多年前開始提供一兩項核心服務，此後匆忙進行補強收購，從而在視覺上完善了 SASE 產品組合。這些廠商的觀點或聲稱的檢查清單可能固有地偏向於其長期優勢。如果您先深入瞭解內部優先事項，以確定您所需的 SASE 使用案例最需要什麼功能，則會感覺準備充分，能夠更好地應對廠商格局。寫下您實際將如何「處理」每個廠商聲稱的主要優勢；畢竟，如果世界上最先進的小工具最終只是擺設，那就毫無意義了。

根據您的主要利害關係人，考慮與廠商討論以下比較主題。由於 SASE 廠商功能快速迭代（甚至可能每個月都有很大的變化），因此，當您在充滿相似產品的擁擠市場中穿行時，找到更深入的準則和討論點將有助於您選擇最佳的長期合作夥伴。

CIO 的辦公室

請注意，以下其中許多問題也可直接用於其他團隊。

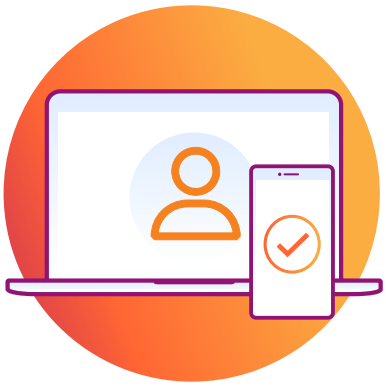
關鍵優先事項

- 提高團隊生產力
- 提升使用者體驗
- 加速數位現代化
- 降低總體擁有成本

向廠商提出的問題

團隊生產力

- 每一種 SASE 功能是有一個集中式使用者介面（即登入一次）還是多個？
- 每一種 SASE 功能是有一個集中式 API（即一個 API 金鑰）還是多個？
- 安全性功能（例如 ZTNA、SWG、CASB）和網路功能（例如 WANaaS、SD-WAN、FWaaS）是預設原生整合，還是需要你們或我們採取手動步驟？
- 我們是將身分識別提供者（例如 Microsoft、Okta、Ping）一次還是多次整合到 SASE 平台，以對每一個應用程式（Web、SaaS 和私人）啟用基於身分識別的存取原則？
- 你們的使用者裝置代理程式是否可組合連線至任何其他網路入口（例如 WAN 連接器、應用程式連接器以及與其他裝置代理程式的網狀/P2P 連線）？
- 我們的安全和 DevOps 團隊能否在不要求我的網路團隊部署設備或變更網路路由的情況下，實現使用者、應用程式和/或服務工作流程之間的雙向任意連線？
- 你們可提供多大程度的自動化（除了擁有 API）？你們的基礎架構即程式碼（例如，Terraform）提供者的完整程度如何？
- 我可以多快開始免費試用你們的完整平台，使用所有安全和網路服務以及入口？我可以立即啟動並執行嗎？



使用者體驗

- 是每一位客戶都可使用你們全球網路地圖上的每一個資料中心位置，還是電信合作夥伴的客戶有一些專屬資料中心？
- 是從你們全球網路地圖上的每一個資料中心位置提供每一項 SASE 功能，還是部分功能（例如，RBI）僅在有限的位置執行？
- 每一個 SASE 網路入口（即裝置代理程式、WAN 連接器、應用程式連接器）能否連線至你們全球網路地圖上的每一個資料中心位置，而不必支付額外費用或頻寬附加費？
- 你們的 POP 與其他網路之間存在多少互連，用於最大限度減少中間轉接提供者躍點和延遲？

數位現代化

- 在每一個位置，每種連線方法和 SASE 服務都可以互通嗎？我可以從哪裡瞭解有關基礎架構的更多資訊？
- 你們的平台獲得了哪些認證？（ISO27701、SOC2、FedRAMP 等）
- 它可與任何現有雲端或內部部署系統互通嗎？第 2-7 層連線可完全透過 API 進行程式設計嗎？
- 如果我們在雲端之間切換，我們的 SASE 服務/成本會發生什麼變化？
- 你們如何為我的組織 5 年、10 年後的目標提供服務？
- 你們目前的生態系統（包括技術合作夥伴）如何支援我的現有投資？

總體擁有成本

- 你們的 Zero Trust 產品如何定價？我是需要為部署的應用程式連接器付費還是為使用的頻寬付費？
- 是否有任何資料中心位置從公有雲端提供者 (Azure、AWS、GCP、Oracle) 執行？
- 你們是否在所有產品方案中都設定了流量使用上限？
- 是否有硬體或虛擬設備要在每個位置啟用、管理或擴展？
- 用於保護分支辦公室的任何網路安全功能是在內部執行，還是全部是雲端原生的？
- 你們在雲端之間移動我的資料需要多少輸出費用？

網路主管

請注意，很多 CIO 辦公室問題也可直接用於網路團隊。

關鍵優先事項

- 減小網路風險和攻擊面
- 強化安全狀態
- 支援效率和減少回應時間

向廠商提出的問題

網路現代化

- SASE 網路是覆蓋所有流量流程（輸入、輸出、WAN、公有雲端網路）還是覆蓋部分？後端架構在不同的流量流程中是相同的還是不同的？
- 你們在多少個不同的城市和國家/地區維護自己的資料中心基礎架構？你們的全球網路地圖上是否顯示了預設情況下我的流量無法路由到的地點？
- 將我的網路連線到你們的網路有哪些不同的選擇？你們的全球網路地圖上的每一個資料中心位置是否提供每一個連線選項，而不必支付額外費用或頻寬附加費？
- 如果我們需要更多的容量或更低的延遲，你們能否立即在每一個資料中心位置佈建每一項 SASE 服務？

業務敏捷性

- 你們提供哪些進階網路功能（例如，私人骨幹網傳輸、快取、通訊協定和應用程式最佳化、進階路由、SaaS 最佳化、私人骨幹網、應用程式最佳化/加速）？
- 你們提供哪些網路監控、可見度和可觀察性功能？
- 你們如何處理流量導引、定型和容錯移轉，來確保我們的封包始終採用最佳路徑？

效能與復原能力

你們的 SLA 是什麼？當任何 SASE 服務（例如，由所有威脅和資料保護功能檢查的解密流量）正在使用時，你們是否提供正常運作時間和/或終端使用者延遲保證？

- 延遲保證是測量從流量來源到 SASE 網路的時間、流量通過 SASE 網路的時間，還是完整的來回（流量來源到目的地）時間？
- 你們是使用 Unicast 還是 Anycast 進行網路路由？如果使用 Anycast，你們是否維護自己的網路硬體？你們如何確保流量不在多個位置之間「擺動」？
- 如果一或多個資料中心整體因為意外服務中斷（例如停電、DDoS 攻擊）或計劃性維護而離線，你們如何確保網路復原能力？次要/後援流量路線是由你們還是我們進行管理？
- 如果在我們的網路位置和你們的資料中心位置之間公用網際網路上的其他地方出現服務中斷，你們將如何確保業務連續性？

