



# McAfee SaaS Email Protection and Continuity

高生產力企業所需的電子郵件保護、可用性與法規遵循檢查

## 保護電子郵件和電子郵件存取，簡單又方便

McAfee SaaS Email Protection and Continuity 主要的電子郵件保護功能包括：

- 周邊 IP 篩選，可在威脅進入您的網路之前及時阻擋
- 進階的垃圾郵件、灰色郵件及詐騙防護
- 階層式病毒和蠕蟲掃描，可百分之百阻擋所有已知病毒
- 電子郵件攻擊保護
- 傳出郵件和附件的篩選與原則強制執行
- 完全地永不間斷的郵件存取能力
- 群組原則管理
- 訊息稽核訊息追蹤和處置工具
- 選購的 McAfee SaaS Email Encryption

McAfee® Security-as-a-Service (SaaS) Email Protection and Continuity 讓您輕鬆確保電子郵件的安全。除了在垃圾郵件、網路釣魚詐騙、惡意軟體、灰色郵件及不當的電子郵件內容進入網路之前及時阻擋，此雲端型服務還可強制執行傳出郵件原則來避免資料外洩。確保電子郵件存取永不間斷，使得組織隨時都能存取電子郵件。不必購買硬體、不需要安裝軟體、使用自動更新來防止最新的威脅，您可以專心維持公司業務，而不是執行應用程式。

電子郵件是今日企業的生產力重要動力，每天都有數以千計的郵件在一般公司的電子郵件伺服器中流通。管理電子郵件來保護安全與連線已成為一項巨大的工程，必須不斷地從朝向企業目標邁進的策略性工作挪用 IT 資源。

## 低成本且可輕鬆管理的電子郵件防護

可輕鬆部署的 McAfee SaaS Email Protection and Continuity 能避免入埠和出埠電子郵件威脅影響您的網路和使用者，同時讓您在任何情況下都永遠能夠存取電子郵件。此安全軟體即服務永不間斷、隨時更新，且您無須投入額外時間和資源來進行維護。因為這項以 Proxy 為基礎的服務可在垃圾郵件和電子郵件威脅入侵您的網路之前及時阻擋，所以電子郵件伺服器的工作負荷能夠大幅減少，節省寶貴的頻寬與伺服器儲存空間。此外，只需要一通電話，世界級的 McAfee 客戶支援隨時待命，全天無休。

## 簡化 Web 型管理與報告

單一、直覺式 Web 型管理主控台內建最佳作法，讓您輕鬆跨所有網域和地點管理電子郵件原則更新，不但能夠釋出 IT 資源，更能降低整體擁有成本。管理員可以設定和強制執行原則，包括內容篩選和附件內容規則。也能以全域方式將原則套用至使用者群組或個人，以獲得最大的彈性。鉅細靡遺的報告、記錄及隔離則提供最深入的可見性。

## 可靠且強大的基礎架構

SaaS 資料中心的策略包括跨四大洲維護多個資料中心。每一個資料中心皆通過 ISO 27001 認證，且為了提供完整備援能力，皆採用主動-主動備援硬體於所有網路層：防火牆、路由器及負載平衡交換器。每一個資料中心內還有自動化網路與應用程式監控機制，讓遠端操作人員掌握關於可疑行跡或問題的警示與警告，而我們全天無休的安全專家也會密切留意系統。



經濟實惠、方便管理的電子郵件安全保護與永不間斷存取能力

- 無須購買、維護、管理或更新硬體或軟體
- 無須事先投入資金
- 無須安裝或升級費用
- 自動的永不間斷存取能力與同步處理，達到永不間斷的運作
- 簡單的 Web 型管理
- 全天候無休的客戶支援，無須額外收費
- 通過 ISO 27001 認證

電子郵件存取永不間斷，保護企業信譽、營運及生產力

- 偵測到中斷時自動啟用服務
- 透過安全的 Web 介面存取在中斷期間所接收的電子郵件
- 完整的電子郵件功能，包括閱讀、撰寫、回覆、轉寄與刪除
- 中斷恢復後聰明的電子郵件活動同步處理
- 中斷通知和系統更新
- 入埠和出埠郵件篩選

**與 Microsoft Office 365 和 Google Apps for Business 相容**

深入瞭解

如需瞭解所有 SaaS 解決方案（包括 McAfee SaaS Email Protection and Continuity）的省時、高生產力及安全優點，請造訪 [www.mcafee.com/tw/products/security-as-a-service/index.aspx](http://www.mcafee.com/tw/products/security-as-a-service/index.aspx)。

