CLOUDFLARE

電子書

CISO 的 SASE 採用指南

如何為高優先順序使用案例評估 SASE 平台

實現網路復原能力的使命

美國國家標準與技術研究院 (NIST) 將網路復原能力定義為使用網路資源或由網路資源支援的系統預期、承受、從中恢復並適應不利條件、壓力、攻擊或入侵的能力。

然而，在減少入侵緩解成本的同時加強網路復原能力也帶來了一些挑戰：

- **網路罪犯不斷發展其策略：**隨著攻擊者開發更複雜的工具、技術和程序，組織更加難以抵禦威脅情勢
- **IT 環境變得越來越複雜：**由於多雲端架構中連線的裝置和應用程式數量眾多，保護這些環境的安全過程不僅成本高昂，而且非常複雜
- **內部團隊負擔過重：**隨著預算收緊和內部團隊負擔過重，組織可能會遇到資源限制

為了克服這些挑戰，許多 CISO 正在轉向安全存取服務邊緣 (SASE) 架構。與過去的網路方法不同，SASE 架構將安全性和網路統一到一個雲端平台上，以實現一致的可見性和控制。SASE 將網路控制置於雲端邊緣（而不是企業資料中心），使企業能夠為任何位置的任何使用者、應用程式、裝置或網路提供簡單、安全的存取。

本指南涵蓋一些最常見的 SASE 使用案例，並簡要介紹了啟動 SASE 實作的主要步驟，以便加強網路復原能力和建立快速致勝方案。

使用案例 1：

採用 Zero Trust 網路存取 (ZTNA)

對於混合工作安排、多雲端環境和未受管理裝置，依賴基於週邊的傳統安全性會讓組織面臨可見性有限、設定衝突和過高的風險。Zero Trust 方法透過精細的存取控制確保預設情況下不信任任何實體，可以透過以下方式幫助您實現安全策略現代化：

取代基於硬體的傳統安全性

虛擬私人網路 (VPN) 之類的傳統網路週邊控制可能難以擴展，影響可見性，並使安全團隊難以發現和修復攻擊。SASE 模型透過實施 Zero Trust 網路存取 (ZTNA) 提供安全的替代方案，同時也跨全球雲端網路路由和處理網路流量，有助於減少終端使用者摩擦和橫向移動。

防止勒索軟體攻擊

勒索軟體可以快速傳播到整個網路，在某些情況下，甚至可能傳播到多個網路和組織。SASE 透過在偵測到感染後立即撤銷網路和應用程式存取權限，來幫助阻止勒索軟體攻擊的傳播。在「最低權限存取控制」的 Zero Trust 原則的支援下，這種方法使攻擊者很難提升特權並在網路內橫向移動。

管理裝置存取

向第三方使用者（例如承包商、代理商和供應商）授予存取權限可能會帶來風險，例如組織意外地過度佈建權限或授予對未受管理裝置的存取權限。SASE 允許組織設定無用戶端 Zero Trust 原則，從而確保第三方使用者只能存取他們需要的內容。

限制資料暴露

當使用者在經批准和未經批准的應用程式中上傳或散佈敏感性資訊時，資料暴露和外洩可能會對組織構成嚴重威脅。SASE Zero Trust 原則可以透過限制每個使用者能夠存取的應用程式來幫助防止資料暴露，同時還掃描流行的 SaaS 套件以查找敏感性資料和錯誤設定。

案例研究

採用 Zero Trust

一家財富 500 強電信提供者使用 Cloudflare 的 SASE 平台來保護超過 100,000 名員工的混合式工作環境——涵蓋 AWS、Azure 和其他雲端環境中託管的數百個應用程式。憑藉基於身分的 Zero Trust 網路架構、安全 Web 閘道和統一存取控制，他們能夠保護使用者免受威脅，而無需兼顧多個原則建置介面、VPN 和網際網路篩選服務。

使用案例 2：

保護攻擊面

數位轉型和遠端工作擴大了攻擊面，更多分散的使用者和未受管理的裝置需要存取內部資源。但是，將內部部署防火牆擴展到雲端並透過 VPN 擴展網路可能會增加外部和內部威脅的暴露程度，同時降低可見度。藉助 SASE 架構，組織可以擴展可見性和控制來支援「無週邊」模型，並透過以下方式實施一致的保護：

避免多通道網路釣魚

攻擊者經常向使用者容易放鬆警惕的通道發動網路釣魚攻擊，尤其是那些通常不受電子郵件安全控制保護的工具。統一的 SASE 平台可以為您的所有環境提供全面的保護，從而降低憑證竊取、帳戶盜用和資料外流的風險。

