McAfee DLP Prevent

強制執行原則以保護您的敏感資訊

主要優點

運用現有基礎架構

- 使用 SMTP 搭配 X-Header 與 MTA 閘道整合，藉由封鎖、退回、加密、隔離及重新導向來保護企業電子郵件
- 藉由與符合 ICAP 的 Web Proxy 進行整合來封鎖透過 HTTP、HTTPS、IM、FTP 或網頁郵件服務傳送的內容違規，提供流量強制措施

主動針對所有類型的資訊強制執行原則

- 保護超過 300 種獨特的內容類型
- 針對已知的敏感資訊與未知的潛在敏感資訊強制執行原則
- 能予以擴充以支援數十萬個同時連線

分類、分析及解決資料漏洞

- 篩選及控制敏感資訊以抵禦已知與未知風險
- 針對所有類型的內容編制索引及強制執行精細的安全性原則
- 套用與內部檔案共用存取權限相關的原則，預防使用者以未經授權的方法存取資訊或存放庫

有越來越多的人以電子化的方式分享資料，因此意外或蓄意將敏感資料傳送給未經授權之對象的機會也隨著增加，導致機密的企業資料暴露在風險中。不論是電子郵件、Web、即時傳訊 (IM) 或 FTP，資訊能經由許多不同的電子管道離開公司。這對企業安全與法規遵循人員造成巨大無比的挑戰。儘管某些訊息或交易是可允許的，但仍應透過加密來維護資料隱私。其他類型的訊息或訊息收件者則是絕對不允許的，因此這些傳輸必須加以封鎖。在正確的時間強制執行適當的原則是確保資料安全性、法規遵循及智慧財產保護的重要一環。

針對傳輸中的資料強制執行安全性原則

不論在公司的哪個部門，使用者經常會使用多種應用程式與各種通訊協定來共用資料。爲了預防意外或蓄意的資料外洩，公司除了必須主動防範敏感資訊離開網路之外，還必須強制執行正確的業務程序。

McAfee Data Loss Prevention (DLP) Prevent 能藉由使用 Simple Mail Transfer Protocol (SMTP) 或符合 ICAP 的 Web Proxy 與郵件傳輸代理程式 (MTA) 閘道整合，以針對透過電子郵件、網頁郵件服務、即時傳訊、Wiki、部落格、入口網站、HTTP/HTTPS 及 FTP 傳輸離開網路的資訊強制執行原則。在發現原則違規的情事時，McAfee DLP Prevent 能讓您採取多種動作 (包括套用加密、封鎖、重新導向、隔離等動作)，因此您可以確保以符合法規的措施來管理敏感資訊的隱私，降低安全性威脅的風險。

與 Web Proxy 及 MTA 進行整合以獲得更完善的保護

McAfee DLP Prevent 能藉由與 Web Proxy (使用 ICAP) 及 MTA 進行整合 (使用 X-Header) 來採取所需的動作。McAfee DLP Prevent 能在應用程式層終止未經授權的交易 (不僅只是將未修改應用程式行爲的 TCP 工作階段丟棄)，因此它能警告啓動作業的應用程式由於傳輸違反原則，因此遭到拒絕。由於 McAfee DLP Prevent 能得知何爲應受保護的資料並阻止應用程式再次嘗試執行相同的行爲，因此能爲組織帶來更完善的資料保護。

保護已知與未知的敏感資訊

憑藉著能分類超過 300 種不同內容類型的能力，McAfee DLP Prevent 可協助您維護已知資訊 (如身分證號碼、信用卡號碼及財務資料) 的安全性，以及學習有哪些潛在的資訊或文件 (如非常複雜的智慧財產) 需要保護。McAfee DLP Prevent 含有多種範圍涵蓋法規遵循與智慧財產之合理使用方法的預建原則，因此您可以根據一組全面的規則集來比對文件的完整與部分內容，進而保護所有已知與未知的敏感資訊。

