McAfee Email Gateway

保護企業電子郵件

在任何企業環境中，電子郵件都是不可或缺的存在，也是最重要的任務關鍵服務之一。其可跨組織、地理和政治界限快速散播各項資訊承載的能力，讓它成為有效的工具，同時也極具安全性挑戰。McAfee® Email Gateway 可協助您提升電子郵件安全性，並將防禦功能與入埠威脅防護、出埠資料遺失防護、加密、進階符合性和集中管理整合為一個易於部署的裝置。

主要優點

完整的入埠與出埠保護

- 完整的入埠安全性，以防範所有來自電子郵件的威脅。
- 內建電子郵件加密功能。
- 內建符合性範本和資料外洩防護，可防止敏感資訊外洩。

進階的安全性、管理功能與擴充能力

- 有虛擬裝置、硬體裝置、刀鋒伺服器，或 McAfee SaaS Email Protection 的整合式混合解決方案可供選擇。
- 集中式管理、訊息搜尋、報告和隔離。
- 叢集與整合式負載平衡，可依據規模調整，以符合最繁重的內部部署要求。

透過 McAfee® ePolicy Orchestrator® (McAfee ePO™) 軟體、McAfee Global Threat Intelligence (McAfee GTI)、McAfee Advanced Threat Defense 和混合電子郵件安全性方式，從 Security Connected 受惠。

電子郵件安全性挑戰

讓我們看看現今企業面臨的重大電子郵件安全性問題：

- 入埠電子郵件攻擊已逐漸成為組織化犯罪行為，以尋求資訊獲取財務利益。攻擊會使用複雜的社交工程技術，並不斷變化以逃避傳統的特徵碼型防禦。
- 電子郵件是機密和敏感資料遭竊或遺失的主要媒介，不論是透過善意但粗心的員工或是帶惡意的內部人員亦然。
- 由於電子郵件在操作上的重要性和其顯而易見的弱點，目前不分政治立場和產業，電子郵件都須受到規範者的審查。強制受審項目包括支付卡 (PCI DSS)、金融服務 (GLBA)、醫療 (HIPAA) 和所有美國公共事業 (SOX)。
- 全球郵件數中，約有75%是垃圾郵件，包括顯示標記不同的國家/地區。魚叉式網路釣魚變得更具目標性、更以財務利益為目標，成效也更勝以往。
- McAfee Labs 在 2013 年第 4 季中，每天都識別出約 2,250 個網路釣魚 URL，且全年都維持此效率。

為什麼要屈就於片段、不當的防禦？

現今企業的電子郵件防禦皆已進化，而值得注意的是，大部分現有電子郵件安全性幾乎都專注於入埠，而沒有針對出埠資料外洩提供保護。也就是說，您會發現防禦機制是由多家廠商個別部署且重複進行重設比列的各種單點解決方案所組成，包括防惡意軟體、防垃圾郵件、防網路釣魚、防毒、加密、資料外洩防護。其中有許多項目都不符合目前的最佳實作表現標準。

2013 年獲得獎項

- Gartner 安全電子郵件閘道魔術象限的領導者象限。
- Forrester Wave 電子郵件內容安全性的領導者。
- SC Magazine 最佳電子郵件內容安全性的五顆星 Best Buy (最值得購買獎)。
- SC Magazine資料防護的產業創新獎。

儘管一流的防垃圾郵件解決方案可達到 99% 或以上的垃圾郵件偵測準確度，但許多電子郵件防禦只達到 95% 或更低。4% 的差異聽起來不大，但實際上在垃圾郵件滲透和潛在系統感染方面是 400% 的差異。當垃圾郵件以數十億為單位計數時，增加 4% 就足以對業務、負荷過重的郵件基礎架構和阻塞的頻寬造成顯著影響。即使只有極少數不需要的電子郵件突破防禦，篩選和刪除垃圾郵件都可能拖累使用者。惡意軟體感染的機會增加，會導致成本增加、損失產能和可能的資料遺失。

最後，不可避免地，大部分 IT 組織花費過多時間和金錢在維護零碎的防禦、保護敏感資訊不從組織外流、顯示法規符合性，以及修復不當電子郵件安全性帶來的後果。現在有一項具說服力的企業方案，提供完整的電子郵件安全性解決方案，可整合入埠和出埠防禦、簡化管理和精簡符合性。這個解決方案就是 McAfee Email Gateway。

全方位的電子郵件保護

領先市場的安全性

McAfee Email Gateway 將進階入埠威脅防護和出埠資料遺失防護、進階符合性與電子郵件加密、效能、報告和統一管理全部整合在一個單一的強化平台，只要一個價格，就可擁有全部功能。