CISO 的辦公室

請注意，很多 CIO 辦公室問題也可直接用於安全團隊。

關鍵優先事項

- 實現網路現代化以滿足未來要求
- 提升業務敏捷性
- 復原能力和保持 100% 正常運作時間

向廠商提出的問題

減少網路風險/攻擊面

- 你們的威脅和敏感性資料偵測引擎（例如 AV、DLP）是否在沒有任何部署說明的情況下，一次性解密和檢查所有應用程式（Web、SaaS、私人）流量？
- 通過 SaaS 套件（例如 Microsoft 365、Google Workspace）的所有資料流程和通訊是否在所有通道（內嵌 Web 活動、內嵌電子郵件活動、頻外 Web 或電子郵件活動）中都受到保護？
- 能否針對每一個使用者和每一個基於瀏覽器的應用程式（Web、SaaS、私人）啟用 RBI，而不會影響使用者生產力或產生其他費用？

一致的安全狀態

- 是否會根據使用的網路入口繞過一些安全功能？
- 你們如何確保客戶流量在多租用戶雲端架構中以隔離和私密的方式傳輸？
- 你們如何提供資料當地語系化功能？啟用這些功能是否會為連線至當地語系化區域以外的遠端使用者增加延遲？

效率和回應時間

- 我們是將資料湖和分析（即 SIEM、XDR、雲端儲存貯體）一次還是多次整合到你們的 SASE 平台，以便讓每一個應用程式（Web、SaaS 和私人）都可以查看存取記錄？
- 我們如何將威脅情報摘要整合到你們的 SASE 架構中？
- 你們或透過技術合作夥伴整合對動態裝置和使用者風險評分提供了什麼樣的分析？當使用者存取任何應用程式（Web、SaaS 和私人）時，能否統一執行這些分數？
- 如何減少威脅情報摘要中的誤判？

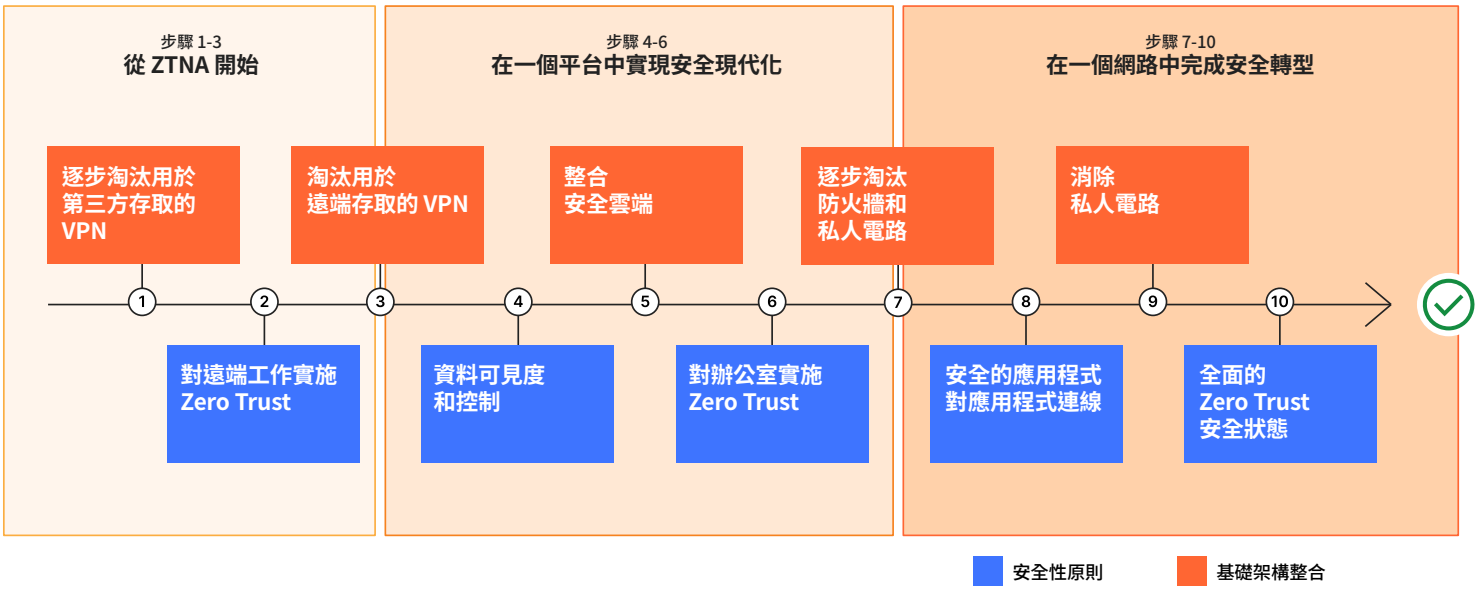
單一廠商 SASE 整合的案例

大多數大型企業可能都會逐步移轉到 SASE 架構，而不是一下子全部實現。在這個過程中，他們可以選擇使用多個廠商的 SASE 服務（特別是因為許多行銷完整 SASE 解決方案的廠商實際上是將單獨的產品拼湊在一起，導致一種不融合的體驗，類似於在管理多個獨立廠商時可能會看到的情況）。

然而，相比將不同的網路和安全解決方案拼湊在一起，使用單一廠商部署和管理 SASE 的所有元件，能夠降低複雜性，繞過安全控制和潛在的整合或連線挑戰，最終大幅簡化部署和管理。

在單一廠商 SASE 平台上整合可讓組織實現 SASE 的真正承諾：**一種簡化、高效且高度安全的網路和安全基礎架構，可降低總體擁有成本，並滿足現代數位環境不斷演變的需求。**

