資料工作表

McAfee Web Gateway Cloud Service

雲端提供的 Web 安全服務，可提供無微不至的防護

主要優點

- 部署 Web 安全最具成本效益的方法：不需要內部部署硬體或軟體。
- 超越基本防護：在處理流量時，行為模擬可在數毫秒內防範零時差惡意軟體侵襲。
- 將防護延伸至網路離線使用者。雲端遞送可消除傳統的網路周邊。
- 採用 McAfee® ePolicy Orchestrator® (McAfee ePO™) Cloud 平台做為 Intel Security 雲端服務的統一管理主控台，造就無可比擬的高效率管理。
- 通過驗證的架構:我們將 McAfee® Web Gateway Cloud Service 打造成 McAfee Web Gateway 的多租戶版本，是獲得全球企業採用之值得信賴的內部部署裝置。

想防禦來自 Web 的複雜威脅雖然需要先進的科技，但卻未必會提高成本和複雜性。提供雲端的 Web 安全，讓安全性團隊在無須使用額外的硬體和資源成本來維護的情況下，即可享有等同內部部署裝置的進階威脅防護功能的優勢。當越來越多 Web 存取都發生在網路周邊時，雲端就變成裝置和使用者在漫遊時，一致的接觸點。相較於建立單一位置的流量的安全性，透過端點來建立安全性是更有效的方法。將端點、甚至是所有位置和雲端結合，可提供無微不至的防護，而且不會因為新的網路周邊移出網路防火牆而結束防護。

具成本效益且無微不至的防護

管理內部部署 Web 安全裝置所費不貲，而且總是要讓運作已經捉襟見肘的安全性小組變更既定週期加以因應。透過部署 Web 安全即雲端服務，可以降低整體擁有成本。您再也不必購買、擁有和維護硬體裝置。所有原先用來維護裝置、執行工作 (例如: 升級或修補軟體) 的資源，都可以重新配置到 IT 或 IT 安全部門中更具策略性的計畫。

在混合部署中，裝置和雲端服務可以一起使用。大多數的組織選擇這種模式來維護擁有權，以及控制網路上的裝置並將雲端式防護功能延伸至小型遠端辦公室與網路漫遊使用者。

IT 團隊使用網路上的 Web 閘道裝置，透過從遠端辦公室以多重通訊協定標籤切換 (Multi Protocol Label Switching，MPLS) 傳回 Web 流量的方式來進行篩選，藉此享受雲端式 Web 安全的優勢。回傳流量的所費不貲，同時也會增加網路的複雜性。然而，遠端辦公室可以直接路由至雲端以獲得保護，並可免除 MPLS 電路及簡化網路架構。

最後，員工存取 Web 再也不會受制於網路周邊、也不會讓網路離線使用者和裝置暴露在風險中，而且 IT 部門更不會無法掌握狀況。轉換 Web 安全和雲端，即可逆轉此周邊態勢。網路離線使用者的 Web 流量和裝置，可自動從端點路由至雲端，讓您不論是在家裡、機場、咖啡廳或是其他地點離線工作，都能維持安全的連線。網路安全再也不會侷限於實體防火牆內的流量。而是從端點延伸出去，無論端點所在何處。

intel Security

全方位的高效能架構

McAfee Web Gateway Cloud Service 專為企業打造，使得許多組織也因此獲得更高等級的效能，超越目前自身內部部署的體驗。以內部部署為例，如果要增加其容量，IT 人員則需要採購並部署新的裝置，這將需要花費數天到數週的時間。由於彈性的雲端設計服務，我們的雲端只需 15 分鐘的時間就可增加容量。

若內部部署裝置故障需要維修則會造成網際網路反應遲緩，而且，若允許 Web 以故障開啟方式運作，則會使安全狀態受到危害。若資料中心所在位置其中之一出現故障的情況時，我們的雲端服務會自動將所有的 Web 流量重新路由至最接近、最快速的資料中心所在地，以確保作業不至中斷。

我們的雲端服務架構也是經過精心打造，可在世界最大的網際網路交換點 (Internet Exchange Point，IXP) 與網際網路骨幹「對等」運作。這能減少中繼網路服務提供者 (ISP) 的路由躍點，這些躍點只會增加連線時的延遲。減少熱門內容提供者 (如 Microsoft Office 365 和 Google) 的躍點，使用者就可以透過我們的雲端服務連線，如此會比他們直接連到公開網際網路還要快速。

McAfee Web Gateway Cloud Service 全世界皆可使用。若要查看資料中心目前所在位置和處理 Web 流量之資料中心的狀態，請造訪 **https://trust.mcafee.com**。Web 內容可以當地地區語言顯示，因此無論使用者從何處連線，都會看到當地 Google 搜尋結果的例子。

