McAfee MVISION Endpoint

Windows 桌面和伺服器的進階端點安全性

組織紛紛採用 Microsoft Windows Defender 這類原生安全性機制，為全功能端點安全平台 (EPP) 尋求更簡單經濟的替代方案。雖然 Windows Defender 提供必要的基礎級保護，但仍然需要採取機器學習等進階對策才能提供完整的防禦，以抵禦複雜的無檔案和零時差惡意軟體威脅。成功關鍵在於善用、強化及管理 Windows 桌面和伺服器環境[1] 所內建的安全性，同時又不產生多個主控台的複雜作業。McAfee® MVISION Insights[2] 在攻擊發生前提供主動的端點安全分析和行動，進一步強化您的安全性狀態。

在安全性與複雜性之間取得平衡

由於這些工具通常是分別管理，增強防護的代價是增加複雜性，這使得安全團隊陷入兩難的局面。通常這也表示將會與他們節省財務與營運成本的目標背道而馳。

更好的選擇：進階防護與集中式管理

有了 McAfee® MVISION Endpoint，您可以兼顧效力與效率，無需在兩者之間做出抉擇。您可以取得檔案、無檔案和行為的機器學習分析，進而為環境中的每個端點進行進階威脅偵測和集中管理。一致的集中式主控台可管理 Windows Defender 防毒軟體、Defender Exploit Guard、Windows 防火牆、McAfee 的防禦機制以及 Mac 或 Linux 系統的原則，免去應對複雜工作流程的麻煩。協同管理和統一管理原則不僅可以省去多餘的資料輸入時間，且能讓您更充分地掌握端點環境。

徹底提升您的防禦和防護能力

McAfee MVISION Endpoint 提供增強的偵測和修正功能，可加強原生安全性控制項，確保永遠保持最新狀態。舉凡機器學習、憑證竊取監控及復原修補，均可大幅提高 Windows 桌面和伺服器作業系統 (OS) 內建的基本安全性，並有效對抗進階的零時差威脅。要選擇投資在原生技術還是協力廠商技術是個棘手問題，而這種方法可以讓您調整和結合兩者的優勢，讓您不會再左右為難。更新您的安全性狀態，在攻擊發生前率先反制亟需優先處理的威脅，讓您的防護能力更上一層樓。

主要優勢

- **針對進階威脅提供進階防禦：**機器學習、憑證竊取防禦以及復原修補，可補強 Windows 桌面和伺服器系統的基本安全性功能。
- **不會增加複雜性：**透過單一原則和主控台管理 McAfee 技術、Windows Defender 防毒軟體原則、Defender Exploit Guard 以及 Windows 防火牆設定。
- **MVISION Insights：**提供現今領先業界的安全性情報解決方案，將情報化為實際行動，針對威脅程度高 (根據是否鎖定您的產業與地理位置) 的潛在持續惡意活動立即做出回應。MVISION Insights 會預測哪些端點缺乏對惡意活動的防護能力，並提供能有效提升偵測效果的引導式指南。