儘管沒有完美的實施順序，而且每個組織都應該評估自己獨特的優先事項，但單一廠商 SASE 架構的長期藍圖可能遵循與以下範例類似的流程

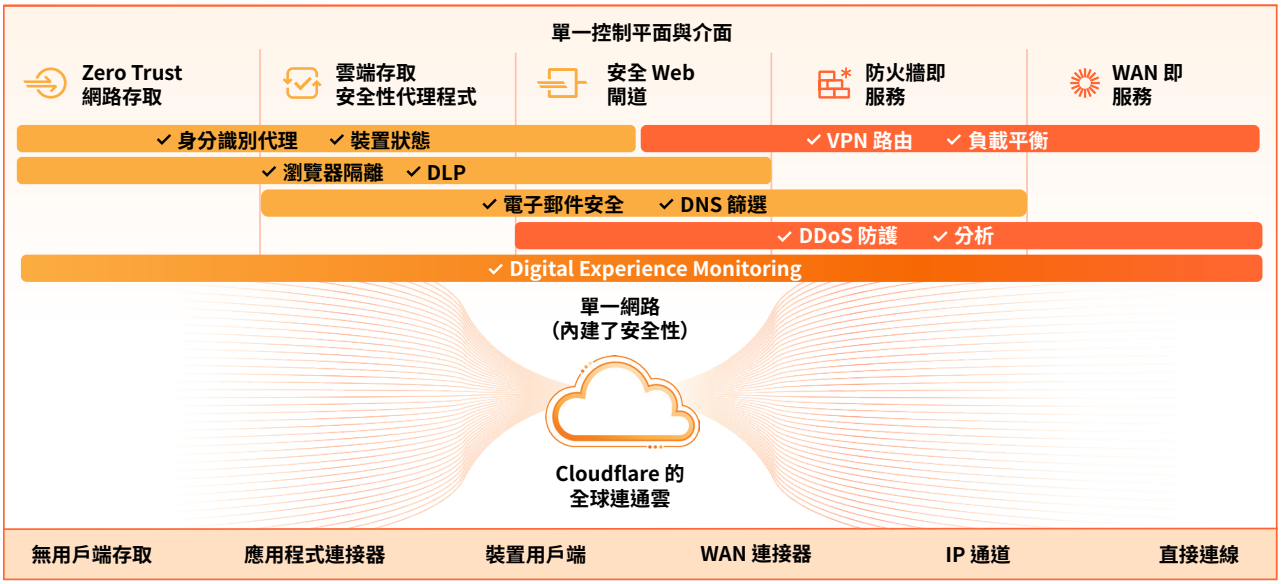


為什麼選擇 Cloudflare One?

Cloudflare 的單一廠商 SASE 平台 Cloudflare One 內建於我們的全球連通雲中。這是公有雲端的演進方向，它為可程式設計的組合式服務提供了一個統一的智慧型平台，可在所有網路（企業和網際網路）、雲端、應用程式和使用者之間實現任意連線。

其他 SASE 廠商透過內部部署裝置，在雲端分別從東西流量覆蓋架構南北網際網路閘道，從而在不使用 MPLS 電路備份的情況下，最大限度減少組織對東西流量路徑的控制，以確保彈性效能。Cloudflare 的中間傳輸全球骨幹網原生融合了南北網際網路閘道和東西私人流量傳輸，以確保所有低成本網際網路連線具有企業級復原能力和效能。

一些 SASE 廠商也基於公有（束縛）雲端構建，並將巨額費用轉嫁給客戶；他們旨在成為資料的最終目的地，而 Cloudflare 旨在將資料傳輸至任何目的地而不犧牲企業敏捷性、彈性或控制能力。我們構建了全球網路和世界級應用程式安全性，因此，未來的服務可以重複使用代理、防火牆、解密、流量掃描、資料處理、管理等。**我們憑藉這個基礎，成為唯一一個從 ZTNA 開始的 SASE 提供者，因此，在我們的整個平台中始終內建了基於身分識別和環境的連線。**



Cloudflare 可幫助組織實現真正的網路現代化，來簡化 SASE 實作，而無需考慮是哪個團隊在領導該計畫。我們的平台讓 SASE 網路對安全團隊而言更加靈活且更易於存取，對傳統網路團隊來說更加高效，並在更大的 SASE 連線相關討論中將覆蓋範圍延伸到服務不足的 DevOps 團隊。我們的全球連通雲具有同類最佳的靈活性，可以讓實作 SASE 架構的組織更輕鬆地實現任意連線，同時符合部署偏好和規範指導。

今天，我們經過整合的安全平台和連接橋樑將 Cloudflare 以及其他超級廠商與其他 SASE 單點產品提供者聚集在一起，從而形成對比。例如，Cloudflare 的全球連通雲提供的其他服務可提高應用程式效能和安全性，如 API 閘道、WAF、內容傳遞網路 (CDN) 和 DDoS 緩解，以上所有服務都可以增強組織的 SASE 架構。

Cloudflare 提供的廣度和深度可幫助組織透過單一廠商 SASE 以及其他方式重新獲得 IT 控制權，全部使用相同的 Cloudflare 代理，可路由傳送約 20% 的網站。隨著數位化計畫和安全風險快速發展，我們的網路是最敏捷的，能夠長期確保組織保持連線和受到保護。

FORRESTER®

Cloudflare 在 2023 年第三季《Forrester Wave™：Zero Trust 平台》中獲評為「卓越表現者」

閱讀報告 >

IDC

Cloudflare 在 2023 年 IDC MarketScape 中獲評為 Zero Trust 網路存取 (ZTNA)「領導者」

閱讀報告 >

kuppingercole ANALYSTS

Cloudflare 在 2023 年 KuppingerCole Leadership Compass 中獲評為 SASE「領導者」

閱讀報告 >

進一步瞭解

無論您從哪裡開始，Cloudflare One 都可以幫助您簡化以下過程：採用 Zero Trust、實現網路現代化、保護攻擊面、實現應用程式現代化以及隨時隨地保護資料。

要瞭解更多資訊，請閱讀我們的參考架構《透過 Cloudflare 進化到 SASE 架構》，或與 Cloudflare One 專家交談。

附錄 A：SASE 入門指南

根據 Gartner®, Inc. 的報告，「未來五年，安全存取服務邊緣 (SASE) 市場將以 29% 的複合年均增長率增長，到 2027 年將超過 250 億美元[2]。」**為什麼會有這樣的需求？**

今天的 IT 和網路安全領導者將幫助完成快速數位現代化優先任務，來實現隨時隨地連接、保護和構建一切的重要目標，並提供可支援以下需求的網路安全和基礎架構：

- **分散的動態雲端服務**，以提供更多保護、更多運算和更多容量
- **保護混合式工作**並以合規的方式連接無處不在的使用者、應用程式和資料
- **降低網路風險**：透過 Zero Trust 安全性，且不會影響快速而可靠的連線
- 透過減少資本支出/營運支出成本以及整合單點解決方案**降低總體擁有成本**
- **敏捷性和靈活性**，從而快速適應新技術、功能和可擴展性要求

