資料工作表

McAfee Complete Endpoint Threat Protection

可抵禦複雜攻擊的進階威脅防護

主要優點

- 利用機器學習與動態遏止技術，持續搶先零時差威脅、勒索軟體及灰色軟體一步。
- 運用自動化行動與分析資料加快修補速度，並保護您的生產力。
- 透過集中化管理簡化您的環境、部署及長期管理作業。

貴組織所面對的威脅類型，讓您需要高可見性與各種工具才能採取動作，並全權控管完整的威脅防禦生命週期。也就是說，您的安全性專員必須獲得充足的功能，而這些功能必須以更高的精準度採取行動，且能提供對進階威脅的深度分析資訊。McAfee® Complete Endpoint Threat Protection 提供的進階防禦機制可調查、遏止零時差威脅與複雜的攻擊，並對這兩者採取行動。核心端點保護搭配整合式機器學習及動態遏止技術，能以近乎即時的速度偵測出零時差威脅，並在這些威脅感染您的電腦前，將其分類並加以阻擋。可行的鑑識資料與報告可讓您隨時瞭解狀況，並在您回應威脅爆發到調查並強化防禦機制期間一路協助您。此外，由於本產品為可擴充架構，因此不論是現在或未來，您皆可視需求與威脅態勢的演變，輕鬆新增其他的進階威脅防禦機制。

自動化的進階威脅防禦機制

您必須在進階威脅啟動之前便搶先阻止。而這就是我們在 McAfee Complete Endpoint Threat Protection 中加入動態應用程式遏制與 Real Protect[1] 技術的原因。偵測到惡意行為時，動態應用程式遏制會自動遏止灰色軟體與可疑的零時差威脅，避免您的系統受感染或使用者受影響。透過機器學習技術，Real Protect 可調查威脅並加以分類，同時儲存取得的分析資訊，以利日後自動採取行動。

intel Security

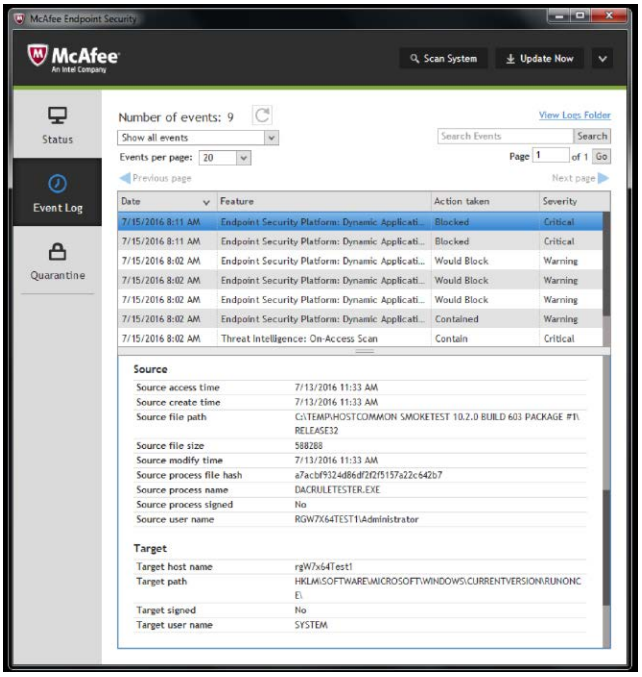

圖 1. 動態應用程式遏制根據嚴重性封鎖並遏止威脅。

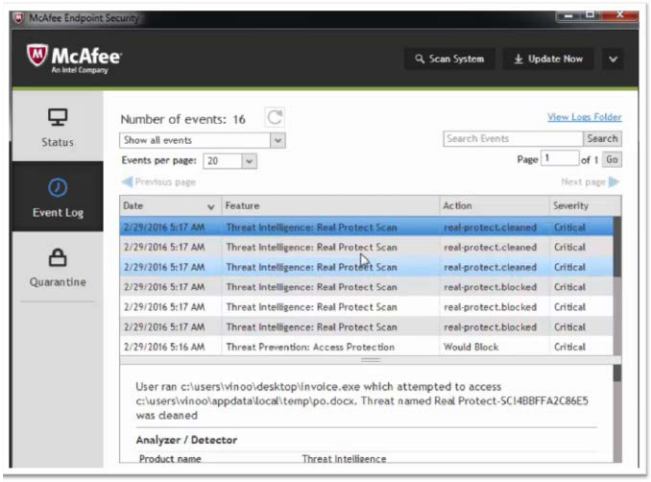

圖 2. Real Protect 運用機器學習技術，以近乎即時的速度偵測出零時差惡意軟體；特徵碼式掃描經常會遺漏這類惡意軟體。

為降低複雜性而生

複雜性是效率的大敵。現在您不必花時間試著管理有著不同介面和管理主控台的多種單點解決方案。要管理 McAfee Complete Endpoint Threat Protection，只需使用單一主控台：McAfee® ePolicy Orchestrator® (McAfee ePO™) 軟體。透過這個單一介面，您即可更快整備完畢、縮短部署時間並減輕持續管理的負擔。環境中有多種作業系統的客戶，將可藉由 Microsoft Windows、Apple Macintosh 及 Linux 系統的跨平台原則提高生產力。

