

McAfee Application Control for Desktops

增加防禦力、取得應用程式可見性、縮短修補週期，且不影響企業的電腦效能

對於公司的 IT 人員來說，桌上型電腦為他們帶來了許多不易處理的安全性難題，而在眾多複雜的成因中，大部分是與使用者不慎下載惡意軟體有關。究其根本原因，實際上是各種新型態的進階持續性威脅 (APT) 不斷鎖定使用者進行攻擊的緣故。APT 會使用社交網路和其他攻擊手法，誘騙使用者載入不可信任的公用程式、擴充功能和應用程式。McAfee® Application Control for Desktops 在防毒之外還新增了一層重要安全防護，不僅可以保護標準化的 IT 管理桌面系統，還能維持使用者與 IT 人員的生產力。

主要優點

- 強化桌上型電腦防護，適用於 PCI DSS 和其他高標準環境。
- 無須更新特徵碼即可抵禦零時差威脅與 APT。
- 運用 McAfee Global Threat Intelligence (McAfee GTI) 軟體提供企業內檔案和應用程式的信用評價。
- 強化安全性同時減少擁有成本。
- 縮短桌上型電腦修補週期。
- 瞭解應用程式在企業中的使用情形。
- 自動接受透過獲得授權之程序新增的軟體。
- 在企業中部署白名單項目前，先探索信任的更新程式原則。
- 桌上型電腦使用者可自行彈性核准新的應用程式。
- 以低負荷解決方案維持使用者生產力。
- McAfee ePolicy Orchestrator® (McAfee ePO™) 軟體的集中式管理平台可有效控制應用程式存取。

McAfee Application Control 軟體能全面防範不需要的應用程式與程式碼，無須更新特徵碼即可封鎖進階威脅。它能讓您統一啓用已知的良好應用程式、封鎖已知與未知的惡意軟體，以及適當管理新軟體。

強化保護

想進行有效率的桌面管理，有賴於運用標準化的 IT 管理作業環境。此外，若想確保系統安全，還需結合防毒、入侵防護的最佳作法，輔以其他用來封鎖病毒、蠕蟲、特洛伊木馬程式、垃圾郵件、廣告軟體、間諜軟體及其他已知惡意軟體的技術。

那麼遇到未知威脅時，又該怎麼辦呢？多型態惡意軟體、APT 和零時差威脅往往會以偽裝成合法應用程式的方式散佈。想要解決這些威脅，最好的辦法就是透過應用程式白名單，限制存取已知可信的應用程式。因此，McAfee 相信保持端點安全性的最佳策略，就是以防惡意軟體掃描，搭配動態應用程式控制。McAfee Application Control for Desktops 利用獨家的集中式管理動態白名單信任模型，可省去與其他白名單技術相關的昂貴使用者支援需求，進而節省成本支出。

McAfee GTI 整合：因應全球威脅的明智之道

McAfee GTI 是 McAfee 的獨家技術，這項技術能利用遍及全球的數百萬個偵測器即時追蹤檔案、IP 和網站的信用評價。McAfee Application Control 軟體會使用此雲端型知識來判定運算環境中所有檔案的信用評價，然後將檔案分類為良好、

惡意及未知。在 McAfee GTI 整合的協助之下，當您不慎將惡意軟體列入白名單時，系統會確切地告知您。

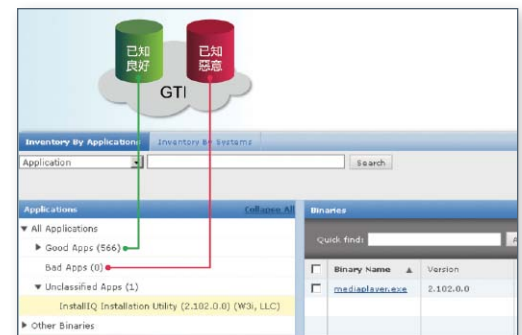


圖 1. McAfee GTI 會持續監控檔案的信用評價，因此能自動封鎖已知惡意檔案，以及將信用評價不詳的檔案列入灰名單。

有庫存，免猜測

我們的應用程式庫存功能可根據應用程式與廠商為全企業中的二進位檔案 (EXE、DLL、驅動程式及指令碼) 分組，並以直覺式的階層格式加以顯示。應用程式可分類為已知、未知及已知惡意。此外，您還可以輕鬆地搜尋有用的資訊，例如本週新增的應用程式、未認證的二進位檔案、信用評價不詳的檔案、執行過期 Adobe Reader 版本的系統等，以便快速地鎖定弱點及驗證軟體授權的法規遵循狀態。

