



McAfee Web Gateway

安全性。控制。效能。

現在組織可透過 Web 進行的事情之多可謂前所未有。當今的 Web 提供動態、即時的使用者體驗。然而，隨著複雜攻擊日益增加，Web 也成為更加危險的場所。McAfee® Web Gateway 裝置是任何組織可用來抵禦不斷演變之惡意軟體威脅的第一道防線。它採用由功能強大之本機意圖分析與 McAfee Labs 所提供之雲端保護結合而成的先進安全性方法，組織不僅能賦予員工存取權限，還能大幅降低面臨的風險。



McAfee Web Gateway

- 通過 Common Criteria EAL2+ 與 FIPS 140-2 Level 2 認證。
- 連續五年獲評為 Gartner Magic Quadrant (魔術象限) 的領導者。
- 評鑑為市場上最佳的防惡意軟體解決方案 (AV-TEST)。

隨著 Web 應用程式的用途與複雜度與日俱增，我們也更加需要靈活的存取能力及進階的 Web 安全性，因為即使表面上看起來「安全」的網站也可能被用來散佈惡意軟體。

在今日的世界，光是封鎖已知的病毒，或限制存取「已知不當」的網站已經不敷需求。雖然特徵碼式的防毒措施與僅限類別的 URL 篩選等反應式技術有其必要性，卻已不足以防護針對雲端應用程式的存取行為，或抵抗現今的攻擊。

而且，因為這些解決方案將重點放在已知的內容和惡意的物件或可執行檔，所以無法防止現今將惡意程式碼隱藏在表面上值得信任之 HTTP 或 HTTPS 流量內的攻擊，也無法針對未知或新崛起的威脅提供保護。能夠安全、精確地存取雲端應用程式，同時主動封鎖未知與已知威脅，現已變得十分重要。

McAfee 是 Intel Security 的一份子，比其他廠商更瞭解 Web 世界的安全性需求，因此能提供業界最有效且經過實證的主動式解決方案：McAfee Web Gateway。

完整的入埠與出埠保護

McAfee Web Gateway 能夠對 Web 流量的各個層面都提供全面性的安全防護，不論其位置或裝置為何。使用者啟動 Web 要求時，McAfee Web Gateway 會先強制執行組織的網際網路使用原則。對於所有允許的流量，它則會針對經由要求之網頁進入網路的所有內容與作用中程式碼，使用本機與全域技術來分析其本質與意圖，藉此提供立即的惡意軟體與其他隱藏威脅防護。此外，McAfee Web Gateway 會檢驗 SSL 流量來提供深入的保護，藉此抵禦透過加密來偽裝的惡意程式碼或不當的應用程式，這點與基本封包檢查技術大相逕庭。

對於接收由外部來源上傳之資料或文件的網站，入埠保護亦能減輕代管這類網站之組織所承受的風險。處於反向 Proxy 模式的 McAfee Web Gateway 能在內容上傳前掃描所有內容，同時保護伺服器與內容。

為了保護出埠流量，McAfee Web Gateway 會透過領先業界的 DLP 技術掃描使用者依據所有主要 Web 通訊協定產生的內容 (包括 HTTP、HTTPS 及 FTP)，除了預防機密、敏感或管制資訊外洩之外，還能避免經由社交網站、部落格、維基百科 (wiki) 或線上生產力工具 (如網頁式電子郵件、記事本與行事曆) 洩露組織資訊。對於透過「受殭屍病毒感染的」機器嘗試回報的安全性資訊或傳輸的敏感資料，McAfee Web Gateway 也會保護不讓這些未經授權的資料離開組織。

McAfee Web Gateway 提供業界最有效的保護

McAfee Web Gateway 獲評為最佳¹的惡意軟體防護方案，可透過 McAfee Gateway Anti-Malware Engine，使用專利申請中的方法進行無需特徵碼的意圖分析。主動式的意圖分析可以即時篩選出 Web 流量中的惡意內容。透過掃描網頁上的主動式內容、模擬並辨識行為及預測意圖，McAfee Web Gateway 可以主動防範零時差與鎖定式攻擊。

