McAfee Complete Data Protection — Advanced

隨時隨地，提供全方位的資料保護

敏感資料持續面臨著外洩、遭竊與被公開的風險。很多時候，這類資料就這樣隨著筆記型電腦或 USB 裝置直接走出公司大門。這會使企業必須承擔資料遺失的嚴重後果，包括：法規處罰、資料公開、品牌聲譽受損、失去客戶信任及財務損失。根據 Ponemon Institute 報告指出，在所有的公司筆記型電腦中，有 7% 的筆電會在其使用年限到達前遺失或遭竊。[1] 而迅速普及的行動裝置不僅具有強大的儲存能力，且經常被用來上網，也造成了更多資料外洩或遭竊的機會；因此，保護敏感、專有、個人身分識別之機密資訊，已成為首要之務。McAfee® Complete Data Protection — Advanced 能為您解決上述問題，並提供更多保障。

主要功能

- McAfee Data Loss Prevention Endpoint
- McAfee Device Control
- Drive Encryption
- File and Removable Media Protection
- Management of Native Encryption
- McAfee ePO Deep Command

主要優點

- 藉由監控及規範員工在公司內部或外部如何透過一般管道 (例如電子郵件、IM、列印輸出及 USB 磁碟機等) 使用或傳輸資料的方式，妥善控管您的資料。
- 阻止因複雜的惡意軟體劫持敏感及個人資訊，而造成的資料外洩問題。
- 為儲存在桌上型電腦、筆記型電腦、平板電腦及雲端上的資料提供保護。
- 直接透過 McAfee ePO 在端點上管理 Apple FileVault 和 Microsoft BitLocker 的原生加密。

有效控管的資料遺失防護技術

即使問題難以察覺，避免端點的資料外洩問題，仍是從改善對資料的掌控能力開始。McAfee Complete Data Protection — Advanced 可讓您實作並強制執行涵蓋全公司的安全性政策，以規範並限制您的員工如何透過一般管道 (例如電子郵件、IM、列印輸出及 USB 磁碟機等) 使用或傳輸敏感資料。無論是在辦公室、在家中或在行動中，您都能持續控管。

企業級磁碟加密

利用企業級安全性解決方案，為您的機密資料提供安全保障；這個安全性解決方案通過 FIPS 140-2 和 Common Criteria EAL2+ 認證，並利用 Intel® Advanced Encryption Standard — New Instructions (Intel AES-NI) 組合加快執行效率。McAfee Complete Data Protection — Advanced 採用磁碟機加密技術，並透過開機前雙重驗證，結合了強大的存取控制功能，避免端點上 (桌上型電腦、VDI 工作站、筆記型電腦、USB 磁碟機、CD/DVD 等) 發生未經授權而存取機密資料的行為。

卸除式媒體、檔案和資料夾以及雲端儲存加密

確保特定的檔案與資料夾隨時處於加密狀態，無論資料於何處進行編輯、複製或儲存。McAfee Complete Data Protection — Advanced 所具備的內容加密技術，可於檔案與資料夾在組織中移動之前，自動以透明化的方式即時加密您所選擇的檔案與資料夾。您可以針對特定檔案與資料夾，根據使用者及使用者群組建立並強制執行中央原則，無須與使用者互動。

Management of Native Encryption

Management of Native Encryption 可讓您直接從 McAfee® ePolicy Orchestrator® (McAfee ePO™) 軟體，管理 OS X 上由 Apple FileVault 和 Windows 平台上由 Microsoft BitLocker 提供的

intel Security

主要優點 (續上頁)

- 不論是為了避免因資安事件、病毒爆發或忘記加密密碼隨之而來的現場檢查和接不完的客訴電話，而使端點處於關機、停用或是加密狀態，仍能與端點通訊並以硬體層級進行控制。
- 利用進階的報告及稽核功能來驗證符合性；監控事件並產生詳細報告，使稽核人員與其他利益關係人瞭解您對於內部與法定隱私權的符合性如何。

