McAfee Advanced Threat Defense

偵測進階鎖定式攻擊

McAfee® Advanced Threat Defense 可讓組織偵測到進階鎖定式攻擊，並將威脅資訊轉化成立即行動與保護措施。這項服務與傳統沙箱的不同之處在於它包含了額外的檢查功能，可以擴大偵測範圍，並使逃逸的威脅無所遁形。這項服務在安全性解決方案之間具有相當緊密的整合，涵蓋範圍包括網路到端點，所以能夠即時共享環境中的威脅資訊，藉此加強保護和調查能力。靈活的部署選項可支援所有網路。

我們的技術整合進階惡意軟體分析功能與既有的防禦機制 (涵蓋網路邊界和端點)，並與整個 IT 環境共用威脅情報，成功促成偵測作業轉型。我們的解決方案可透過管理、網路以及端點系統之間的威脅情報共享機制，立即關閉指令及控制通訊、隔離遭到入侵的系統、封鎖具有相同或類似威脅的其他執行個體，對可能受損的地方進行評估，並採取行動。

McAfee Advanced Threat Defense：偵測進階威脅

McAfee Advanced Threat Defense 透過創新的分層方法，可偵測到現今潛藏的零時差惡意軟體。結合低技術的靜態分析引擎 (例如防毒特徵碼、信用評價與即時模擬) 以及動態分析 (沙箱作業)，來分析實際行為。使用調查檔案屬性和指令集的深層靜態程式碼分析來繼續調查，以判斷意圖或規避行為，並評估與已知惡意軟體系列的相似性。作為分析的最後一步，McAfee Advanced Threat Defense 會特別尋找經由深層神經網路的機器學習技術而發現的惡意指標。結合上述所有功能，本產品具有市面上最強大的進階惡意軟體安全防護能力，更能有效兼顧深層檢查與效能需求。本產品一方面使用特徵碼和即時模擬這類分析強度較低的方法找出已知的惡意軟體，進而確保高效能，另一方面也為沙箱作業加入深層靜態程式碼分析和經由機器學習技術取得的分析資訊，針對高度偽裝、擅於規避的威脅提供更完善的防護。可能無法在動態環境中執行的惡意指標，可以透過解壓縮、深層靜態程式碼分析和機器學習分析來加以識別。

惡意軟體編寫者會以封裝方式改變程式碼的組成，或是藉此隱藏程式碼以躲避偵測。大多數產品都無法確實解壓縮整個原始 (來源) 可執行程式碼以供分析。McAfee Advanced Threat Defense 具備多重解壓縮功能，可去除模糊處理的手法；還可呈現原始可執行程式碼。這讓深層靜態程式碼分析可在高階檔案屬性以外發現異常情況，進而分析屬性和指令集以判斷預期行為。

McAfee Advanced Threat Defense 主要特色

與 McAfee 解決方案緊密整合

- 針對整個組織，縮短從遭受攻擊、遏止攻擊到提供防護等階段之間的時間差距。
- 簡化工作流程，加快回應和修補速度。

強大的分析能力

- 強化的解壓縮功能可提供更佳、更完整的分析。
- 結合深層程式碼分析、動態分析與機器學習，運用無可比擬的分析資料提供更精準的偵測功能。

靈活的集中式部署

- 可透過支援多種通訊協定的集中式部署降低成本。
- 靈活的部署選項可支援所有網路。

深層靜態程式碼、機器學習和動態分析結合後，將可完整而詳盡地評估可疑惡意軟體。無可比擬的分析輸出結果可產生摘要報告，提供更全面的瞭解以及行動優先順序；還可產生更詳盡的報告，提供分析師等級的惡意軟體資料。

增強保護

順利找到進階惡意軟體是很重要。不過，如果解決方案的功用僅止於提供報告或發出警示，管理員仍然必須親自處理大量工作，而網路還是無法受到保護。

無論在網路邊界或端點，McAfee Advanced Threat Defense 皆與安全裝置緊密整合，每當 McAfee Advanced Threat Defense 判定某一檔案懷有惡意時，整合的安全裝置便可立即採取行動。這種「偵測」與「保護」之間緊密且自動化的整合方式十分重要。

McAfee Advanced Threat Defense 可用不同方式進行整合：直接與特定安全性解決方案整合、透過 McAfee Threat Intelligence Exchange 整合，或是透過 McAfee Advanced Threat Defense Email Connector 整合。

直接整合之後，一旦 McAfee Advanced Threat Defense 判定檔案懷有惡意，McAfee 解決方案即可立刻採取行動。這能立即結合威脅情報與既有的原則執行程序，封鎖整個網路中相同或類似檔案的其他執行個體。

McAfee Advanced Threat Defense 的判定結果會顯示在整合後的產品記錄與儀表板上 (彷彿分析全程都在機上完成一般)，進而簡化工作流程，讓管理員可以在單一介面上工作，有效率地管理各種警示提醒。

整合 McAfee Threat Intelligence Exchange 後，McAfee Advanced Threat Defense 的功能得以延伸涵蓋其他防護產品 (包含 McAfee Endpoint Protection)，並允許多種整合式安全性解決方案存取分析結果與損害指標。若 McAfee Advanced Threat Defense 判定某一檔案有害，McAfee Threat Intelligence Exchange 會立即透過評價更新發佈威脅資訊，供組織內整合所有對策時參考。

端點啟用了 McAfee Threat Intelligence Exchange 之後，不僅可及時封鎖尚未造成災害的惡意軟體安裝程序，日後該惡意檔案再次出現時，也能提供主動防護。閘道啟用了 McAfee Threat Intelligence Exchange 之後，則可防止惡意檔案入侵組織。此外，若端點啟用了 McAfee Threat Intelligence Exchange，將能在離線時持續收到檔案判定的更新資訊，避免因承載傳送超出訊號範圍而形成防護死角。

