

McAfee Security for Email Servers

為 Microsoft Exchange 提供強大的內容安全性

McAfee® Security for Email Servers 可偵測並篩選病毒、蠕蟲、特洛伊木馬程式及其他可能不需要的程式。除了可相容於 Microsoft Exchange，還可封鎖垃圾郵件並篩選訊息，避免不當內容或機密資訊進出網路，協助您滿足原則與符合性需求。

在 McAfee 推出的眾多產品當中，McAfee Security for Email Servers 能夠為傳入與傳出電子郵件提供多層防護，無論是按指定掃描惡意軟體，或是避免機密資料遺失或濫用的原則強制執行等，全都一應俱全。

- **領先業界的防護** — 使用我們屢獲殊榮的記憶體內和按指定增量掃描功能，來移除病毒、蠕蟲、特洛伊木馬程式及其他來自傳入和傳出電子郵件的威脅。
- **進階威脅偵測** — 透過 McAfee Threat Intelligence Exchange 緊密整合 McAfee Advanced Threat Defense，提供深層分析功能，並識別電子郵件附件內潛在的零時差威脅。
- **強大的內部防護** — 偵測可能會繞過周全防禦機制，或透過受感染筆記型電腦或內部電子郵件進入網路的威脅；還會利用防垃圾郵件模組封鎖垃圾郵件。

- **功能強大的內容篩選** — 篩選禁止的檔案類型和不當內容，並杜絕機密資料洩漏，藉此強制執行公司的電子郵件使用原則。
- **單一主控台管理** — 使用 McAfee ePolicy Orchestrator® (McAfee ePO™) 平台部署、管理安全性及顯示詳細的圖表報告。

多層電子郵件防護

全方位惡意軟體防護

McAfee Security for Email Servers 憑藉即時檔案信用評價防惡意軟體功能，大幅降低暴露在新型威脅下的風險。透過雲端型 Global Threat Intelligence (GTI)，若有任何可疑檔案，我們會將該檔案的特徵傳送至 McAfee Labs 以即時分析信用評價。若特徵經辨識後確定為惡意軟體，幾毫秒內您

McAfee 結合內容檢查、信用評價分析以及惡意軟體保護等功能，可維護電子郵件安全。我們提供多層式電子郵件安全性防禦和部署選項，包括網路周邊的邊緣傳輸、中央傳輸伺服器以及郵箱伺服器。

與我們聯絡



資料工作表

就會接收到適當的回應，並封鎖或隔離該檔案。若檔案經辨識後仍舊可疑，系統會自動將其傳送至 McAfee Advanced Threat Defense 進行深入的沙箱分析。透過 McAfee Threat Intelligence Exchange 進行整合，啟用 McAfee Security for Email Servers 及共生系統內所有連接的解決方案，以便採取動作處理惡意附件，增強防護能力。

郵件信用評價

McAfee GTI 訊息信用評價是我們的一項全方位即時雲端型訊息與寄件者信用評價服務，利用我們的產品為客戶提供防護，避免遭到已知威脅及垃圾郵件等新型訊息型威脅。訊息信用評價結合了垃圾郵件傳送模式及 IP 行為等因素，判斷有問題的訊息是惡意訊息的可能性。評分不僅依據由偵測器查詢 McAfee 雲端以及 McAfee Labs 執行分析等所提供的共同情報，還有來自 Web、電子郵件及網路威脅資料等多方位情報的交互關聯。

IP 信用評價

根據傳送伺服器的 IP 位址偵測電子郵件訊息的威脅。IP 信用評價可封鎖閘道上電子郵件訊息，避免造成損害和資料遭竊。

URL 信用評價

以電子郵件內嵌 URL 的信用評價為基礎，防範已知及新興的 Web 型威脅。

全天候保護您的伺服器

檢查傳入與傳出的電子郵件是否有病毒、蠕蟲、特洛伊木馬程式及其他惡意軟體。此外，您也可以掃描所有內部電子郵件，封鎖從內部傳播的蠕蟲。McAfee Security for Email Servers 可透過 HTTP、FTP、網路檔案共用或 McAfee ePO 集中管理主控台自動下載最新的病毒定義 (DAT 檔案)。