然而，傳統的實體和虛擬化網路系統以「城堡加護城河」方法為基礎，無法有效滿足以上全部需求。儘管這些系統在當時是有意義的，但如今，不僅構建成本太過高昂，維護起來非常複雜，也沒有針對雲端或遠端工作進行最佳化。

換言之：早就應該使用 SASE 對網路進行現代化改造了。

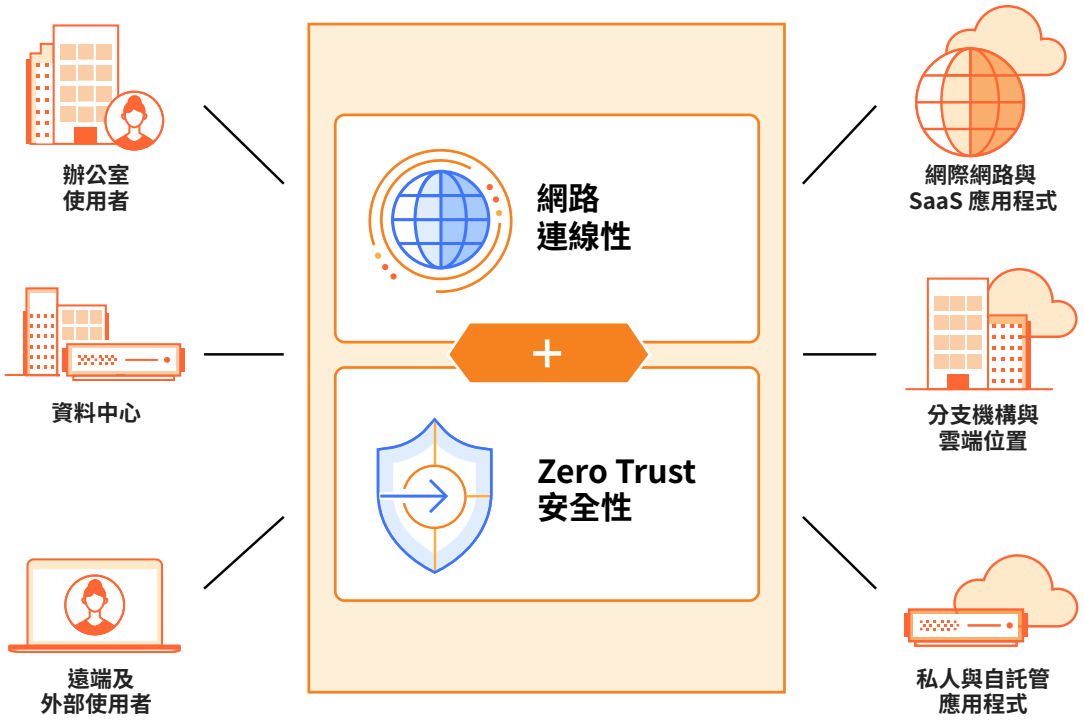
儘管 IT 環境變化的完整「前後」範圍可能讓人感覺難以承受，但大多數組織都已開始制定一張為期數年的 SASE 藍圖以保持實作的可行性，並隨著時間的推移，逐步採用其他使用案例。在實現完全取代之前，SASE 平台可以分階段對傳統設備進行少量加強，從而為業務帶來新的價值。現在，IT 現代化已成必然，而將跨部門的利害關係人聚集起來，透過內部共同作業來實現 SASE 成功亦是如此。

什麼是 SASE？

在傳統的企業網路（與 SASE 不同）中，資料和應用程式位於核心資料中心內。為了存取這些資源，使用者、分支機構和應用程式必須從本地私人網路或次要網路（通常透過安全租用線路或 VPN 連線到主要網路）連線到資料中心。

然而，這種基於周邊的模式無法應對遠距/混合式工作、SaaS 和雲端遷移以及多手段、多通道的網路威脅的興起。

與過去的網路方法不同，SASE（讀作「sassy」）架構將安全性和網路統一到一個雲端平台上，以提供一致的可見度和控制。SASE 將網路控制置於雲端邊緣，而不是企業資料中心。**這就讓企業無論位於何處，都能簡單安全地存取任何使用者、應用程式、裝置或網路。**



具體而言，SASE 平台將網路連線與多項 Zero Trust 安全功能融合在一起，從一個介面進行管理，並從一個控制平面提供。透過將這些服務合併到一個統一的組合式架構中，SASE 簡化了網路和網路安全基礎架構，讓企業能夠在優先事項隨時間轉換時保持敏捷。

下面將詳細介紹核心 SASE 服務及元件。**不過，在深入討論個別 SASE 架構元件和功能之前，請先明確您希望解決的最重大的挑戰。**

為 SASE 制定商業案例

因為 SASE 架構涉及到融合許多傳統上不同的服務，剛開始踏上 SASE 之旅可能會令人不知所措。在技術方面開始之前，您應該先讓業務、IT、安全性和網路利害關係人就其他組織正在透過 SASE 實現的所有業務成果達成一致，同時優先處理對具體目標最重要的事項。

在開始漫長的 RFP 流程和列出候選廠商名單之前，請為 SASE 轉型準備好商業和 IT 案例，並決定進行變更的先後順序。

定義商業和 IT 驅動因素

安全和網路現代化將幫助您的組織實現哪些目標？

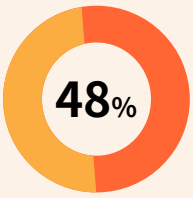
根據 Cloudflare 委託 Forrester Consulting 進行的一項全球調查，在過去三年中，全球 IT 和安全決策者的職責顯著增加。如果您正在考慮 SASE，則您的組織很可能正在面臨類似的挑戰：

過去五年間
IT 和安全團隊責任增加
（表明「我們五年前不對此負責」）

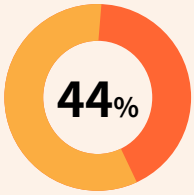
基數：449 位董事級或具有更高影響力的全球決策者或選擇企業級解決方案的直接組織
附註：顯示四種回應
來源：Forrester Consulting 代表 Cloudflare 開展的一項委託研究，2023 年 8 月

「您組織的 IT 和安全團隊目前面臨哪些重大挑戰？」

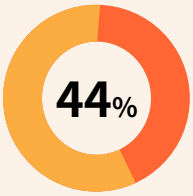
排名前五



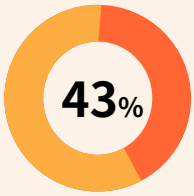
要支援的使用者類型不斷演變，使用者數量日益增長（例如，人類、機器、內部部署、混合以及第三方）