McAfee Web Gateway 現已整合進階防惡意軟體偵測技術 McAfee Advanced Threat Defense，具備了結合靜態與動態分析的開創性沙箱功能。不但大幅提高準確度，保護功能也更為強大，足以防禦進階的動態惡意軟體威脅。

我們將這種本機即時意圖分析與全面性 McAfee 防毒保護加以結合，以迅速封鎖已知病毒，再搭配 McAfee Labs 提供的數種雲端式技術。由於 McAfee Web Gateway 採用多重技術，因此能提供更嚴密的保護，同時在單一平台上以相輔相成的技術，達到最佳的安全性，而這正是許多組織一致追求的深入防禦安全性方法。

- **McAfee 防毒搭配即時的 McAfee Global Threat Intelligence (McAfee GTI) 檔案信用評價：**憑藉著雲端式 McAfee GTI 檔案信用評價查詢功能，McAfee 能弭平病毒探索與系統更新/保護之間的斷層。
- **McAfee GTI Web 信用評價和 Web 分類：**McAfee Web Gateway 透過信用評價與分類篩選功能，提供更強大的 Web 篩選功能與防護。McAfee GTI 能根據 McAfee Labs 運用全球大量資料收集能力蒐羅而來的數百種屬性建立所有網際網路實體 (包括網站、電子郵件及 IP 位址) 的概要資料，然後再根據呈現的安全性風險指派信用評價分數，因此管理員能針對要允許或拒絕的項目套用非常精細的規則。

McAfee Web Gateway 提供擴充的雲端型 Web 信用評價功能，現更包括地理位置，讓您可根據 Web 流量的來源國家/地區，檢視地理位置並進行原則管理。對於 Web 分類與以安全為中心的 Web 信用評價，組織現可選擇內部部署、雲端查詢或兩者之組合等選項。雲端搜尋能夠消弭從探索/變更到系統更新之前的保護斷層，並且大幅增加資料涵蓋範圍，包含的唯一惡意軟體樣本高達數千萬筆。

保護加密流量

技術精良的網路罪犯已能穿越企業的安全屏障，將 SSL 流量 (HTTPS) 變成新的後門。諷刺的是，專為提供安全性而設計的通訊協定現在也必須受到保護以防遭到濫用，就像傳統的 HTTP 流量必須受到保護一樣。McAfee Web Gateway 是第一個將惡意軟體偵測、SSL 檢查以及憑證驗證等功能完全整合的安全性產品。您不需要將加密流量路由傳送至其他機器即可進行惡意軟體檢測。McAfee Web Gateway 可以直接掃描所有的 SSL 流量，以確保加密交易絕對的安全性、完整性以及隱密性，並強制執行合理的使用原則。

資料遺失防護

McAfee Web Gateway 能掃描所有主要 Web 通訊協定上的出埠內容 (包括 SSL)，協助組織抵禦出埠威脅 (如機密資訊外洩)。這項功能使它成為預防智慧財產遺失、確保文件遵循法規，以及在發生資料外洩時提供鑑識資料的必備工具。McAfee Web Gateway 充分運用了 McAfee Data Loss Prevention (DLP) 解決方案的能力，可支援預先定義的 DLP 字典，並且可透過關鍵字比對和/或規則運算式來建立自訂字典。

內建的檔案加密機制可保護上傳至檔案分享/協作網站的資料，避免未經授權的存取。若未使用 McAfee Web Gateway，使用者將無法擷取和檢視資料。

遠端使用者的行動篩選

隨著工作人力日趨分散與機動，將 Web 篩選與保護功能從辦公室完整地移轉至適用於行動環境的需求，也日漸重要。McAfee Client Proxy 是防竄改的用戶端代理程式，可讓漫遊使用者順利進行驗證並重新導向至位於雲端中的 McAfee SaaS Web Protection 解決方案，或是位於 DMZ 中的內部部署 McAfee Web Gateway。這使得網際網路存取原則的強制執行以及完整安全性的掃描能夠套用在漫遊或位於遠端的使用者身上，即使使用者是透過公用網路 (例如咖啡廳、飯店或其他 Wi-Fi 熱點) 存取網際網路也不必擔心。

