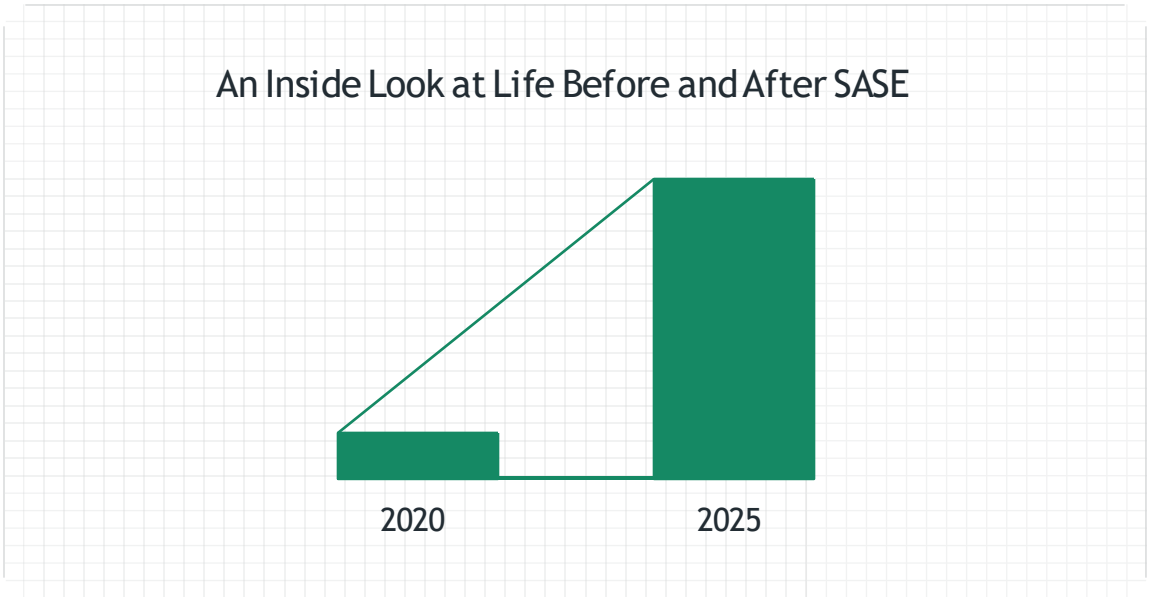
深度觀點：

SASE服務如何重塑企業IT環境

根據 Gartner 的資料，2020 年僅有 10% 的企業採用 SASE 融合策略；到了 2025 年，這個比例將提升至 65%。



但這些數字實際上代表什麼？在導入 SASE 之後，企業的日常究竟會有什麼不同？它真的如外界所說的那麼好嗎？

為了找到答案，我們特別訪談了 **BrandLoyalty 的資安主管 Ben De Laat** —— 他親自導入了 **Cato 的 SASE 雲服務**；同時也邀請了 **IPknowledge 的董事總經理 Steven de Graaf**，這位值得信賴的 Cato 合作夥伴負責執行導入專案。我們將他們的想法與見解收錄於這本電子書中。

簡而言之，SASE 的成果遠超 Ben 的預期，不僅帶來了安心感，更提供了全新的可視性，還獲得了高階主管團隊的一致肯定。對一位 IT 經理而言，還能有比這更好的收穫嗎？

Contents

何時是考慮SASE的最佳時機？

- **在探討導入 SASE 之後的轉變之前，先來了解何時應該考慮導入 SASE。** 雖然「現在就是最佳時機」常被提出，但仍有一些特定情境更適合作為推動轉換的時機點，特別是在您需要說服高階主管（C-suite）核准遷移計畫時。這些情境包括：

當 MPLS 合約即將到期續約時

MPLS 合約常讓企業被綁定在特定廠商及高昂的服務費用上。因此，當 MPLS 合約即將到期時，就是重新評估的好時機，可以開始研究更安全、效能更佳，且成本更低的替代方案。

員工分布於全球各地

當企業員工分散在多個國際據點時，需要一個能安全串連所有地點的解決方案，同時確保使用體驗順暢無阻，並消除連線上的各種障礙。

IT 正在管理複雜的網路環境

多層次且繁瑣的網路環境難以管理、維護與保護，不僅讓 IT 團隊與使用者都感到挫折，更會阻礙生產力，甚至導致資安漏洞被忽視。企業需要一個簡單易用的替代方案，能同時提供最佳化且安全的連線能力。