專為 McAfee ePO Deep Command 設計的特定功能

- 減少修補次數。
- 以存取硬體的方式，管理全球各地任一台電腦的遠端修補程序。
- 提高使用者生產力。
- 在下班時間執行耗用大量資源的工作，以減少對使用者的影響。
- 減少頻繁的現場檢查和冗長的服務通話，進而降低 IT 成本。
- 採用節能方案來減少電腦的電費支出，但仍可針對安全性或修補作業保有存取能力。
- 藉由輕鬆辨識搭載 Intel vPro AMT 技術的電腦，接著啟用 Intel AMT 以執行簡化的啟動程序，快速探索及佈建 Intel AMT。

原生加密功能。因此，Management of Native Encryption 可提供與 Apple OS X 和 Windows 修補程式、更新及韌體更新零時差的相容功能，以及 Apple 新硬體的零時差支援。Management of Native Encryption 可讓管理員手動將復原金鑰匯入至使用者已啟用 FileVault 和 BitLocker 的位置。

遠端頻外管理可降低運作成本

McAfee ePO Deep Command 軟體採用 Intel® vPro Active Management Technology (Intel vPro AMT)，有助於降低運作成本、提高安全性與符合性，並可加快修補遠端電腦的速度。McAfee ePO Deep Command 軟體可喚醒電腦、更新原則，然後安全地將電腦恢復為原本的電源狀態。[2]

集中式安全管理與進階報告功能

您可使用 McAfee ePO 集中式軟體主控台實作並執行涵蓋全公司的強制性原則，藉此控管如何對資料進行加密、監視及避免資料外洩。可集中定義、部署、管理及更新安全性原則，這些原則可加密、篩選、監控敏感資料，並封鎖未經授權的存取行為。

McAfee Complete Data Protection — Advanced 功能

裝置控制

- 即使員工並未連線至公司網路，也能監控及規範員工將資料傳輸至卸除式媒體的方式。

資料遺失防護

- 控制使用者如何從端點 (無論為實體或虛擬)，透過應用程式及在儲存裝置上傳送、存取及列印敏感資料。
- 阻止因劫持員工憑證的特洛伊木馬程式、蠕蟲病毒以及檔案共用應用程式所造成的機密資料外洩。
- 即使當資料已修改、複製、貼上、壓縮或加密，仍會保護所有的資料、格式及衍生項目。

