Trellix Endpoint Security

適用於 Microsoft 環境的進階端點安全性

為全功能端點安全平台 (EPP) 尋求更簡單經濟的替代方案的組織，都紛紛採用 Windows Defender 這類原生安全性。雖然 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。成功的關鍵在於善用 Windows 10 中內建的安全性，並加強和管理其功能，又不會帶來多個主控台的複雜性。

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 Trellix Endpoint Security ，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。而一致且集中的主控台可管理 Windows Defender、Trellix 的防禦機制以及 Mac 或 Linux 系統的原則，讓您避免複雜的工作流程。協同管理不僅可以省去多餘的資料輸入時間，而且讓您更充分掌握端點環境。

徹底提高您的防護能力

Trellix Endpoint Security 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。機器學習、憑證竊取監控以及復原修補，可大幅提高 Windows 10 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。

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，可大幅提高 Windows 10 的基本安全性功能
- **不會增加複雜性：**針對 Windows Defender 和 Trellix 防禦提供集中式原則管理。

善用、強化和管理 Windows 10 基本安全性的統一防禦機制

復原時間

Trellix 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。

Trellix Endpoint Security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。

提高可見性

Trellix Endpoint Security 使用單一窗口進行管理，讓您全面掌握環境中的威脅和符合性的狀況。您不必從一個主控台轉至另一個，以串連威脅事件發生的內容、位置及方法，而是透過簡單易用的儀表板和可設定的警示，引導您找出最重要的資料。

管理的靈活度

Trellix Endpoint Security 提供以下選項：

- **單純的 SaaS 管理：**多租戶、可全域擴展，而且由 Trellix 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 Trellix 技術。

入門容易

- 開箱即用的原則適用於您的 Defender 環境。
- 使用現有的 Trellix 管理或利用 SaaS 型主控台快速部署。
- 小型用戶端讓下載更快更輕鬆。

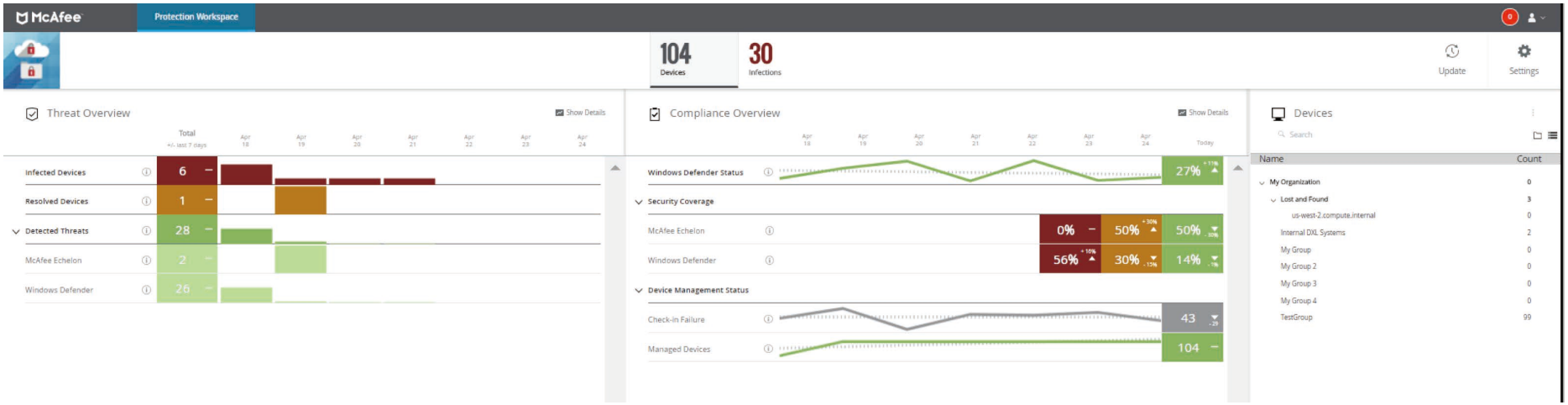

圖 1. 威脅防護工作區可讓您檢視 Trellix 和 Microsoft 技術之間的威脅和符合性。

高效能的設計

Trellix Endpoint Security 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，系統會自動安裝任何日後的更新，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。

Trellix 的一部分

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，Trellix 推出了 MVISION 這項全新的策略性服務以及創新的安全技術產品組合，以簡化管理、提升 Windows 安全性、機器學習以及擴大行動裝置的涵蓋範圍為主。

Trellix 技術產品組合為裝置安全性提供了雲端優先的方法，讓安全專業人員透過單點可見性和控管機制，全面管理 Trellix、協力協商和原生作業系統 (OS)。

借助 Trellix，您就能獲得整個攻擊面上所需的保護，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？

- 所有裝置的集中式管理
- 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
- 降低整體擁有成本並簡化工作流程

選擇 Trellix 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