McAfee Endpoint Threat Defense and Response 系列

偵測零時差惡意軟體、保護感染源並對抗進階攻擊

要因應複雜性日益增加的網路威脅，就需要新一代的端點防護能力。不斷進階的威脅與未知漏洞所增加的風險，正使得組織將重疊且互相無連結的安全性解決方案拼湊在一起，但也只能提供有限的可見性且提高複雜度。而 Intel Security 利用 McAfee® Endpoint Threat Defense 與 McAfee Endpoint Threat Defense and Response 解決了這個問題。這兩種解決方案均利用靜態與行為式分析以及彙整情報來保護、偵測、修正及自我調整以對抗新型威脅。藉由共用的可見性、威脅情報及簡化的工作流程，以開放的整合方式，使安全性元件以整體的形式運作。連結的安全性機制與可行的威脅鑑識結果可提供安全的基礎架構，以快速又安心地判定威脅，並搶先潛在攻擊者一步。

主要優點

- 偵測、保護及修正防禦機制，同時主動加以調整以抵禦零時差惡意軟體、灰色軟體及勒索軟體。
- 使用動態信用評價、行為式分析及機器學習技術，更有效地保護。
- 透過增強型防護，將對使用者與受信任企業應用程式的影響降到最低。
- 透過在整個安全性生態系統中共用的威脅情報，更快對更多威脅做出回應並予以修正。
- 透過 McAfee® ePolicy Orchestrator® (McAfee ePO™) 軟體以統一的工作流程與適用於管理的單一主控台，簡化事件調查與修正作業。

擊敗零時差惡意軟體、灰色軟體及勒索軟體

透過利用了增強型信用評價與行為式分析資料的靜態與動態威脅分析，偵測出潛在入侵，藉此搶先新型威脅一步。利用 McAfee Threat Intelligence Exchange 套用彙整的情報，立即封鎖與遏止威脅，並即時更新威脅信用評價以預防日後的攻擊。

McAfee Endpoint Threat Defense 與 McAfee Endpoint Threat Defense and Response 可透過雲端查詢（於美國託管的資料中心）識別出現的惡意行為和 Real Protect 中廣泛的威脅模型間的相似性，以擊敗零時差惡意軟體。此行為分類技術可用來根絕目前的威脅，而這些威脅可能曾規避其他安全性軟體防禦機制。此技術會透過 McAfee ePolicy Orchestrator 軟體提供可行的威脅情報，以利進行零時差探索與即時修補。行為分類能透過動態機器學習技術自動演進，提供最大防護力與最高效率，同時又能限制安全性曝露程度。

intel Security

減少事件數量並更快解析威脅

藉由減少安全性事件的數量、自動判定更多威脅、共用情報及運用主動式警示定義自動回應，讓您能專注在最重要的事情。想要減少心力，就必須透過簡化的工作流程調查並解析威脅；而這類工作流程可更快解析事件並擴展安全機制能力，同時又能提高對整個組織的防護力。

連結的元件會透過 McAfee Data Exchange Layer 自動共用有價值的安全性資訊。McAfee Threat Intelligence Exchange 可讓彙整整個生態系統 (包括 McAfee Global Threat Intelligence 與其他協力廠商來源) 的完整威脅情報，並立即共用威脅資訊以自動調整防護機制。

保護感染源

偵測並阻止零時差惡意軟體惡意變更端點系統。動態應用程式遏制可監看灰色軟體的行為，並防止惡意變更，讓系統在入侵行為發生前就有效阻止。保護連線和離線端點，並利用隱形的防護機制遏止惡意行為。

運用安全性流程以擴充和調整

透過 McAfee ePO 軟體與單一介面管理主控台，全盤掌握所有系統，藉此簡化原則強制執行、事件調查及修補作業，讓您做好萬全準備來評估端點的安全計劃並即時實行防護機制。使用統一工作流程與單鍵式修補功能，減少在單一端點或整個基礎架構中監視、搜尋及回應的心力。McAfee Endpoint Threat Defense 與 McAfee Endpoint Threat Defense and Response 可運用自動化機器學習技術來更新行為分類模式，並可立即與所有安全性元件共用威脅情報，如此一來，這兩種產品便能以單一且統一的系統，防禦新型威脅。預防未來攻擊與運用預先設定的反應遏止潛在威脅，您便可釋出作業人員，讓他們專注在其他安全性管理優先要務。

揭露、排定優先順序及修正進階攻擊

McAfee Endpoint Threat Defense and Response 可協助您判斷攻擊的來源、範圍以及帶來的影響。該產品採用的 McAfee Active Response 技術，可讓您全盤掌握基礎架構中所有端點的即時和歷史情況。藉由強大的背景資訊可找出攻擊指標並予以排定優先順序，以加快回應速度。

以精準、快速又靈活的方式主動追捕，擊敗主動傳播、等待時機發動，或已抹除蹤跡而成功規避偵測的威脅。知識導向的可見性與控制項，可精準指出威脅嘗試立腳處，並讓您的應變人員立即遏止並予以修正，將曝露時程從數月縮減至數分鐘甚至數毫秒。