McAfee Web Gateway 還能讓企業將安全性原則延伸至行動裝置上並強制執行。時下熱門的智慧型手機和平板電腦都可將 Web 流量導向至 McAfee Web Gateway，並透過標準的裝置管理和安全性控制，確保行動裝置受到先進的防惡意軟體保護和企業 Web 篩選原則的保護。對於過去在內部企業伺服器 (如內部網路、Wiki、Microsoft SharePoint 伺服器與其他 Web 型解決方案) 上提供的內容，McAfee Web Gateway 亦能將保護效力擴及至存取這些內容的行動裝置。雖然一般來說，基於安全上的考量不會將此資訊提供給某些行動裝置，但只要將 McAfee Web Gateway 部署為反向 Proxy，便可在經控管的情況下安全存取這些內部資源。

透過 McAfee Web Gateway 落實全面掌控

McAfee Web Gateway 透過強大的規則引擎來保護現今以 Web 為中心之企業，可在原則彈性和控制上取得最佳成效。為了簡化原則的建立，McAfee Web Gateway 提供鉅細靡遺的預建規則庫與常用的原則動作。組織可以挑選各種規則並輕易地加以修改，以及透過線上社群分享自己的規則。互動式規則追蹤則可簡化規則偵錯程序。

McAfee Web Gateway 平台也將合理的使用原則和控制延伸到 Web 應用程式，能以 Proxy 的方式精細控制 Web 應用程式的使用方式。組織能控制超過 1,000 個熱門的 Web 應用程式、視需求啟用或停用特定功能，以及控制 Web 應用程式的使用者與使用方式。想要讓使用者存取 Facebook，但不允許使用聊天功能？沒問題。

彈性和控制可延伸至使用者驗證與存取。McAfee Web Gateway 支援多種驗證方法，包括 NTLM、RADIUS、AD/LDAP、eDirectory、Cookie 驗證、Kerberos 或本機使用者資料庫。McAfee Web Gateway 驗證引擎允許管理員實作彈性的規則，包括使用多種驗證方法。例如，McAfee Web Gateway 能嘗試以透明的方法驗證使用者，然後再依據結果提示使用者提供認證、使用其他驗證方法、套用限制原則或直接拒絕存取。

McAfee Web Gateway Identity 是選用的附加元件，其包含適用於數百種雲端型熱門應用程式的單一登入 (SSO) 連接器。McAfee Web Gateway Identity 以 SSO 為基石，讓使用者按一下滑鼠即可存取授權的雲端應用程式，可改善當今以 Web 為中心之企業的安全性，並減少與密碼相關的求助電話。

支援 HTTP POST 和安全宣告標記語言 (Security Assertion Markup Language, SAML) 連接器，涵蓋各種應用程式。佈建連接器後，系統管理員便

能夠在特定 SaaS 應用程式中建立並終止使用者帳戶。在授予敏感 SaaS 應用程式的存取權之前，若客戶需要強式驗證，可透過 Pledge 用戶端部署 McAfee One Time Password 伺服器軟體，以使用可與任何智慧型手機、行動電話或桌上型電腦系統 (Windows、Mac 和 Linux) 相容的多重要素驗證。

McAfee Web Gateway 還能透過原生的串流 Proxy 支援將存取控制延伸至串流內容，提供頻寬節約效益及縮短延遲。

McAfee Web Gateway 提供靈活的基礎架構與效能

McAfee Web Gateway 是一款高效能的企業級 Proxy，它能提供現今要求最嚴苛之企業所需的快取、驗證、管理及授權控制。藉由提供可擴充的裝置機型系列 (具有針對虛擬機器、McAfee SaaS Web Protection 雲端服務，以及甚至高效能刀鋒選項的整合式高可用性與支援)，McAfee Web Gateway 能提供您需要的部署彈性與效能，以及在單一環境中輕易支援數十萬名使用者的可擴充性。(如需 SaaS 的詳細資訊，請參閱 McAfee.com/tw 上有關 McAfee SaaS Web Protection 的資訊。)

