McAfee Web Gateway

安全性。相互關聯的情報。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 是任何組織皆可用來抵禦新興惡意軟體威脅的重要防護。結合功能強大的本機意圖分析與 McAfee Labs 所提供的雲端防護，形成先進的安全防護方式，讓組織擁有安全的網際網路存取權限，並大幅降低面臨的風險。

隨著網際網路的用途與複雜程度不斷增加，進階 Web 安全的需求也隨之上升。甚至連看起來「安全」的網站都可能成為散播惡意軟體的目標。現今的世界，光是封鎖已知的病毒，或限制存取已知不當的網站，都已經不敷安全需求。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看似值得信任的 HTTP 或 HTTPS 流量內的這類攻擊，也無法針對未知或新崛起的威脅提供保護。能夠安全、精細地存取雲端應用程式，同時主動封鎖未知與已知威脅，是十分重要的關鍵。

全面的入埠與出埠保護

McAfee Web Gateway 能在單一高效能裝置軟體架構中，對 Web 流量各個層面提供全面性的安全防護。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 會檢驗安全通訊端層 (SSL) 流量來提供深入的保護，藉此抵禦惡意程式碼，或控制透過加密隱藏的應用程式，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。在反向 Proxy 模式中，McAfee Web Gateway 會在上傳內容前掃描所有內容，保護伺服器與內容。

為了保護出埠流量，McAfee Web Gateway 使用了領先業界的 McAfee 資料遺失防護技術，來掃描 HTTP、HTTPS 與 FTP 等重要的 Web 通訊協定上，由使用者所產生的內容。同時也防範機密、敏感或管制資訊，透過社交網路網站、部落格、維基百科，或 Web 型郵件、分類資料夾與行事曆等線上生產力工具，從組織中外洩。McAfee Web Gateway 進一步防範未經授權的資料透過感染殭屍病毒的電腦 (會嘗試撥打家用電話或傳輸敏感資料) 流出組織。

McAfee Web Gateway

- 適用於多種硬體機型，且可做為虛擬機，並支援 VMware 與 Microsoft Hyper-V。
- 整合輔助性 McAfee 解決方案，包括 McAfee Endpoint Security、McAfee Advanced Threat Defense、McAfee Threat Intelligence Exchange、McAfee Cloud Data Protection 以及 McAfee Cloud Visibility—Community Edition。
- 通過 Common Criteria EAL2+ 與 FIPS 140-2 Level 2 認證。
- 支援多種密碼編譯金鑰儲存選項，包括 Gemalto SafeNet 硬體安全模組 (HSM)、Thales nShield HSM 和 Thales PCIe 卡。
- 獲評選為安全 Web 閘道類別的最佳防惡意軟體 (AV-TEST)。

McAfee Web Gateway 提供業界最佳的保護

McAfee Web Gateway 獲評選為惡意軟體防護中最佳[1] Web 安全性解決方案，透過 McAfee Gateway Anti-Malware Engine，使用已註冊專利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 流量中先前未知或零時差的惡意內容。藉由掃描網頁的主動式內容、模擬並理解其行為，與預測其意圖，McAfee Web Gateway 可防範零時差惡意軟體散播至端點，大幅降低系統清理與修補的相關成本。

我們結合意圖分析與 McAfee Labs 的 McAfee 防毒與全域信用評價技術，快速封鎖已知惡意軟體與惡意網站。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階層式防禦安全性方法。

- **McAfee 防毒搭配即時的 McAfee Global Threat Intelligence (McAfee GTI) 檔案信用評價：**雲端式 McAfee GTI 檔案信用評價查詢能弭平發現病毒與系統更新/保護之間的落差。
- **McAfee GTI Web 信用評價和 Web 分類：**McAfee Web Gateway 透過結合信用評價與分類篩選兩大功能，提供 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。
- **地理位置：**McAfee Web Gateway 配備地理位置功能，可啟用地理檢視，以及根據 Web 流量與使用者來源國家/地區進行的原則管理。

對於 Web 分類和 Web 信用評價，組織可以選擇內部部署或雲端查詢，或是同時使用兩者。雲端搜尋能夠消弭從發現/變更到系統更新之前的保護空窗期，並依靠數億筆唯一惡意軟體樣本相關資料，提供廣泛的涵蓋範圍。

