

沒有網路周邊？ 該怎麼做？

雲端應用程式、行動裝置及遠端工作人員破除了網路周邊的概念，
因此現在需要跳脫傳統的安全思維。





選擇專為雲端世代打造的網路防護功能，擊退現今的安全挑戰風暴。

您如何保衛行動使用者、遠端辦公室及雲端應用程式？您要如何遵循持續演變的合規責任，同時對抗無止盡且日趨精密的網路安全攻擊？

導回方式是將分公司及遠端網際網路流量傳回企業資料中心，並在過程中套用各項安全及威脅防護政策。但隨著企業將營運移往雲端，導回模式的熱門程度逐漸下滑，原因是透過私有多重通訊協定標籤交換 (MPLS) 連結傳送的導回流量非常昂貴，加上導回流量會產生延遲問題，影響嘗試取得雲端應用程式及 Web 的異地員工。或者，員工可直接使用雲端提供的安全服務、消除導回流量，而流量直接前往 Web 及雲端應用程式時將套用安全政策。

建議：

- 以雲端型 Secure Web Gateway 作為安全基礎架構的基礎，不論使用者及資料在何處，都能獲得保護
- 獲得您需要的安全，無需犧牲網路效能或實惠價格
- 讓您擁有領先業界的威脅防護技術
- 透過統一的安全政策保護內部部署及遠端/行動使用者
- 選擇全方位解決方案，提供有效且嚴密的防護

2017 年

有 1/13

在閘道分析的 URL 屬於惡意 URL 的

數量比 2016 年的 1/20 更多。

惡意軟體隱藏在加密流量中，可滲透並突破傳統網路防禦。現今大部分網際網路流量均為加密，因此有越來越多不肖份子利用加密技術散播惡意軟體。

利用雲端型 Secure Web Gateway 打造安全防禦機制



雲端世代需要的 **Secure Web Gateway (SWG)**，不只提供 **Web** 及雲端應用程式所需的基本安全功能。

Secure Web Gateway (SWG) 可加速資料安全流往 Web 及雲端應用程式，以獨特方式掃描流量，即使加密也沒問題，協助掌握各種惡意軟體及違反資訊安全合規事件。因此 SWG 是您的網路安全最佳基礎。進階的雲端型 Secure Web Gateway 更勝傳統基本功能，例如執行公司可接受的 Web 使用政策；利用威脅情報資料評估 URL 風險，避免員工進入危險網站；此外也納入各種檢測技術，檢查流量中是否有網路威脅或資料遺失。部分 SWG 納入 Web 隔離等創新技術，為您的使用者多增添一層安全防護。全功能 SWG 可提供您需要的全方位功能，讓您輕鬆面對各種關鍵安全及合規挑戰。最厲害的是透過雲端提供，您能隨時讓使用者流量通過 SWG，使用者不論身在何方、使用任何裝置，都能獲得保護。

建議：

- 選擇性檢測加密流量，精確掃描內容，掌握惡意軟體及違規事件。
 - 迅速安全地檢測 SSL/TLS 加密流量，提供企業需要的防護，以及使用者講求的效能。目前大部分網際網路流量都採用加密處理，因此關鍵在於網路安全能夠解密流量，並引導送往安全及資料合規檢測引擎。能直接對抗針對使用者網頁瀏覽器的新興威脅，提供保護也是一項重要條件。
- 讓員工以受保護的方式存取具潛在風險的網站。安全存取內嵌在電子郵件中的 **URL**，預防在網路釣魚網站輸入企業存取憑證。
 - 使用 Web 隔離技術，預防鎖定使用者網頁瀏覽器的各種威脅及網路釣魚攻擊，以保護員工裝置。Web 隔離不會在端點上執行網頁階段作業，只會傳送安全的轉譯資訊至使用者瀏覽器，進而預防任何網站傳送零時差惡意軟體到您的裝置上。