支援的平台

Microsoft Windows XP、Vista 和 Windows 7



圖 2. 安全更新流程。

瞭解應用程式的使用情形

在觀察模式下觀看及學習

觀察模式能讓您無須事先啓用白名單，即可探索動態桌面環境的原則。它可讓您逐步進行 McAfee Application Control 軟體的部署作業，並在此同時探索新的受信任更新程式，而不致中斷應用程式運作。管理員可以透過 McAfee Application Control 使用單一原則探索頁面，為觀察和自我核准要求定義原則。

內建具建設性的建議

McAfee Application Control for Desktops 軟體含有建議介面，它能根據端點的執行模式提出新的更新原則建議。此外，您也可以針對不同使用者採用彈性原則，藉以調整控制與監督使用者的力度。

以使用者自行核准機制協助使用者參與解決方案

使用者有時會需要存取尚未獲得公司核准的應用程式，而遇到這種情況時，他們不需等待 IT 人員核准，即可自行安裝新軟體。

IT 人員會檢查這些自行核准動作，建立適用於全企業的原則，以規定在所有系統上禁止或允許這個應用程式。無法自行核准的使用者將會收到快顯通知訊息，說明為何系統不允許存取未經授權的應用程式。這些訊息會提示使用者透過電子郵件或客服來請求核准。



圖 3. 當使用者嘗試安裝未經核准的應用程式，畫面上會顯示「自行核准要求」方塊，以及仍待 IT 人員核准請求的通知。IT 人員核准後，應用程式隨即列入白名單，未來其他使用者也不再提出相同的請求。

減少修補期間的慌張失措

McAfee Application Control for Desktops 能搭配 McAfee Host Intrusion Prevention 運作，抵禦遠端記憶體威脅。這項經過驗證的對策能讓您將修補部署作業延後到正常的修補週期。

McAfee ePO 軟體：透過單一窗口進行安全管理

McAfee ePo 軟體可整合及集中管理作業，讓您以無死角的全域觀點檢視企業安全性。這項強大的安全管理平台整合了 McAfee Application Control for Desktops 軟體、McAfee Host Intrusion Prevention、McAfee Firewall 及其他 McAfee 安全性與風險管理產品。除此之外，McAfee ePO 軟體還能輕鬆結合 McAfee Security Innovation Alliance 合作夥伴的產品與自製的管理應用程式。



圖 4. 除了桌上型電腦之外，McAfee Application Control 軟體還能將伺服器與固定功能裝置納入保護範圍內，大幅降低各種應用程式的風險。

後續步驟

McAfee Application Control for Desktops 能有效在公司的桌上型電腦和筆記型電腦上，封鎖未經授權的應用程式與程式碼。此集中管理的白名單解決方案使用動態信任模型與創新的安全性功能，可遏止進階持續性威脅，完全不需要更新特徵碼及管理惱人的清單。

保護公司的桌上型電腦與筆記型電腦免受未知 APT 侵擾。若要查看您是否符合 McAfee Application Control for Desktops 的免費試用資格，歡迎立即造訪 www.mcafee.com/apps/downloads/free-evaluations。



邁克菲有限公司台灣分公司
台北市 110 基隆路一段
333 號 22 樓 2210 室
886-2-2757-6677
www.mcafee.com/tw

McAfee、McAfee 標誌、ePolicy Orchestrator 及 McAfee ePO 皆為 McAfee, Inc. 或其附設公司在美國及其他國家地區的商標或註冊商標。其他名稱與品牌可能為他人所宣告的財產。本文中的產品計劃、規格和描述只提供參考，如有變更，恕不另行通知，並且不包含任何明示或暗示的保證。
Copyright © 2014 McAfee, Inc.
61007ds_app-control_0314_kg