企業級磁碟加密

- 可自動加密整個裝置，無需使用者操作、省卻訓練，且不會影響系統資源。
- 利用強大的多重驗證確認及驗證經授權的使用者。

卸除式媒體加密

- 可自動即時加密幾乎任何行動儲存裝置，無論是否為公司配發之裝置。
- 無須任何額外軟體，即可在任何地方存取加密資料。

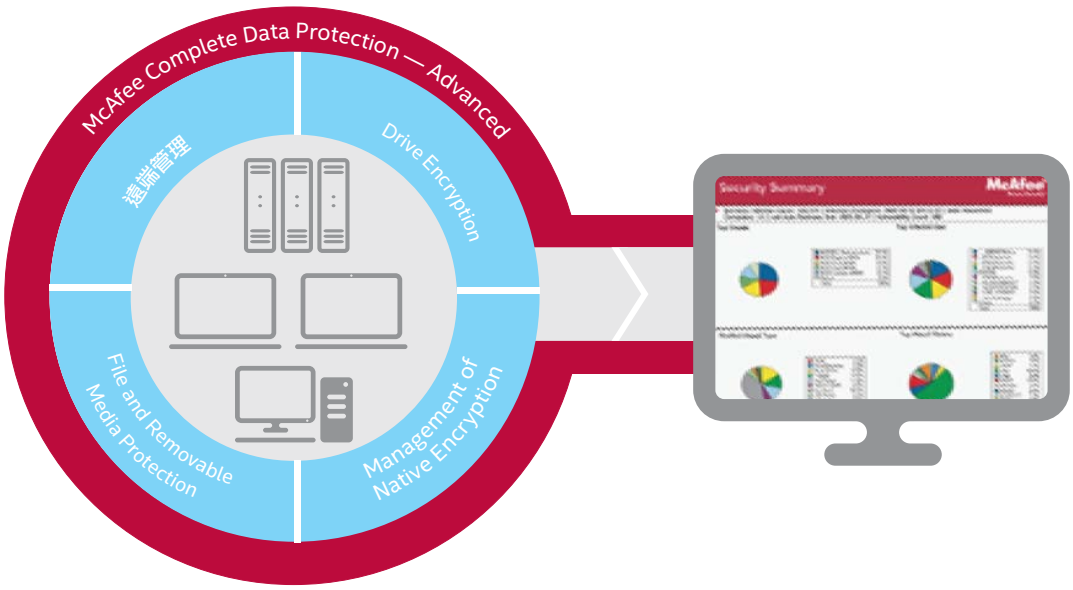

圖 1. McAfee Complete Data Protection — Advanced。

McAfee Complete Data Protection — Advanced 規格

Microsoft Windows 作業系統

- Microsoft Windows 7、8 與 10 (32/64 位元版本)
- Microsoft Windows Vista (32/64 位元版本)
- Microsoft Windows XP (僅限 32 位元版本)
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003 (僅限 32 位元版本)

硬體需求

- CPU：Pentium III 1GHz 或速度更快的筆記型電腦與桌上型電腦
- RAM：最低 512 MB (建議 1 GB)
- 硬碟：至少 200 MB 的可用磁碟空間

Apple Mac 作業系統

- Mac OS X El Capitan、Yosemite、Mountain Lion、Mavericks

硬體需求

- CPU：含 64 位元 EFI 的 Intel 核心 Mac 筆記型電腦
- RAM：至少 1 GB
- 硬碟：至少 200 MB 的可用磁碟空間

集中式管理

- 請參閱 McAfee ePO 平台資料工作表，以取得技術規格

McAfee ePO Deep Command 規格

- 支援 Intel vPro AMT 6.1.2、7.0、7.1.4 版本，8.0 Intel Setup and Configuration Software (SCS) 8.2

檔案、資料夾和雲端儲存加密

- 無論檔案和資料夾儲存在任何位置皆可受到保護，包含儲存於本機硬碟、檔案伺服器、卸除式媒體和雲端儲存空間，如 Box、Dropbox、Google Drive 和 Microsoft OneDrive。

管理 Mac 和 Windows 的原生加密

- 直接透過 McAfee ePO 軟體，管理任何 Mac 硬體 (可以在 Mac OS X Mountain Lion、Mavericks、Yosemite 或 El Capitan 上執行) 中的 FileVault。
- 直接透過 McAfee ePO 軟體，管理 Windows 7、8 和 10 系統中的 BitLocker，無需獨立設置一個 Microsoft BitLocker Management and Administration (MBAM) 伺服器。

遠端頻外管理

- 跨越作業系統範疇，從遠端在硬體層級管理電腦。
- 即使電腦處於加密狀態，仍可啟動和喚醒個人電腦以執行安全性工作。

集中式管理主控台

- McAfee ePO 軟體基礎架構管理可用來管理全磁碟、檔案與資料夾及可卸除式媒體加密；控制原則與修補程式管理；回復遺失的密碼；以及示範法規符合性。
- 將安全性原則與 Microsoft Active Directory、Novell NDS、PKI 等解決方案同步化。
- 可驗證裝置是否已使用各種稽核功能進行加密。
- 記錄資料交易，以保留寄件者、收件者、時間戳記、資料證據，以及上次成功登入的日期與時間等資訊。

如需 McAfee 資料保護的詳細資訊，請造訪：**www.mcafee.com/tw/products/data-protection/index.aspx**。

1. *The Billion Dollar Lost Laptop Problem Study* (價值十億美元的筆記型電腦遺失問題之研究)，Ponemon Institute，2010 年 9 月。
2. *Keep Your Client PCs Safer, Wherever They Go:* (隨時隨地為您的用戶端電腦提供更周全的保護) **http://www.mcafee.com/tw/resources/solution-briefs/sb-keep-your-client-pcs-safer.pdf**

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

62238ds_complete-data-adv_0116_ETMG