McAfee SaaS Web Protection

雲端型 Web 安全性，提供安全有保障的網路

網路爲您的業務開啓了無限商機，但也帶來數不盡的網路犯罪意圖。每個 Web 連線都可能是感染、惡意滲透與企業風險的潛在進入點。McAfee SaaS Web Protection 採用進階資料關聯性以及由 McAfee® Global Threat Intelligence™ 永不間斷持續更新的廣泛威脅資料，針對動態 Web 型惡意軟體攻擊，提供簡易且功能多元的重要防護。McAfee SaaS Web Protection 由 Web 與雲端安全性領域的 McAfee 專業人員負責管理，並採用 Web 安全性最佳作法，能夠協助您以有效且經濟實惠的方式控管威脅與不當的網際網路存取。

主要優點

- 透過持續的更新，保護所有使用者 (包括離線使用者) 免受快速變化的惡意軟體、間諜軟體與網路釣魚的零時差攻擊。
- 實施網際網路使用原則，並讓您透過詳細的報告 (依使用者或群組分類) 瞭解 Web 使用情形。
- 有 100 多種內容類別，可讓您透過彈性的內容控制來避免企業承擔法律責任。
- 能夠控制上百種線上媒體類型和應用程式，包括導致產能低下的社交媒體網站。
- 以可預測、可順暢擴充的訂閱服務，取代逐漸攀高的內部部署重要設備成本與人力需求。

主要動機

- 想要降低現有 Web 安全技術的維護工作開銷。
- 惡意軟體相關問題逐漸增加。
- 已識別出 1 億 2 千萬個以上流通中的獨特惡意軟體。
- 每天可識別出超過 16 萬個新惡意軟體。
- 每個月可識別出超過 5 萬個新網路釣魚 URL。
- 每一季可辨識出超過 90 萬個獨特的偽防毒軟體套件。
- 根據 McAfee Labs 的記錄，每個月平均有 260 萬個新的可疑 URL。

(資料來源：McAfee Labs)

Web 的動態內容與互動性，使得可規避傳統安全方法之偵測作業的複雜 Web 威脅擴散開來。爲了保護員工、客戶、網路與智慧財產，您的組織必須要有主動式的 Web 安全。亦即這個解決方案不但要能封鎖已知不當的 URL，也能封鎖未知的隱藏攻擊、混合型威脅以及間諜軟體。McAfee SaaS Web Protection 可透過 McAfee Gateway Anti-Malware Engine 瞭解 Web 內容的行爲與運作環境來預測惡意意圖，進而封鎖其他安全性解決方案輕易放過而得以入侵網路的威脅。

Web 的使用若毫無限制，也可能會導致使用者生產力下降與法律問題。管理安全、適當的網際網路存取常會耗用資源，但此結果並非必然。透過雲端型主控台設定原則規則非常簡單，並可精確地控制線上內容、媒體類型、應用程式，甚至還能隨時存取特定的 Web 服務。

McAfee SaaS Web Protection 無須安裝任何硬體或軟體，是可靠又符合成本效益的全方位 Web 安全性解決方案。此服務建立在經過實證的軟體即服務 (SaaS) 平台上，不僅近乎無延遲、持續運作時間領先同業，且擴充性達企業級水準，因此即使面對要求最嚴苛的分散式環境，也能夠提供所需的效能來確保環境的安全。如果您已有內部部署的 Web 篩選功能，我們的服務是低風險、低成本的解決方案，絕對能協助您藉由進階防惡意軟體強化保護設定檔，亦或保護分公司辦公室和行動使用者。

全面的 Web 保護

McAfee SaaS Web Protection 可全面保護 Web 2.0 流量的安全。它會自動對所有受原則管制的使用者套用存取規則，以實施組織的網際網路使用原則。違反原則的流量在進入您的網路前即會遭到封鎖。對於允許的流量，McAfee SaaS Web Protection 會透過基於防毒與全球威脅信用評價篩選程式的進階反惡意軟體引擎，使用精密的技術對要求的網頁上所有的內容與使用中程式碼分析其性質與意圖。這將封鎖惡意網頁並去除有威脅的元素，以提供因應惡意軟體、病毒及其他攻擊的立即保護，讓使用者得以繼續完成工作。

透過內容分析偵測不斷變化的惡意軟體

網站上的惡意軟體可透過無訊息的方式下載至不具戒心之造訪者的裝置，結果便是智慧財產或客戶資訊的資料外洩。我們採用屢獲殊榮的 McAfee Gateway Anti-Malware Engine 掃描網頁上的主動式內容並辨識其意圖或預期行爲，主動防範試圖竊取資訊的零時差惡意軟體、混合型威脅、網路釣魚網站與目標式攻擊。

Web 威脅與惡意內容遍佈全球無所不在，而 McAfee 研究也涵蓋了這些範圍：

- 垃圾郵件 URL 在北美洲佔所有 Web 威脅的比例達 41%，其後為惡意網站及可疑的惡意網站。
- 在歐洲/中東/非洲，垃圾郵件 URL 和網路釣魚 URL 各佔總數的 31%，另外的 29% 則是惡意網站。
- 在拉丁美洲和南美洲則有 36% 的惡意 URL 與垃圾郵件主控有關，30% 為主控網路釣魚網站，25% 則是主控其他類型的惡意網站。
- 而在亞太地區，總數的 31% 為可疑的網站 (伺服器登錄的方式使得必須嚴密監控該網站)。垃圾郵件 URL 佔 29%，為第二大的群組，其後則是佔 24% 的惡意網站。

