Solution Brief

Netskope 智能安全服務周界 (SSE)

Netskope 智能安全服務周界 (SSE) 讓使用者不論身在何處、使用什麼裝置，都具備高效的速度與使用彈性；透過自適應零信任控制框架，降低資料及雲端的風險；藉由其雲原生的整合解決方案，能夠減少組織的運作成本與架構的複雜性，有效協助組織進行數位轉型並提升商業價值。

Quick Glance

- 從網頁、應用程式、使用者和資料等面向，產出企業商業活動和風險的洞察報告，提供絕佳的可視性與脈絡。
- 落實在IaaS、PaaS、SaaS的安全網路與雲端存取，確保設定符合公司政策、合規性管控與最佳化實踐。
- 偵測並阻止潛藏在網頁、SaaS應用、雲端服務和私有應用中的威脅。
- 確保遠距工作者在工作時無論是進行網頁連線、存取雲端應用或是使用私有應用，都能享有安全與穩定的連線。
- 能夠識別在網頁、雲端、 Email 、私有應用或是設備中的機敏資料，並提供保護。

SSE 使用以雲端為中心的整合架構，執行資訊安全策略，不論企業工作者身在何處、何時使用，確保企業能穩定支援用戶的雲端使用安全！[1]

The Challenge 面臨挑戰

現在越來越多的雲端應用服務、使用者還有資料存在於公司外部網路環境中，以及新興的遠距辦公模式，再加上企業中通往雲端應用的流量已經大幅超過了網頁，這會讓原本設計成先通過內網層層防禦，再存取到資料中心的傳統地端安全防護思維，產生了盲點且設定變得複雜，為了應對這些使用情境，企業必須要採用全新的思維，構思資訊系統的安全與網路基礎架構。

為了克服這些難題，需要一個有效簡化且彈性調整企業在執行數位轉型的過程中時所需的存取控管、安全與效能需求，同時能保護關鍵數位資產的安全，以及運用零信任原則的雲端安全新策略。這些挑戰也需要一個採用雲端原生架構的整合性智能解決方案，不能僅依靠過時的防護策略或是被廠商定位成「SSE」但功能卻有所侷限的解決方案。

Netskope Intelligent Security Service Edge (SSE)

無論企業中的「人」和「資料」走向何處，Netskope智能安全服務周界 (SSE)可以讓您簡單且快速地確保他們的安全性：透過提高網路服務速度；降低風險；還有提升雲端、網頁以及私有應用程式活動的可見性；並減少建構完整網路安全所需的成本與複雜度。讓一個把雲端和資料安全作為優先考量的SSE解決方案，與您一同為企業的SASE轉型之旅做好準備。

[1] 4 Must-Have Technologies That Made the Gartner Hype Cycle for Cloud Security

Netskope 強大整合 簡易操作

Netskope智能安全服務周界(SSE)讓管理員能對網頁、SaaS應用、雲端服務與私有應用等所有流量進行深入解析。透過對超過41,000個雲端應用的深入剖析與帳戶識別，提供對其活動更細緻的管控措施，讓管理者能保護遠距辦公者的安全、並確保雲端服務與其架構能順利採用。

Netskope 智能安全服務周界(SSE) 把存取控制、威脅防護和資料保護等強大功能，彙整成一個操作簡單且直覺化的模組。讓管理員能夠輕易理解且使用單一個管理平台統一 Netskope 的正向代理 Forward Proxy 與反向代理 Reverse Proxy ，並一致透過零信任引擎執行，在網頁、私有應用與核可或未核可 SaaS應用上落實一致的安全防護。

雲端安全 精巧構建

Netskope 用零信任引擎作為智能安全服務周界 (SSE) 的基礎框架，構建精密的安全防護，深入與細緻地解析應用、使用者和資料間的脈絡。在這樣的基礎框架之下，讓作為一個有效安全服務周界 (SSE) 所需的關鍵功能，可以被作為骨架與類別屬性來具體實踐：

