netskope

SOLUTION BRIEF

Next Generation Secure Web Gateway

次世代網頁安全閘道（Next Gen SWG）可防堵惡意軟體、偵測先進式威脅、使用設定類別過濾網站、進階數據防護，並能隨時隨地、不論用戶和裝置限制的控管應用程式和雲端服務。單一串聯式 inline 代理伺服器可解碼雲端和網頁流量的帳戶與活動。

快速了解Netskope

- 透過網路和雲端細化規則控管，篩選條件涵蓋控管區分公私帳戶（instance）、細部活動與機敏資料
- 透過透過單一閘道偵測異常行為，可分析先進式威脅及進行資料防護
- SWG，Cloud/SaaS, DLP的規則控管整合，可透過單一雲端管理平台實現整合控管規則，能同時在安全網路閘道（SWG）、雲端／「軟體即服務」（Cloud / SaaS）以及資料外洩防護（DLP）上實行一致的防護準則
- 成熟的串聯式代理伺服器，連續8年獲《財星》雜誌百大客戶青睞
- 全球性雲端架構不論何時何地、使用者或裝置，提供滴水不漏的資安防護

企業平均會使用 2,415 個雲端應用程式，但其中有 98%未受 IT 人員控管，且有89%的帳戶都是雲端應用的使用者帳號。

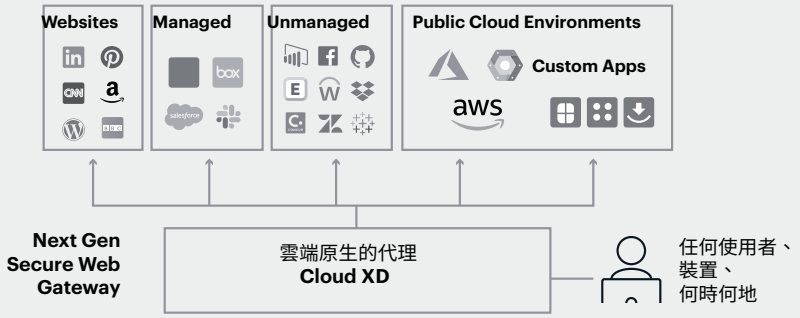
CHANGING LANDSCAPE FOR WEB SECURITY

為網路安全賦予全新面貌

企業平均會使用 2,415 個雲端應用程式[1]，且 89% 的帳戶類型都是雲端應用的使用者帳號。鑒於這些應用有超過 98% 未受納管，而傳統使用 API 機制的解決方案又僅限於已納管者，最有效的解決之道，就是採用 Netskope 次世代網頁安全閘道（Next Gen SWG），對數以千計的雲端應用程式進行串聯式解析。以2020年為例，以雲端為基礎的攻擊手法散布在駭客攻擊鏈的每個階段，更占了惡意軟體下載的 70%[2]。傳統防護思維通常是透過允許 / 阻擋名單進行管控，而隨著網路攻擊紛紛利用這些受信任網域（Trusted Domain）和核可的憑證規避傳統防護，「軟體即服務」（SaaS）開始淪為頭號攻擊目標。

採用雲端防護通常會需要突破既有防護思維的框架。傳統網路防護往往欠缺可視性（Visibility），或在未釐清相關脈絡的情況下，執行粗糙的允許 / 封鎖管控機制。舉例來說，資料的流動可能會在雲端應用程式的企業及個人帳戶之間、未納管和已納管的雲端應用程式之間，甚至是在高風險和低風險的雲端應用程式之間。 而除了帳戶與雲端應用的資安意識外，也有必要對活動是否異常、數據的內容以及脈絡有所了解。作為「安全存取服務邊界」（SASE）的架構核心，次世代網頁安全閘道可為用戶提供數據脈絡以及雲端網路更細化的規則管控。

[1] 2020 Netskope Cloud and Threat Report
[2] Ibid



次世代網頁安全閘道：
針對以下情境有效防護網路及雲端

- 存取網站和URL
- 控管和自行研發的雲端應用程式
- 上千個的未納管雲端應用程式
- 公有雲端環境
- 納管裝置和自帶辦公設備（BYOD）
- 掌握SASE數據脈絡
- 可驅動人工智慧／機器學習（AI/ML）分析的元數據

GRANULAR POLICY CONTROLS WITH CLOUD XD

透過CLOUD XD達成細化規則控管

不論是當前大大小小的網站，或是雲端應用程式及服務，都是使用相同的程式語言。而次世代SWG解決方案的一大功能正是解析這些內容，為的就是讓雲端威脅以及雲端上的敏感數據流向無所遁形。因此，在未納管應用程式之間進行數據傳輸時，有必要部署雲端SWG，確保用戶在任何地點及裝置上的安全性。這也連帶推動SWG、串聯式雲端 / SaaS和DLP功能的整合，以針對雲端及網頁瀏覽進行先進式威脅分析與資料防護。

傳統網路防護中的粗糙「允許」或「封鎖」規則，如今已由　細化規則管控所取代，識別使用者、應用程式、雲端公司 / 私人帳戶、風險評等、數據以及活動內容與之間的脈絡。以在應用程式上處理機密資料為例，某個活動在公司帳戶中也許合理，但出現在個人帳戶時，就可能是即將離職的員工打算洩露或竊取數據。

DEFINING THE NEXT GENERATION OF SWG

劃清新世代SWG的定義

嘗試使用傳統防護機制解決資訊安全上的挑戰恐怕會漏洞百出。企業通常會使用舊有SWG監控網路流量，同時搭配雲端存取安全性代理程式（CASB），藉此透過API機制保護已納管的雲端應用程式。儘管這聽起來相當完善，但面對數位轉型時企業單位或個人所採用的上千種未納管雲端應用程式對企業和個人使用帳戶的界定，這類解決方案往往束手無策。

不論是透過傳統SWG針對這類雲端應用程式增設允許／封鎖控管機制，或是使用次世代防火牆（NGFW），一旦雲端應用程式獲得允許，就會錯失對資料流（data flow）、雲端威脅以及相關脈絡的管控判別能力。即使透過評估使用風險來封鎖風險較高的應用程式，並教育使用者採用相對安全的替代方案，還是得直接「允許」部分雲端應用程式，而終究無法控管到使用活動、內容及脈絡。事實上，隨著雲端轉型和遠端工作的發展，傳統的SWG、NGFW，甚至是端點防護正逐漸失去對網路活動的可視性，且不再如以往有效。

有許多原因可說明數據及脈絡何以成為次世代SWG的核心，以及作為SASE架構的根本準則。雲端DLP現在已是勢不可擋的未來趨勢，因為當今越來越多的使用者和資料位處在企業資訊中心外部，甚至要比內部還來得多。使用者辦公時，都會需要存取網路、受監管的應用程式、未納管的應用程式、公有雲以及私有雲端應用程式，這五大領域的資料流向，都可透過串聯式雲端DLP規則與策略加以保護。然而，威脅也開始從雲端著手，在駭客攻擊鏈的各個階段和技巧上應用，就像網路釣魚（phishing）透過社交工程滲透存取管道入侵公司，並避開像是端點防護在內的傳統防禦。次世代SWG則超越了傳統的網路行為紀錄，能夠提供豐富的元數據metadata，藉此驅動以機器學習（ML）為基礎的偵測技術，防範雲端與網路流量中的威脅及異常行為。。