(資料來源：*McAfee 威脅報告*)

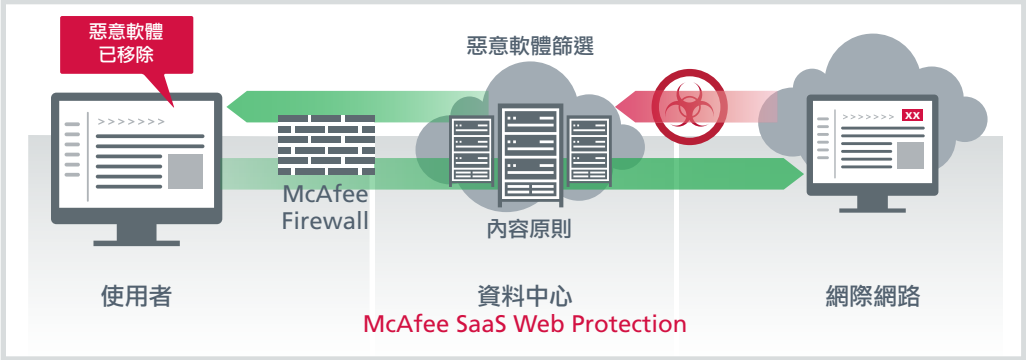

圖 1. McAfee Saas Web Protection Web 請求流程。

彈性的全面性控制

在企業環境中使用網路就如一把雙刃劍；通常是生產力核心所在，但有時對不當活動而言，卻也是便利的昂貴平台。協助使用者抵禦惡意軟體相當重要，但並非您的首要之務。防止資料外洩並讓員工保有生產力有助於節省金錢，同時避免承擔可能危及企業的法律責任。

透過全面性的 Web 篩選選項，包括約 100 種網站類別、數以百計的媒體類型、超過 1000 個的線上應用程式，甚至還有加密 SSL 流量，便可確保 Web 存取得以擺脫攻擊性、不當或不具產能的活動。使用者仍可自由探索網路，不再接觸到耗時的干擾項目。在此同時，您也能夠：

- 深入查詢特定的 Web 應用程式，並允許員工於特定時間存取社交媒體網站。
- 停用線上檔案分享網站的上傳功能以便將資料存留於企業內部，同時仍可讓外部協作者下載檔案。
- 提供高階主管更有彈性的排程功能，使其能夠自行存取 Web，並將獨立工作者置於工作日原則群組中。

如此的細部控制會比不分好壞一律封鎖網際網路存取來得有效，同時也能創造更具生產力且安全的線上使用經驗。

簡化透明驗證以及-網路內、外保護

使用 McAfee Saas Web Protection 讓員工的 Web 流量路由更加容易。您可以使用瀏覽器 Proxy 設定或 Proxy 自動設定 (PAC) 檔等標準路由技術，或者使用 McAfee Client Proxy 讓路由更容易進行。您可以利用免費、選用的用戶端軟體技術執行無縫驗證和重新導向，而無須研發瀏覽器外掛程式或 Cookie、回傳流量至集中區，或甚至寫入 PAC 檔。即使是由受控制的入口網站 (如咖啡廳、旅館或其他 WiFi 熱點) 提供網際網路供離線、漫遊使用者使用，McAfee Client Proxy 仍可將 Web 保護原則和 Web 安全性套用至這些使用者。

方便的管理與報告

可自訂的儀表板可協助每一位管理員監控趨勢，並進一步瞭解組織使用 Web 與電子郵件資源的情形。您可以從任何瀏覽器隔離問題、記錄不當活動、遵循法規報告以及微調篩選設定，以施行 Web 使用原則。有違反原則與 Web 內容遭封鎖的情況發生時，使用者會收到專屬的通知警示。管理警示可即時提供重要安全性事件的相關資訊。

深入瞭解

透過 McAfee 雲端型安全性服務，保護企業安全變得簡單又經濟實惠。除了我們的 McAfee SaaS Endpoint Protection、McAfee SaaS Email Protection 以及 McAfee SaaS Email Archiving 服務之外，還可使用 McAfee SaaS Web Protection 全方位防禦數位威脅和法規漏洞。

除了 SaaS 以外，McAfee 也為任何尋求最具彈性解決方案的使用者提供內含裝置、虛擬與 SaaS 規格的全方位產品項目。

如需深入瞭解，請至 www.mcafee.com/tw/products/security-as-a-service/index.aspx 或 www.mcafee.com/tw/products/web-protection.aspx。

McAfee
An Intel Company

邁克菲有限公司台灣分公司
台北市 110 基隆路一段
333 號 22 樓 2210 室
886-2-2757-6677
www.mcafee.com/tw

60363ds_saas-web-protection_0713_fnl_ETMG