McAfee Advanced Threat Defense Email Connector 讓 McAfee Advanced Threat Defense 能從電子郵件閘道取得電子郵件附件以便分析。McAfee Advanced Threat Defense 會在郵件標題內分析附件內的檔案，並向轉寄電子郵件閘道傳送裁定結果。這樣電子郵件閘道就可採取基於原則的行動，例如刪除或隔離附件，以避免惡意軟體感染內部網路或在其中傳播。 為了加強對電子郵件伺服器的偵測，McAfee Advanced Threat Defense 藉由 McAfee Threat Intelligence Exchange 整合了 McAfee Security for Email Servers。

整合式解決方案

- McAfee Active Response
- McAfee Advanced Threat Defense Email Connector
- McAfee Enterprise Security Manager
- McAfee ePolicy Orchestrator® 軟體
- McAfee Network Security Platform
- McAfee Threat Intelligence Exchange
  - McAfee Application Control
  - McAfee Endpoint Protection
  - McAfee Security for Email Servers
  - McAfee Server Security
- McAfee Web Gateway

尋找及修正受到入侵的系統

若要修復攻擊，組織需要全面且清晰的情報，其不僅清楚標示優先順序，更能化為具體行動，以便管理員擬定更完善的決策，並根據實際情形做出適當回應。McAfee 的各解決方案均可相互搭配，提供完全符合組織需求的產品。

McAfee Enterprise Security Manager 會使用 McAfee Advanced Threat Defense 和其他安全性系統提供的詳細檔案評價及執行事件並建立關聯性，據以提供進階的警示提醒和歷程記錄，進而統整為安全性情報、排定風險優先順序，並促進即時情境感知。當 McAfee Advanced Threat Defense 發出資料受到危害的警示時，McAfee Enterprise Security Manager 會追查過去六個月所保留的任何網路或系統資料，試圖找出這些惡意產物留下的蹤跡，揭露系統與新發現的惡毒軟體來源在這段期間曾有過的互動行為。McAfee Enterprise Security Manager 可讓您清楚瞭解風險，進而立即採取更正動作 (包含互動式及自動化的行動)。緊密整合 McAfee Endpoint Protection、McAfee Threat Intelligence Exchange 及 McAfee Active Response，可透過環境監控和行動，充分改善安全性回應強度和效率，例如發佈新設定、實作新原則、移除檔案及部署軟體更新，進而積極降低風險。當整個網路中受感染的端點都可由 McAfee Active Response 自動找出，並列於 McAfee Advanced Threat Defense 的報告中，便可輕鬆因時制宜採取適當行動。

部署

靈活的進階威脅分析部署選項可支援所有網路。McAfee Advanced Threat Defense 可作為內部部署裝置或虛擬機型。所有機型均可當作多項 McAfee 解決方案之間的共用資源，以符合成本效益的方式擴充並降低成本。

安全性作業中心與惡意軟體分析師也能使用 McAfee Advanced Threat Defense 執行各種調查。

McAfee Advanced Threat Defense 提供多種進階功能，包括：

- 可設定作業系統及應用程式支援：使用特定環境變數制訂分析影像，以驗證威脅和支援調查。
- 使用者互動模式：讓分析師可以直接與惡毒軟體樣本進行互動。
- 強大的解壓縮功能：以往動輒耗費數天的調查作業，現在只要幾分鐘的時間即可完成。
- 完整的邏輯路徑：強制執行其他潛伏在常見沙箱環境中的邏輯路徑，讓樣本分析內容更加透徹深入。
- 將樣本提交至多種虛擬環境：判定執行檔案所需的環境變數，以加快調查速度。
- 報告內容詳盡完善，包括反組譯碼輸出與記憶體傾印至圖像式函式呼叫圖解和內嵌或已卸除的檔案、使用者 API 記錄檔，以及 PCAP 資訊：提供相關的重要資訊，供分析師進行調查。

如需有關 McAfee Advanced Threat Defense 的資訊或是想要開始評估，請連絡您的代表人員或造訪 **www.mcafee.com/tw/products/advanced-threat-defense.aspx**。

資料工作表

McAfee Advanced Threat Defense 規格		
實體機型	ATD-3100 1U 機架安裝	ATD-6100 1U 機架安裝
虛擬機型	v1008、v1016、v3032、v6064 ESXi 5.5、6.0	v1008、v1016、v3032、v6064 ESXi 5.5、6.0
偵測		
支援的檔案樣本類型	PE 檔案、Adobe 檔案、Microsoft Office 套件檔案、影像檔案、封存檔、Java、Android 應用程式封裝、URL	
分析方法	McAfee Anti-Malware Engine、GTI 信用評價 (檔案/URL/IP)、Gateway Anti-Malware (模擬與行為分析)、動態分析 (沙箱作業)、深層程式碼分析、自訂 YARA 規則、機器學習: 深層神經網路	
支援的作業系統	Windows 10 (64 位元)、Windows 8.1 (64 位元)、Windows 8 (32 位元/64 位元)、Windows 7 (32 位元/64 位元)、Windows XP (32 位元/64 位元)、Windows Server 2016、Windows Server 2012、Windows Server 2012 R2、Windows Server 2008、Windows Server 2003、Android Windows 作業系統支援皆提供所有語言版本。	
輸出格式	STIX、OpenIOC、XML、JSON、HTML、PDF、純文字	
提交方式	單點產品整合、RESTful API、手動提交以及 McAfee Advanced Threat Defense Email Connector (SMTP)	

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

2017 年 8 月