

McAfee MVISION ePO

提供簡易的單點可見性與控管機制，不受地點所限

安全性管理相當複雜，需要在工具和資料之間進行繁複操作。此外，網路安全性專業人員不應將時間耗費在管理與更新安全性基礎架構上。相反，他們需要專注於處理關鍵的安全性工作，例如偵測和執行；否則在專業人員在分神處理其他瑣碎雜事的時候，攻擊者便會趁機發動攻擊，並會造成重大損失。McAfee® MVISION ePolicy Orchestrator® (McAfee MVISION ePO™) 省去了內部部署安全性基礎架構的維護作業，讓安全性專業人員能夠專責維持安全性。只要使用您的憑證即可從瀏覽器存取並管理安全性。

有鑑於網路安全性專業人員人才短缺，您需要加強現職員工的能力，以簡化網路安全性的協調作業。此外，他們也要針對任何裝置類型上的威脅迅速做出回應，以將損害降至最低。有鑒於此，他們更需要對貴組織的安全性狀態有充分瞭解，這可說是風險管理的首要任務。McAfee MVISION ePO 為全域多租戶企業安全即服務 (SaaS) 版 McAfee ePO 軟體，這個獨特的安全性管理平台獲得實證肯定。

McAfee MVISION ePO 讓您不必再處理費時的內部部署安全性管理基礎架構維護作業，有助於降低發生錯誤的可能性，讓您的資安團隊能發揮更大的效益，並且更有效率地管理安

全性，不受地點所限。透過 McAfee® MVISION Endpoint 技術，McAfee MVISION ePO 甚至可管理 Microsoft Windows 作業系統內建的原生控制項。

基本安全性管理變得更簡單

一切安全性解決方案都離不開對裝置和資料的監控與控制能力，這也是 IT 安全符合性的基礎。網際網路安全性中心 (CIS) 控制和美國國家標準技術研究院 ([NIST SP 800-53](#)) 安全性與隱私控制等業界標準，皆呼籲將監控及控制網路安全性基礎架構視為健全安全性的必要項目。

主要優勢

- 獲得業界肯定的集中式管理
- 省去內部部署安全性平台維護作業的麻煩
- 可在 Windows Defender 等作業系統中管理 McAfee 產品和原生控制項的全方位平台
- 自動化工作流程，讓管理工作更有效率
- 簡化事件調查及修補作業
- 通用的安全性管理，適用於市面上大多數裝置類型
- 可擴充至數十萬個裝置，涵蓋範圍從裝置到雲端

與我們聯絡



資料工作表

McAfee MVISION ePO 主控台能讓您監看關鍵性的資料，設定並自動執行原則，以便從任何地方皆可確保整個企業維持健全的安全性狀態。現在您可以透過整合的單一窗口，在整個企業中管理和強制執行原則，省去協調多個產品的麻煩。

防護工作區可協助您排定風險的優先順序，並在單一圖形檢視中提供整體數位領域的網路安全性狀態摘要，讓您更有效率地管理風險。管理員可深入檢視特定事件，以獲得更多的分析資訊。此摘要檢視可縮短建立報告及合理化現有

