資料表

McAfee DLP Prevent

強制執行原則以保護您的敏感資訊

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，資訊都能經由許多不同的管道離開公司。儘管某些訊息或交易是可允許的，但仍需透過加密來維護資料隱私。無論何時均不接受其他的通訊類型，而且必須加以封鎖。在正確的時間強制執行適當的原則，是確保資料安全性、法規符合性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。主動防範敏感資訊離開網路，以預防意外或蓄意的資料外洩，並強制執行正確的業務程序。

McAfee® DLP Prevent 能藉由使用簡易郵件傳送通訊協定 (SMTP) 或符合 ICAP 的 Web Proxy 與郵件傳輸代理程式閘道整合，協助您針對透過電子郵件、網頁郵件服務、IM、Wiki、部落格、入口網站、HTTP/HTTPS 及 FTP 傳輸而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。

透過 McAfee ePolicy Orchestrator 軟體達到完全統合

透過通用的原則管理、事件管理和案例管理，讓 McAfee DLP Prevent 與 McAfee® ePolicy Orchestrator® (McAfee ePO™) 軟體可和 McAfee® Data Loss Prevention Endpoint (McAfee DLP Endpoint) 達到完全統合。管理員可以在 McAfee ePO 軟體建立單一電子郵件與 Web 防護原則，並將其部署到端點和網路。此外，McAfee DLP Endpoint 與 McAfee DLP Prevent 共用通用分類引擎，因此適用單一的電子郵件與 Web 原則。通用字典和規則運算式

主要優點

運用現有基礎架構

- 使用 SMTP 搭配 X 標頭與郵件傳輸代理程式 (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。
- 藉由與符合網際網路內容調適通訊協定 (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，提供流量強制管制措施。

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資訊強制執行原則。
- 能予以擴充以支援數十萬個同時連線。

與我們聯絡

(Regex) 語法為建立通用 Web 和電子郵件保護規則提供連貫性。McAfee DLP 解決方案採用集中式管理，提供透過單一窗口掌握可見性，有助於提升營運效率，並減少管理的經常性開支。

監控行動電子郵件

適用於行動電子郵件的 McAfee® DLP Prevent 能透過 ActiveSync Proxy 搭配 DLP 功能，攔截下載至行動裝置的電子郵件，為行動電子郵件提供內容方面的保護。此外，此套件能夠在內部部署的 Microsoft Exchange 以及 Microsoft Office 365 Hosted Exchange 上攔截 ActiveSync。此套件可由 McAfee ePO 軟體全面管理，而且包含在 McAfee DLP Prevent 授權當中，不需要在行動裝置上安裝任何代理程式。有了適用於行動電子郵件的 McAfee DLP Prevent，企業可以監控電子郵件的符合性和收集證據，並能一併保護受管理和未受管理的行動裝置。

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 標頭) 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為的 TCP 工作階段丟棄)，因此它能警告啟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 能得知何為應受保護的資料並阻止應用程式嘗試執行相同的行為，因此能為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 不但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，還能幫您瞭解有哪些資訊或文件 (如非常複雜的智慧財產) 需要保護。McAfee DLP Prevent 含有一系列廣泛的預建原則，從法規符合性到智慧財產的合理使用方法都涵蓋在內，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。

可自訂檢視方式與事件報告

McAfee ePO 軟體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切換為清單與詳細資料檢視，以及附有趨勢走向的摘要檢視。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。

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。

規格

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的路徑外裝置。

內容類型

支援超過 300 種內容類型的檔案分類：

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

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**：包括資訊變更時的識別特徵碼。
- **文法分析**：偵測文字文件、試算表或原始程式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與特徵碼、文法或生物識別特徵相符項目的出現次數。
- **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。

鑑識與規則調整功能

獨家擷取技術可讓您利用自有的歷程資料，以更快、更有效率的方式部署，無需盲目猜測及花時間反覆試驗，也不必承受業務中斷的風險。您可根據瞬息萬變的業務需求，輕鬆地精準微調 DLP 規則 (包括分類調整)。擷取技術亦有助於鑑識調查，可作為數位錄影機使用，並重播事後 DLP 事件，徹底深入調查。擷取技術可用於虛擬環境，亦可透過 SAS 纜線連接至 NDLP 6600 設備，作為 2U 16TB 儲存陣列。

機型與裝置選項

McAfee DLP Prevent 以硬體或虛擬裝置的形式提供。如需詳細資料，請參閱 **McAfee DLP 6600 硬體裝置資料工作表**。

支援的通訊協定

支援透過 ICAP 通訊協定通往符合 ICAP 規範之 Proxy 的 HTTP、HTTPS、FTP 和 IM 通訊協定。如需瞭解 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，包括法規符合性、智慧財產及合理使用方法等。
- 您可以運用 McAfee 擷取資料庫來完成徹底的規則自訂化，以滿足業務的特定需求。

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