# McAfee Email Protection

## 隨時隨地為信箱提供進階防護

如今的企業比以往更需要進階電子郵件保護。根據 SANS Institute 的研究顯示，95% 的網路攻擊是魚叉式網路釣魚 (Spear Phishing) 成功所直接造成的結果。[1] 使用者一直迷信著社交工程技術，而網路罪犯則擴展其技能，以便納入其他巧妙的手法，儘管組織擁有安全意識仍會措手不及。惡意軟體日益精良，以及公司的智慧財產遺失，是越來越嚴重的問題，對所有組織都可能造成極大的負面影響。企業也開始將電子郵件遷移至寄存信箱，此舉則招致了更大的風險。最後，舊版的電子郵件保護解決方案缺乏彈性，迫使公司得尋求更好的替代方案。McAfee® Email Protection 是解決之道。這個強大的解決方案可針對鎖定式網路釣魚威脅提供企業級保護，並且整合資料外洩防護 (DLP) 技術及電子郵件不間斷功能，使得解決方案臻至完備。透過彈性的部署選項 (如雲端型、內部部署或整合型混合解決方案)，您隨時可以按照想要的方式來建置電子郵件安全性。

### 主要優點

**抵禦鎖定式網路釣魚攻擊**

- 以 ClickProtect 即時偵測惡意 URL 威脅。
- 整合McAfee Advanced Threat Defense 以抵禦潛藏的惡意軟體。
- 內建資料遺失防護技術。

**適用於寄存信箱的安全性**

- 無論電子郵件在哪裡，都能抵禦鎖定式攻擊。
- 灰色郵件的使用者控制選項。
- 電子郵件不間斷。
- 細微的資料遺失防護及加密功能。

**彈性的部署選項**

- 可隨時依照個人需求進行部署。
- 單一管理及報告主控台可提供混合部署選項。

### 超越社交工程的範疇：全新的魚叉式網路釣魚手法

在網路釣魚攻擊方面，使用者是最弱的環節。*Verizon 發布的《2014 年度資料外洩調查報告》(Verizon Data Breach Investigation Report, 2014)*[2] 指出，將近五分之一的使用者會按下網路釣魚電子郵件內的連結。網路罪犯不僅持續利用使用者在社交工程技術上的漏洞，他們進一步發展出其他複雜手法，讓使用者難以追蹤電子郵件威脅。請參考以下範例：

- **單次 URL：**在使用者淪為網路釣魚詐騙的受害者，並發生感染後，網路罪犯便撤下惡意 URL。即便使用者能夠完成偵測及鑑識作業，過程也是相當困難。
- **延遲感染：**在某些情況下，攻擊者會等到電子郵件經過掃描、核准並傳送到公司收件匣*之後*，才會將承載植入目標網站。員工通常會信任其收到的工作電子郵件，結果便按下了惡意連結。
- **沙箱感知惡意軟體：**這類惡意程式碼會維持潛伏狀態以迴避偵測，以便於之後大肆破壞。

### 進階階層式防禦

**隨按即保護**

McAfee Email Protection 提供多層保護，協助您防止複雜的魚叉式網路釣魚攻擊，以及潛藏的相關惡意軟體。McAfee Email Protection 利用在McAfee Web Gateway 上評選第一的McAfee Gateway Anti-Malware Engine[3]，包括URL隨掃描即保護，以及URL隨按即保護(合稱為ClickProtect)，可在任何地方並從任何裝置運作，能有效阻擋魚叉式網路釣魚的嘗試攻擊。ClickProtect 可偵測並消弭電子郵件訊息中內嵌 URL 的威脅。在掃描訊息期間，以及使用者按下 URL 時，ClickProtect 會檢查 URL 意圖的變更 (無論變更看似多麼無害)。

intel Security

讓我們看看延遲惡意軟體的範例：攻擊者精心製作了一封電子郵件，並附上看似無害的 URL，用意是鎖定您組織內的財務主管。您的電子郵件安全性解決方案收到電子郵件，在進行查閱後，發現該郵件是安全的，並將其傳送到目標收件匣。但是該電子郵件目前在財務主管的收件匣內，而攻擊者在目的地網頁上植入了惡意軟體。如果主管按下連結，您的網路就會遭受感染。

透過 ClickProtect，按下電子郵件內的 URL 時就會詢問：「這個 URL 仍然安全嗎？」McAfee Gateway Anti-Malware Engine 會重寫並檢查所有傳送的 URL，並使用行為模擬來偵測惡意網頁內容，不需仰賴特徵碼。

安全預覽功能可讓使用者安全地檢視惡意網站並瞭解最佳作法，讓安全性更上一層樓，並且降低整體風險。您可以安全地轉寄訊息，即使收件人沒有 ClickProtect，ClickProtect 也會如影隨形地保護電子郵件。