與我們聯絡

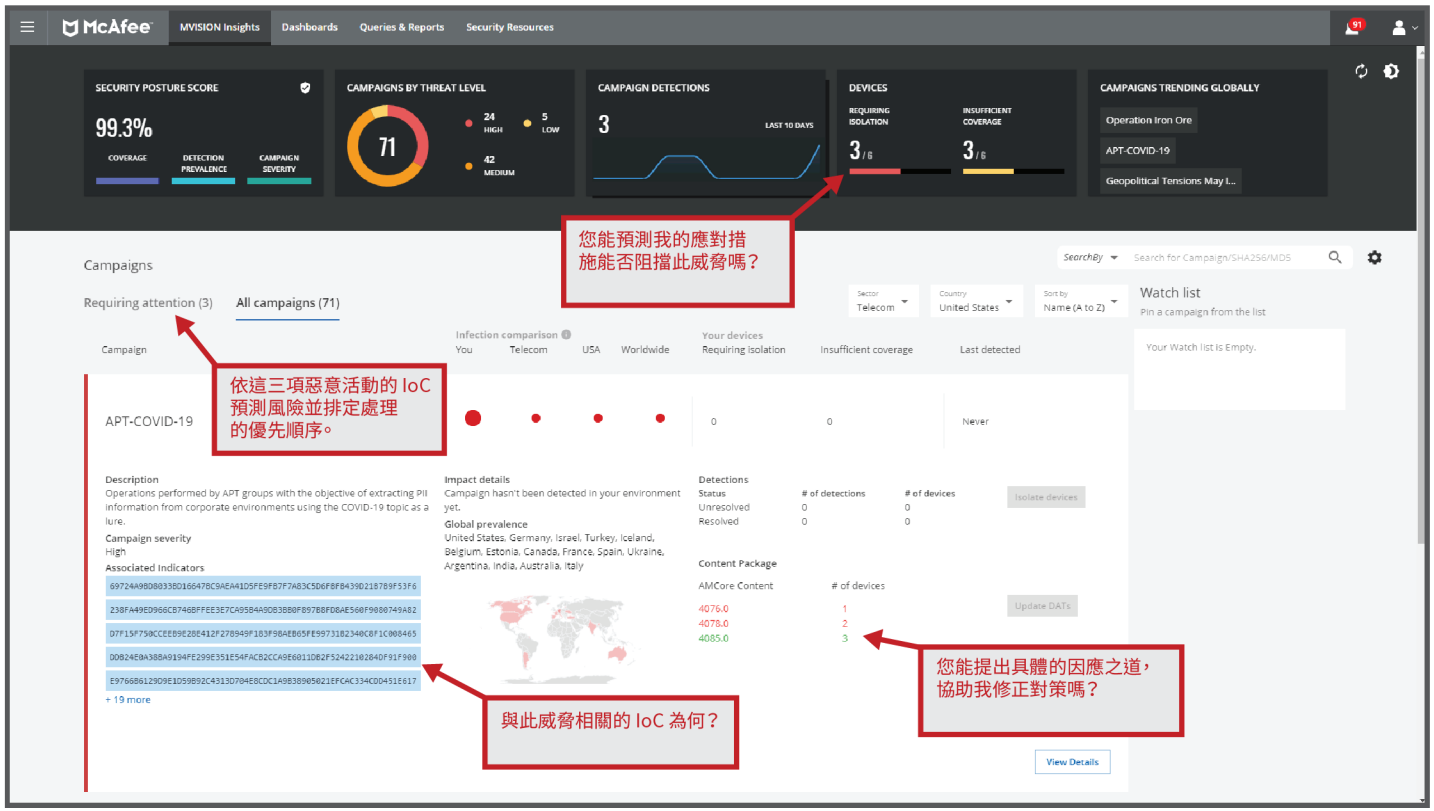

圖 1. MVISION Insights 的統合式儀表板能解答關鍵問題，提供主動的網路安全防護。

復原時間

McAfee 機器學習技術提供的偵測率遠遠高於單獨的特徵碼型防禦機制，其誤報率也較同業解決方案更低。這有助於管理員專注於處理環境中的真正威脅，而不是剔除非惡意威脅。

MVISION Endpoint 還能監控受可疑程序影響的檔案，並且將這些檔案還原至原始版本，以及刪除可能引進的其他惡意檔案或程序。對於使用者而言，這意味著他們可以在修補和復原期間同時維持生產力，而不是處理停機問題。對於管理員而言，這意味著他們可以減少重新製作映像或復原遭入侵端點所花費的時間，並將更多時間用於提高組織的工作效率。

善用、強化及管理 Windows 10、Windows Server 2016 和 Windows Server 2019 基本安全性的統一防禦機制

入門容易

- 立即檢視貴組織不容輕忽的威脅並採取行動。
- 將立即可用的原則套用至 Windows Defender 防毒軟體、將 Defender Exploit Guard 的管理作業簡化成最重要的規則，並將最佳做法規則設定套用至 Windows 防火牆。
- 使用現有的 McAfee 管理或利用 SaaS 型主控台快速部署。
- 使用 Story Graph 將威脅以及對其所採取的動作迅速視覺化，並判斷如何進一步強化您的端點，以抵禦日後遭受的攻擊。
- 小型用戶端讓下載更快更輕鬆。

