McAfee Embedded Control

涵蓋系統完整性、變更控制及原則遵循的單一解決方案

McAfee® Embedded Control 能限制唯有取得授權的程式碼才能執行，以及唯有取得授權的變更才能生效，協助您維護系統的完整性。它能自動在嵌入式系統上建立動態的「授權程式碼」白名單。一旦建立白名單並加以啟用後，它會將系統鎖定在已知的良好基準之上，未經授權的程式或程式碼將無法執行，而未經授權的變更也將無法生效。結合 McAfee Embedded Control 與 McAfee ePolicy Orchestrator® (McAfee ePO™) 主控台的 McAfee Integrity Control 能提供整合的稽核與法規遵循報告，協助您滿足多個法規遵循的要求。

McAfee Embedded Control 著重於解決嵌入式系統中採用商業作業系統而引發的安全風險問題。McAfee Embedded Control 是資源耗用量少、低負荷且獨立於應用程式之外的解決方案，它能提供「部署後即可放心使用」的安全性。McAfee Embedded Control 能將以商業作業系統為基礎的系統轉變為「黑盒子」，使其成為類似封閉的專屬作業系統。它能禁止磁碟中或植入記憶體中的未經授權程式執行，也能避免授權的基準遭到未經授權的變更。這項解決方案使製造商得以享用商業作業系統帶來的優勢，而不需要擔心衍生的額外風險或無法掌握系統在領域中的用途。

確立的系統完整性

可執行的控制

在 McAfee Embedded Control 的控制之下，唯有 McAfee 動態白名單中的程式才能執行。其他程式 (exe、dll、指令碼) 均會被視為未經授權的程式。它會禁止未經授權程式的執行，並且會將失敗記錄下來 (預設值)。如此可預防會自我安裝的蠕蟲病毒、病毒、間諜軟體及其他惡意軟體非法執行。

記憶體控制

記憶體控制能確保執行中的處理程序受到保護，避免讓劫持處理程序的惡意嘗試得逞。針對執行中處理程序被植入的未經授權程式碼，它能設陷攔截、阻止與記錄。如此一來，嘗試利用緩衝區溢位、堆積溢位、堆疊執行及類似弱點取得系統控制的企圖均會失去作用，同時也會被記錄下來。[1]

主要優點

- 控制嵌入式裝置中的執行項目以及保護裝置的記憶體，藉以降低安全性風險。
- 可讓您授與存取權、保留控制權，並減少支援成本。
- 選擇性的強制措施。
- 部署後即可放心使用。
- 使您的裝置符合法規遵循要求並可供稽核。
- 即時可見性。
- 全面性稽核。
- 可搜尋的變更封存。
- 封閉迴路調整。

McAfee GTI 整合：因應隔離環境之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。這項功能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。連線至網際網路以及隔離的 McAfee ePO 軟體環境皆可使用 GTI 信用評價服務。

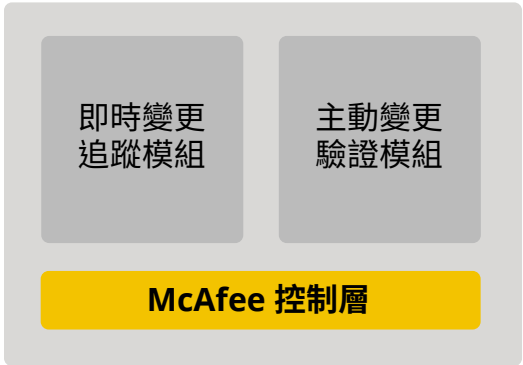
變更控制

McAfee Embedded Control 能即時偵測變更。它能讓您深入變更的源頭，並確認變更是否部署於正確的目標系統上。它也提供變更的稽核追蹤，以及僅允許經由授權的方式執行變更。

McAfee Embedded Control 能讓您藉由指定授權的變更執行方式來強制執行變更控制程序。您可以控制能套用變更的人員、允許變更所需的憑證、能變更的項目 (例如，您可以限制只能變更某些檔案或目錄)，以及套用變更的時間 (例如，唯有在一星期內某些時間才能開啟更新 Microsoft Windows)。

主動式變更能在將變更套用至目標系統前加以驗證。此模組啟用時，使用者只能以受控制的方法變更軟體系統。

即時變更追蹤模組能將所有變更記錄在系統狀態中，包括程式碼、組態及登錄。此模組能在變更事件發生時立即記錄事件，並將事件傳送到系統控制器以供彙總與封存之用。



部署在端點的變更代理程式

圖 1. McAfee 控制層。

系統控制器模組能管理系統控制器與代理程式間的通訊。它能彙總來自代理程式的變更事件資訊，並將資訊儲存在獨立的記錄系統中。

圖 2. 報告、搜尋與分析模組。

稽核與原則遵循

McAfee Integrity Control 提供儀表板與報告來協助您滿足法規遵循需求。您可以經由 McAfee ePO 主控台來產生儀表板與報告，它能為使用者與管理員提供 Web 型的使用者介面。

