McAfee ePolicy Orchestrator

啟發和強化安全性專業人員

安全性管理需要在工具和資料之間進行繁瑣的處理，通常對外部威脅的可見性不足。這使得對手處於優勢，因為對手會有更多的時間可以入侵工具之間隱而未現的落差並且造成更多損害。網路安全人力有限，因此需要強化才能因應複雜的網路安全環境。他們需要變得更為主動才能領先對手，而不是被動回應。

當管理階層需要看見安全性成效的證據時，貴組織需要對任何裝置類型上的威脅快速作出回應，以將損害降到最低。McAfee® ePolicy Orchestrator® (McAfee ePO™) 管理平台適用於內部部署和雲端環境 (有兩種模型可供選擇：SaaS 或 IaaS)，可省去耗時的工作並避免可能的人為錯誤，還可以主動協助安全管理人員加快回應速度及提升工作成效。McAfee® MVISION Insights 是 McAfee ePO 主控台獨有的首款技術，可在威脅與攻擊活動襲擊您之前主動排列其優先順序、預測您的對策是否可以遏止它們並同時精準描述您需要採取的威脅應對措施。

基本的安全性

我們先介紹必備功能。任何安全性架構的核心都是對裝置和系統健康狀況的監控能力。網際網路安全性中心 (CIS) 控制和測試基準以及美國國家標準技術研究院 (NIST) SP 800-53 安全性與隱私控制之類的業界標準，皆呼籲將監控和控制安全性基礎架構視為必要項目。McAfee ePO 主控台能讓您監看關鍵性的資料，協助您設定並自動執行原則，以確保整個企業維持健全的安全性狀態。您可以透過單一主控台，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。MVISION Insights 延伸模組提供主動式強化建議與功能，

主要優點

- 獲得業界肯定的集中式管理，整合的獨特單一窗口操作簡易，並且適用於雲端或內部部署環境
- 主動式可採取動作的情報讓您能領先對手
- 自動化工作流程簡化了管理工作並提升效率
- 開放式全方位平台整合 McAfee 和超過 150 個第三方解決方案，讓您更快做出更準確的回應
- 通用的安全性管理，適用於市面上大多數裝置類型
- 善用並提升 Windows Defender 等作業系統內建的原生控制項
- 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

還有可採取動作的情報。此必要的安全性管理功能是您 IT 法規遵循的基礎。

簡化進階安全性管理，而且經證實有效已簡化

目前已有超過 36,000 個企業和組織信賴 McAfee ePO 主控台，並採用它來管理安全性、簡化與自動化法規遵循流程，以及提升裝置、網路和安全性作業的整體可見性。大型企業仰賴 McAfee ePO 主控台具有高度擴充性的架構，使大型企業得以透過單一主控台管理數十萬計的節點。此儀表板檢視可協助您排定風險的優先順序，並在新的防護工作區中以單一圖形檢視方式為您提供整個數位領域的安全性狀態摘要。此外，借助 MVISION Insights，您可以獨家獲得對貴組織很重要的外部預期威脅的主動式檢視以及您需要採取的應對舉措的優先指引。如此可推進端點安全性，讓其變得更為主動，而不是被動回應，同時讓安全管理工作不再壓力重重。此外，還有一個「安全資源」區域，您可在此輕鬆取得最新威脅資訊和相關研究。

管理員可以深入檢視特定事件，以獲得額外的分析資訊。此摘要檢視可縮短建立與合理化現有資料的時間，並減少因需要手動介入而可能發生的錯誤。McAfee ePO 主控台簡化了企業安全管理人員的原則維護作業。此外，還加入運用 Data Exchange Layer (DXL) 的第三方威脅情報、使用我們領先業界的訊息網狀架構。同時將原則與各式各樣的產品進行雙向整合。這些作業效率可降低處理和共用資料的開銷，從而提升回應的速度和精準度。

支援中心旨在方便使用者存取 McAfee 產品資訊，並針對客戶環境的 McAfee ePO 伺服器運作狀態提供概觀。內部部署的 McAfee ePO 主控台和 Amazon Web Services (AWS) 上的 McAfee ePO 主控台皆適用。您可以主動接收支援與產品通知、搜尋 McAfee 內容存放庫，並在 McAfee ePO 主控台內存取最佳實務作法和說明等資源。您也可以輕鬆評估系統運作狀態，並接收有助於提升運作狀態的建議步驟，藉此管理 McAfee ePO 基礎架構的運行狀況。

