McAfee Application Control

降低未獲授權之應用程式的風險以控制端點、伺服器及固定裝置。

經由遠端攻擊或社交工程傳播的進階持續性威脅 (APT) 使企業防護日益艱難。McAfee® Application Control 可協助您戰勝網路犯罪分子，維護企業安全與生產力。此 McAfee 解決方案使用動態信任模型和創新的安全性功能 (例如，本機與全域信用評價情報、即時行為分析及端點自動免疫)，無須耗費大量人力管理清單或更新特徵碼，便可立即阻擋 APT。如果您無法容忍零時差威脅，不妨進一步瞭解 McAfee Application Control。

智慧型白名單

McAfee Application Control 可封鎖未獲授權之應用程式的執行作業，以防範零時差及 APT 攻擊。您可以運用我們的庫存功能，輕鬆尋找及管理與應用程式相關的檔案。庫存功能可根據應用程式與廠商將企業中的二進位檔案 (.EXE、.DLL、驅動程式及指令碼) 加以分組，不僅能以直覺式的階層格式加以顯示，還會進行智慧型分類，將檔案分為舊有、未知及已知的惡意應用程式。使用白名單功能，僅允許列在名單中的已知良好應用程式執行，您即可防範未知惡意軟體的攻擊。

實施適當的安全計劃

由於使用者要求在社交與啟用雲端的企業環境中使用應用程式時須更具彈性，McAfee Application Control 提供組織三種充分發揮白名單策略的選項，以達到以上所述之威脅防護目標：

圖 1. 充分發揮白名單策略的三種方法。

主要優點

- 無須更新特徵碼即可抵禦零時差與 APT。
- 充分運用 McAfee Global Threat Intelligence 與 McAfee Threat Intelligence Exchange 的優點，以提供檔案及應用程式的全域與本機信用評價。
- 動態白名單可強化安全性及降低擁有成本，還能自動接受透過受信任通道所新增的軟體。
- McAfee® ePolicy Orchestrator® (McAfee ePO™) 軟體，為 McAfee 安全性解決方案的集中式管理平台，可有效控制應用程式存取。
- 安全的白名單與先進的記憶體保護可縮短修補週期。
- 利用受信任的更新程式，以最新的修補程式使系統處於最新狀態。
- 針對已連線或已中斷連線的伺服器、虛擬機器、端點、固定裝置 (如銷售點終端機) 以及舊版系統 (如 Microsoft Windows XP) 強制執行控制措施。

內建具建設性的意見

使用庫存搜尋與預先定義之報告，您可以快速尋找並修正漏洞、符合性及您環境中的安全性問題。您還可以探索實用的資訊 (如最近新增的應用程式、未認證的二進位檔案、信用評價不詳的檔案、執行過期版本軟體的系統)，並且快速鎖定漏洞及驗證軟體授權的符合性。

完整又快速的回應

白名單是透過來自 McAfee Global Threat Intelligence (McAfee GTI) 的全域威脅情報而得以獲得強化；此為 McAfee 的獨家技術，能利用遍及全球的數百萬個偵測器即時追蹤檔案、訊息及寄件者的信用評價。McAfee Application Control 會運用此知識來判定運算環境中檔案的信用評價，並將檔案分類為良好、惡意及未知。

搭配另售的選購模組 McAfee Threat Intelligence Exchange 進行部署時，McAfee Application Control 會更新以本機信用評價情報為基礎的白名單，以便立即對抗威脅。若搭配使用 McAfee Threat Intelligence Exchange，則 McAfee Application Control 可與 McAfee Advanced Threat Defense 協同合作，在沙箱中動態分析未知應用程式的行為，使端點自動免受最新偵測的惡意軟體襲擊。

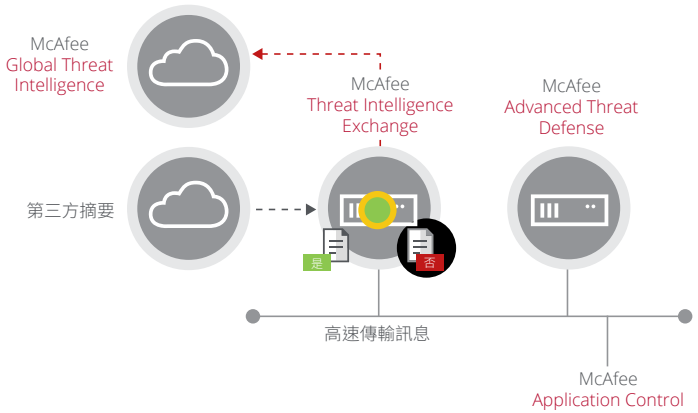

圖 2. McAfee GTI 持續監控檔案與寄件者的信用評價。搭配 McAfee Threat Intelligence Exchange 進行部署時，McAfee Application Control 會根據本機信用評價情報自動更新白名單；如需檔案的詳細資訊，還可與 McAfee Advanced Threat Defense 協同合作。