- 透過人工智慧與機器學習，創建網頁與雲端應用的類別分類、並探查私有應用，讓企業能有效落實穩健且細化的規則控管。
- 在資料保護與雲端威脅防護上，Netskope的專利技術 — TrueInstance 能十分關鍵地識別雲端應用帳戶、規模化地動態偵測雲端應用的帳戶類型。
- 對應用服務的 API 整合擴大了 Netskope 對雲端應用的涵蓋範圍， 透過 Inline 串聯和 API， 與應用介接的架構，無論是任何雲端應用和服務，能對夠個人與企業管理的帳戶之間，提供最佳的可視性和控制措施（像是能支援在AWS上超過250個以上、包含了針對 instance 執行個體的雲端服務）。
- 透過機器學習演算出的信任評級，藉此評估對雲端應用的 Netskope 雲端信心指數 CCI ，還有對使用者的 Netskope 使用者信心指數 UCI ，捕捉潛在異常的可疑行為與變化，觸發適應性的規則控管和自動化的調查工作流程。

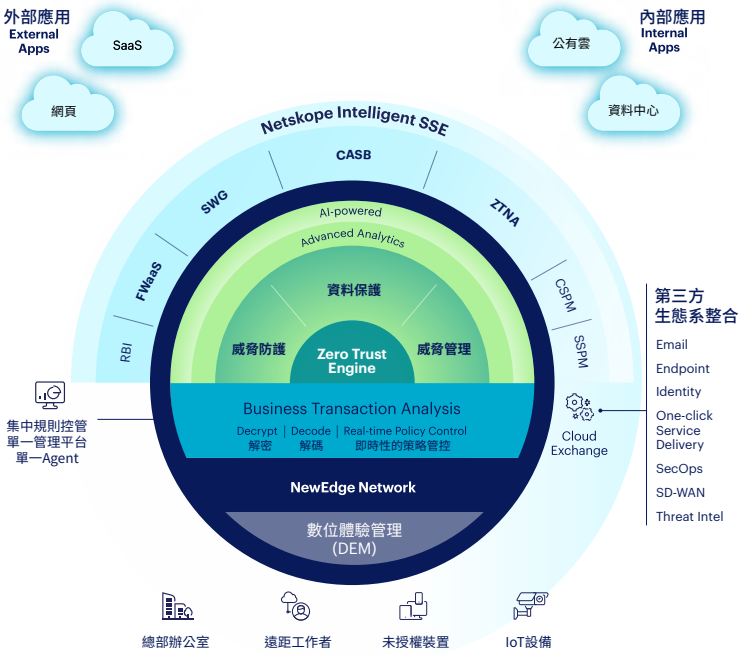
具備了 Netskope零信任引擎建構的豐富脈絡資訊, Netskope 智能服務周界(SSE) 能夠透過精簡的操作, 強化企業資安風險管理, 涵蓋了所有雲端、網頁、以及私有應用, 執行適應性的單程 Single-pass 規則控管。

持續適應性控制措施
執行零信任原則

Netskope 把持續的適應性控制措施，導入零信任安全原則且實施在SASE、多雲以及混合架構上，進而控管用戶存取、防護威脅與掌握資料移動。顯而易見地，從應用、使用帳戶與執行個體、還有在應用上的行為活動等層面落實細化的存取控管，能減少會被駭客鎖定的攻擊媒介，像是從高風險的雲端應用、雲端釣魚攻擊和透過個人帳戶或被公司授權可使用的雲端應用如M365和Google Workspace。透過零信任引擎的驅動，在有資料無意或未經許可地移動到雲端應用，或是在雲端間流動時，Netskope智能安全服務周界(SSE) 能夠透過即時的使用者告警通知和要求再次確認的警示訊息，持續對資料的移動落實管控與防範威脅。