攻擊面區域不斷擴大



難以保持或提高 IT 和安全團隊生產力



合規性要求複雜性日益增加

基數：449 位董事級或具有更高影響力的全球決策者或選擇企業級解決方案的直接組織
附註：顯示前四種回應
來源：Forrester Consulting 代表 Cloudflare 開展的一項委託研究，2023 年 8 月

如果有人要求您介紹 SASE 的商業和 IT 案例，請先考慮如何回答以下問題：

- *您目前的架構能否有效連接並保護所有使用者、裝置、應用程式和資料？*
- *在未來 12 個月內維護/升級目前系統（通常來自雜亂的不同廠商，維護起來非常複雜）的成本是多少？未來 3-5 年呢？未來 10 年呢？*
- *您需要或者擁有哪些 IT 預算和資源來滿足組織不斷擴大的數位化需求？高管對技術投資回報率的預期是否發生了變化？*
- *過去的網路停機和其他網路漏洞是否對客戶體驗、員工生產力或創新能力產生了重大影響？*
- *您的組織最近是否因為安全或網路廠商的漏洞而成為可預防的供應鏈漏洞和/或資料丟失的受害者？*

在制定採用 SASE 架構的藍圖之前，企業通常從整體需求開始，如提高業務敏捷性、降低 IT/安全複雜性、減少網路風險以及提高整體技術效率，而所有這些加在一起，則會改進總體擁有成本。

下圖可以幫助您評估，透過將網路和安全整合到 SASE 架構中，可以解決哪些最高優先順序的挑戰。

清單和排名：您面臨的最大挑戰有哪些？

挑戰：加快業務敏捷性

這是一個**核心商業驅動因素**，如果您的現代化目標是...	→ 為使用任何裝置、處於任何地點的任何使用者簡化並加速安全連線 → 為位於任何位置、使用任何裝置的使用者提高網路可靠性並減少延遲 → 減少或消除新增網路處理能力/功能時的停機時間和服務中斷 → 減少 IT 管理和疑難排解所花費的時間
不過，您需要一個全新的解決方案，因為**您目前的基礎架構...**	⊘ **不能隨業務擴展。**過去，組織僅需要網路來支援辦公室人員，但現在，應用程式涉及到每一種工作職能。因此，如果您的架構基於「城堡加護城河」方法，則更多的連線要求就意味著，在您的所有營運地點都要增添更多的資料中心設備。但是，隨著員工隊伍的壯大，佈建更多的防火牆、路由器、負載平衡器以及其他設備會帶來新的風險、停機時間和潛在的服務中斷。 ⊘ **造成了糟糕的使用者體驗。**過去，組織部署 VPN 設備以將使用者連線至託管應用程式的公司網路。然而，由於需要遠端存取，現在很多應用程式位於雲端基礎架構即服務 (IaaS) 平台中，傳統 VPN 解決方案很難在其中設定。這通常會導致終端使用者的應用程式和連線效能較差。 ⊘ **低效。**傳統網路透過邊界/資料中心防火牆集中輸出。例如，無論分支機構流量是前往資料中心還是雲端/網際網路，都會透過總部進行路由傳送。這對存取網際網路而言特別低效，因為它需要將流量回傳才能存取輸出的安全服務。

	⊘ **不靈活。**管理多個雲端提供者可能會對每個個別提供者的安全方法產生依賴。同時應對每個提供者的特定設定和要求可能會變得極其複雜，從而導致安全漏洞。
挑戰：降低複雜性	
這是一個**核心商業驅動因素**，如果您的現代化目標是...	→ 淘汰傳統資料平台、整合廠商和最佳化雲端支出 → 降低硬體成本和維護網路安全設備的營運 (包括頻寬) 成本 → 為更長期的策略專案和新技術釋放 IT 和安全資源
不過，您需要一個全新的解決方案，因為**您目前的基礎架構...**	⊘ **不斷推高成本。**由於多種原因，企業網路成為巨大的成本中心。為了支援預計處理能力而不得不過度佈建網路；必須成對購買設備 (例如，VPN、硬體防火牆和 MPLS 連線) 以便進行容錯移轉，每隔幾年還要更新一次；更多的使用者和裝置需要更多的連線；更多的應用程式意味著更高的頻寬成本；如此等等。 ⊘ **固有的複雜性。**例如，可能在兩台本機伺服器之間擁有網路層連線 (透過防火牆加強安全性)、很多使用者透過 NAC WiFi 或 VPN (每個都有自己的存取原則) 進行連線，以及大量使用者來自受管理裝置、未受管理的裝置、企業管理的瀏覽器、自有裝置 (BYOD) 應用程式等等。隨著技術的增加，複雜性加劇，反過來，您的網路設計則會變得更脆弱且難以變更。 ⊘ **構成了複雜、反應式且不可擴展的流程。**您的 IT/安全團隊花費了太多時間來管理孤立的部署、多個儀表板、複雜的使用者介面以及備援功能。

挑戰：減小網路風險和保護不斷擴大的攻擊面	
這是一個**核心商業驅動因素**，如果您的現代化目標是...	→ 降低發生以下風險的可能性：資料外洩、多通道網路釣魚、勒索軟體、商業電子郵件入侵、API 濫用和 DDoS 攻擊 → 確保您的組織可以安全地使用產生型 AI，而不會將智慧財產權和客戶資料置於風險之中 → 監控和保護受監管的資料（例如，財務資料、健康資料、個人識別資訊、完全相符資料） → 減少在事件回應上花費的總時間
不過，您需要一個全新的解決方案，因為**您目前的基礎架構...**	⊘ **缺乏 Zero Trust 方法**。基於周邊的網路設計原則著重於信任內部使用者和應用程式，並封鎖外部威脅。但它無法連接和保護任何位置的使用者（內部或外部）、任何位置的應用程式（內部部署、資料中心或雲端）以及封鎖任何位置的威脅。換言之：您目前的系統缺少精細、一致的安全性原則，來覆蓋所有使用者、裝置和環境。 ⊘ **缺乏完整可見度和執行**。由於使用者和應用程式連線方式數量不確定，存在不一致的安全和網路控制，從而影響了您瞭解風險所在的能力。 ⊘ **越來越易受攻擊**。傳統基礎架構（例如，資料中心和 WAN）和傳統安全單點解決方案（例如，防火牆和 VPN）本身就是橫向移動的入口。激增的遠端工作給您的 VPN 帶來了壓力——易受攻擊的 VPN 幾乎可讓網路攻擊者在您的網路中隨意移動。 ⊘ **缺乏內建的隱私和資料保護**。隨著您不斷地將更多應用程式和資料遷移至雲端，部分傳統廠商很難遵循不斷變化的資料隱私和資料保護要求。