### 強大的電子郵件安全保護

享受優異的垃圾郵件防護

採用專利技術的 Stacked Classification Framework 垃圾郵件偵測系統採取多層分析，以判斷電子郵件（不論語言）是否為垃圾郵件。由於每一項篩選技術各具獨特的設計能夠識別特定的威脅，包括影像型垃圾郵件，結合起來打造出業界最精準與最完整的篩選程序。

McAfee Global Threat Intelligence (McAfee GTI) 郵件信用評價可檢查每一封郵件，偵測已知和新興的郵件型威脅（例如，垃圾郵件），即使郵件的來源可靠也不放過（例如，白名單公司裡的受感染系統）。所得出的分數不僅根據由 McAfee 雲端查詢偵測器以及 McAfee Labs 研究員和自動化工具執行的分析所提供的綜合情報，也根據檔案、Web 及網路威脅資料的各種媒介情報關聯，能夠更有效且準確地阻擋或隔離電子郵件，發揮最高的效能。

灰色郵件篩選技術讓您的收件匣能夠保持簡潔並保有更多可用空間

不想要的郵件可能是大量的合法郵件，而這類郵件是使用者曾經要求取得但現在不再需要的郵件（例如，業界電子報和通知）。管理員可以使用灰色郵件篩選工具，為個人或群組設定灰色郵件原則，甚至准許使用者能夠使用此功能，讓信箱拒收不想要的郵件。

依賴多層式掃描來確實阻擋病毒和蠕蟲

McAfee SaaS Email Protection and Continuity 採用我們專利的 WormTraq 偵測技術。透過採用以 McAfee GTI 技術設計的領先業界、特徵碼型防毒引擎，它也能夠掃描郵件內文和所有附件中的惡意軟體。就像阻擋入埠攻擊一樣重要，出埠電子郵件也會經過篩選，保護用戶端避免受到惡意軟體的威脅。

完整的擴充性可保護您的企業免受大規模電子郵件攻擊

我們完整的解決方案可保護您的網路及重要的郵件閘道避免受到電子郵件攻擊，並能立即阻擋阻絕服務攻擊和其他 SMTP 型攻擊，包括目錄收集攻擊、電子郵件炸彈和通道癱瘓攻擊。

內建的傳輸層安全性（TLS，Transport Layer Security）加密可保護組織間的通訊安全

如果組織對於傳入和傳出電子郵件需要高度安全性，TLS 通訊協定可接受並篩選加密的傳入和傳出郵件、加入 TLS 憑證授權單位驗證，然後透過安全通道來傳送郵件。

在任何情況下，電子郵件永遠不間斷

即便您的電子郵件網路中斷，業務也不致停止。不論網路是因為天災、停電或甚至是定期維修而無法使用，McAfee SaaS Email Protection and Continuity 都能讓員工、客戶、合作夥伴及供應商全天候地繼續通訊。安全易用的 Web 介面可讓使用者在持續受保護的情況下收發郵件、搜尋和取出已存的郵件，以及管理隔離區和郵件存放區。

包含預先建立的規則、先進的內容掃描及文件指紋辨識

您可以使用進階的資料外洩防護（DLP）和法規遵循功能，充分運用領先業界的 McAfee 技術。除了 McAfee SaaS Email Protection and Continuity，有了 McAfee SaaS Email Encryption 可讓您存取預建的內容規則來遵守 PCI DSS、醫療保健、財務資料、區域隱私權法規等，快速建立法規遵循原則。掃描和保護 300 種以上的文件，避免組織的出埠資料外洩。

先進的文件指紋辨識技術能讓您建立及儲存選定文件的數位指紋，使電子郵件安全性措施瞭解該以原則控管的內容。您可以針對電子郵件與附件中完全相符或部分相符的內容，執行精細的原則。也可以使用規則運算式技術來識別關鍵字詞。

### 易於使用的推送/提取加密

McAfee SaaS Email Encryption 能讓您一手掌握敏感資訊的加密作業，即使收件者沒有加密解決方案也不會造成任何困擾。針對商務使用者設計的推送/提取加密技術簡單易用，即使在行動裝置上，也能防止資料遭到竊取。

### 運用 Security Connected 來最佳化保護、管理及法規遵循作業

所有功能結合在一起後的優點包括簡化管理，確保各項安全解決方案緊密結合，使學習曲線縮到最短，並可隨時從單一窗口掌握一切。透過單一主控台即可管理整個 McAfee SaaS 解決方案套件。

### 改變的時刻已來到

瞭解如何減輕維護工作的負擔，使分身乏術的 IT 員工能專注於更具有策略性的專案。請至 [www.mcafeesaas.com](http://www.mcafeesaas.com) 深入瞭解並註冊免費試用。