您也可以混合部署選項。例如，您可以在尖峰時刻將部分 Web 流量卸載到雲端以提升高可用性效能，或將此混合模型當做高成本效益的容錯移轉選項。針對混合型內部部署和雲端部署的自動原則同步和報告，都有助於提高管理效率、確保一致地強制執行原則，並能簡化報告、追蹤和調查流程。

McAfee Web Gateway 提供眾多實作選項 (不論是明確 Proxy、透明橋接或路由器模式)，能確保您的網路架構受到支援。

McAfee Web Gateway 受眾多的整合標準支援，旨在搭配您獨特的環境。不論是網頁快取通訊協定 (WCCP)、網際網路內容調適通訊協定 (ICAP/ICAPS)，乃至於安全通訊端 (SOCKS) 通訊協定，McAfee Web Gateway 都可有效地與其他網路裝置和安全性裝置進行通訊。

除此之外，McAfee Web Gateway 現已提供 IPv6 支援，能協助規模較大的組織與聯邦機構遵循法規。它能縮短內部 IPv4 與外部 IPv6 網路間的差異，將所有可用的安全性措施與基礎架構功能套用到流量。

洞見未來趨勢的價值與平台

McAfee Web Gateway 能結合許多各自要求多種獨立產品的保護措施並進行整合。您只需要這一台經濟實惠的裝置，即可獲得 Web 篩選、防惡意軟體、防間諜軟體、SSL 掃描、資料遺失防護以及內容控制篩選等保護功能。而簡化的管理資源耗用則表示能在多個保護措施與通訊協定當中共用一個安全性原則，節省您寶貴的時間與金錢。

安全性風險管理和報告

McAfee Web Gateway 支援最熱門、最廣受好評的安全性管理技術：McAfee ePolicy Orchestrator® (McAfee ePO™) 平台。由於 McAfee ePO 平台是彙總資訊的單一來源，因此能協助您迅速識別及緩和問題，提升法規遵循管理的效力。

McAfee ePO 軟體透過 McAfee Content Security Reporter 延伸模組來支援詳細 Web 報告。McAfee Content Security Reporter 提供您所需的資訊和鑑識工具，讓您瞭解組織如何使用 Web、辨識未知或惡意的「影子 IT」應用程式例項，並協助您遵循法規、找出趨勢、隔離問題、記錄不當的 Web 活動以及自訂篩選設定以強制執行 Web 使用原則。它結合了儀表板檢視，並利用功能強大的離線處理功能深入剖析 Web 流量，只要一個易於使用的解決方案即可獲得所有情報。McAfee Content Security Reporter 提供一個外部的獨立報告伺服器，其設計是用於從現有的 McAfee ePO 伺服器，卸載耗用大量資源的資料處理與儲存，並使該伺服器得以擴充，即使是最大型全球化企業的報告需求也可以滿足。

授權

為了極致的部署彈性及讓投資經得起時間考驗，McAfee 將 McAfee Web Gateway 與 McAfee SaaS Web Protection Service 的所有功能併入單一套件：**McAfee Web Protection**。不論是內部部署、在雲端部署，抑或是同時部署兩種形式以提升彈性與高可用性，決定權在您手上。不管您的選擇為何，必定能體驗 McAfee 獲得獎項肯定的防惡意軟體保護效力與全方位的 Web 篩選。

McAfee Web Gateway 硬體則另外單獨販售。



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

1. 根據 AV-TEST 主導的測試結果，McAfee Web Gateway 可偵測到 94.5% 的零時差惡意軟體、99.8% 的惡意 Windows 32 可攜式可執行檔 (PE) 以及 98.63% 的非 PE 檔案。「McAfee Web Gateway 安全性裝置測試」，AV-TEST GmbH。