

# McAfee DLP Endpoint

別成為下一家因資料遺失而登上媒體頭版的企業

## 主要優點

- **無與倫比的保護**—避免資料在必經之處遺失：辦公室、家中或行動中
- **全方位的裝置管理**—針對任何卸除式存放裝置中的機密資料指定詳細的內容型篩選、監控及封鎖功能
- **多層次保護**—跨越作業系統與裝置類型的限制，確保所有端點中的資料受到保護
- **McAfee ePO 集中式管理**—運用 McAfee 安全性風險管理架構來預防資料遺失
- **完整的可見性**—向稽核人員、資深管理人員及其他股東證明公司履行內部與法規遵循措施

您的資料是否在神不知鬼不覺當中遺失？也許您的客戶資訊、智慧財產、財務資料及個人檔案正悄悄流出公司邊界。而犯罪者不僅只是駭客，您自己的員工也參與其中。意外與惡意的資料遺失能經由電子郵件、網頁貼文、USB 磁碟機與列印等常見的管道發生，並造成數百萬元的損失。

## 及早預防資料遺失

每天都有規模與您公司相仿的公司由於惡意與意外的資訊外洩而成為大規模資料遺失的受害者。近期的研究結果指出，財星前 1000 大公司中有 75% 的公司曾經由於意外或惡意的資料外洩而蒙受損失。最近發表的研究結果指出，每週都有超過 55% 的員工使用可攜式裝置將機密資料攜出工作場所。<sup>1</sup> 由資料外洩與修補而導致的公司成本花費是相當驚人的。2008 年內所花費的平均成本為 665 萬元美金。<sup>2</sup>

如果能以簡單的方式有效遏止資料遺失，該有多好。如果可以同時管理業界與政府規範的法規遵循，該有多好。只要利用提供監控、稽核及控制使用者操作敏感資料之行為的解決方案，您就可以實現願望。

## 保護及遵循

利用 McAfee® DLP Endpoint 來取得完整的可見性，以及控制重要資料的傳輸。藉由即時監控來避免機密資料於辦公室、家中及行動中遺失。McAfee DLP Endpoint 能協助組織預防財務損失、商譽損害、客戶流失、競爭劣勢及違反法規等風險。

有了 McAfee DLP Endpoint 之後，您可以在不影響日常業務活動的情況下快速而輕易地監控即時發生的事件、套用集中管理的安全性原則以規範及限制員工對敏感資料的使用與傳輸方式，以及產生詳細的鑑識報告。協助企業預防如電子郵件、即時傳訊、CD 燒錄、網頁貼文、USB 複製及列印等源自內部的資料遺失威脅。您也可以遏止由特洛伊木馬程式、蠕蟲病毒，以及暗地劫持員工認證之檔案共用應用程式所引起的機密資料遺失。

## 保護不代表中斷

在不干擾合法業務活動的情況下預防資料遺失與外洩，即便是在修改、複製、貼上、壓縮或加密資料時亦是如此。保護超過 390 種資料檔案中的內容。獨特的指紋演算法與內容標記選項（依據位置、應用程式、檔案類型、規則運算式、關鍵字等）提供廣泛而深入的資料保護，確保公司資訊安全。

## 簡化的法規遵循管理

McAfee ePolicy Orchestrator® (McAfee ePO™) 軟體實現的簡易管理功能可提供事件監控與事件詳細資料，向稽核人員、董事會成員及其他股東證明公司履行內部與法規遵循措施。McAfee DLP Endpoint 與 McAfee ePO 軟體的整合能讓您輕易地收集如寄件者、收件者、時間戳記與資料證據等重要的使用資料。只要按一下按鈕，McAfee ePO 軟體便能提供事件監控與詳細的報告，以供您向稽核人員、資深管理人員及其他股東證明公司履行內部與法規遵循措施。

## 效益：無與倫比的資料保護

深入掌控離開端點的資料，使您能在資料遺失及負面新聞爆發前及早預防。

McAfee DLP Endpoint 是全方位資料保護解決方案的一部分。McAfee Total Protection™ for Data 結合了 McAfee DLP Endpoint 與 McAfee Endpoint Encryption，提供更全面的資料保護解決方案。

## 系統需求

### McAfee ePO 伺服器作業系統

- Microsoft Server 2003 SP1、2003 R2

### 桌上型電腦與筆記型電腦端點作業系統

- Microsoft Windows XP
- Professional SP1 或更新版本
- Microsoft Windows 2000 SP4 或更新版本

## 硬體需求

- CPU：Pentium III 1 GHz 或速度更快的處理器
- RAM：建議 512 MB
- 磁碟空間：至少 200 MB
- 網路連線：供遠端存取的 TCP/IP

## 功能

### 無與倫比的保護

- 控制使用者在網路、應用程式及存放裝置間傳送、存取及列印敏感資料的方式。保護電子郵件、網頁郵件、點對點應用程式、即時傳訊、Skype、HTTP、HTTPS、FTP、Wi-Fi、USB、CD、DVD、印表機、傳真機與卸除式存放裝置。
- McAfee DLP Endpoint 強制選項包括：
  - 監控—允許資料傳輸
  - 預防—封鎖資料傳輸
  - 警示—通知管理員與一般使用者
  - 加密—在資料傳輸前確保加密<sup>3</sup>
  - 隔離—等候授權<sup>3</sup>

### 全方位的裝置管理

- 控制及封鎖複製到 USB 裝置、快閃磁碟機、iPod 及其他卸除式存放裝置中的機密資料。
- 使用任一 Windows 裝置參數指定及分類可供使用的裝置，參數包括產品 ID、廠商 ID、序號、裝置類別、裝置名稱等

### 適用於端點的多層式保護機制

- 主機型保護能藉由監控及禁止使用者在操作敏感資料時的危險行為來遏止資料遺失
- 在結合 McAfee Endpoint Encryption 之後，McAfee DLP Endpoint 能提供全方位、分層式的資料遺失預防方法

### McAfee ePO 集中式管理

- 透過 McAfee ePO 管理主控台存取 McAfee DLP Endpoint 集中式原則與事件監控
- 使用 McAfee ePO 軟體來集中管理原則及監控事件
- 從 McAfee ePO 軟體部署及更新代理程式
- 與 McAfee ePO 軟體整合，提供先進的 Web 型管理與更多報告/稽核功能

### 完整的可見性近在指尖

- McAfee DLP Endpoint 的全方位事件報告與監控功能可用來收集任何所需的資料，如寄件者、收件者、時間戳記和資料證據，以進行適當分析、調查、稽核、損害控制與風險評估



<sup>1</sup> Illuminas 2007，「Threats Within，Volume II: Data Loss Disaster」（內部威脅第二期資料遺失嚴重損壞）

<sup>2</sup> Ponemon Institute 的 2008 「Cost of Data Breach Study」（資料洩露成本研究）

<sup>3</sup> 隨附於 McAfee Data Loss Prevention 裝置中。