利用雲端型 Secure Web Gateway 打造安全防禦機制



- 自動向所有 **Web** 流量套用資料隱私性及防護政策，加密與否都沒問題，並使用儀表板及線上報告監控活動。
 - 傳送解密的 SSL/TLS 流量至任何 Data Loss Prevention (DLP) 系統，進行精準快速的分析。支援法規合規性及保護資料。
- 正確識別使用中的雲端應用程式、評估風險，並依據使用者、群組、位置及其他項目控制存取。
 - 透過雲端存取安全中介程式 (CASB) 控管保護雲端應用程式及和公用雲端互動的資料。獲得能見度掌握員工使用的所有雲端應用程式，例如 Office 365 等「已知」雲端，以及各種「影子 IT」雲端 (由員工自行佈建)，確保遵循公司的雲端使用政策。
- 整合雲端型 **SWG** 與內部部署及行動端點防護。
 - 透過整合網路安全與端點安裝的安全功能，獲得完整的多層網路至端點防護，以及簡化的行動裝置應用程式管理。建立多層式防禦機制，保護所有企業端點，包括直接連結網際網路的行動及遠端使用者。
- 讓遠端辦公室/分公司員工連結網路，同時利用 **SD-WAN** 效能及彈性。
 - 以選購的 SD-WAN (以及類似) 裝置，將遠端流量送往雲端安全，輕鬆保護遠端辦公室及行動員工的安全。您可輕鬆開始操作，透過變更防火牆或代理設定，或微調使用者裝置。

獲得高度安全及效能， 無需負擔高額成本



使用網路安全作為雲端提供的服務，獲得您需要的所有功能以保護員工。

不論使用者身在何處、使用何種裝置，都將執行一致的政策。最棒的是，由於這是雲端型的完整網路安全基礎，所以能以雲端級速度輕鬆提供全方位安全。您需要的一切都整合至符合成本效益的單一服務，只要為新使用者增加額外訂購授權，就能依需求隨時擴充部署。



直接連網的優異效率

由雲端提供安全功能，可讓辦公室及行動使用者享有出色效能，因為員工可在連往 Web 位置或雲端應用程式途中連結安全服務，也就是所謂的「直接連網」安全性。您也可留意整合 SD-WAN 方案的服務，可讓您的辦公室輕鬆連上雲端。



高效 SSL/TLS 加密掃描

別讓重要的 SSL/TLS 流量檢測衍生出麻煩的延遲問題、耗用大量運算資源。使用次世代防火牆等不適當的裝置，可能導致效能大幅下滑。



單一代理程式網路安全存取

越來越多員工透過一系列持續成長的遠端及行動裝置連網。為什麼要增加額外的代理程式，才能讓每個人連線至雲端提供的網路服務？如果單一輕量代理程式能提供全方位的端點安全，並額外將 Web 流量重新引導至雲端的網路安全基礎，如此便能滿足需求。

針對 Office 365 等應用程式獲得能見度、盡可能降低風險及維持合規



利用 **CASB** 控制以正確識別使用中的雲端應用程式、評估風險，並依據使用者、群組、位置及其他項目控制存取。

遵循規範需要掌握及控制敏感資料，不論資料位於何處。其中包括雲端應用程式分享文件中的資料，甚至包括員工未經 IT 同意所使用的應用程式 (所謂的影子 IT)。CASB 功能可保護與公用雲端應用程式互動的資料，例如 Office 365。



正確識別使用中的應用程式

獲得深入各種雲端應用程式和服務中使用者活動的能見度，並強制執行精細的內容和情境式政策。持續監控雲端應用程式的使用情形，並在分享敏感資料時進行偵測。確認員工遵循雲端使用政策。

評估雲端應用程式風險

針對員工使用的每種雲端檢驗數十種屬性。判別高風險活動、惡意行為及惡意軟體威脅，並即時封鎖以保護資訊。



控制雲端應用程式存取

依據雲端屬性資料以使用者、群組、位置及其他項目設定存取及控制政策。識別及分類關鍵的合規相關資料，然後監控前述資料在雲端應用程式內上傳、下載或共享的情形。

統一安全政策管理達到簡單及一致的目標



在您適應快速變遷的規範要求及企業命令之際，在內部部署及雲端環境中，迅速制定及執行政策。

說真的，變更安全基礎架構是一項複雜作業。如果您並未事先規劃，最後可能造成雲端及內部部署平台需要不同政策，落入需要維護兩種不同系統的困境之中。如果您選擇的解決方案，能在內部部署及雲端部署類似功能，並以一組政策管理兩者，如此便能讓您的日子更輕鬆。如果您希望百分之百移轉至雲端，您需要的解決方案就是：只要按一下按鈕，就能將現有安全政策移轉至雲端網路安全服務。