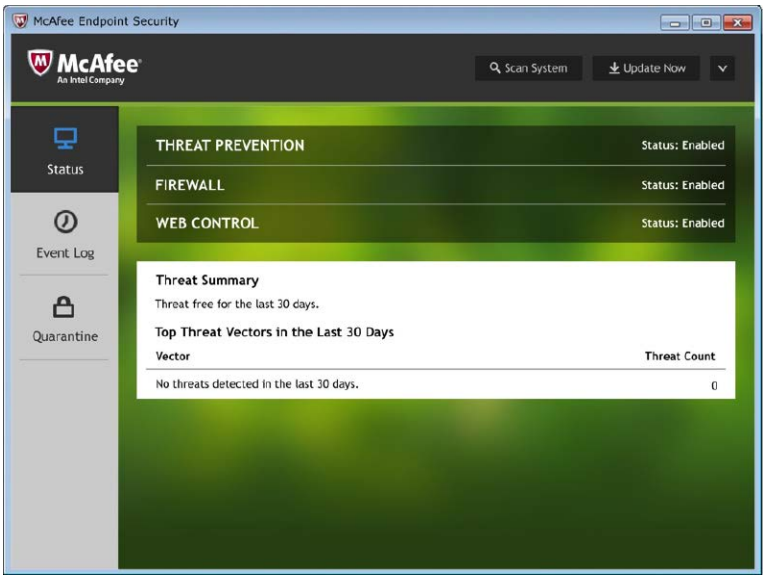

圖 3. 直覺式使用者介面讓管理員和使用者更輕鬆操作。

為現在與未來做好準備的靈活架構

McAfee Complete Endpoint Threat Protection 可提供您連結的協作架構以及運用多種防護技術、近乎即時的防護能力。這不僅讓您獲得更有力的威脅分析資料，也可讓收集而來的威脅鑑識資料與其他防禦機制共用，讓防禦機制變得更聰明。透過共用的通訊層，核心端點防護防禦機制即可在與進階威脅防禦機制合作的當下，對其發出通知並向其諮詢，以取得更有力的分析資料與判定結果。

而多虧了這個方式，部署作業也能更加靈活，讓您得以安裝目前所購買產品隨附的所有軟體。您可以決定目前和日後要設定與啟用的功能，並藉由原則變更輕鬆啟用之後要使用的功能。