自訂檢視與事件報告

McAfee ePolicy Orchestrator® (McAfee ePO™) 管理主控台能讓您依據任兩個內容相關樞紐點來自訂安全性事件與後續行動的摘要檢視。您只需點擊滑鼠即可使用清單與詳細資料檢視，以及能指出趨勢的摘要檢視。McAfee DLP Prevent 亦含有大量的預建報告，您可以檢視報告、儲存報告以供日後使用，或排定報告的時程以便定期產生報告。

規格

擷取與索引功能

- 為 McAfee DLP 4400 裝置中高達 80 TB 的資訊與 5000 萬份文件編列索引

系統輸送量

- 高達 150 Mbps 的完整內容分析、索引及儲存輸送量

網路整合

- 能整合到網路中作為使用 MTA 與符合 ICAP 之 Web Proxy 且於資料路徑中作用之路徑外裝置

內容類型

支援超過 300 種內容類型的檔案分類，包括：

- Microsoft Office 文件
- 多媒體檔案
- P2P
- 來源碼
- 設計檔案
- 封存檔
- 加密檔案

支援的通訊協定

支援透過 ICAP 通訊協定通往符合 ICAP 之 Proxy 的 HTTP、HTTPS、FTP 和即時傳訊通訊協定。如需取得 Proxy 支援的通訊協定，請洽詢 Proxy 廠商。透過與 MTA 的整合支援 SMTP。

內建原則

提供多種適用於共同需求的內建原則與規則，包括法規遵循、智慧財產及合理使用方法等。您可以運用 McAfee 擷取資料庫來進行徹底的規則自訂化，以滿足業務的特定需求。

複雜資料分類

McAfee DLP Prevent 能讓您的組織保護所有類型的敏感資料，不論是常見的固定格式資料，或是複雜且型態不一的智慧財產。藉由合併這些物件分類機制，McAfee DLP Prevent 能運用精準度高且詳細的分類引擎，並透過引擎來封鎖敏感資訊及識別隱藏或未知風險。物件分類機制包括：

- *多層式分類* - 涵蓋內容相關資訊與階層格式中的內容
- *文件註冊* - 包括資訊變更時的生物識別特徵碼
- *文法分析* - 偵測文字文件、試算表或來源碼等所有內容中的文法或語法
- *統計分析* - 追蹤特定文件或檔案中出現與特徵碼、文法或生物識別相符之項目的次數
- *檔案分類* - 跨越檔案或壓縮檔的副檔名限制，識別內容的類型

規格：McAfee DLP 4400 裝置

元件	說明
主機板	Intel Timber Creek System (S5520URR)
CPU	2 個 Intel X5660 12 M 快取，2.8 GHz (6 核心)
記憶體	24 GB P1333 DDR3 記憶體
RAID 控制器	Intel RS2MB044 RAID 控制器
電源供應器	2 個 760 W 熱交換電源供應器模組
硬碟機	12 個 Seagate Constellation ES 1T 7,200 rpm 3 1/2" SATA 磁碟機
NIC 卡	Intel Dual Copper 1 Gbps Ethernet I/O Module
DVD 光碟機	SATA DVD-ROM
IPMI	Intel Remote Management Module 3 (AXXRMM3)
產品大小	2 機架單位 (2U)

規格：虛擬機器

McAfee DLP Prevent 可做爲於 VMware ESX 或 VMware ESXi 4.1 伺服器中運作的虛擬裝置。以下是執行虛擬裝置的硬體需求下限。

元件	需求
CPU	Intel 四核心
記憶體	8 GB RAM
硬碟	磁碟機 1：至少 128 GB (供 VM 軟體使用) 磁碟機 2：至少 640 GB (供 DLP 虛擬映像使用)
網路連接埠	1 個適用於 McAfee DLP Prevent 應用程式的連接埠
BIOS	啓用 VT 執行緒

McAfee
An Intel Company

邁克菲台北辦公室
台北市 104 南京東路三段132 號 4 樓 A2
886-2-2721-7766
www.mcafee.com/tw

39802ds_dlp_prevent_1111