- 結合區域網路資訊與 McAfee GTI 的信用評價情報，McAfee Email Gateway 可針對入埠威脅、垃圾郵件和惡意軟體提供最完整的可用保護。
- McAfee Gateway Anti-Malware Engine 的點擊時連結掃描功能與行為模擬功能可阻擋透過惡意 URL 進行的攻擊。
- 與 McAfee Advanced Threat Defense 整合後，透過靜態程式碼與動態分析 (沙箱作業) 的創新結合，可偵測到最複雜的規避式惡意軟體。
- 其精密的內容掃描技術、多元加密技術和精確的原則型訊息處理可避免出埠資料遺失並簡化符合性。
- 與 McAfee ePO 軟體的完全整合為叢集內或各叢集間的解決方案提供完整管理功能，以及企業級的記錄與報告功能，以簡化管理和符合性工作負擔，可明顯降低成本。

全方位的入埠威脅防護

McAfee Email Gateway 識別和阻擋傳入垃圾郵件的準確率達 99% 以上，同時針對病毒、惡意軟體、網路釣魚、目錄收集、阻絕服務攻擊(DoS)和退回攻擊提供整合式保護。它可防範零時差威脅、鎖定式和混合型攻擊，並透過動態垃圾郵件分類與威脅回應之可能組合大幅降低垃圾郵件突增的影響。McAfee Email Gateway 使用 McAfee GTI 的寄件者、訊息和 URL 信用評價來提供更新。

同時也使用次要防毒引擎，協助客戶針對惡意軟體提供分層保護，並處理符合性要求。

點擊時連結掃描可阻擋不斷進化的攻擊。

McAfee ClickProtect 是 McAfee Email Gateway 的功能，可消弭電子郵件中內嵌 URL 的威脅。無論 URL 看起來多麼無害，它都會檢查在掃描郵件時 (掃描時間) 及使用者點擊 URL 時 (點擊時間)，URL 是否意圖進行變更。此時進行的再次檢查包含 URL 信用評價檢查與主動式模擬。主動式模擬則採用 McAfee Web Protection 所使用的領先業界的 Gateway Anti-Malware 技術。管理員可以設定掃描時間與點擊時間原則，並且啟用 URL 模擬避免使用者進行點擊。Safe Preview 則可提供快速預覽，藉此利用使用者情報作為額外安全防護層。為了全面防止源自電子郵件的 Web 存取，程式可偵測到 URL 並加以移除，或是以說明文字取代 URL。

McAfee Advanced Threat Defense 可偵測到複雜的規避式惡意軟體。

McAfee Advanced Threat Defense 透過創新的分層方法，可偵測到現今潛藏的零時差惡意軟體。其結合深層靜態程式碼與動態分析 (沙箱作業)，可分析惡意軟體的實際行為。Mcafee Email Gateway 與 McAfee Advanced Threat Defense 緊密整合後，可對電子郵件夾帶的可疑檔案進行前述分析，在惡意軟體入侵收件匣前加以封鎖。

其使用特徵碼和即時模擬這類較初階的強度分析方法來確保效能，再加上沙箱作業的全靜態程式碼分析功能，更可提供詳細的惡意軟體分類資訊，針對高度偽裝、規避式威脅提供更完善的防護，同時運用程式碼重複使用功能，找出相關的惡意軟體。延遲或無法預期的執行路徑，通常不會在動態環境中執行，但可以透過解壓縮與全靜態程式碼分析偵測到。

靜態程式碼與動態分析相結合後，可提供完整評估和詳細資訊，例如行為摘要、惡意軟體嚴重性、惡意軟體系列關聯、執行路徑，以及在動態分析期間已執行程式碼的百分比。

灰色郵件篩選可進一步減少不需要的郵件。

不需要的郵件可能是使用者曾提出請求的合法大宗郵件，但現在已不再需要 (例如，業界新聞稿和通知)。雖然灰色郵件一般不會被視為垃圾郵件，但對收件者來說也可能極為擾人。套用篩選以啟用動作 (包括阻擋和隔離)，有助於維持收件匣的整潔。

完整出埠保護，維護內容安全

內含電子郵件加密功能。

整合式原則強制電子郵件加密是 McAfee Email Gateway 的標準功能，合併使用B2B (TLS、S/MIME 和 OpenPGP) 和 B2C 技術 (推送或提取)，確保即使沒有加密能力的收件者也能接收和回覆安全電子郵件。各品牌的網頁郵件用戶也可使用推送/提取技術，並可在行動裝置上擷取及檢視加密訊息。以在閘道處套用加密取代在桌上型電腦加密，可讓使用者不須再判斷加密要求，並可避免使用者忘記將敏感資料加密這類常見問題。