最後，我們的架構可讓您依需求變動來擴展防護能力，而這要歸功於可包含額外技術的架構。

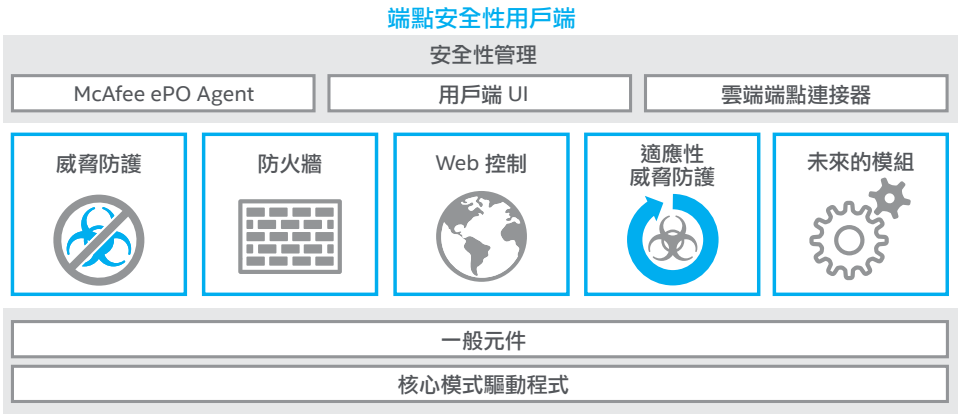

圖 4. McAfee 端點安全性用戶端架構。

元件	優點	客戶利益	獨到之處
動態應用程式遏制	防止灰色軟體對端點惡意地進行變更，藉此保護感染源。	• 增強防護能力卻不影響使用者或信任的應用程式。 • 縮短發現威脅到予以遏止的時間，且僅需極少人力介入。 • 保護感染源並隔離網路避免感染。	• 不論是否連線至網際網路皆可運作，且無須外部建議或分析資料。 • 使用者可清楚瞭解過程。 • 觀察模式可讓您立即掌握環境中的威脅乃至於潛在的入侵行為。
Real Protect	可套用機器學習的行為分類，在零時差威脅執行前即加以封鎖，並即時阻止已規避先前偵測的威脅執行。	• 輕鬆擊敗更多零時差惡意軟體，包括難以偵測的物件 (例如勒索軟體)。 • 無須人力介入即可自動取消遮罩、分析並緩解威脅。 • 可運用自動化分類與連結式安全性基礎架構調整防禦機制。	• 可偵測出透過動態行為式分析才能找到的惡意軟體。 • 深度整合可共用即時信用評價最新消息，並增強所有安全性元件的安全效力。
威脅防護	可運用多層防護機制快速尋找、凍結並修正惡意軟體的全方位防護。	• 阻止未知與已知惡意軟體使用啟發式、行為式及常駐掃描技術。 • 運用適用於 Windows、Mac 及 Linux 桌上型電腦與伺服器的防護機制，簡化原則與部署作業。 • 避免掃描信任的處理程序並優先處理可疑的處理程序，藉此提高效能。	多層式防惡意軟體可與 Web 及防火牆防禦機制協作，以提供更有力的分析資料與威脅防護效果。
整合式防火牆	保護端點，防範殭屍網路、分散式阻絕服務 (DDoS) 攻擊、不受信任的執行檔、進階持續性威脅和有風險的 Web 連線。	• 強制執行原則以保護使用者與生產力。 • 封鎖不需要的入埠連線並控制出埠請求以保護頻寬。 • 通知使用者目前有信任的網路、執行檔、具風險的檔案或連線，讓他們做好準備。	應用程式與位置原則可在筆記型與桌上型電腦不使用企業網路的狀況下，提供進一步防護。
Web 控制	利用 Web 保護與端點篩選功能，確保瀏覽網路時安全無虞。	• 在使用者造訪惡意網站前即先警告使用者，藉此降低風險與保護符合性。 • 授權或封鎖網站存取動作，以防止威脅並保護生產力。 • 在下載有危險的項目前即加以封鎖，藉此安全地阻止危險下載行為。	全面防護 Windows、Mac 及多種瀏覽器。
McAfee Data Exchange Layer	連結所有安全機制，以整合並簡化 Intel Security 與其他協力廠商產品之間的通訊作業。	• 整合可降低風險並縮短回應時間。 • 較低的營運開支與作業人員成本。 • 最佳化流程與實用建議。	在多個安全性防禦機制間共用最重要的威脅資訊。
McAfee ePO 管理	此單一介面適用於具高度延展性、靈活性且自動化的安全性原則管理作業，讓您找出安全性問題並做出回應。	• 可統一並簡化安全性工作流程，達到經實證的效率。 • 得以放心採取行動的更高可見性與彈性。 • 運用可自訂的原則強制執行快速部署和管理單一代理程式。 • 透過直覺式儀表板與報告，縮短從取得資料到做出回應的時間。	• 透過單一主控台更有效掌控、降低成本並更快進行營運安全管理作業。 • 經實證有效的介面已廣獲業界公認極為出色。 • 適用於廣大安全性生態系統的拖放式儀表板。 • 開放式平台有助於快速採用安全性創新技術。

支援平台

- Microsoft Windows：Windows 7、Windows To Go、Windows 8、Windows 8.1、Windows 10、Windows 10 November、Windows 10 Anniversary
- Mac OS X 10.5 版或以上版本
- Linux 32 和 64 位元平台：RHEL、SUSE、CentOS、OEL、Amazon Linux 及 Ubuntu 最新版本

伺服器：

- Windows Server (2003 SP2 或以上版本、2008 SP2 或以上版本、2012)、Windows Server 2016
- Windows Embedded (Standard 2009、Point of Service 1.1 SP3 或以上版本)
- Citrix Xen Guest
- Citrix XenApp 5.0 或以上版本

深入瞭解 McAfee Complete Endpoint Threat Protection 的優勢：**www.mcafee.com/tw/products/complete-endpoint-threat-protection.aspx**。

1. 此解決方案包含位於美國的託管資料中心，此資料中心可用來檢查檔案信用評價，以及儲存有關可疑檔案偵測結果的資料。即使沒有必要，動態應用程式遏制仍會透過雲端連線以最佳方式執行。完整的動態應用程式遏制與 Real Protect 產品功能皆須雲端存取權和主動式支援，且受雲端服務條款與條件的約束。

McAfee. Part of Intel Security.
台北市 110 基隆路一段
333 號 22 樓 2210 室
886-2-2757-6677
www.intelsecurity.com

2016 年 10 月