McAfee Embedded Control 提供整合、封閉迴路、即時的法規遵循與稽核機制，而能記錄授權活動與未授權嘗試的防竄改記錄系統則使這項機制益臻完善。

關於 McAfee 嵌入式安全保護

McAfee 嵌入式安全解決方案能協助製造商，確保產品與裝置免受網路威脅與攻擊的侵擾。McAfee 解決方案採納應用程式白名單、病毒與惡意軟體保護、裝置管理、加密及風險與法規遵循等多元技術，這些技術皆運用了領先業界的 McAfee Global Threat Intelligence。我們能根據製造商之裝置與架構的特定設計需求，量身打造解決方案。

後續步驟

如需詳細資訊，請造訪 **www.mcafee.com/tw/partners/oem-alliances/index.aspx**，或連絡當地 McAfee 代表或附近的經銷商。

資料工作表

功能	說明	優點
保證系統完整性		
抵禦外部威脅	確保唯有取得授權的程式碼才能執行。未經授權的程式碼將無法植入記憶體中。取得授權的程式碼將無法加以竄改。	▪ 省去緊急修補的必要性、減少修補週期的次數與頻率、能在修補前進行更多測試、降低難以修補之系統的安全性風險。 ▪ 降低以蠕蟲病毒、病毒、特洛伊木馬程式等惡意軟體為媒介之零時差、多型態攻擊的安全性風險；預防緩衝區溢位、堆積溢位及堆疊溢位等程式碼植入攻擊。 ▪ 維護經授權檔案的完整性，確保生產系統處於已知與確認的狀態。 ▪ 透過限縮非計劃性修補與復原停機時間來降低作業成本，並提升系統可用性。
抵禦內部威脅	本機管理員鎖定可提供停用彈性，即便是管理員也不能變更已獲授權在受保護系統上執行的項目，除非提供驗證金鑰。	▪ 抵禦內部威脅。 ▪ 鎖定可在嵌入式生產系統上執行的項目，避免遭到包括管理員在內等使用者的變更。
進階的變更控制		
保護獲製造商授權的更新	限制唯有經授權的更新可在現場嵌入式系統上執行。	▪ 限制沒有頻外變更能部署在領域系統上。在未經授權的系統變更導致停機及產生支援通話前，先行阻止。 ▪ 製造商能選擇自行保留所有變更的控制權，或授權讓信任的客戶專員控制變更。
確保變更發生於核准的時間區段內	確保不會在非授權的變更時間區段部署變更。	▪ 防止在財務相關時間區段或業務高峰時段進行未經授權的變更，以預防營運中斷與/或法規遵循違規的情況發生。
取得授權的更新人員	限制唯有取得授權的更新人員(人員或處理程序)才能將變更執行於生產系統上。	▪ 確保所有頻外變更都無法部署在生產系統上。
即時、封閉迴路、稽核與法規遵循		
即時變更追蹤	當變更發生時，在整個企業內進行追蹤。	▪ 確保所有頻外變更都無法部署在生產系統上。
全面性稽核	擷取每個系統變更的完整變更資訊：人員、項目、位置、時間及方式。	▪ 為所有系統變更留下正確、完整及明確的記錄。
找出變更的來源	將每個變更與變更的來源連結起來：執行變更的人員、引發變更的事件序列、影響變更的處理程序/程式。	▪ 驗證經核准的變更、快速找出未經核准的變更，並提高變更成功率。

資料工作表

功能	說明	優點
低作業開銷		
部署後即可放心使用	軟體能在幾分鐘之內完成安裝，毋須進行初始組態或設定，亦不需要進行後續的組態。	▪ 立即可用，安裝後即可立即生效。不需要持續的維護開銷，因此最適合低營運支出的安全性解決方案組態。
免規則、免特徵碼、不需要學習期間、獨立於應用程式之外	不需要仰賴規則或特徵碼資料庫，不需要經歷學習期即可立即於所有應用程式中生效。	▪ 管理員只需在伺服器生命週期期間偶爾注意。 ▪ 只需要少量的後續營運支出，即可於伺服器修補之前提供保護，或保護未修補的伺服器。 ▪ 不需要仰賴任何規則或原則的品質即可發揮效用。
資源耗用量少，低執行階段開銷	只佔用不到 20 MB 的磁碟空間。不會干擾應用程式執行階段的效能。	▪ 適合部署於所有業務關鍵生產系統上，且不會影響系統的執行階段效能或儲存需求。
保證無誤報或漏報	只記錄未經授權的活動。	▪ 與其他主機入侵預防解決方案相較之下，精確的結果能大幅減少每天/每週用來分析記錄的時間，因此能降低營運支出。 ▪ 提高管理員效率，降低營運支出。

1. 僅適用於 Microsoft Windows 平台。

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