附錄 B：定義 SASE 的範圍

SASE 已成為解決上文重點介紹的 IT 和商業挑戰的理想架構。

在真正的 SASE 方法中，網路連線和安全服務融合在一個雲端平台上，並從一個控制平面提供，從而降低了複雜性。

因此，您的候選廠商名單應提供一個可程式設計的組合式網路架構，以最短的延遲提供您需要的全部服務：

- ☑ **網路服務**：將來自多種網路的第 2-7 層流量轉寄至單一的全球企業網路中。這些服務提供防火牆、路由和負載平衡等功能。
- ☑ **安全服務**：檢查在網路上流動的流量，允許使用預設拒絕控制對第 3 層 (IP)、第 4 層 (TCP、UDP、ICMP) 和第 7 層 (DNS、HTTP、SSH) 流量進行基於防火牆代理的篩選，來劃分哪些人員可以存取哪些內容。
- ☑ **營運服務**：透過 Terraform 等提供者提供全平台功能，如記錄、API 存取以及全面的基礎架構即程式碼支援。
- ☑ **整合所有服務**：允許管理員定義一次原則，然後在所有連線服務中根據環境重複使用。

SASE 架構的核心元件

Zero Trust 網路存取 (ZTNA)

這是什麼？

Zero Trust 安全模型假設網路內外都存在威脅；因此，每當人員、應用程式或裝置嘗試存取企業網路上的資源時，都需要進行嚴格的環境驗證。

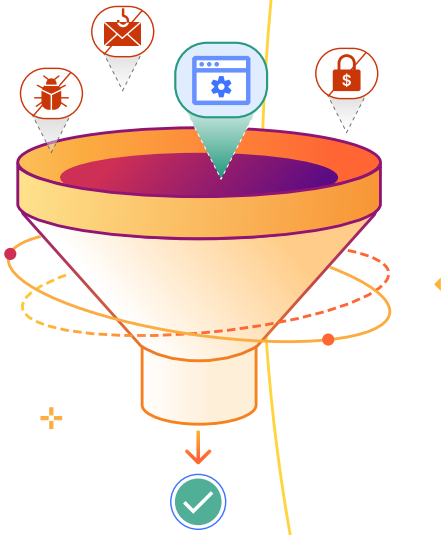
與 VPN 等過度佈建網路存取權限的傳統遠端存取工具相比，Zero Trust 網路存取 (ZTNA) 是一種實現 Zero Trust 方法的主要技術，它在使用者和他們所需的資源之間建立一對一的連線，並要求定期重新驗證和重新建立這些連線。

考量事項：

- 驗證 SASE 廠商提供的 ZTNA 解決方案類型能否滿足您的短期和長期架構需求。例如：
- **基於用戶端的 ZTNA** 要求在所有端點裝置上安裝稱為「用戶端」或「代理程式」的軟體應用程式。如果一個組織擔心私人網路存取、不斷增長的受管理與未受管理裝置組合或裝置狀態，則基於用戶端的 ZTNA 可能是一個有效的選擇。
- **無用戶端 ZTNA** 無需端點軟體即可強制執行 Zero Trust 存取原則。如果一個組織主要專注於封鎖某些基於 Web 的應用程式，或針對承包商或未受管理的裝置強制執行簡單安全的存取，則可以立即推出無用戶端模型。

其他重要的 ZTNA 考量事項包括：

- **投入程度**：應用程式連接器工作流程可能會因為廠商架構的不同而存在巨大的差異，例如，虛擬機與安裝在客戶基礎架構上的輕量級精靈，及其相關聯的輸送量限制（如果有的話）。
- **對舊版應用程式的支援**：一些組織仍有對業務至關重要的舊版內部部署應用程式。大多數 ZTNA 解決方案都可以輕鬆支援雲端和 Web 應用程式，但實作細節可能會因企業需要支援的長尾資源（如私人網路內的資源或涉及雙向流量的資源）而異。
- **身分識別提供者 (IdP) 整合：許多組織已經有了一個 IdP**。在同時支援多個 IdP，甚至相同 IdP 的多個執行個體方面，一些 ZTNA 解決方案比其他解決方案更靈活，這對易受併購 (M&A) 或資產剝離影響的組織而言特別有幫助。



安全 web 閘道 (SWG)

這是什麼？

安全 Web 閘道 (SWG) 透過篩選掉不需要的 Web 流量內容和阻止危險或未經授權的使用者線上行為，來防止網路威脅。SWG 可以部署在任何地方，因此非常適合用於保護混合工作。

與許多安全性產品一樣，SWG 是一款單點產品，通常與其他網路和網路安全功能分開管理。但是，使用 SASE 架構，公司可以從單個基於雲端的廠商整合並維護其網路與網路安全。

考量事項：

SWG 必須快速，這是因為它負責檢查一個組織的網際網路相關流量。如果 SWG 速度較慢，則使用者傳輸至網際網路的任何流量都會很慢；如果傳輸至網際網路的流量較慢，則使用者可能會看到網頁載入緩慢、視訊通話有抖動或遺失，或者通常無法完成工作。

要減少延遲並確保良好的使用者體驗：

- **盡量靠近終端使用者**：您選擇的 SASE 平台中的 SWG 服務應縮短請求在公用網際網路上花費的時間。
- **網路互連合作夥伴關係**：如果您的 SASE 提供者與全世界多個 ISP 或代管提供者擁有強大的對等互連關係，則那些提供者會將流量直接傳送至網路，而不是第三方。這可跳過轉接服務提供者之間的擁塞路徑，讓使用者快速獲得所需服務。

此外，SWG 還可以與內嵌雲端存取安全性代理程式 (CASB) 控制（將在下一節中介紹）結合使用來控制資料移動，從而保護資料。

雲端存取安全性代理程式 (CASB)

這是什麼？

雲端和 SaaS 應用程式的採用使得確保資料的私密性和安全性更加困難。團隊可能會在未經 IT/安全團隊許可的情況下使用某些 SaaS 應用程式（例如，影子 IT），這可能會導致潛在的資料丟失和資料外洩。

為了保護雲端的資料，組織通常也使用基於雲端的安全性服務。CASB 與資料丟失預防 (DLP) 功能完美結合，從而更有效地保護 SaaS 應用程式，但很多組織仍然保留傳統的內部部署 DLP 設備，它們根本無法為雲端提供保護。這不僅會加劇「單點解決方案」的問題，還帶來了挑戰：必須分別協商多個合約，必須多次設定安全性原則，實作和管理多個平台會增加 IT 複雜性。

現代化的雲端存取安全性代理程式 (CASB) 包含 SaaS 安全狀態管理 (SSPM) 作為一種原生功能，而不是附加產品，它是應對這些挑戰的一種解決方案：CASB 為組織的雲端託管服務和應用程式提供了資料安全控制（和可見度）。