進階威脅分析整合

McAfee Web Gateway 整合了我們的進階惡意軟體偵測技術：McAfee Advanced Threat Defense，該技術結合可自訂的沙箱功能與深度靜態程式碼分析。McAfee Advanced Threat Defense 搭配 McAfee Web Gateway 中 Gateway Anti-Malware Engine 的內嵌掃描功能，便成為可抵禦網際網路威脅的最強大防護。想要降低成本、簡化進階威脅分析選項的組織，可以將雲端沙箱 McAfee Cloud Threat Detection 與其他多個威脅分析層加以整合。

共用威脅情報

儘管關鍵情報位於端點、網路、安全資訊與事件管理 (SIEM) 解決方案、閘道等之中，但現今許多安全性工具以孤立形式存在，而非專為共用威脅情報而設計。共用情報時，可運用情報更妥善地抵禦威脅、偵測現有的漏洞，並透過有效修正受損系統改進事件回應。若使用 McAfee Threat Intelligence Exchange，包含 McAfee Web Gateway 在內的 McAfee 解決方案便可彼此共用情報以弭平落差。McAfee Web Gateway 會針對由 McAfee Gateway Anti-Malware Engine 所發現的零時差惡意軟體，建立及共用新的檔案信用評價，然後在此流程中提供大量的值，如此一來，舉例來說，就能在新 DAT 發行前保護端點裝置。此外，McAfee Web Gateway 可使用 McAfee Threat Intelligence Exchange 提供的擴充威脅情報，遏止更多威脅。

加密流量內的分析與保護

技術精良的網路罪犯已能穿越企業安全屏障，將 SSL 流量 (HTTPS 和 HTTP/2) 轉化為後門。諷刺的是，專為提供安全性而設計的通訊協定也必須接受風險評估。McAfee Web Gateway 整合惡意軟體偵測、SSL 檢查以及憑證驗證功能，成為全面的加密流量檢查方式。

不必添購其他 SSL 掃瞄硬體，McAfee Web Gateway 就能在單一硬體或虛擬裝置架構中執行這一切。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。

想要主動深入檢查 SSL 流量的組織，可以透過 McAfee Web Gateway 中的安全通訊端層 (SSL) 分流裝置，根據原則分擔整個未加密流量或單一流量。這個支援軟體的功能允許將全部或部分解密的 SSL 流量鏡像傳送到其他安全性解決方案，例如入侵防護系統 (IPS) 或網路型資料外洩防護 (DLP) 解決方案。

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)。這點使其在避免智慧財產遺失、確保並記載法規符合性，以及在侵害發生時提供鑑識資料等方面，成為強而有力的工具。McAfee Web Gateway 充分運用 McAfee Data Loss Prevention (McAfee DLP) 解決方案組合的能力，納入內建的預先定義 DLP 字典，並提供透過關鍵字比對和/或規則運算式來建立自訂字典。

若為使用雲端儲存空間的組織，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。若無使用 McAfee Web Gateway，使用者將無法擷取和檢視資料。

適用於離線使用者的保護措施

有鑑於越來越多的員工分散於各地並四處行動，從辦公室轉換到外地之時仍能隨時提供 Web 篩選和保護，就成為日益迫切的需求。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，並重新導向至位於隔離區域 (DMZ) 中的內部部署 McAfee Web Gateway，或 McAfee Web Gateway Cloud Service。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，即便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 還能藉由將 Web 流量導向至 McAfee Web Gateway，讓企業將安全性原則延伸至行動裝置上並強制執行。透過我們與行動裝置管理供應商 AirWatch 和 MobileIron 的合作關係，McAfee Web Gateway 能確保 Apple iOS 與 Google Android 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。

McAfee Web Gateway 的無比彈性

McAfee Web Gateway 具備強大的規則型引擎，可獲得原則彈性和控制。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，以及透過我們的線上社群分享自己的規則。若要執行進階管理，情境式規則準則與共用清單的獨特組合，可開啟通往解決問題與最佳化 Web 安全的康莊大道。互動式規則追蹤則可簡化規則偵錯程序。