強制執行符合性

根據大小、訊息內容或附件內容來篩選訊息。封鎖或隔離主旨行、訊息本文或附件中包含控制內容的訊息。

節省時間和資源

預先建立的內容篩選器可簡化原則的建立和強制執行流程。建立一個全域式的規則，但能根據個人或部門的需要設定例外狀況。透過內建的 HTML 介面或 McAfee ePO 平台管理。

內容篩選

掃描主旨行的內容和文字或電子郵件訊息本文，以及電子郵件附件。根據規則運算式 (Regex) 建立專屬的內容篩選規則。

資料外洩防護和符合性

資料外洩防護 (DLP) 可確保已傳送 (傳輸中) 或儲存中的電子郵件合乎組織的機密性和符合性。針對企業和特定國家/地區符合性規則預先建立一組字典，以便提供快速設定。內建的工作流程會自動將遭隔離的電子郵件轉送給稽核人員進行檢閱。

主要優點

- **保持系統運作不中斷：** 避免病毒、蠕蟲和進階威脅透過電子郵件入侵，或透過 Microsoft Exchange 從內部傳播。
- **維持員工生產力：** 封鎖垃圾郵件和網路釣魚攻擊。
- **單一主控台管理：** McAfee ePO 軟體提供功能強大的單一管理主控台來控制、管理及檢視報告。
- **保護重要資料：** 利用 DLP 和信用評價技術 (IP、訊息、URL 及檔案信用評價) 篩選傳入和傳出電子郵件，藉此維護資訊安全性並降低企業的法律風險。
- **直覺化的圖形式使用者介面：** 此介面簡單好用，而且提供各式各樣的報告、圖表與即時電子郵件流量統計資料。

篩選垃圾電子郵件並提升產能

利用防垃圾郵件模組攔截垃圾郵件和網路釣魚電子郵件，藉此維持員工生產力，並減少浪費電子郵件伺服器儲存空間。使用者可以建立自己的白名單或黑名單。與我們的閘道電子郵件解決方案共用的單一隔離解決方案，可讓使用者輕鬆存取單一隔離區。

產品健康狀態警示

McAfee Security for Email Servers 會傳送有關產品狀態的通知給指定的管理員，同時監控掃描各檔案時所使用的時間。為避免發生問題，McAfee Security for Email Servers 也會採取修正動作，避免對 Exchange 伺服器效能造成不利影響。

規格

隨著電子郵件和電子郵件伺服器共用資料呈指數級增長，McAfee Security for Email Servers 支援 Microsoft Exchange 環境，讓員工保有生產力，組織也能全天候保持營運不中斷。

McAfee Security for Microsoft Exchange 的需求

作業系統需求

- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

Microsoft Exchange 伺服器需求

- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2013
- 支援含叢集的 Microsoft Exchange 伺服器

