McAfee Change Control

預防未經授權的變更，並使法規遵循控制自動化。

主要功能

- *檔案完整性監控* - 持續追蹤檔案與登錄機碼的變更，並識別哪位人員變更了哪些檔案
- *變更預防* - 預防重要檔案與登錄機碼遭到竄改，並只允許符合更新原則的變更
- *變更協調* - 透過 McAfee ePolicy Orchestrator® (McAfee ePO™) 軟體整合 McAfee Change Control 與企業變更管理系統，包括滑鼠單鍵點擊與 BMC Remedy 進行整合

少量的耗用與低負荷

- 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

對現今許多組織來說，伺服器環境經常發生變更，而且是無法偵測的變更。從安全性與法規遵循的角度看來，這是很危險的情況。McAfee® Change Control 能在企業中持續偵測獲得授權的變更。它能封鎖未經授權的重要系統檔案變更、目錄變更及組態變更，同時簡化新原則與法規遵循措施的實作。

McAfee Change Control 軟體能消除在現今企業中過於頻繁的變更活動，這些活動可能會導致安全缺口、資料遺失及業務中斷等。McAfee Change Control 附有檔案完整性監控、變更預防及選用的變更協調元件，能強制執行變更原則、持續監控重要系統，以及偵測在分散式與遠端位置中所做的變更。它也能封鎖不需要的變更。

McAfee Change Control 含有直覺式的搜尋介面，能協助使用者迅速鎖定變更事件資訊。例如，您可以在介面中查詢所有發生於 xyz.acme.com 伺服器之 c:\windows\system32 目錄中的變更資料。

升級的檔案完整性監控

「PCI DSS 需求」10 與 11.5 要求追蹤及監控網路資源與持卡人資料的所有存取作業及部署檔案完整性監控 (FIM) 工具，以在重要系統、組態或內容檔案遭到未經授權的修改時通知相關人員。McAfee Change Control 能讓您以有效率、符合成本效益的方法實作即時 FIM 軟體及驗證 PCI 法規遵循。McAfee Change Control FIM 會提供人員、時間、物件及原因等重要資訊。它能即時提供使用者名稱、變更時間、程式名稱及檔案/登錄內容資料等資訊，讓您一目了然。此外，若發生業務中斷事件，它也能在您進行疑難排解時協