保護遠端工作者

遠端工作要求使用者從多個位置和裝置進行連線，而這些位置和裝置通常超出了其僱傭企業的管理範圍。SASE 架構讓組織能夠保護員工和第三方對關鍵環境和資料的存取，幫助確保採用受保護的、高效的隨處辦公方法。

提升使用者體驗

清理辦公室流量的傳統方法通常需要將流量回傳到集中式企業資料中心，這可能會增加延遲並損害生產力。但另一種選擇——讓使用者直接存取網路，則會帶來安全風險並造成不一致的使用者體驗。SASE 智慧管理和最佳化與任何雲端或網際網路目的地的直接連線，並盡可能在靠近終端使用者的位置實施原則和保護。

保護廣域網路 (WAN)

一些 WAN 為分支機構之間的流量繞過雲端安全性，因此安全性服務和軟體定義 WAN 之間的整合聲明可能並不像最初看起來的那樣。SASE 讓組織能夠透過篩選和檢查辦公室、資料中心、公有雲端以及更廣泛的網際網路內外的其他位置之間的流量，來簡化和保護其透過 WAN 進行的連接方式。

案例研究

保護不斷擴大的攻擊面

Werner Enterprises 在雲端遷移期間無縫部署 SASE 服務，不會造成任何關鍵業務或客戶服務中斷。部署後，他們的惡意電子郵件減少了 50% 以上，同時也將每天的手動電子郵件分類工作減少了幾個小時，因此他們的安全團隊可以專注於更具策略性的業務目標。

使用案例 3：

隨時隨地保護資料

隨著資料跨越更多環境，組織通常會發現很難對資料進行追蹤。未經批准使用生成式人工智慧和影子 IT 可能會暴露敏感性資料，從而導致入侵或外洩，而修復成本可能會很高。SASE 整合了 Web、SaaS 和私人應用程式環境中的資料可見性和控制，可協助組織實現以下目標：

簡化對資料隱私權法規的合規性

隨著大型語言模型 (LLM) 和其他 AI 工具的興起，合規標準需要不斷發展以保護使用者資料。SASE 透過統一資料控制來確保資料的安全性和私密性，因此安全團隊可以鎖定受監管的資料類別、降低外洩風險，並確保持續遵守嚴格的資料要求。

管理影子 IT

如果將敏感性資料移入影子 IT（未經批准的應用程式，不受使用它們的組織管理或保護）或讓敏感性資料通過影子 IT，則可能會帶來風險。SASE 透過內嵌式雲端存取安全性代理程式 (CASB) 代理流量，來幫助最大限度地降低這種風險。CASB 會記錄每個連線和請求，以揭示未經批准的應用程式的存在，然後讓組織能夠控制對這些應用程式的存取和使用方式。

安全使用生成式 AI

隨著越來越多的組織採用 AI，暴露敏感性資料的風險也隨之增加。藉助安全 Web 閘道和內嵌式雲端存取安全性代理程式，SASE 方法使安全團隊能夠偵測和核准 AI 應用程式的使用、掃描可能導致資料外洩的錯誤設定，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。

保護敏感性資料

SASE 架構可讓組織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並檢查流量中是否存在受監管的個人資料和智慧財產權，封鎖網路釣魚和勒索軟體等網際網路威脅，以及針對資料竊取和意外洩漏實施額外的保護。

案例研究

隨時隨地保護資料

Applied Systems 採用 SASE 服務來保護 2,500 多名員工對自託管應用程式和基礎架構的存取。這種新方法使他們的安全團隊能夠靈活地套用嚴格的控制來滿足不同的使用者需求，同時也控制與 AI 工具分享資料的方式。

選擇 SASE 解決方案：

單一廠商整合與多個單點解決方案

單一廠商 SASE 提供者將網路和安全功能整合到單一的雲端交付服務中。這使得企業能夠整合不同的單點產品、消除設備並確保一致的原則執行。雖然多廠商 SASE 實施可能會獲得與單一廠商方法類似的結果，但它通常會增加複雜性和成本，同時降低內部可見度和靈活性。