遠端或混合辦公的員工

在疫情之後，企業需要一個安全且穩固的環境，能夠支援居家辦公（WFH），同時提供與辦公室相同等級的網路與資安能力。這意味著需要一個可擴展且安全的解決方案，能在不經過流量回傳（backhauling）的情況下，根據最小權限原則（least-privileged access）連結所有員工。

「在導入 SASE 之前，我們面臨 MPLS 合約即將到期、全球 16 個辦公據點以及分散的遠端員工。整個環境相當複雜，我們希望能找到一種方式來簡化連線、提升使用便利性，並讓所有人都能享有相同的網路與資安能力。」

Ben De Laat
Head of IT Security, BrandLoyalty

導入 SASE 的考量要點

- **雖然 SASE 的操作性轉換可能在數週內完成，但整體導入的成功則取決於多項其他因素。**
  事先準備周全的遷移計畫，不僅有助於說服董事會支持，也能在轉換過程中進行監控並追蹤成效。我們建議制定一份遷移計畫，並聚焦於三大核心考量：

策略性商業價值	技術價值	財務價值

讓我們來看看每個考量點：

SASE 為企業帶來的策略性商業價值

網路與網路安全對企業而言是業務的推動力，應該支援員工專注於核心工作——如研發、銷售、財務等。然而，傳統解決方案常讓員工變成「網路與資安戰士」，需要處理防火牆、入侵防護系統，甚至排除連線問題。
SASE 則讓員工「卸下戰袍與武器」。它成為日常工作的入口，確保網路不會中斷，讓員工能專注於自己真正的工作職責。
要從 SASE 達成這項商業價值，遷移計畫必須說明解決方案如何支援所有企業使用者，包括分布在全球各地的同事、居家工作的員工，或是在機場、飯店等地工作的員工。

> 「我們的員工各自都有自己的工作職責，他們的工作不是與防火牆、入侵防護系統或連線問題作戰。他們的薪水是用來做銷售、管理薪資等本職工作。企業提供的解決方案，應該成為他們日常工作的入口，而不是增加額外的麻煩與障礙。」
>
> Ben De Laat
> Head of IT Security, BrandLoyalty

SASE 為企業帶來的技術價值

SASE 可以取代大量的單點解決方案，包括 MPLS、SD-WAN、IP-VPN、WAN 優化、次世代防火牆（NGFW）、安全網路閘道（Secure Web Gateway）、入侵防護系統（IPS）、雲端存取安全閘道（CASB）、資料外洩防護（DLP）、VPN、零信任網路存取（ZTNA）等等。
這些單點產品都被 SASE 所整合，形成一個單一、融合、雲端原生的架構，提供完整功能，同時減少管理與整合上的麻煩。此外，SASE 的網路基礎設施透過全球 PoP（Points of Presence）確保來自世界各地的最佳化連線。最後，單一軟體堆疊提供穩健且完整的資安防護，消除盲點，並加速風險識別與緩解。
為確保 SASE 廠商能兌現技術承諾，建議深入了解擬導入的廠商所提供的 SASE 架構。不同廠商的 SASE 方案往往有所差異。此外，應要求從一開始就提供成功案例證明，並以企業最迫切的使用情境啟動快速且易於驗證的概念驗證（POC），通常只需數天或數週，而非數月。透過這些步驟，您可以找到架構最適合企業需求的 SASE 解決方案，而不是僅憑行銷宣傳選擇。

「電信業者常把各種單點解決方案簡單黏合在一起，但這樣容易留下漏洞，使系統同步與協調困難，並影響最終使用者的體驗。」

Steven de Graaf
Managing Director, IPknowledge

SASE 為企業帶來的財務價值

SASE 的投資回報率（ROI）如何？根據 BrandLoyalty 資安主管 Ben De Laat 表示，導入 SASE 後，企業享有兩種類型的財務節省：

年度成本：轉向 SASE 後，企業在網路與資安上的年度支出低於以往。

策略性成本：透過導入 SASE，IT 與資安團隊能提供高品質的使用者體驗，進而正向影響整體企業支出。

此外，IT 與資訊安全團隊得以專注於更具策略性的業務計畫，使其從傳統的成本中心轉變為創造收入的推動中心。
根據 Cato Networks 委託 Forrester Consulting 進行的總體經濟指數（TEI）研究，綜合組織可透過 Cato SASE Cloud 享有以下 ROI 成效：

- 246% 投資報酬率（ROI）
- 淨現值（NPV） 433 萬美元
- 回收期不到 6 個月
- 透過降低運維成本節省 380 萬美元
- 在新據點部署 Cato 時，透過縮短設定時間節省近 44,000 美元
- 透過淘汰被 Cato 取代的系統節省 220 萬美元
- 縮短時間與運輸成本
- 維持資安一致性