考量事項：

- **可擴展性**：CASB 需要管理大量資料以及多個雲端平台和應用程式。您的 SASE 廠商的 CASB 功能應該能夠隨著您的組織的成長而擴展。
- **易於整合**：確保 CASB 將利用 API 驅動的快速整合，與您的主要應用程式（例如，Google Workspace、Microsoft 365、Salesforce）整合。如果未對您的首要應用程式進行可靠的整合，CASB 將無法充分瞭解未經授權的 IT 和潛在的安全威脅。
- **資料隱私**：CASB 服務可以確保資料私密，還是只是接觸敏感性資料的其中一個外部方？如果 CASB 解決方案將他們客戶的資料移動到雲端，其安全性和隱私性如何？這些問題對於遵照嚴格的資料隱私法規而運作的組織來說尤其重要。
- **緩解**：並非所有 CASB 都能夠在識別安全威脅後阻止它們。一些 SASE 解決方案使用「尋找並修復」工作流程，不僅進行偵測，還可幫助管理員針對安全調查結果更有效地採取補救措施。
- **整合式 DLP**：與資料丟失預防 (DLP) 整合的 CASB 服務可以更輕鬆地擴展可見度，並統一所有應用程式、使用者和服務中的資料保護。

遠端瀏覽器隔離 (RBI)

這是什麼？

RBI 將 Zero Trust 原則套用至 Web 瀏覽，假定預設情況下不得信任任何網站程式碼 (例如 HTML、CSS、JavaScript) 執行。RBI 載入網頁並在雲端中執行任何相關程式碼——遠離使用者的本機裝置。這種分離有助於防止惡意程式碼下載，最大限度地降低 zero-day 瀏覽器漏洞的風險，並防禦其他源於瀏覽器的威脅。

廣泛的資料保護控制還可以防止在隔離的瀏覽器內執行高風險的使用者動作，如限制下載、上傳、複製/貼上、鍵盤輸入和列印功能。一些組織使用 RBI 的無用戶端部署，幫助保護資料不受未受管理裝置的影響。

考量事項：

- **相容性**：文件物件模型 (DOM) 操作和像素推送等第一代技術破壞了使用者與現代 SaaS 和基於 HTML5 的應用程式的互動性。基於 SKIA 的網路廠商呈現 (NVR) 會推送 HTML5 繪製命令而不是像素，從而與任何瀏覽器中任何應用程式的使用者互動無縫合作。
- **可擴展性**：如果遠端瀏覽器距離本機裝置太遠，則單憑 NVR 技術不足以對所有終端使用者的日常瀏覽保持透明。RBI 服務必須在全球網路中提供，其中資料中心可在數毫秒內連線至所有網際網路使用者。而每一個資料中心位置的每一台伺服器都必須使用大量的運算資源來設計架構，以便真正將 RBI 服務擴展到任何地方。
- **部署**：由於混合式工作以及現在由承包商組成的大量員工，需要基於用戶端和無用戶端部署兩種選項才能覆蓋任何使用者。無用戶端選項應支援已接入 SASE 網路 (例如，透過 WAN 連接器) 的辦公室使用者，以及未受管理裝置上的遠端使用者。
- **可組合性**：所有 SWG、ZTNA 和 DLP 功能應在遠端瀏覽器內提供，可用於基於用戶端和無用戶端部署，並提供相同的原則控制和可見度。與無用戶端 ZTNA 的原生整合可保護承包商和未受管理裝置在 SaaS 應用程式中使用的資料。而與雲端電子郵件安全性的原生整合能夠隔離可疑的電子郵件連結，實現多通道網路釣魚防護。

軟體定義的 WAN (SD-WAN) 或 WANaaS

這是什麼？

在 SASE 架構中，組織可以採用軟體定義網路 (SD-WAN) 或 WANaaS (有時也稱為網路即服務 (NaaS))，來連接和擴展遠距離營運場所 (如辦公室、零售店、資料中心)。

- **SD-WAN**：大型組織通常使用廣域網路 (WAN) 將各個分支辦公室和位置 (區域網路，即 LAN) 連接到中央企業網路。軟體定義的 WAN (SD-WAN) 是一種更具彈性的 WAN 架構，它使用控制軟體連接 LAN 來進行路由，可與各種網路硬體平台和連線選項搭配使用。
- **WANaaS**是一種雲端服務模式，其中客戶使用的網路服務由雲端提供者提供。它遵循「輕分支，重雲端」方法，主要使用軟體執行網路功能，本質上允許公司對自己的網路進行現代化改造，而無需對網路基礎架構進行重大變更——他們只需要網際網路連線即可。WANaaS 可以取代 VPN、多重通訊協定標籤切換 (MPLS) 連線或其他傳統的網路設定。它還可以取代傳統的內部部署網路硬體，例如，防火牆設備和負載平衡器。

考量事項：

- 如果一些 SD-WAN 實作針對分支機構之間的流量繞過雲端安全性，則可能會增加風險。因此，對於希望最大限度減少效能和安全性折衷的組織而言，通常更需要提供原生網路連線和 Zero Trust 安全性的 SASE 解決方案。
- 使用 WANaaS，網路服務是從雲端提供者處購買的，而不是由組織單獨設定自己的網路。對於 WANaaS，您的組織只需要網際網路連線就可設定和使用內部網路。根據服務的設定方式，與 SD-WAN 相比，這可以提供更大的靈活性並節省更多的成本，就像 SaaS 和 IaaS 等其他雲端服務模型與傳統的內部部署運算相比一樣。

企業網路防火牆或 FWaaS

這是什麼？

企業使用防火牆來保護網路、控制流量流程並強制執行用於與網際網路互動的原則。防火牆的用途及其提供的服務隨著時間推移不斷演變，具有各種各樣的功能和外形。

- **企業網路防火牆：**大多數組織在網路邊緣使用企業防火牆設備，用於將組織的內部網路與網際網路隔離。組織也可以使用硬體和虛擬化防火牆組合，來隔離前往內部私人雲端的流量。
- **防火牆即服務 (FWaaS)：**企業網路防火牆在地理上受限制，因為他們僅位於有限的幾個位置。這在支援混合員工和雲端應用程式方面產生了問題。為了支援此類使用案例，FWaaS 強制執行防火牆原則，而不必管理和部署設備。這可幫助組織透過使用雲端的防火牆服務來應對擴展和架構挑戰，而無需管理防火牆設備。