透過濫用納管雲端應用和公有雲環境的個人帳戶作為攻擊手法的雲端駭客威脅與資料竊取越趨猖獗，Netskope是前幾個識別這種攻擊手法嚴重性的公司。Netskope 的進階威脅防護能對任何網頁、SaaS應用、IaaS、所有關聯埠與協定提供最先進的威脅防護，處理弱點利用的剝削攻擊，並透過即時性的規則管控與回應，減少企業對於內部使用者和實體裝置設備等異常行為的盲點。

即時的使用者教育訊息能有效地降低因使用者無意行為所造成的企業困擾，像是分享檔案到私人帳戶；把檔案上傳到不同的事業單位；或是無意間洩漏了機敏性資料到其他未授權第三方使用者的雲端空間。透過細緻化的管控減少駭客攻擊管道，並且透過對使用者訓練，降低因使用者操作失誤所造成的企業雜訊，讓組織可以有效落實進階資料外洩防護，保護商業關鍵以及機敏資料等組織最重要的資產。



Netskope 創建一個集結微服務的雲端原生平台，涵蓋了在SASE架構中的多種功能，提供了豐富的資料脈絡與細緻的規則控管。

雲端資料外洩 黃金準則

Netskope在保衛雲端的資料上一直是企業的黃金準則。領先業界地提倡現代化資料防護在多雲和混合環境上應該精簡而強大。不像傳統使用地端DLP防護地僵化使用體驗，Netskope開創地提出為SASE架構設計的雲端資料防護，具備規模化、準確性和精準度，達到迅速響應的安全防護。Netskope也將人工智慧與機器學習應用在規模化、效率與自動化上，作為探查新雲端應用、資料偵測與界定在雲端中商業關鍵資料時的重要技術。

時至今日，企業有平均20%的網路用量是圖像或是以圖片作為傳播形式的文字，這讓資料安全的規範越來越複雜。Netskope透過人工智慧與機器學習構建的影像辨識技術具備深度學習模型，能對像是護照、政府證件、信用卡影像、社會安全卡等影像內容。不須從圖像讀取所有的文字，就能高度精準與快速地識別出圖像類型。Netskope還偵測螢幕截圖，這對近年來常見的遠距工作型態而言十分重要，尤其當這些截圖很有可能是處理機敏資料的員工所擷取的。有了這個功能，資安團隊能大規模且低誤攔率地偵測比對影像，偵測特定部門的員工是否擷取螢幕畫面。Netskope也能為包含原始碼、專利、契約、履歷和合約協定的文件提供使用人工智慧與機器學習判定的分類功能。

順暢使用者數位體驗 造就企業生產力與敏捷活性

Netskope 透過NewEdge安全私有雲提供最順暢的使用者體驗並優化應用的效能，提升企業的生產力與敏捷度。透過延伸與網頁、雲端服務及SaaS應用供應商們的對接連線（Peering），結合快速、低延遲的流量通路閘道；再加上遍布全球超過59個據點，即時計算並提供串聯式（Inline）的安全流量處理分析，Netskope能夠在用戶最近的據點提供運算服務的同時，也具備了業界領先的服務等級協議SLA，保證其提供的雲端安全服務水準維持一致穩定且順暢。使用Netskope 彈性多樣的部署（包括Netskope Client）引導流量到NewEdge，並與現有的網路架構（SD-WAN等）整合，讓您能使用以資料為本的穩健安全防護，且無需擔心影響系統效能表現、要汰換傳統地端防護架構，或只能妥協使用其他僅僅依賴公有雲、無法保證網路表現的解決方案。不少客戶反饋中提到：「透過NewEdge強化的使用者體驗是他們使用Netskope服務以來最物超所值的項目之一」。客戶也常發現「使用雲端應用的性能也提高了50%」，而在一個最常被客戶使用的SaaS應用上甚至「提升了六倍的效能」。與此同時，Netskope也提供數位體驗管理，讓管理員監控、量測並調查NewEdge還有資料中心安全服務的效能表現。