產業分析師認為 McAfee ePO 軟體是客戶選擇和繼續使用 McAfee 的原因。

整合平台的優勢

相較於未建置整合式平台的組織，這些組織可以獲得更完善的防護和更迅速的回應時間。

已建置整合平台的組織

- 78% 的組織去年遭到入侵的次數不到五次。
- 80% 的組織在八小時內發現威脅。

未建置整合平台的組織

- 只有 55% 的組織去年遭到入侵的次數不到五次。
- 只有 54% 的組織在八小時內發現威脅。

(資料來源：2016 Penn Schoen Berland)

以開放式平台的效率克服日益猖獗的威脅

ESG 研究顯示，40% 的組織使用 10 到 25 項工具，而 30% 的組織使用 26 到 50 項工具來管理數十億的新威脅和裝置。使用多樣產品會提高從安裝到報告的單一管理體驗的複雜性，並大幅增加營運開銷。超過半數的組織預估可透過整合安全性工具節省超過 20% 的開銷 (資料來源：2018 年 MSI 研究)。

McAfee 接納了這些需求，並將開放式平台的方法應用在安全性管理，讓您得以整合擴充作業，同時保護種類繁多的資產、支援威脅情報、管理開放原始碼資料以及整合第三方產品。McAfee 對各種安全性產品之法規遵循和管理提供集中式控制。分析人員可以快速統合所有產品，從中找出關鍵的資料，並根據原則採取必要行動。McAfee ePO 主控台也允許您投入新一代技術，並透過單一架構與現有資產整合。

我們的開放式平台提供多種整合方法 (指令碼、應用程式開發介面 (API)、非 API 以及最有效率的開放原始碼 DXL 訊息網狀架構)，讓您選擇最符合需求的方法，而無需進行過多自訂或使用多種服務。透過 McAfee® Security Innovation Alliance 方案，我們加速開發可互通的安全性產品，簡化這些產品與客戶的複雜環境之間的整合作業，以及提供真正相互連接的整合式安全性生態系統，讓客戶現有的安全性投資能夠發揮最大效益。McAfee Security Innovation Alliance 方案目前整合超過 150 個合作夥伴。

此外，DXL 通訊網狀架構可橫跨多家廠商的產品以及內部開發與開放原始碼解決方案，來連接並最佳化安全性行動。您可以透過 Cisco pxGrid 和 DXL 的整合，存取來自其他 50 種安全性技術的資料。McAfee ePO 主控台是管理我們強大開放式平台的重要元件。

廣泛的裝置安全性：管理原生安全性工具

可擴充的 McAfee ePO 平台可管理許多裝置，包括含有原生控制項的裝置。McAfee 可提升並集中管理 Microsoft Windows 10 內建的安全性，提供最佳化防護，同時讓組織善加利用原生的 Microsoft 系統功能。McAfee ePO 主控台可管理 McAfee® MVISION Endpoint，其中包含特別為 Microsoft 作業系統 (OS) 原生安全性調整的進階機器學習功能，同時避免額外管理主控台增加複雜性和成本。McAfee ePO 軟體透過 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。

節省時間

此外，2018 年 MSI 研究也顯示，客戶相信若整合安全工具，將最多可節省 20% 的時間。

整合的價值

- 提升工具和流程的效益：61%
- 降低複雜性並減少手動工作，讓安全性專業人員專注於需要關鍵思維的工作：61%
- 以圖形和情境形式呈現資料可提升可見性：58%
- 簡化工作流程，加快回應速度：57%

(資料來源：2018 年 MSI 研究)

維持自動化工作流程中的一致性

McAfee ePO 主控台提供彈性的自動化管理功能，讓您可以從單一主控台迅速找出漏洞、安全計劃的變更和已知威脅，並加以管理及因應。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。

您可以在 McAfee ePO 軟體的單一檢視中，按下幾個展開邏輯步驟，即可輕鬆部署和強制執行安王性原則。單一窗口檢視模式可在您執行工作期間提供持續性內容，讓您查看每個步驟以及步驟之間的關聯，有助於降低複雜度，並將發生錯誤的可能性降到最低。您可以定義 McAfee ePO 主控台的運作方式，使其根據環境中安全性事件的類型與嚴重性以及您的原則和工具，給予警示和安全性回應。

如果要支援開發作業和安全性作業，您可以透過 McAfee ePO 平台來建立安全性與 IT 作業系統之間的自動化工作流程，以便快速修補問題。您可以使用 McAfee ePO 主控台來觸發 IT 作業系統的修補動作，例如指派更嚴格的原則。運用 Web 應用程式設計介面 (APIs) 減少人工作業。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。