簡化轉移至雲端型安全的過程

指定您要自動移轉至新型雲端安全的內部部署政策。



建立及管理一致的政策

以一次性建立並推送至所有安全閘道的方式建立新政策，以便在混合內部部署及雲端安全環境中一致地強制執行。



充分發揮您既有投資的效益

在可能情況下充分利用原有的安全系統。利用您投資的 DLP，但現在要將其延伸至雲端。在合理情況下，請在主要資料中心維持內部部署 SWG，但將分公司及行動使用者移往雲端。由單一管理主控台管理任何環境，涵蓋範圍從私有至公用、實體、虛擬或雲端，或彼此之間的任何組合。

概要：沒有周邊？不必擔心。 透過雲端供應之網路讓您獲得保護



賽門鐵克的雲端型 **Web Security Service** 可保護中央位置、分公司、遠端及漫遊使用者，以及任何地點的公司資料，使用強大的企業級安全功能，由高效能全球雲端服務提供。



與眾不同的網路安全功能

雲端型 Web Security Service 採用相同的進階代理技術 Symantec ProxySG，過去 11 年來，這項技術都獲選為 Gartner Secure Web Gateway 神奇象限的領導者。這是一整套網路安全的基礎所在：進階的 Secure Web Gateway 位於核心，加上惡意程式分析、沙箱、Web 隔離、雲端應用程式控制 (稱為 CASB)、Data Loss Prevention、整合式 SD-WAN 及其他各種功能，全部採用獨一無二的威脅情報，在員工嘗試造訪每個網站時協助判定風險。

全球雲端網路：深獲肯定的效能

我們採用分散及彈性的全球雲端資料中心基礎架構，提供「五個 9」(99.999%) 系統運轉率的服務等級協議。我們以各種方式展現最佳效能，例如與 Microsoft、Amazon、Google 及其他廠商進行網路對等連線，以及利用 TCP 窗口最佳化讓大型檔案加速在雲端儲存應用程式之間移動。



整合防護簡化營運

我們瞭解您也需要在端點部署安全解決方案。因此我們整合了獲獎肯定的 Symantec Endpoint Protection (SEP) 與 Web Security Service。如此一來，當您共同使用這些產品，就能減少安裝一個代理程式，並能在您的端點管理。SEP 可設定讓 Web 流量前往 Web Security Service，以便執行網路安全政策。賽門鐵克提供獨一無二的端點及網路安全深度防禦服務，讓您的使用者在沒有周邊的世界中安全無虞。



如需更多詳細資訊，請造訪

symantec.com/zh/tw/products/web-and-cloud-security

關於賽門鐵克

賽門鐵克公司 (NASDAQ: SYMC) 是世界首屈一指的網路安全公司，無論資料位在哪處，賽門鐵克皆可協助企業、政府和個人確保他們最重要資料的安全。全球各地的企業均利用賽門鐵克的策略性整合式解決方案，在端點、雲端和基礎架構中有效地抵禦最複雜的攻擊。同樣地，全球各地超過 5,000 萬的人們和家庭社群，也仰賴賽門鐵克的諾頓產品和 LifeLock 產品套裝軟體來保護自身的居家數位生活及各種裝置。賽門鐵克經營的安全情報網是全球規模最大的民間情報網路之一，因此能成功偵測最進階的威脅，進而提供完善的防護措施。若想瞭解更多資訊，請造訪 www.symantec.com.tw。

台灣賽門鐵克股份有限公司 | 地址：台北市信義區忠孝東路 5 段 68 號 29 樓
電話：+886 2 8729 9277 | 傳真：+886 2 8729 9257 | www.symantec.com.tw



Copyright © 2019 Symantec Corporation. 版權所有 © 2019 賽門鐵克公司。All Rights Reserved. 保留所有權利。Symantec、Symantec 標誌和打勾標誌是賽門鐵克公司或其子公司在美國及其他國家或地區的商標或註冊商標。其他名稱可能是其各自擁有者的商標。

19C210137_SB_VANISHING_PERIMETER_TW