防禦複雜的威脅

安全性團隊通常無法因應極為複雜的惡意軟體和目標式攻擊，這些攻擊能迴避傳統的防禦措施，導致系統耗用大量資源並持續採取「應變」措施不斷地修補端點。不同於傳統的 URL 篩選以及採用特徵碼來預防 Web 威脅的方法，McAfee Web Gateway Cloud Service 透過檔案的 In-Line 模擬、JavaScript 和 HTML，保護端點免受零時差和無檔案惡意軟體的威脅。這種方法能夠在零時差惡意軟體感染使用者之前加以防範，並可透過 URL 篩選以及以特徵碼為基礎的解決方案改善封鎖比率約達 20%。減少惡意軟體事件的總數，可以讓安全性作業得以享有低成本和高資源彈性的優勢。

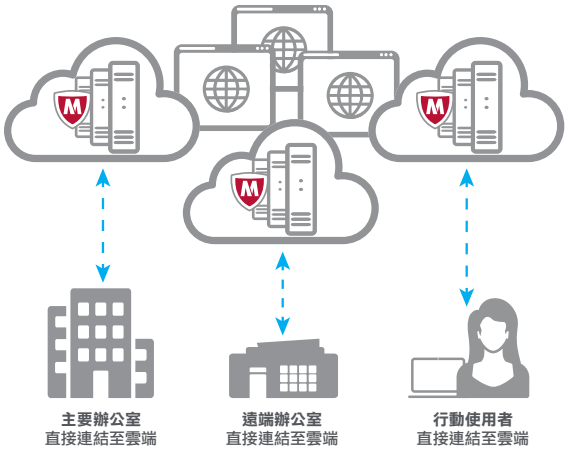

圖 1. McAfee Web Gateway Cloud Service 部署。

Web 威脅通常透過加密的流量傳播，以規避 Web 安全防禦措施。幾乎所有雲端應用程式 (例如雲端儲存空間或社交媒體) 都是預設使用加密的流量。McAfee Web Gateway Cloud Service 可完全解密並檢查 HTTPS 加密流量，啟動惡意軟體防護與顯示雲端應用程式中的加密通道。

對大多數的 IT 團隊而言，控制雲端應用程式的快速增長的情形並不容易，尤其是「影子 IT」以及交由使用者選擇服務所引起的風險更加困難。充分掌握 Web 流量 (包含 HTTPS) 與預建報告，可顯示所有存取過的網站、使用中的雲端應用程式和對應的資料點以評估風險。藉由比較實際使用的 IT 和受到管制的 IT，就能輕鬆發現影子 IT。雲端應用程式 (尤其是雲端儲存空間)，正不斷獲得惡意軟體使用做為散佈機制。辨別哪個應用程式散佈惡意軟體，有助於做出通知原則決定。藉由完整評估雲端服務的涵蓋範圍，執行 1600 個以上的雲端應用程式控制項可將風險降至最低，例如徹底防範上載、訊息傳遞或封鎖應用程式。

世界哪些地區提供 McAfee Web Gateway Cloud Service ?

請造訪 **https://trust.mcafee.com** 我們的資料中心所在位置、可用性狀態和更多其他的即時更新和可見度。

有效率的安全性管理

管理跨越多個主控台與多項原則管理安全性十分繁瑣，尤其是當內部部署和雲端 Web 安全分別管理的時候更是如此。在混合環境中，僅有一個管理主控台可同時管理內部部署和雲端部署，以及一套原則和一個報告介面。

當單獨部署而不採用內部部署硬體或軟體時，McAfee Web Gateway Cloud Service 會由 McAfee ePO Cloud、Intel Security 所有雲端安全服務的統一管理主控台和端點安全性來管理，提供安全性管理前所未有的高效率。

為端點裝置部署 Web 安全極具挑戰性，尤其是路由和驗證。McAfee Client Proxy 為選用的端點用戶端，會自動路由至我們的雲端服務並驗證，確保普遍的雲端連線和實施強制執行的一致性。藉由內部部署裝置，以及透過智慧型方式路由至連線至網路的裝置，或在離線時路由至雲端服務等措施，保持 McAfee Client Proxy 得以在混合式環境中順暢運作。其他路由和驗證選項可根據組織要求選擇使用。

深入瞭解

如需詳細資訊，請造訪 **www.mcafee.com/tw/products/web-protection.aspx**。

McAfee. Part of Intel Security.
台北市 110 基隆路一段
333 號 22 樓 2210 室
886-2-2757-6677
www.intelsecurity.com