從 MVISION Insights 取得獨特的主動式自動化工作流程：從常見角度而言，MVISION Insights 會依據行業與地理位置情報主動警示外部與未知的威脅和攻擊活動，並排列其優先順序。如此可讓您預先評估您目前的安全性狀態是否可以遏止該威脅。更為重要的是，還會提供特定的行動，例如更新 .DAT 或隔離威脅。

常見使用案例

- 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。
- 主動應對並獲取有關預期威脅的可採取行動的深入分析、如何在您所屬行業或地區追蹤它們、目前的安全舉措是否可以應對該威脅，如果不能的話則需要採取哪些措施，這些全都可以透過利用 MVISION Insights 來實現。
- 善用強大的 API 輕鬆整合 McAfee ePO 主控台與您現行的業務流程和功能，以獲得更多分析資訊並加速工作流程。舉例來說，McAfee ePO 主控台可與票證系統、Web 應用程式以及自助服務入口網站整合。
- 藉由同步 Microsoft Active Directory 與 McAfee ePO 主控台，讓您在新機器加入公司網路時，可以部署代理程式或機器學習安全性解決方案，來維護安全計劃。

「McAfee ePO [軟體] 引領**整合式安全自動化與協調解決方案的開發腳步。**...當今的安全專業人員必須以簡化的體驗提供傳統 [McAfee] ePO [軟體] 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

快速緩解和修補

McAfee ePO 平台具有內建的進階功能，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 ePO 主控台的自動回應功能可以根據發生的事件來觸發動作。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或簡訊通知管理員出現新威脅、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 (以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。
- 觸發已註冊執行檔來執行外部指令碼和伺服器命令，例如在服務台產生票證或整合到其他業務流程中。
- 以較多限制的原則自動隔離工作流負載或容器 (任何裝置)。

雲端型安全性管理

組織必須簡化並加速進階威脅解決方案的部署作業。雲端型安全性管理能降低內部部署基礎架構的成本和維護作業，讓不少組織都看見效率獲得改善。您可以隨時隨地透過兩種替代部署選項從雲端實作 McAfee ePO 主控台：AWS 上的 McAfee ePO 軟體或 McAfee® MVISION ePO™。兩者都能在一小時內啟用和運作。

- AWS 上的 McAfee ePO 軟體可讓組織運用許多原生 AWS 服務，例如自動擴充和 Amazon RDS，而不必購買和管理個別的資料庫。如此管理員就可以專注於處理關鍵的安全性工作，而非基礎架構。AWS 上的 McAfee ePO 軟體可管理 McAfee® Endpoint Security、McAfee® Data Loss Prevention、McAfee® Cloud Workload Security、DXL 以及整合至 McAfee ePO 軟體的第三方解決方案。
- MVISION ePO 充分利用 McAfee ePO 軟體即服務 (SaaS) 特性的優勢，可大幅簡化平台管理作業，讓您專心處理關鍵的安全性工作。提供持續性的平台更新，過程清晰透明。部署代理程式後，裝置安全性就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。如此一來，企業就可以透過單一主控台管理 McAfee MVISION Endpoint 和 DXL，不受地點所限。

「McAfee ePO 軟體在其他解決方案中獨樹一幟。是一站式的端點防護。讓我可以透過單一介面掌控我們所有的 McAfee 產品。易於使用的儀表板和內建功能，可讓使用者從檢視、報告、部署、更新、維護到決策，一切變得更加輕鬆。」

— Christopher Sacharok，資訊安全工程師，Computer Sciences Corporation

MVISION ePO 可讓您的裝置針對安全性資訊與事件管理 (SIEM) 提供重要見解，並確保分析人員可以輕鬆取得相關資訊，藉此改善威脅獵捕和修補作業。此外，現有的內部部署或混合雲端 McAfee ePO 軟體客戶如今可以快速輕鬆地移轉至 MVISION ePO，並充分利用 SaaS 型安全管理平台的諸多效率和優勢。

由 McAfee ePO 軟體管理的 McAfee 產品

McAfee 產品*
McAfee® Endpoint Protection (威脅防護、防火牆、Web 控制)
McAfee® MVISION Endpoint 為 Microsoft Windows Defender 提供進階威脅防護
McAfee® MVISION Mobile
McAfee® MVISION Insights
McAfee® Drive Encryption
McAfee® File and Removable Media Protection
McAfee® Active Response
McAfee® Management for Optimized Virtual Environments (McAfee® MOVE)
McAfee® Data Loss Prevention (McAfee® DLP)
McAfee® Policy Auditor
McAfee® Enterprise Security Manager
McAfee® Threat Intelligence Exchange
McAfee® Application Control
McAfee® Cloud Workload Security
McAfee® Advanced Threat Defense
McAfee® Content Security Reporter
McAfee® Database Activity Monitoring
Data Exchange Layer (DXL)