考量事項：

- 考慮雲端服務能夠提供哪些合適的功能，而不是讓硬體防火牆執行從不具備的功能。
- 作為基準，組織可以使用 FWaaS 提供縱深防禦，從而提供上游保護以防流量攻擊組織的網路。
- FWaaS 額外增強了安全 Web 閘道，透過 Web 和雲端檢查傳送流量並阻止使用規避技巧，幫助組織提高了安全性。
- 當採用「輕邊緣」（即最少硬體，最少管理）理念來連接和保護遠端地點（如店鋪和分支辦公室）時，請考慮使用 FWaaS。

基於全球連通雲構建的平台中的其他元件

SASE 將使用者的安全存取納入網路架構之中。*(這裡值得注意的是，產業分析公司 Forrester 將 SASE 模型歸類為「Zero Trust 邊緣」，即 ZTE。)* 但並不是所有組織都能在 IT、網路安全和網路團隊中採取協調一致的方法。因此，他們可能會優先考慮安全服務邊緣 (SSE)，這是 SASE 功能的一部分，主要側重于確保安全存取 Web、雲端服務和私人應用程式。

雖然大多數 SASE 平台都包括前面提到的核心功能，但**基於全球連通雲構建的單一廠商 SASE 平台會搭售其他 SASE 功能**（在下文詳述）。全球連通雲是一個統一的雲端原生服務平台，簡化了 IT 環境中的「任意」連線性。

基於全球連通雲構建的 SASE 平台中的其他功能	
雲端電子郵件安全性 (CES)	電子郵件是組織的首要通訊方式，研究表明，超過 90% 的網路攻擊都是從網路釣魚電子郵件開始的。網路釣魚攻擊利用使用者的信任，無需依賴網路入侵、惡意程式碼偷渡或命令和控制回呼即可進入。而且，多通道網路釣魚活動（如前文所述）加劇了這一問題，這種攻擊活動試圖在各種應用程式中欺騙使用者。 為了應對這種不斷增長的風險，雲端電子郵件安全性不僅額外增強了雲端電子郵件提供者內建的安全功能，還與其他 SASE 服務整合，可以提供全面的保護，來防禦超出電子郵件範圍的多通道威脅。
資料丟失預防 (DLP)	為防止資料在未經許可的情況下被竊取或銷毀，DLP 技術可偵測 Web、SaaS 和私人應用程式中是否存在傳輸中、使用中和待用的敏感性資料，尤其是作為更廣泛的 SASE 平台的一部分。例如，當與 SWG 結合使用時，DLP 解決方案可以控制傳輸中的資料；當與 CASB 結合使用時，DLP 解決方案可以偵測到待用資料。
數位體驗監控 (DEX)	DEX 是一種監測使用者行為及其網站流量和應用程式效能體驗的工具。DEM 可協助組織獲取有關網路問題、效能下降和應用程式中斷的即時資料。這有助於準確定位網路問題，找出連線異常的根本原因。

遞迴 DNS 篩選	DNS 篩選可透過封鎖或覆寫網域名稱到 IP 目的地的解析，阻止透過任何裝置上的任何連接埠和通訊協定存取惡意、有風險或不可接受的網站和應用程式。當它作為遞迴 DNS 解析服務的一部分提供時，能夠快速透明地保護連線至大量網路位置（例如，分散式辦公室）的任何內容，而無需裝置代理程式、網路連接器或路由變更。它可以與確保內部使用者和裝置安全的其他技術一起納入 SWG。
權威 DNS 安全性	DNS 安全性可保護 DNS 基礎架構免受網路攻擊，以便保持其快速且可靠地執行。有效的 DNS 安全性策略包含了許多重疊的防禦措施，包括建立備援 DNS 伺服器、套用 DNSSEC 等安全通訊協定，以及要求嚴格的 DNS 記錄。 透過擴展的單一廠商 SASE 平台提供的權威 DNS 安全性，可以進一步增強透過無用戶端 ZTNA 保護的公用主機名稱的安全性。
內容傳遞網路 (CDN)	CDN 為網站和網際網路服務快速、高效和安全地交付內容。如果設定正確，CDN 還可以幫助保護網站免遭 DDoS 攻擊等威脅。 當透過擴展的單一廠商 SASE 方法提供時，CDN 會進一步提高面向公眾的資源的效能，從而最大限度地減少流量通過其他單程安全步驟（如 CASB 或 SWG）時的躍點。
Web 應用程式及 API 保護 (WAAP)	WAAP 是安全解決方案的一個總體類別，旨在保護 Web 應用程式及 API。它包括 Web 應用程式防火牆 (WAF)、機器人管理、DDoS 緩解和 API 保護服務（例如，限速、結構描述驗證、API 驗證）。 這些功能透過針對內部人員威脅和橫向移動加強防禦，為第 7 層資源（例如，受內部 ZTNA 保護的應用程式）增強核心 SASE 服務。WAAP 和核心 SASE 服務可以融合在全球連通雲中，甚至在將其他安全服務引入 Web 流量流程時，也能保持強大的效能。
私人骨幹網	儘管 SASE 提供者承諾透過雲端交付網路服務，但實際上，很多廠商都會為輸出至網際網路的流量構建自己的網路，並且資料中心位置之間沒有互連。因此，遠距離 WAN 網路連線的效能變得無法預測。 若要提供企業級的網路體驗，請確保您的 SASE 廠商具有合適的私人骨幹網來支援您的 WAN 流量。私人骨幹網是一種專用網路，充當不同地區資料中心之間的快車道。這透過避免公共網路的壅塞和無法預測的效能，消除了延遲的主要來源。

儘管每個企業 IT 環境都包含高度特定的工具、流程和架構設定，但全球連通雲不僅可以滿足組織的獨特需求，還能提供一致的使用者體驗。這為技術領導者提供了一個可自訂的控制平面，以供整個 SASE 平台使用。

在 Cloudflare 的 SASE 參考架構中，進一步瞭解如何進化到基於全球連通雲構建的單一廠商 SASE 架構。

引文

[1] Gartner，「Critical Capabilities for Single-Vendor SASE」（單一廠商 SASE 的關鍵功能）。Andrew Lerner、Jonathan Forest、Nat Smith、John Watts。2023 年 8 月 21 日。

[2] Gartner，「Forecast Analysis: Secure Access Service Edge, Worldwide」（預測分析：全球安全存取服務邊緣）。Nat Smith、Neil MacDonald、Christian Canales、Andrew Lerner、Jonathan Forest、John Watts、Shailendra Upadhyay、Charlie Winckless。2023 年 10 月 10 日。

+ 886 8 0185 7030 | enterprise@cloudflare.com | cloudflare.com/zh-tw

REV:BDES-5482.2024FEB07