業界分析師表示，McAfee ePO 軟體是許多組織選擇和繼續使用 McAfee 產品的原因。

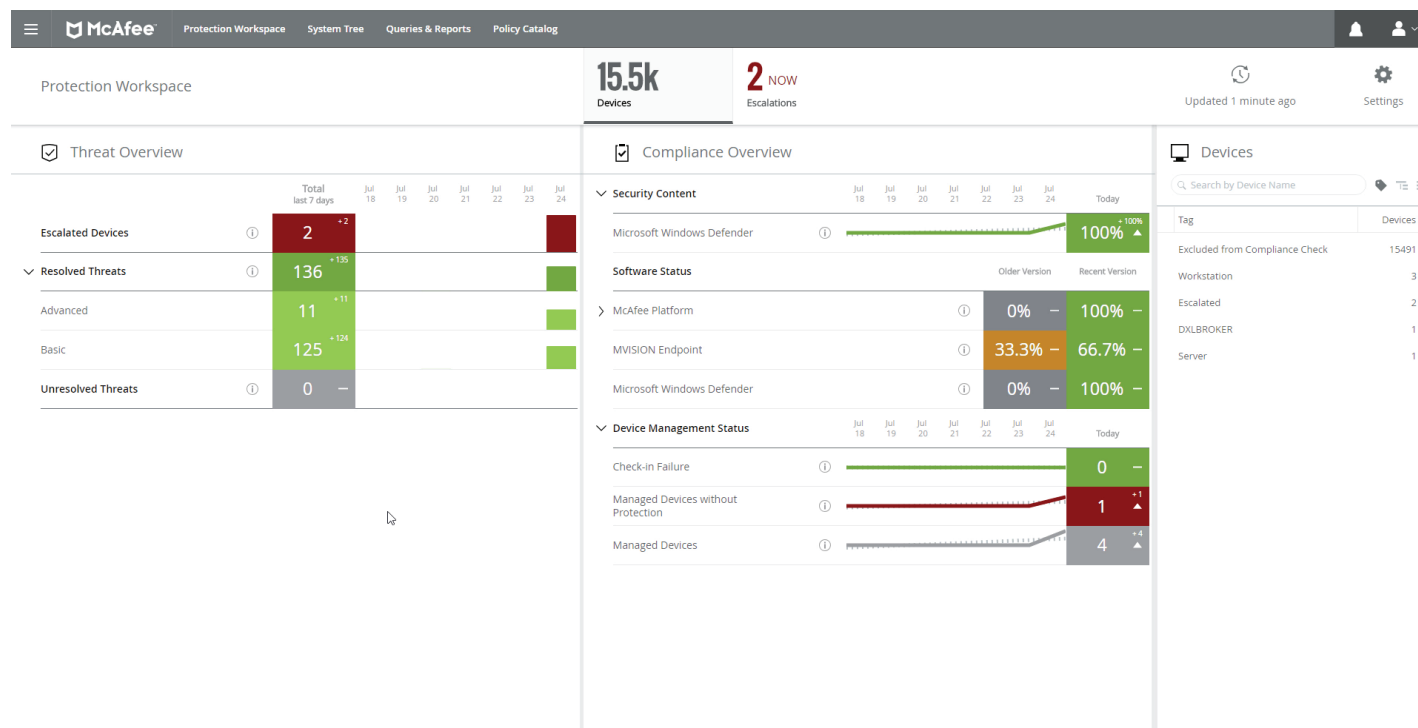


圖 1. McAfee ePO 防護工作區。

資料工作表

資料所需的時間，並減少因需要手動介入而可能發生的錯誤。McAfee MVISION ePO 是一項 SaaS 產品，因此無需設定和維護安全性基礎架構，讓您可以專責監控及控制所有裝置。持續性的平台更新，過程清晰透明。裝置安全性會在整個企業中自動部署，無需再花費人力為每個裝置手動安裝或更新安全性，可確保提供更強的威脅防禦執行力。McAfee MVISION ePO 以超過 36,000 位 McAfee ePO 軟體客戶的經驗追蹤記錄為基礎所設計，這些客戶都需要管理安全性、簡化與自動化符合性流程，並希望提升對企業中所有裝置的掌控。

提升威脅分析能力

McAfee MVISION ePO 為統一安全性管理而設計，可藉此達到更佳效率和效用。McAfee MVISION ePO 將風險管理和事件分析結合在一起，讓您的裝置可以為安全性資訊和事件管理 (SIEM) 解決方案提供重要見解，並確保您的分析人員可輕鬆取得重要資訊，協助改善威脅獵捕及修補作業。

廣泛的裝置安全性：管理原生安全性工具

McAfee MVISION ePO 的可擴充平台可管理多個裝置，包括含有原生控制項的裝置。McAfee 可提升與共同管理 Microsoft Windows 10 內建的安全性，以提供最佳化的防護能力，讓