**適用於 McAfee ePO 軟體內部部署。*

彈性的部署

部署	主要優點
McAfee ePO 內部部署	全面掌控資料和功能集
AWS 的 McAfee ePO	免去內部部署解決方案所需的硬體維護作業
McAfee® MVISION ePO 軟體即服務*	多租戶 SaaS 產品完全不需要任何基礎架構和更新的維護作業

**McAfee MVISION ePO 僅提供部分 McAfee ePO 軟體功能。*

使用案例：McAfee ePO 主控台如何運用安全性集中式管理

產品與技術	使用案例	優點
MVISION ePO MVISION Endpoint Microsoft Windows 10	McAfee MVISION ePO 軟體可管理 McAfee MVISION Endpoint，透過進階防護加強 Microsoft Windows 10 的原生控制項。您可以透過通用管理平台以及一致的 Microsoft Windows 和 McAfee Endpoint Security 原則發現並管理進階威脅。	為 Microsoft Windows 的原生控制項提供更完善的防護能力，以及經證實更為有效的管理
McAfee ePO McAfee Endpoint Security	McAfee Endpoint Security 可探索端點上的已知惡意檔案。McAfee ePO 主控台在端點上設定較為嚴格的原則以便隔離惡意檔案。一切都可透過通用設定管理介面來完成。	迅速抑制受感染的端點
McAfee ePO McAfee Data Loss Prevention McAfee Enterprise Security Manager	McAfee Enterprise Security Manager 可偵測端點上重大的資料外洩，並在 McAfee ePO 主控台中加以標記。McAfee ePO 主控台套用資料外洩防護原則來封鎖資料，並針對此不符合法規遵循的行為提醒使用者。	資料外洩自動強制執行原則
McAfee ePO MVISION ePO McAfee Endpoint McAfee MVISION EDR McAfee MVISION Insights	McAfee MVISION Insights 可針對排列好優先順序的外部預期威脅提供可採取動作的資訊。MVISION Insights 圍繞 McAfee® MVISION EDR 提供了入侵指標 (IoC)，從而在目前調查中判定它們是否存在於環境之中。如果是，會在相關攻擊活動中提供詳細資訊以及您應採取的措施。	加速調查與解決

整合範例

產品與技術	整合式使用案例	優點
McAfee ePO McAfee Endpoint Security DXL Cisco Identity Service Engine (ISE) Cisco PxGrid	McAfee Endpoint Security 標示一個可疑的主機。McAfee ePO 主控台可觸發其他掃描，並且透過 PxGrid 傳送至 Cisco ISE 和 DXL 訊息交換 (透過 McAfee ePO 主控台)。Cisco ISE 可隔離主機，直到主機被視為可接受為止。	增強主動式保護
Rapid7 Nexpose McAfee ePO DXL	McAfee ePO 會與 Nexpose 共用資產清單，讓您可以透過 McAfee ePO 主控台瞭解風險狀態，並據此設定相關原則。漏洞資料會與 DXL 廠商社群共用。	▪ 降低複雜性 ▪ 透過單一儀表板即可全面又可靠地掌握資安態勢，同時排定行動的優先順序，藉此將風險降至最低
Check Point NGTX Check Point NGTP McAfee ePO DXL McAfee Active Response McAfee Enterprise Security Manager	此一整合可以促進網路和端點間的雙向即時情報共享。 相關事件也會分享到 DXL 社群。 Check Point Anti-Bot 軟體刀鋒會阻止指令與控制 (C&C) 流量並警示 McAfee ePO 軟體，同時還提供有關常見 DXL 主題的其他經整合的第三防安全解決方案。藉由這些情報，McAfee 便可以自動啟動相關的端點裝置修補工作流程。Check Point 和 McAfee 也可以偵測和防範零時差攻擊，無論攻擊來自網路或端點，都會轉化成已知攻擊。整合作業會透過即時交換關鍵任務情報，使得我們個別的產品能自動偵測、封鎖和修補威脅。	▪ 縮短偵測時間 ▪ 封鎖和修補攻擊

台灣
台北市信義區忠孝東路五段 68 號 29 樓，
11065
www.mcafee.com/tw

2020 年 6 月