

# McAfee Application Control

降低未獲授權之應用程式的風險，同時強化端點、伺服器及固定裝置的控制力

## 主要優點

- 無需更新特徵碼即可抵禦零時差與進階持續性威脅
- 動態白名單可強化安全性及節省擁有成本
- McAfee ePO 軟體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
- 針對連線、中斷連線的伺服器、虛擬機器 (VM)、端點及固定裝置 (如銷售點終端機) 強制執行控制措施
- 自動接受透過獲得授權之程序新增的軟體
- 透過便於使用的選用通知將禁用應用程式的相關資訊傳達給桌面使用者
- 低負荷的解決方案能維護使用者生產力與伺服器效能
- 輕鬆保護不受支援的舊版系統，如 Microsoft Windows NT 與 2000

經由遠端攻擊或社交工程傳播的進階持續性威脅使企業防護日益艱難。但在 McAfee，您的安全永遠是第一要務。我們日以繼夜地積極尋找維護企業安全與生產力的有效方法。採用 McAfee® Application Control 軟體來取得先機，驅退網路惡霸。這項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，可封鎖未取得授權的應用程式及遏止進階持續威脅，完全不需要管理惱人的清單。如果您無法容忍零時差威脅，不妨進一步瞭解 McAfee Application Control。

McAfee Application Control 軟體能全面防範不需要的應用程式與程式碼，無需更新特徵碼即可封鎖進階威脅。它能讓您一致地啟用已知的良好應用程式、封鎖已知與未知的惡意應用程式，以及適當管理新軟體。我們的動態白名單信任模型能省去與其他白名單技術相關的昂貴手動支援需求，節省成本支出。

## 有庫存，無猜測。

您不需要處心積慮地尋找及管理應用程式相關的檔案。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 (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)，然後快速地鎖定弱點及驗證軟體授權的法規遵循狀態。

## 協助使用者參與解決方案

在嘗試存取或安裝禁用的應用程式時若收到晦澀難解的錯誤訊息，只會讓使用者更加灰心。有了 McAfee Application Control 軟體中便於使用的選用通知與核准申請後，使用者便會收到通知快顯訊息，說明禁止存取未獲授權之應用程式的原因。這些訊息會提示使用者透過電子郵件或客服來請求核准。

## McAfee ePolicy Orchestrator 軟體：單一窗口

McAfee® ePolicy Orchestrator® (McAfee ePO™) 軟體能使管理作業統合與集中，讓您以無死角的全域觀點檢視企業安全性。這項獲獎的平台整合了 McAfee Application Control 軟體、McAfee Risk Advisor、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1.除了桌上型電腦與伺服器之外，McAfee Application Control 軟體還能將固定功能裝置納入保護範圍內，大幅降低消費者承受的風險。

## 支援的平台

### Windows (32 和 64 位元)

- 內嵌：XPE、7E
- 伺服器：NT、2000、2003、2003 R2、2008、2008 R2
- 桌上型電腦：XP、Vista、7

### Linux

- RHEL 3、4、5、6
- Suse 9、10、11
- CentOS 4、5
- SLED 11

### Solaris

- 8、9、10 (於 SPARC 上)
- 10 (於 x86、x86-64 上)

## 少量的耗用與負荷

McAfee Application Control 是低負荷的軟體解決方案：

- 設定輕鬆，而且初始與進行中的作業負荷低
- 微不足道的記憶體使用量
- 檔案掃描絕對不影響系統效能
- 能在中斷連線與離線模式下運作
- 不需要更新特微碼

## 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 軟體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。

## 內建具建設性的建議

McAfee Application Control 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。這個方法最適合用來管理由受封鎖應用程式產生的例外。只要檢查受封鎖應用程式的例外與詳細資料，接著再核准檔案並將其加入白名單，抑或是略過檔案 (如果是應當封鎖的應用程式)。



圖 2. 安全的更新流程。

## 保護舊版系統

需要保護諸如 Microsoft Windows NT 與 Microsoft Windows 2000 等舊式的作業系統嗎？即便是 Microsoft 與其他安全性廠商不支援這些舊版系統，McAfee Application Control 軟體仍會將這些系統納入保護。

## 減少修補次數及保護記憶體

McAfee Application Control 軟體能搭配 McAfee Host Intrusion Prevention 運作，供您測試進入及離開列入灰名單之應用程式的流量。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 Application Control 軟體還能預防列入白名單的應用程式在 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。

## GTI 整合：因應全球威脅的明智之道

McAfee Global Threat Intelligence™ (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、訊息及寄件者的信用評價。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 3. McAfee Global Threat Intelligence 會持續監控檔案與寄件者的信用評價，因此能自動封鎖已知的惡意檔案，以及將信用評價不詳的檔案列入灰名單。