**潛藏惡意軟體偵測及封鎖**

由於整合了 McAfee Advanced Threat Defense，McAfee Email Protection 能夠在可疑的檔案附件進入收件匣前，就偵測並封鎖潛藏其中的零時差惡意軟體。創新的分層方法結合了深層靜態程式碼 (反向工程) 與動態分析 (沙箱作業)，可分析惡意軟體的實際行為。全靜態程式碼分析提供詳盡的惡意軟體分類資訊，同時針對高度偽裝、規避性威脅提供更完善的防護；還可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，通常不會在動態沙箱的環境中執行，但可以透過解壓縮與全靜態程式碼分析偵測到。

**內建資料遺失防護**

鎖定型魚叉式網路釣魚攻擊最終的核心目標是：侵佔珍貴及敏感資料。將 DLP 解決方案中領先業界的技術整合至 McAfee Email Protection。包括內建的內容字典，適用於 PCI DSS、醫療照護、財務資訊、當地隱私權規範等，可協助您開發符合性原則，以便在識別、儲存及傳輸敏感資料時遵循。

透過建立和儲存所選文件的數位指紋，McAfee Email Protection 可以瞭解哪一種內容需要交由原則控制和保護。規則運算式工具、可自訂的字典、閾值計數器、深層內容掃描 (超過 300 種文件類型)，以及白名單，可讓您建立和強制執行附件和內容原則 (適用於組織內不同的使用者群組)。

McAfee Email Protection 可為虛擬裝置、硬體裝置或刀鋒伺服器等部署方式免費提供本機推送、提取或 TLS、S/MIME、PGP 電子郵件加密。

**電子郵件不間斷功能，保持業務持續運作**

生意不會因為電子郵件網路發生服務中斷而停止上門。不論網路是因為天災、停電或甚至是定期維護而無法使用，McAfee Email Protection 提供的選項可讓員工、客戶、合作夥伴及供應商全年無休保持聯繫。電子郵件不間斷功能會保留中斷運作期間所傳送或接收的全部郵件，而直到您的電子郵件伺服器恢復運作時，更能聰明地同步處理中斷期間所有郵件活動的正確記錄。

**情報和威脅信用評價**

McAfee Email Protection 的寶庫中還有另一項強大工具—McAfee Global Threat Intelligence (McAfee GTI)，這是業界最全面的威脅情報服務，可從檔案、網路、電子郵件及網路媒介上的1億多個偵測器中，收集並重新分配即時資料。McAfeeGTI 的信用評價分析可封鎖來源可疑、包含可疑網站導向連結，以及具有已知惡意檔案附件的電子郵件，將風險降至最低。

## McAfee Email Gateway

**虛擬裝置環境及系統需求**

- VMware vSphere 4.x 或更高版本
- VMware vSphere Hypervisor (ESXi) 4.x 或更高版本
- 處理器：兩個虛擬處理器
- 可用的虛擬記憶體：2 GB
- 可用硬碟空間：80 GB

**硬體裝置**

- 提供兩種型號，單獨銷售
- 在刀鋒伺服器機型上也可使用


McAfee Email Protection 已連續三年榮獲 **SC Magazine 的五星評等。**

藉由大幅降低惡意軟體、網路釣魚攻擊及進階持續威脅攻擊滲入網路的機率，您的組織更可保持安全，同時也較不需要昂貴的補救措施。

### 寄存電子郵件的安全性挑戰

由寄存電子郵件服務所佈建的企業電子郵件地址越來越多，例如 Microsoft Office 365、Google Apps for Work 等。許多寄存電子郵件解決方案在其服務中提供安全性。但是這樣就夠了嗎？或許並非如此，當網路釣魚嘗試攻擊、垃圾及灰色郵件一再接踵而來，內建安全性功能並不具有防止資料外洩的能力。此外，舉例來說，與Office365相關聯的郵件中斷會影響生產力。McAfee Email Protection 可在測試、遷移及遷移後的期間，提供企業級保護來防護鎖定式網路釣魚攻擊及進階惡意軟體。無論您何時何地部署信箱，McAfee Email Protection 都可提供全面保護，讓電子郵件服務不受間斷。

### 適用於目前及未來的彈性部署選項

McAfee Email Protection 可讓您靈活地依照個人方式部署電子郵件安全措施。選擇雲端型軟體即服務 (SaaS) 解決方案、內部部署解決方案 (虛擬裝置、硬體裝置或刀鋒伺服器)，或混合使用兩種解決方案。透過 McAfee Email Protection，您可以依照最能符合目前需求的方式來部署電子郵件安全措施，讓您能夠在日後垂直擴充或變更方針。

不論您選擇何種部署選項，McAfee Email Protection 都能為您提供單一集中式的管理主控台，可統一進行報告，讓您輕鬆地評估電子郵件安全性方案的效能。這些原則適用於解決方案的雲端型及內部部署元件。

如需有關 McAfee Email Protection 的資訊或是想要開始評估，請連絡您的 McAfee 代表或造訪 http://www.mcafee.com/tw/products/email-and-web-security/email-security.aspx。


1. **http://blogs.mcafee.com/business/security-connected/is-there-something-phishy-in-your-inbox**
2. **https://dti.delaware.gov/pdfs/rp_Verizon-DBIR-2014_en_xg.pdf**
3. AV-TEST：*McAfee Web Gateway Security Appliance Test (裝置測試)*

**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