導入效益	描述
透過雲端原生的SSE解決方案降低成本與複雜度	**Netskope智能安全服務周界(SSE) 將以下優勢統合在單一平台運作：** • 雲端原生次世代網頁安全閘道（NGSWG）、多樣部署方式的雲端存取安全代理 （Multimode CASB）、和零信任網路存取（ZTNA） • 其他額外整合功能如：資料外洩防護（DLP）、進階威脅防護（ATP）、雲端防火牆（CFW）、遠端瀏覽器隔離（RBI）、使用者行為分析（UEBA），都能在單程Single-Pass架構下於單一平台上實踐、使用同一個管理平台集中管控，並且透過一致的零信任規則引擎所驅動。 • 透過整合即時流量分析與雲端API互動偵測，能夠感知機敏資料、即時執行規則、並對存放資料進行審查，達到全面的威脅與資料防護。 • 雲端原生的系統架構 NewEdge，是專為雲端超大規模（Cloud-Hyperscale）的可用性與韌性所設計的，再加上領先企業的服務等級協議SLA，確保穩定的上線時間和低延遲保證。
透過提升混合工作模式的使用者體驗來改善企業敏捷度	**混合的工作型態需要讓所有員工與辦公地點能有直接的存取權限：** **隨時隨地的工作模式要能：** • 直接存取雲端、網頁與內部私有應用 • 開啟橫跨應用與服務的協作模式 • 透過順暢與全球一致的使用者體驗提高工作生產力 **簡化與轉變企業分部的網路與安全可以：** • 讓企業分部直接存取網路，降低不必要的流量導向成本 • 不論地點，持續地實施雲端資安控管 • 對像是在分部的SD-WAN使用其他網路導流參考方案，降低成本和更在地化的連線服務
重新定義風險管理與資料防護	**現代化的風險管理搭配對所有用戶及資料的進階資料與威脅防護：** **進階資料保護涵蓋了：** • 使用人工智慧與機器學習的偵測，能打造出更準確且全面的涵蓋範圍 • 偵測較新型態的機敏資料風險，如螢幕截圖和影像辨識 • 細化管控資料移動，包含在個人與公司帳戶之間的轉移 • 雲端組態管理確保能有正確的存取和權限，降低因錯誤設定或配置飄移造成的威脅，確保管理上符合法律規範 **橫跨SSE的威脅防護可做到：** • 呈現網頁與雲端傳遞的威脅 • 自動化雙向分享IOC保持最新威脅情資 • 在檔案執行前進行拆解與解密情資分析並執行沙箱掃描 • 對包含惡意的Office文檔，執行以機器學習作為基礎的分析技術 • 對高風險的網站類型使用遠端瀏覽器隔離（RBI） • 判定使用者異常行為，評估潛在風險與內部威脅 • 對使用者與辦公室的所有對外埠Port連線與協定執行防火牆控管
精簡企業運作流程	**將安全防護整合並串流到雲端架構，精簡企業運作流程：** **將IT架構整合到雲端能夠：** • 把對網頁、雲端和私有應用的關鍵資安服務轉移到雲端原生的安全平台 • 透過減少設備、軟體訂閱授權和維運服務等，降低企業總體持有成本（TCO），並且藉由單一雲端平台整合相關資安服務，優化企業資源使用效率 • 對雲端應用和網頁一次到位的完整審查，強化資安效能，阻擋威脅與防止資料外洩 **透過以下方式，增強並簡化操作：** • 運用單程Single-Pass策略讓規則設定簡化10倍以上 • 即時使用者訓練與可細緻調整的規則設定，有效精簡資安運作 • 動態視覺分析能即時讓調查與分析往下追查

netskope

Netskope 作為全球資訊安全的領導者，正在重新定義雲端、資料與網路安全，協助組織導入零信任架構來保護資料。
不論員工、設備和資料在何處，Netskope平台隨時能提供最佳化的存取權限和零信任安全原則。
若想要了解更多Netskope是如何協助客戶準備好SASE的轉型之旅，歡迎造訪 **netskope.com**。