McAfee Change Control

防止未經授權的變更。自動控管法規遵循。

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 屬於 McAfee 產品系列，能在企業中持續偵測經過授權的變更。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 軟體可消除變更活動，這類活動在當今的企業中非常普遍。變更活動可能導致安全漏洞、資料外洩及服務中斷。McAfee Change Control 具備檔案完整性監控和變更預防功能，可強制執行變更原則並提供連續監控重要系統。此外還能偵測零散與遠端位置的變更以及防止不必要變更。

McAfee Change Control 具有直覺式的搜尋介面，可協助使用者快速找到變更事件資訊。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

支付卡產業資料安全標準 (PCI DSS) 規範 10 與 11.5，均要求追蹤及監控網路資源與持卡人資料的所有存取作業，並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。它會以集中方式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助識別根本原因。

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

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
- 檔案掃描不會影響系統效能

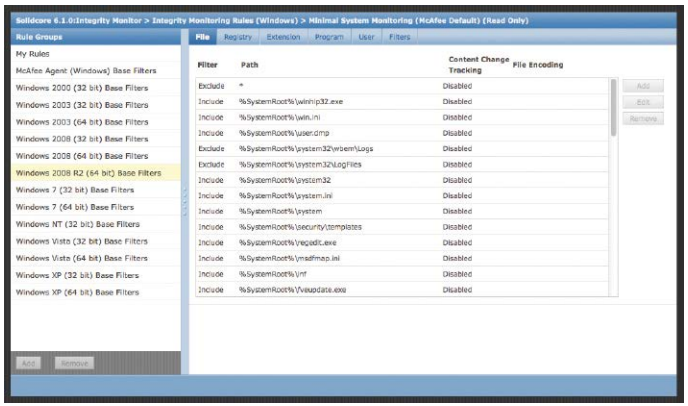

圖 1. McAfee Change Control 附有立即可用的 FIM 規則與精細的篩選，可讓您只監控相關檔案。

追蹤內容變更

McAfee Change Control 可讓您追蹤檔案內容及分類變更。您可以並列檢視和比較檔案內容變更，瞭解有何新增、刪除或修改之處。當您疑難排解與組態相關的中斷事件時，這項功能就十分好用。

您可以設定包含/排除篩選，以便僅擷取相關、可供動作的變更。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服務中斷，這是資訊技術基礎架構庫 (ITIL) 最佳建議作法。同時提供合格安全評估機構 (QSA) 表單，提供簡易的 PCI 回報功能。

預防因未預期變更導致的服務中斷

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。此外，McAfee Change Control 能免去對於手動、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 能讓您建置自動化的 IT 控制架構，在此架構中您可在單一報告系統中，取得驗證法規遵循所需的所有資訊。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 ePO 軟體能統合並集中管理作業，讓您全面掌握企業安全性。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。預設設定檔是針對最常見的伺服器作業系統與企業應用程式類型開發而成，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，您可以隨時啟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，通通沒問題。

McAfee ePO 軟體富有擴充性並可立即延伸。它能將 McAfee Change Control 軟體、我們的其他安全性管理軟體產品與我們合作夥伴的產品加以整合。

主要優點

- 針對重要系統、組態或內容檔案的變更提供持續的可見性與即時管理能力
- 預防重要檔案與登錄機碼被未經授權的對象竄改
- 充分實踐檔案完整性監控系統的 PCI DSS 法規規範
- 立即可用的 FIM 規則讓您快速上手
- 提供 QSA 適用的報告當作簡易的 PCI 回報
- 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
- 與 McAfee® ePolicy Orchestrator® (McAfee ePO™) 主控台整合以提供集中式 IT 管理

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

我們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，並達到最佳安全性。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。

後續步驟

McAfee Change Control 軟體會消除可能在伺服器環境中導致安全漏洞、資料遺失及服務中斷的變更活動，並讓您更輕易符合法規遵循要求。立即使用 McAfee Change Control，不僅能自動符合法規遵循，還可預防未經授權的變更。

支援的平台

Microsoft Windows (32 位元與 64 位元)

- 內嵌：Windows XPE、7E、WEPOS、Pos Ready 2009、WES 2009
- 伺服器：Windows NT、2000、2003、2003 R2、2008、2008 R2、2012
- 桌上型電腦：Windows XP、Vista、7

Linux

- RHEL 5、6
- Suse 10、11
- CentOS 5、6
- OEL 5、6
- SLED 11
- OpenSUSE 10/11

AIX

- AIX 6.1、7.1

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