組織也可以善加利用原生的 Microsoft 系統功能。McAfee MVISION ePO 可管理 McAfee MVISION Endpoint，其中結合了特別為 Microsoft 作業系統原生安全性調整的進階機器學習功能，此舉同時省去額外管理主控所產生的麻煩和成本。McAfee MVISION ePO 透過 Microsoft Windows 10 裝置和各個不同企業中所有裝置的共用原則，提供通用的管理體驗，確保操作簡易且一致。

自動化工作流程，更穩定、更省時

由 McAfee 於 2018 年委託的 MSI 研究發現，透過自動化重複性工作，組織預計每天能夠省下大約 25% 的時間。McAfee MVISION ePO 提供彈性的自動化管理功能，讓您可以從單一檢視迅速找出漏洞、安全性狀態的變更及已知威脅，並加以管理及做出回應。在這單一檢視中，您只要按下幾個連續步驟即可部署並執行安全性原則。

當管理員執行工作期間提供持續性內容，讓他們可以查看每個步驟以及步驟之間的關聯，省去麻煩而且減少發生錯誤的可能性。推送全新或更新原則之前，您可以選擇要求執行核准流程，以降低發生錯誤的風險並確保品質控管。

「McAfee ePO 引領整合式安全自動化與協調解決方案開發腳步。...當今的安全專業人員必須以簡化的體驗提供傳統 ePO 的效能，使其兼具高效率及效益...MVISION 是以 SaaS 形式提供的工作區，結合了分析、原則管理和事件，可適用於企業和中型市場。」

—IDC 安全性產品部研究副總裁
Frank Dickinson

資料工作表

關聯路由會根據環境、原則和工具中安全性事件的類型與嚴重性，給予警示和安全性回應。McAfee MVISION ePO 平台可讓您建立安全性與 IT 作業系統之間的自動化工作流程，以便快速修補問題。

常見使用案例

- 將原則部署至所有裝置，包括具有原生控制項的裝置，藉此維持一致性並節省時間。
- 藉由排定符合每位利益關係人需求的安全性符合性報告，可以節省時間，消除無謂且需要耗費大量人力的作業。
- 藉由同步 Microsoft Active Directory 與 McAfee MVISION ePO 主控台，讓您在新的裝置加入公司網路時，可以部署代理程式或機器學習安全性解決方案，來維護安全性狀態。

迅速緩解和修補

McAfee MVISION ePO 平台具有進階功能，可以提升安全性作業人員在緩解威脅或變更設定以回復符合性時的效率。

McAfee MVISION ePO 的自動回應可根據發生的事件自動觸發動作。動作可以是簡單的通知或是核准的修補。

自動回應的常見使用案例

- 根據預先設定的閾值以電子郵件通知管理員有新威脅、失敗的更新或高優先順序的錯誤
- 根據用戶端或威脅事件來套用原則，例如在主機遭到入侵時阻斷外部通訊（這會阻絕命令與控制活動）的原則，或封鎖資料外洩/向外傳輸，直到管理員重設原則為止
- 標記系統和執行額外的修補工作，例如在偵測到威脅時按指定掃描記憶體
- 以較多限制的原則自動隔離工作流程或容器（任何裝置）
- 標記系統後，升級狀態即會自動顯示在 Protection Workspace 儀表板上

主要功能

- 圖形式安全狀態儀表板
- 角色型存取控制
- 雙重驗證
- 自訂報告與查詢
- 零停機時間的升級作業
- McAfee® Endpoint Security 和 McAfee® VirusScan® Enterprise 適用的遷移輔助工具

McAfee 技術的特色和優勢將因系統設定而有所不同，並且可能需要啟用軟體或啟動服務。任何電腦系統皆非絕對安全。

McAfee 並未控制或稽核本文中提及的第三方基準資料或網站。您應造訪提及的網站並確認提及的資料是否準確。

McAfee 和 McAfee 標誌、ePolicy Orchestrator、McAfee ePO 及 VirusScan 是 McAfee, LLC 或其附設公司在美國及其他國家地區的高標或註冊商標。其他標誌與品牌可能為其各自擁有者的財產。Copyright © 2018 McAfee, LLC. 4076_0718

2018 年 7 月



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