McAfee Web Gateway 將控制延伸到雲端應用程式，能以 Proxy 的方式精細控制 Web 應用程式的使用方式。組織能將數千個控制項套用至雲端應用程式、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 Dropbox，但不允許上傳？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NT LAN Manager(NTLM)、遠端驗證撥入使用者服務(RADIUS)、Active Directory(AD)/輕量級目錄存取通訊協定(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為基礎，讓使用者按一下即可存取授權的雲端應用程式，從而改善安全性，並減少與密碼相關的求助電話。支援HTTP開機自我測試(POST)和安全宣告標記語言(SAML)連接器，並涵蓋各種應用程式。佈建連接器後，系統管理員便能夠在特定軟體即服務(SaaS)應用程式中，建立與終止使用者帳戶。

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。其他頻寬控制項可用來強制決定流量類別的下限、上限和優先順序，讓組織能充分善用自身的可用頻寬。

McAfee Web Gateway提供靈活的基礎架構與效能

McAfee Web Gateway為高效能的企業級Proxy，由可擴充的裝置機型系列提供，該系列具有整合的高可用性、虛擬化選項，以及具備McAfee Web Gateway Cloud Service的混合部署。McAfee Web Gateway具備部署彈性和效能，以及可在單一環境下支援數十萬使用者的絕佳擴充能力。

您也可以混合部署選項。例如，您可以將所有Web流量導向至連網使用者適用的內部部署裝置，並將所有離線使用者路由傳送至雲端服務，藉此大幅降低在多通訊協定標籤交換(MPLS)線路或虛擬私人網路(VPN)上回傳流量的成本。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)和WebSocket通訊協定，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。

此外，McAfee Web Gateway還提供IPv6支援，有助於大型企業和美國聯邦機構符合法規。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至流量。

未來的整合平台

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。URL篩選、防毒、零時差防惡意軟體、安全通訊端層(SSL)掃描、資料外洩防護與集中管理，所有功能都整合於單一裝置軟體架構中。管理部署整合適用所有外型規格，因此可將某個原則從單一管理主控台擴展至內部部署裝置、裝置叢集、虛擬裝置與雲端服務。

安全性風險管理和報告

McAfee Web Gateway 支援熱門且廣受好評的安全性管理技術，McAfee ePolicy Orchestrator® (McAfee ePO™) 軟體，作為所有安全報告的單一來源。

McAfee ePO 軟體透過 McAfee Content Security Reporter 延伸模組，提供詳細 Web 安全報告。McAfee Content Security Reporter 提供資訊和鑑識工具，讓您瞭解組織如何使用 Web、遵循法規、找出趨勢、釐清問題，以及自訂篩選設定以強制實行 Web 安全原則。McAfee Content Security Reporter 提供一個外部的獨立報告伺服器，其設計是從現有的 McAfee ePO 伺服器，分擔耗用大量資源的資料處理與儲存工作，並使伺服器得以擴充，即使是最大型全球化企業的報告需求也可以滿足。

此外還有 McAfee Web Gateway 與 McAfee Cloud Visibility—Community Edition 整合，後者是提供給 McAfee 資料遺失防護、加密以及 McAfee Web 保護客戶的免費服務，可用來掌握雲端應用程式使用情形和風險。員工正在使用雲端應用程式，但 IT 人員對這些事卻所知不多，這種缺乏掌握的情形會帶來風險。將所有雲端應用程式存取、風險等級和資料分類一併放在簡單的儀表板上，就能消除這類負擔，讓安全專業人員可以將時間和精力集中在保護資料遷移至雲端，同時控制雲端存取，達到降低組織風險的效益。

McAfee Cloud Data Protection 亦包含 McAfee Cloud Visibility—Community Edition 免費服務，作為保護雲端資料的後續步驟。

授權

為了彈性部署的最終目標以及讓投資經得起時間考驗，McAfee 將 McAfee Web Gateway 與 McAfee Web Gateway Cloud 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，決定權都在您手上。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 篩選能力。

McAfee Web Gateway 硬體則另外單獨販售。

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 Security Appliance Test（McAfee Web Gateway 安全性裝置測試），AV-TEST GmbH。

台灣
台北市信義區忠孝東路五段68號29樓，11065
電話：+886 2 8729 9222
www.mcafee.com/tw