符合性與資料遺失防護

大量的內建符合性範本集合也是已整合的內建標準功能，與 McAfee Data Loss Prevention 提供的範本相同。指紋辨識、語彙分析及叢集技術可補強關鍵字及模式比對，以便全方位偵測結構化與非結構化資料。閘道會準確識別規範內容 (HIPAA、SOX、GLBA)、個人可識別資訊 (如信用卡)、社會安全號碼、特定區域識別碼和其他客戶及員工資料，亦可偵測原始碼、專利、財務資訊及業務計劃等非結構化資料與智慧財產，並採取行動。一旦偵測到目標，它會支援各種原則型動作，包括強制加密 (推送、提取、TLS)、警示、重新路由、隔離、阻擋和其他自訂動作。

完整的管理執行能力

McAfee Email Gateway 協助管理員提供最好的電子郵件保護，讓管理員能使用企業級報告、完整可匯出記錄、即時可設定儀表板與警示，以及深入報告進行記錄，並以靈活的遞送模式，同時兼顧效能、可擴充性與穩定性，確保用最少的管理開銷提供最大 ROI。您可由 McAfee Email Gateway 管理主控台或 McAfee ePO 軟體全面管理此解決方案，同時享有下列功能：

精密多樣的使用情形與原則控制項可簡化管理作業。

- 流暢、簡單易懂的介面，包含精靈型安裝與設定。
- 目錄/輕量級目錄存取通訊協定 (LDAP) 整合。
- 集中管理電子郵件安全性，附帶精細的原則強制、訊息搜尋和詳細的對話記錄。
- 即時報告，包括互動式儀表板和深入報告功能。

先進架構提供高效能。

- 非同步的記憶體掃描。
- 整合叢集和負載平衡，提供高可用性。
- 本機或具備高度擴充能力的 McAfee Quarantine Manager 可針對多項 McAfee Email Gateway 裝置提供合併隔離服務、自訂隔離佇列，並以最高可容納 150 萬筆訊息、支援 20 萬名使用者的容量，減輕儲存和處理工作負擔。

憑證與支援

- EAL2+ 的 Common Criteria 認證，包括 NDPP 符合性。
- 經 FIPS 140-2 L1 軟體驗證與認證。
- 通用存取卡 (x.509) 支援。
- IPv6 支援。

完全經得起時間考驗：適合每個企業的完整電子郵件保護

靈活的部署方式

McAfee Email Gateway 可部署為硬體裝置 (四種不同的裝置大小)、虛擬機器，或在刀鋒伺服器架構進行部署。這樣的靈活度可為要求最高的企業通訊環境提供經濟實惠的保護和擴充能力。此外，McAfee Email Gateway 是 McAfee Email Protection 提供的服務之一，有了 McAfee Email Protection，您便可以單一訂閱價格靈活選擇將電子郵件安全性部署為內部部署電子郵件閘道 (硬體或虛擬)、雲端型 Security-as-a-Service (SaaS)，或整合的混合式組合。

對於想要善用雲端優勢又想維持現場控制的組織，則可以使用整合的混合式解決方案，同時享有以 McAfee Email Gateway 作為雲端型和內部部署原則管理的控制中心、合併報告、訊息搜尋及隔離等功能。通常，希望將惡意或擾人內容阻擋於網路之外、減少頻寬，以及在現場裝置上處理敏感資訊和加密的組織，會選擇混合型解決方案。

Security Connected

Security Connected 架構可協助客戶改善安全性狀態、提供最佳安全性以獲得更高的成本效益，並策略性調整安全性以符合業務提案。與 McAfee ePO 軟體整合，可將安全性解決方案內與各安全性解決方案間的管理和報告功能結合。McAfee Global Threat Intelligence (McAfee GTI) 充分利用 McAfee 解決方案的各項產品組合，從解決方案產品所保護的各種可能的威脅媒介中收集大量情報。相關的資料和情報會在我們的各項產品和解決方案間互相分享。換句話說，McAfee (Intel Security 的一份子) 的電子郵件安全性永遠具有最新、最即時的零時差資訊。McAfee Advanced Threat Defense 可偵測到現今潛藏的零時差惡意軟體，還能與多種產品完美整合，包括 McAfee Email Gateway。McAfee Advanced Threat Defense 可當作多個解決方案之間的共用資源，以符合成本效益的方式在網路中擴充，藉此降低營運成本。

您可以享有企業級的功能，以應付最多、最繁重的工作量，而這一切只需要最少的管理監督和費用。只有 McAfee Email Gateway 能同時兼具功能、效能、穩定性和價值，使得財星 500 大 IT 組織中有半數以上將其視為電子郵件安全性解決方案首選。如需 McAfee Email Gateway 解決方案的詳細資訊，請造訪 **www.mcafee.com/tw/products/email-and-web-security/email-security.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