將這些功能整合到統一的平台上，使您能夠實現 SASE 的真正承諾：簡化、高效的網路和安全基礎架構，可降低您的總體擁有成本並輕鬆適應不斷變化的業務需求。

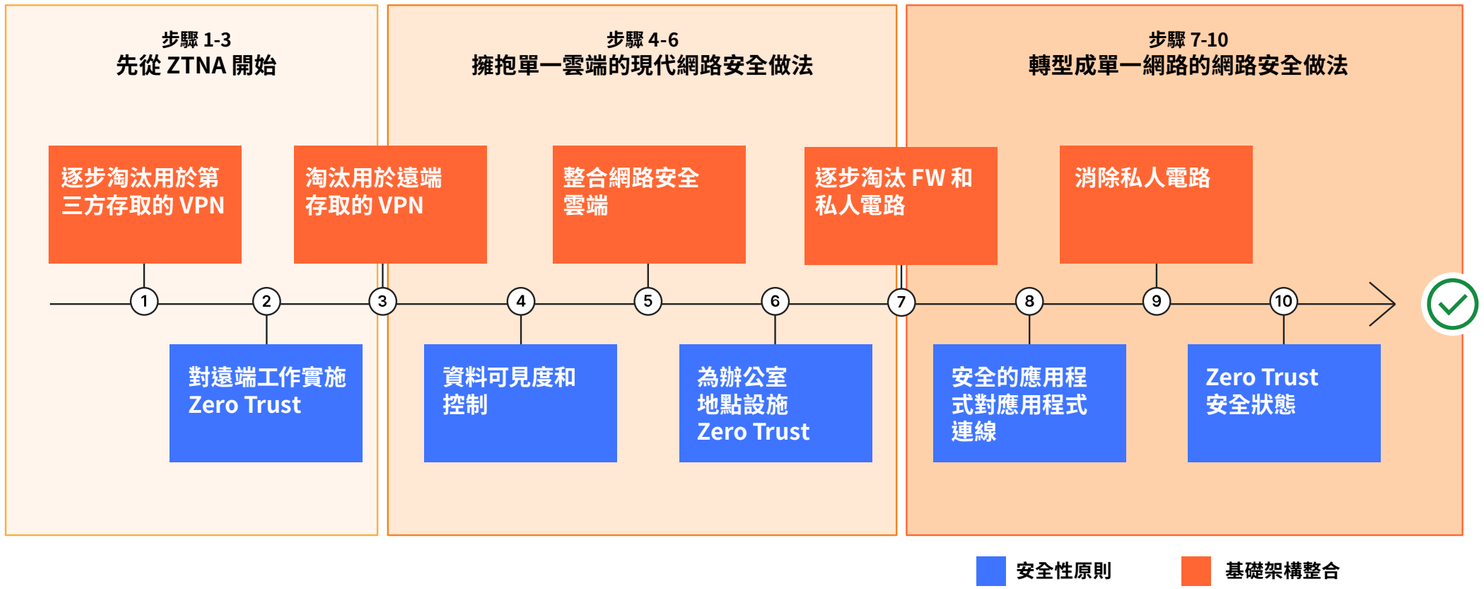
在評估潛在的 SASE 提供者時，請記住以下問題：

1. 應用程式流量是否由威脅和敏感性資料偵測引擎一次性解密和檢查？有任何部署注意事項嗎？
2. 通過 SaaS 套件的所有資料流和通訊是否在每個通道（內嵌、帶外 Web 和電子郵件活動）都受到保護？
3. 是否為每個使用者和應用程式啟用了遠端瀏覽器隔離？這對生產力有何影響？是否需要支付額外費用？
4. 是否會根據任何網路入口繞過任何安全功能？
5. 是否可以確保客戶流量在多租用戶雲端架構中隔離且私有？
6. 提供哪些資料當地語係化功能？啟用資料當地語係化是否會增加在本地區域之外連接的遠端使用者的延遲？
7. 您能否將威脅情報摘要整合到他們的架構中？該平台如何減少來自威脅情報摘要的誤判？
8. 提供哪些類型的使用者/裝置風險評分和分析？是否可以在所有應用程式中統一執行風險評分？

Cloudflare 如何實現 SASE

為了完成統一 SASE 平台的旅程，許多企業都信任 Cloudflare。我們是唯一從 Zero Trust 網路架構開始的 SASE 提供者，在整個平台上一致內建身分和基於環境的連線。

完整 SASE 架構的長期路線圖可能遵循與以下範例類似的流程：



Cloudflare 由覆蓋全球 310 多座城市的全球網路提供支援，可協助 CISO 實現企業級安全性、復原能力和效能。我們的單一控制平面整合了多個安全領域的單點解決方案，因此組織可以簡化其安全操作並確保針對不斷變化的威脅提供一致的保護。

請造訪我們的網站進一步瞭解 Cloudflare 和 Cloudflare SASE 平台。

致電：+ 886 8 0185 7030
電子郵件：enterprise@cloudflare.com
造訪：cloudflare.com/zh-tw