毫不影響業務持續性

為了避免干擾業務持續性，新的應用程式將根據應用程式的信用評價自動獲得允許。建議介面能根據端點的執行模式提出新的更新原則建議，以應對未知應用程式。這個方法最適合用來管理遭到封鎖應用程式所產生的例外情況。例外情況與遭到封鎖之應用程式的詳細資料經過檢查後，只需核准檔案並列入白名單，或略過檔案便可封鎖應用程式。

主要優點 (續)

- 允許新的應用程式根據應用程式分級或自行核准程序，以改善業務持續性。
- 低負荷的解決方案能維護使用者生產力與伺服器效能。
- 輕鬆保護舊版系統與新型技術投資。

支援平台

Microsoft Windows (32 位元與 64 位元)

- 內嵌：Windows XPE、7 Embedded、WEPOS、POSReady 2009、WES 2009、Embedded 8、8.1 Industry、10
- 伺服器：Windows Server 2008、2008 R2、2012、2012 R2
- 桌上型電腦：Windows NT、2000、XP、Vista、7、8、8.1、10

Linux

- Red Hat/CentOS 5、6、7
- SUSE/openSUSE 10、11
- Oracle Enterprise Linux 5、6、7
- Ubuntu 12.04

協助使用者參與解決方案

McAfee Application Control 可針對未知應用程式，為 IT 人員提供多種方式，方便使用者安裝新應用程式。

- **使用者通知** — 使用者會收到快顯通知訊息，說明系統為何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。
- **使用者自行核准** — 具有此權限的使用者，可自行安裝新軟體，不須等待 IT 人員核准。IT 人員可以檢查這些自行核准動作，並建立適用於全企業的原則，以便在所有系統上禁止或允許這個應用程式。

保持系統處於最新狀態

我們瞭解，保持您的系統與最新的修補程式處於最新狀態是至關重要的一環。這就是我們提供動態信任模型的原因，其目的在於方便您自動更新系統，並且不會讓業務持續性受到影響。透過受信任的使用者、憑證、程序與目錄，保持您的系統處於最新狀態。McAfee Application Control 還能預防列入白名單的應用程式在 Microsoft Windows 32 與 64 位元系統上經由記憶體緩衝區溢位攻擊遭到入侵。

取得進階執行控制

為了增強型防護，McAfee Application Control 可讓您結合以檔案名稱、程序名稱、上層處理程序名稱、命令列參數及使用者名稱為依據的規則。您可以使用進階執行控制來阻擋略過檔案的輸入/輸出攻擊、為系統偵測器封鎖互動模式及預防系統工具攻擊。還可以取得更強大穩固的 SHA-256 演算法來建立原則。

McAfee ePolicy Orchestrator 軟體：單一窗格

McAfee ePO 軟體能統合並集中管理作業，讓您全面掌握企業安全性，絕無盲點存在。此獲獎肯定的平台整合了 McAfee Application Control、McAfee Host Intrusion Prevention 及其他 McAfee 安全性產品，包括具有黑名單功能的防惡意軟體。McAfee Application Control 部署的單一步驟安裝和更新還可從 Microsoft System Center 進行。

在觀察模式下觀看及學習

觀察模式能讓您無需強制執行白名單鎖定即可探索動態桌面環境的原則。它讓您可以逐步將 McAfee Application Control 部署在預先生產或早期生產環境中，而不致使應用程式受損。透過 McAfee Application Control，管理員可使用單一原則探索頁面，依照觀察與自行核准請求來定義原則。

保護舊版系統及最新的技術投資

需要保護諸如 Microsoft Windows NT、2000 及 XP 等舊版的作業系統嗎？即便 Microsoft 與其他安全性廠商皆不支援這些舊版系統，McAfee Application Control 仍會將這些系統納入保護。此外，McAfee Application Control 還能支援您最新的作業系統，如 Microsoft Windows 10。

後續步驟

如需詳細資訊，請造訪 **http://www.mcafee.com/tw/products/application-control.aspx**，或是在上班時間撥打我們的專線電話：886-2-2757-6677。

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

McAfee 和 McAfee 標誌、ePolicy Orchestrator 與 McAfee ePO 是 McAfee, LLC 或其附設公司在美國及其他國家地區的商標或註冊商標。其他標誌與品牌可能為其各自擁有者的財產。Copyright © 2017 McAfee, LLC. 2183_1216
2016 年 12 月