企業在導入 SASE 後的改變

「我們已完成里程碑 #1 —— 決定轉向 SASE，以及里程碑 #2 —— 制定 SASE 遷移計畫。那麼，一旦完成 SASE 遷移，IT 領導者、資安專業人員以及企業主管可以期待獲得哪些效益呢？」

全新的網路可視性

一旦企業接入 SASE，就能獲得對網路流量與系統的可視性，甚至可能發現過去未曾注意的流量，這要歸功於 SASE 的端到端深度封包檢測、管理與對所有資料流的洞察力！就像 詹姆斯·韋伯望遠鏡（James Webb Telescope） 能比哈伯望遠鏡（Hubble）提供更精細的宇宙影像，SASE 也能呈現更細緻的網路與流量全貌。
這種全面可視性，傳統靠零散安全單點解決方案拼湊幾乎無法達成，容易留下盲點並增加資安風險。新的可視性不僅提升資安防護姿態，也支援營運監控，並帶來更多其他效益（如下文所述）。

> 「幾乎是一夜之間，導入 Cato 解決方案後，我們就擁有了統一的網路規則總覽。檢視規則、找出問題點並尋求解決方案變得非常輕鬆。」
>
> Ben De Laat
> Head of IT Security, BrandLoyalty

最佳化的資安防護姿態

透過 SASE，技術、IT 與資安團隊能掌握內部系統使用情況的洞察與資訊。這些資訊有助於修補可能產生隱形漏洞的盲點，同時也能消除影子 IT（Shadow IT），並提供更安全且易於透過 SASE 存取的替代方案。封堵這些漏洞不僅建立了最佳化的資安防護姿態，也降低風險並維持良好的資安衛生。

為企業與使用者提供更優化的 IT 服務

SASE 提供一個無縫且統一的解決方案，取代過去靠「膠帶拼湊」的單點產品，如防火牆、VPN 和安全網路閘道（SWG）。這種穩固且強健的架構讓 IT 團隊的工作更簡單、更安心，因為他們知道這是一個可以長期依靠的解決方案，就像日常用水或電一樣可靠。
因此，IT 團隊能夠掌握流量動態、監控營運狀態（如延遲與封包遺失），並檢查任何異常情況。透過這些資訊，他們可以優化線路配置，確保所有使用者都能獲得所需的服務。現在，IT 可以專注於支援業務，執行其他策略性任務。

Spotlight:

Cato Socket 的由來

連接到 Cato SASE 雲端非常簡單：
只需插上 **Cato Socket**——一款輕量級的邊緣 SD-WAN 裝置。（告別以往堆滿辦公室的傳統硬體堆疊吧！）這種 **零接觸設定（zero-touch provisioning）** 只需幾分鐘就能完成，立即連上 Cato SASE 雲端。事實上，「Cato Socket」這個名稱的選擇，正是為了傳達 **網路與資安就像用電一樣簡單、易於使用** 的概念。

無縫支援遠端工作

SASE 提供真正安全且高效能的遠端連線能力。企業不再需要透過 VPN 連接遠端使用者，也不必限制他們能存取的應用程式，或依賴安全的本地網路配置。透過 SASE，使用者流量會經由供應商所提供的全球私有骨幹網路（非公用網際網路）進行最佳化路由。從資安角度來看，所有流量都會持續監控，並受到威脅防護保障。

最佳化的連線與效能

SASE 提供隨處可用的連線，不再依賴昂貴且僵化的 MPLS 網路，而是建立在 SD-WAN 架構上。SASE 的承諾與真正價值在於其對各個網路邊緣的最佳化效能，包括：最大化的傳輸量、提升且成本合理的頻寬、雲端原生的全球私有骨幹網路（具有多重網際網路接入鏈路與主動-主動配置），以及整合與簡化管理的能力。
結果： 提升網路可用性與可靠性，並優化最終使用者體驗。