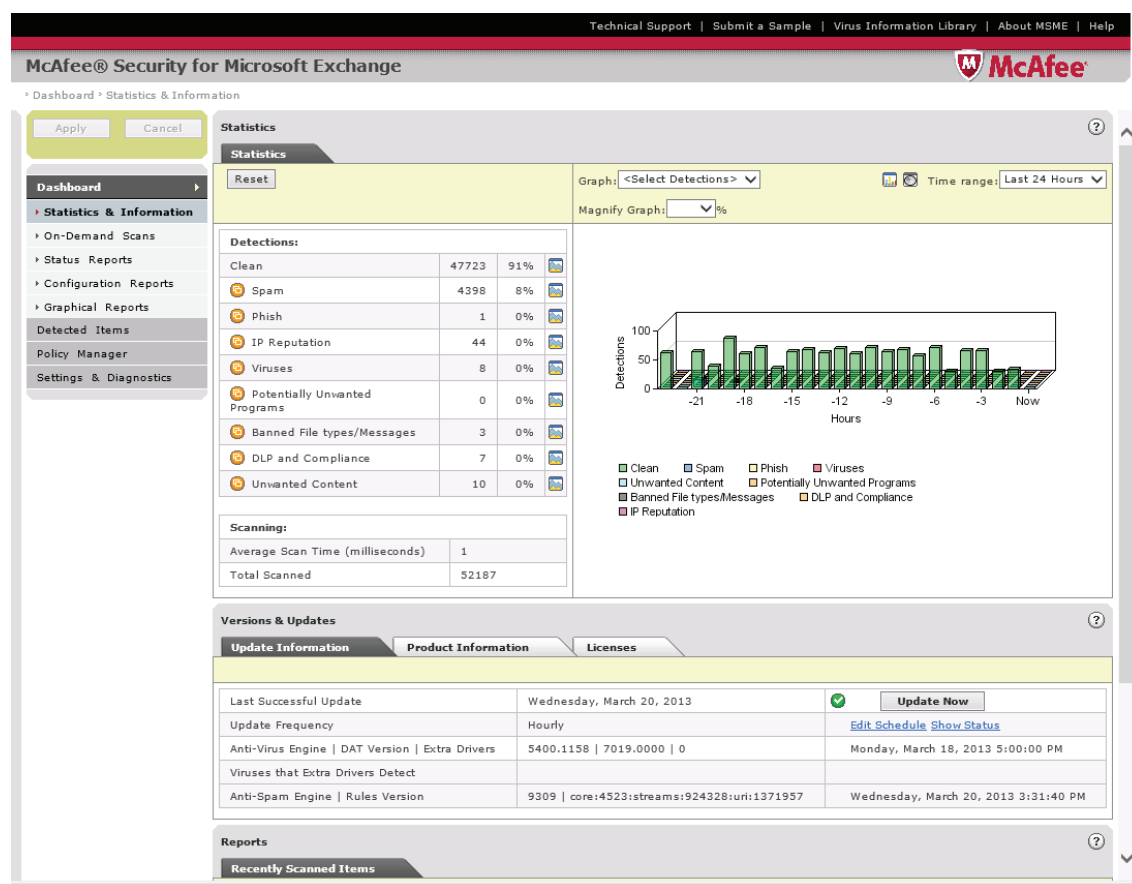


圖 1. 此介面簡單好用，而且提供各式各樣的報告、圖表以及即時電子郵件流量統計資料。

更新輕鬆方便

自動更新功能可讓您隨時掌握全球頂尖威脅研究中心 McAfee Labs 提供的最新安全性情報。

集中與合併電子郵件隔離區

隨附在解決方案中的 McAfee Quarantine Manager 將隔離區和防垃圾郵件管理功能合併成單一解決方案。McAfee Quarantine Manager 管理容易，不但能夠將樣本提交給 McAfee Labs，還可提供精細的管理控制、自動從 LDAP 伺服器進行使用者同步、管理使用者或全域黑名單/白名單以及詳細報告等，全都可透過 McAfee ePO 平台進行管理。

掃描和保護電子郵件儲存

McAfee Security for Email Servers 的詳細設定選項可支援排程按指定掃描，比起傳統的完整掃描方式，更能迅速完成掃描。其中一個選項可以只掃描含附件的電子郵件、未讀取電子郵件、主旨、寄件者、收件者、副本、訊息 ID 以及在特定時間收到和特定大小的郵件。

如需詳細資訊，請造訪 [McAfee Security for Email Servers](#)。



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

McAfee 和 McAfee 標誌、ePolicy Orchestrator 與 McAfee ePO 是 McAfee, LLC 或其附設公司在美國及其他國家地區的商標或註冊商標。其他標誌與品牌可能為其各自擁有者的財產。Copyright © 2020 McAfee, LLC. 4446_0420
2020 年 4 月