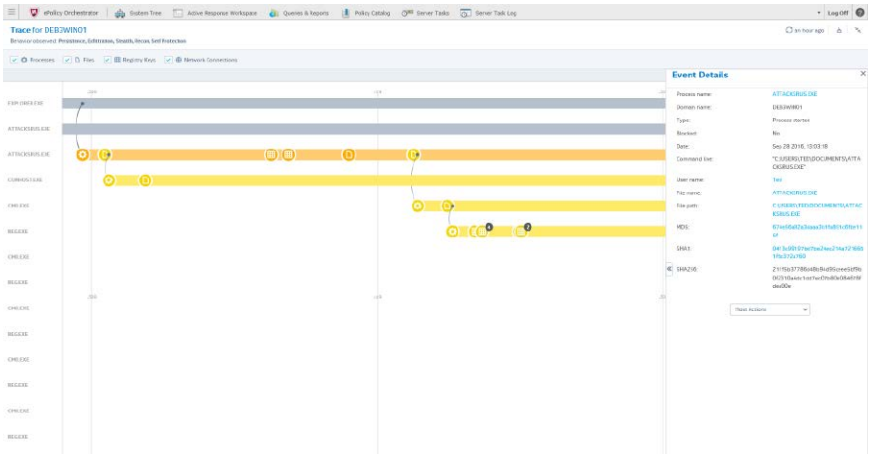

圖 1. 威脅工作區能追溯可疑事件的來源與行為，以加快事件回應速度。

McAfee Endpoint Threat Defense and Response 系列功能

元件	優點	客戶利益	獨到之處	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
動態應用程式遏制[1]	不論是連線或離線，都能防止灰色軟體對端點惡意地進行變更，藉此保護感染源。	• 確實分析潛在威脅又不必犧牲感染源。 • 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。 • 保護感染源又能同時保有端點生產力並隔離網路避免感染。	• 整合部分 Intel Security 基礎架構以提供最佳防護力與效率。 • 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，在零時差惡意軟體執行前即加以封鎖，並即時阻止已規避先前偵測的威脅。	• 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。	• 靜態與動態行為分析，可提供比單一階段方式更優質的防護。 • 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。	√	√

系列資料工作表

元件	優點	客戶利益	獨到之處	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
McAfee Threat Intelligence Exchange	連結安全性元件以共用背景資料，讓您全盤掌握整個組織的適應性威脅防護情況。	• 可進行感染源識別並立即在安全性系統中共用資訊，以預防下一次感染。 • 降低整體擁有成本並有效運用端點安全機制。 • 將獨立安全性技術轉換為協調的單一系統，藉此連結安全性元件以建立封閉迴路防護機制。	• 彙整 McAfee Global Threat Intelligence 摘要、協力廠商及本機情報。 • 透過本機或協力廠商情報，定義哪些是可信任與不可信任的資料。 • 立即連結端點、Web、網路及雲端產品的威脅信用評價資訊。 • 擷取可行威脅情報的詳細報告以調整防禦機制。	√	√
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。	• 降低風險與縮短回應時間。 • 較低的營運開支與作業人員成本。 • 最佳化流程與實用建議。	• 在所有安全性產品之間共用威脅資訊。 • 立即與其他所有端點共用感染源的威脅分析資料，以防止感染並更新防護機制。	√	√
McAfee ePO 管理平台	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。 • 所有系統的單一介面可見性，方便即時迅速地評估安全計劃與防護機制。 • 運用自訂的原則強制執行快速部署和管理 Intel Security 防護機制。 • 透過動態的自動化查詢、儀表板及回應機制，縮短從取得資料到做出回應的時間。	• 透過單一主控台更精細地掌控、降低成本並更快進行營運安全管理作業。 • 拖放式儀表板可提升整個生態系統的即時可見性。 • 開放式平台軟體開發套件可加快未來安全創新技術的採用速度。	√	√
McAfee Active Response	主動式威脅可見性、時間表、即時與歷史追捕以及偵測，皆可立即採取行動並調整防護機制。	• 快速搜尋即時和歷史威脅資料，以判斷攻擊的完整範圍、加快調查速度並縮短回應時間。 • 自動化威脅回應並提供即時安全防護，無須人力介入。 • 優先處理高優先順序的威脅。 • 使用持續性監控與可自訂收集器，深入搜尋攻擊的指標 (不只是正在執行或潛伏，甚至是過去可能已刪除的)。	• 立即掌握環境中防護技術未偵測到，而正在執行的未知入侵嘗試動作與具風險行為。 • 利用整合式即時搜尋調查所有端點中每個端點的事件時間表，以追捕威脅。 • 單鍵動作即可保護、修正及調整，減少單一作業中使用的多個工具與步驟。		√

規格

McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
支援的平台： • 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：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	**支援的平台：** • Microsoft Windows：Windows 7、Windows 8、Windows 8.1、Windows 10、Windows 10 Anniversary • RedHat 6.5 • CentOS 6.5 • Windows Server 2008、2012、2016

1. McAfee Endpoint Threat Defense and Response 包含位於美國的託管資料中心，此資料中心可用來驗證客戶真偽、檢查檔案信用評價、儲存有關可疑檔案偵測與追捕結果的資料。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 McAfee Active Response、動態應用程式遏制及 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。

深入瞭解

深入瞭解 McAfee Endpoint Threat Defense 的優勢：
www.mcafee.com/tw/products/endpoint-threat-defense.aspx。

深入瞭解 McAfee Endpoint Threat Defense and Response 的優勢：
http://www.mcafee.com/tw/products/endpoint-threat-defense-response.aspx。

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