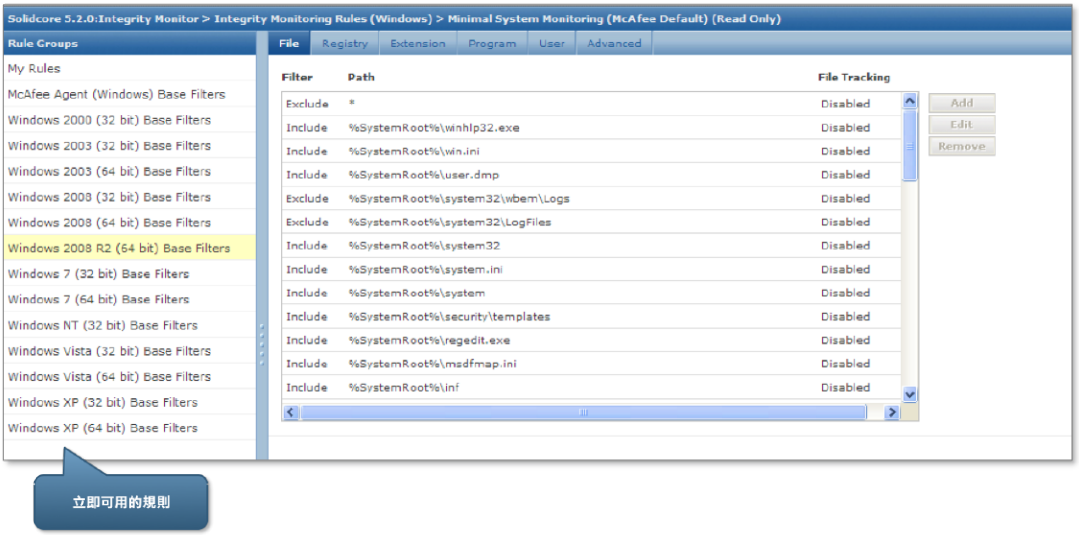

圖 1. McAfee Change Control 附有立即可用的 FIM 規則與精細的篩選，可讓您只對相關檔案進行監控。

主要優點

- 獲得有關重要系統、組態或內容檔案之變更的持續可見性與即時管理能力
- 預防重要檔案與登錄機碼遭到未經授權之對象竄改
- 達到 PCI DSS 檔案完整性監控系統的法規需求
- 立即可用的 FIM 規則讓您快速上手
- 針對簡易 PCI 報告作業的 QSA 適用之報告
- 滑鼠單鍵點擊排除功能可避免追蹤不相關的資訊
- 在程序外與不需要的變更發生前即先行主動封鎖，藉此強制執行嚴厲的原則
- 能與 McAfee ePolicy Orchestrator® (McAfee ePO™) 主控台整合以獲得集中式的 IT 管理
- 滑鼠單鍵點擊即可使 McAfee ePO 與 BMC Remedy 進行整合

支援的平台

Microsoft Windows (32 位元與 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
- OpenSUSE 10/11

Solaris

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

AIX

- AIX 5.3、6.1

HPUX

- HPUX 11i v1、v2、v3

助識別根本原因。您可以設定包含/排除篩選，以便只擷取相關、可動作的變更。除此之外，特殊的警示機制能在發生重要變更時立即傳送通知，使您得以預防與組態相關的業務中斷，這是建議的 Information Technology Infrastructure Library (ITIL) 最佳作法。另提供 Qualified Security Assessor (QSA) 表單以便進行簡易的 PCI 報告作業。

預防由未預期變更導致的業務中斷

McAfee Change Control 能讓 IT 輕鬆地解決事件、自動執行法規遵循控制，以及預防與變更相關的業務中斷。再者，McAfee Change Control 能省去手動、易產生錯誤及耗用大量資源之法規遵循原則的需求 (這些原則通常與沙賓法案 (SOX) 法規相關)。McAfee Change Control 與 McAfee Change Reconciliation 軟體 (選用) 搭配使用，能讓您建置自動化的 IT 控制架構，在此架構中您只需要一個報告系統即可取得驗證法規遵循所需的任何資訊。可以對根據授權所做的變更自動執行驗證。自動記錄及調整緊急修正與其他程序外的變更，以利稽核。

集中式的安全性與法規遵循管理

McAfee ePolicy Orchestrator® (McAfee ePO™) 軟體能使管理作業統合與集中，讓您以全域觀點檢視企業安全性。它能賦予調整涵蓋系統之類型與範圍的彈性，讓您決定要納入變更警示的檔案、目錄和組態，以及決定警示的優先順序。預設設定檔乃是針對最常見的伺服器作業系統與企業應用程式類型而開發的，不需要重新建立新設定檔即可監控重要元件。藉由 McAfee Change Control 與 McAfee ePO 軟體的協助，您可以隨時啓用新的設定檔來提升保護，不論是簡單的監控作業或堅如磐石的強制執行作業。

McAfee ePO 軟體富有擴充性並可立即延伸。它能將 McAfee Change Control 軟體和其他 McAfee 安全性管理軟體產品與 McAfee Security Innovation Alliance 合作夥伴的產品整合。此外，當 McAfee Change Control 與選用的變更協調軟體搭配運作時，會提供 McAfee ePO 軟體與 BMC Remedy 的滑鼠單鍵點擊整合。

強制執行改變萬事萬物

McAfee Change Control 軟體能即時追蹤及驗證所有在伺服器上嘗試執行的變更。它會要求只能在某個時間區段內進行變更、只能由信任來源進行變更，以及只能採用核准的工作票證進行變更，藉此強制執行變更原則。您可以對 McAfee Change Control 軟體的變更預防元件進行微調，以允許原生應用程式持續更新檔案而不受到干擾，同時禁止其他所有應用程式或使用者進行變更或甚至讀取指定的檔案。

針對多方面降低風險並提升法規遵循

McAfee 提供多種風險與法規遵循解決方案，以協助您將風險降到最低、使法規遵循自動化，並讓安全性達到最佳化。McAfee Change Control 與 McAfee Application Control 尤其是能摒除弱點及維護企業法規遵循的強力組合。

McAfee
An Intel Company

邁克菲台北辦公室
台北市 104 南京東路三段132 號 4 樓 A2
886-2-2721-7766
www.mcafee.com/tw

41100ds_mcc_1211_fnl_ETMG