安心保證

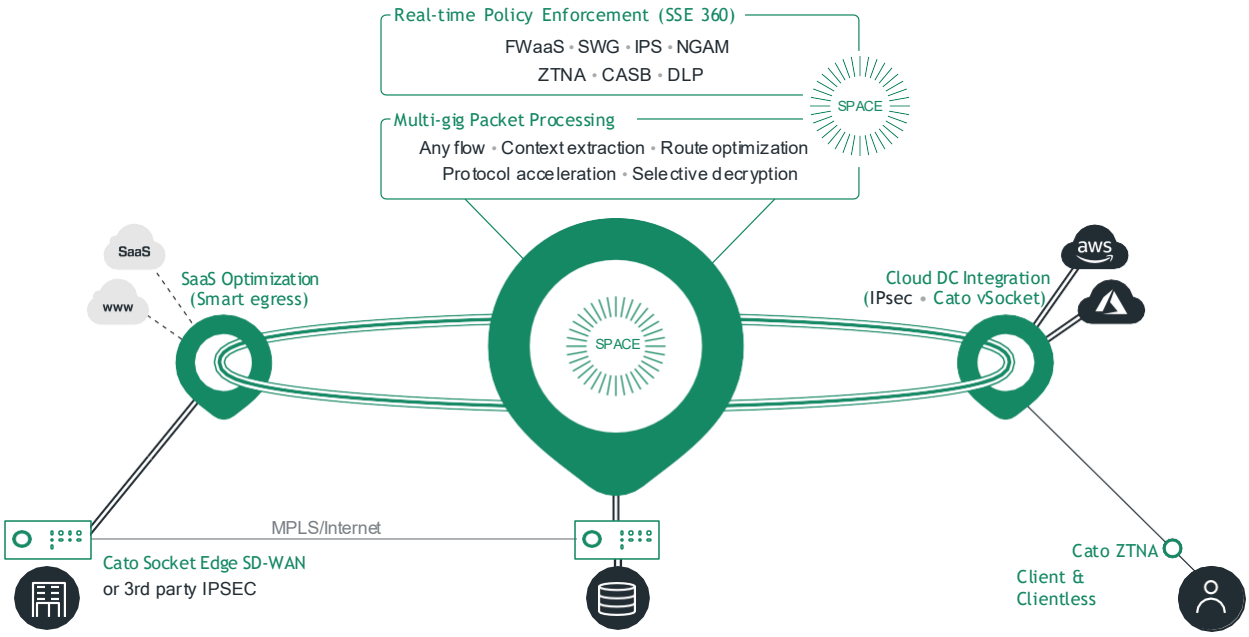
SASE 為所有使用者提供卓越的使用體驗，讓各方利害關係人能專注於關鍵業務計畫。對 IT 與資安團隊而言，SASE 降低了營運負擔，提供自動化且頻繁的系統更新，並透過單一管理介面監控所有指標。對終端使用者而言，登入簡單且連線最佳化。這種可用性與可靠性，帶來了真正的安心無虞。（人生已經夠壓力了，不必再為連線與效能煩惱。）
如果您在閱讀「全新網路可視性」、「無縫支援遠端工作」、「最佳化連線與效能」、「最佳化資安姿態」以及「安心保證」時點頭同意，我們誠摯邀請您體驗 **Cato Networks SASE Cloud 的實機示範**。與 SASE 產品專家討論您的獨特網路與資安挑戰，從低成本 MPLS 替代方案，到為中國據點提供最佳化的全球連線，再到為所有使用者提供安全的零信任遠端存取，Cato Networks 將協助分析您的現有網路與資安架構，並規劃出最適合解決當前與未來挑戰的架構。

「從終端使用者的角度來看，唯一真正改變的就是工作流程變得更簡單了。」

Ben De Laat
Head of IT Security, BrandLoyalty

關於
Cato Networks & Twister5

- **Cato Networks 提供全球領先的單一廠商 SASE 平台**，將 **Cato SD-WAN** 與雲端原生安全服務邊緣（Cato SSE 360）整合成全球雲端服務。Cato SASE Cloud 可優化並保護所有使用者與地點的應用程式存取。
- 使用 Cato，企業能輕鬆以現代化 SD-WAN 網路架構取代昂貴且僵化的傳統 MPLS，安全且最佳化地支援分散式員工從任何地點工作，並促進雲端遷移的順利進行。Cato 可執行細緻的存取政策、防護使用者免於威脅，並防止敏感資料外洩，所有管理皆可透過單一管理介面完成。使用 Cato，您的企業將隨時準備迎接未來挑戰。



- Twister5 極風雲創 是全方位應用資安專家。我們提供全訂閱雲資安服務，結合 CDN 加速、DDoS 防禦、WAF 等高效防護，打造完整的雲端防禦體系。
- 極風雲創為 Cato Networks 台灣唯一MSP 廠商，擁有豐富SASE架構經驗，提供全方位的顧問與技術諮詢服務。

想了解更多Cato Networks 或SASE架構，歡迎填寫表單或來電與我們的顧問聯繫

+886 8979-8887

info@twister5.com.tw

Cato. Ready for Whatever's Next.

SASE, SSE, ZTNA, SD-WAN: Your journey, your way.