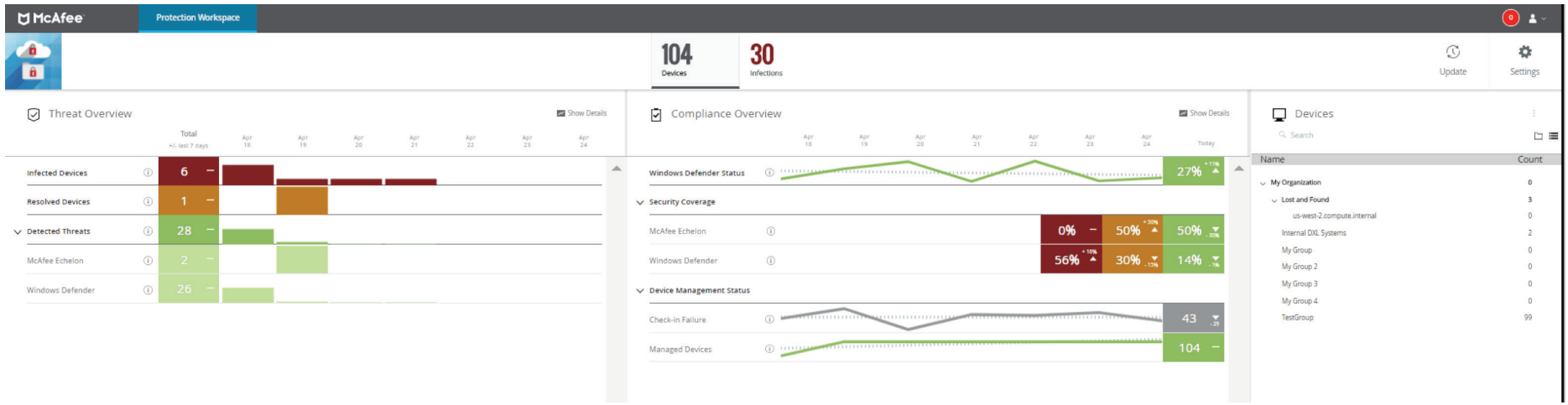

圖 2. 威脅防護工作區可讓您檢視 McAfee 和 Microsoft 技術之間的威脅和符合性。

提高可見性

MVISION Endpoint 可透過單一面板輕鬆管理，讓您全面掌握環境中的威脅和合規狀況，包括 BitLocker 相關報告。您不必在主控台之間來回切換，試圖串連起威脅事件的詳情、位置及處理方法，只要透過簡單易用的儀表板和可設定的警示，就能找到最重要的資料。

Story Graph 功能是一種額外工具，可簡化調查並協助管理員強化端點，以抵禦攻擊。這能針對偵測到威脅事件的動作提供追蹤資訊，讓使用者能審查這些動作，以便更進一步判斷造成威脅的原因。

管理的靈活度

MVISION Endpoint 提供以下選項：

- **單純的 SaaS 管理：**多租戶、可全域擴展，而且由 McAfee 維護。
  - *優點*：隨時隨地存取管理主控台，自動更新和管理維護，可降低整體擁有成本 (TCO)。
- **虛擬部署：**在 Amazon Web Services (AWS) 環境中部署管理，一小時內即可完全運作。
  - *優點*：善用虛擬化環境中的現有投資，降低部署和維護成本，同時保留自訂的控制項。
- **本機部署：**現場本機安裝在伺服器上的管理軟體部署。
  - *優點*：客戶可以使用現有部署並集中管理多項 McAfee 技術。

高效能的設計

MVISION Endpoint 透過雲端型服務提供大部分功能，因此體積十分小巧輕便，而且入門迅速，用戶端檔案也較小，因此下載時間短，也不會造成頻寬的負擔。

您的防禦機制在安裝後便不需要更新，系統日後會自動安裝更新，管理員無需採取任何動作。

透過預設平衡效能設定，您可以根據需求擴充運算能力和頻寬，而不必維持在始終開啟的狀態，此舉可以大幅降低對端點環境和使用者的影響。

為整體環境提供整合平台

自行攜帶裝置 (BYOD)、行動裝置和物聯網 (IoT) 裝置日漸盛行，許多組織都需要為其他作業系統和裝置類型提供防護。為了因應日趨繁複的環境，McAfee 已推出創新的 MVISION 技術，將我們對簡化管理、提升 Windows 安全性、行動以及 IoT 裝置安全的策略願景導入 McAfee 產品組合。

McAfee MVISION 技術針對裝置安全性採用雲端優先的方法，讓安全專業人員透過單點檢視平台和控管機制，全面管理 McAfee、協力協商和原生作業系統 (OS)。

有了 McAfee Device Security 產品組合，您的整個攻擊面就能獲得所需的保護，包括桌上型電腦、筆記型電腦、平板電腦、行動裝置、實體/虛擬伺服器、雲端工作負載和 IoT。

這項解決方案對您的企業有什麼幫助？

- 所有裝置集中管理
- 進階、檔案、無檔案和行為機器學習防禦機制
- 保護您的 Mac、Linux、IoT 和行動裝置
- 在攻擊發生前做好網路安全措施
- 降低整體擁有成本並簡化工作流程

選擇 McAfee 的原因

- 完成更多工作、效率更高、操作更簡單
- 業內唯一針對原生控制項提供整合式管理和預先調整的進階防禦的廠商
- 提供整個裝置環境的可見性
- 多方整合的大型開放式生態系統
- 截然不同的主動式端點安全

深入瞭解

如需詳細資訊，請造訪：www.mcafee.com/enterprise/zh-tw/products/mvision-endpoint.html。

1. Microsoft Windows 10、Microsoft Windows Server 2016 和 Microsoft Windows Server 2019 系統
2. 本文件內含開發中產品、服務和/或程序的相關資訊。文中所述的優勢會因系統設定而有所不同，而且可能需先啟用軟硬體和/或啟動服務，才能享有。McAfee 可單方面變更本頁面提供的所有資訊，恕不另行通知。若要取得最新的預測、排程、規格和藍圖，請聯絡您的 McAfee 業務代表。

本文所述之降低成本時間案例，旨在舉例說明具備最佳化組態和部署的特定 McAfee 產品如何影響日後成本並節省成本和時間。實際情況和結果會因組態和部署而有所不同。McAfee 不保證能降低時間或成本。

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

McAfee 和 McAfee 標誌皆是 McAfee, LLC 或其附設公司在美國及其他國家/地區的商標或註冊商標。其他標誌與品牌可能為其各自擁有者的財產。
Copyright © 2020 McAfee, LLC. 4496_0620
2020 年 6 月