McAfee Advanced Threat Defense

偵測進階鎖定式攻擊。

McAfee® Advanced Threat Defense 屬於 Intel Security® 產品的供應項目，這項服務讓組織能夠偵測到進階鎖定式攻擊，並將威脅資訊轉換為立即的行動和保護。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 Intel Security 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功能。

McAfee Advanced Threat Defense 主要特色

緊密的 Intel Security 解決方案整合

- 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。
- 結合進階靜態程式碼與動態分析，運用無可比擬的分析資料提供更精準的偵測功能。

集中式惡意軟體分析

- 透過共用分析結果，以符合經濟效益的方式減少整個網路所需的裝置數目。
- 簡化的部署方式。

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。而且結合了低技術防毒特徵碼、信用評價、即時模擬防禦、深層靜態程式碼與動態分析 (沙箱作業)，藉此分析實際行為。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，更能有效兼顧防護與效能需求。

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新增全靜態程式碼分析功能，針對高度偽裝、擅於規避的威脅提供更完善的防護。這可提供詳細的惡意軟體分類資訊，並利用程式碼重複使用功能，找出相關的惡意軟體。延遲或無法預期的執行路徑等沙箱規避技術通常不會在動態環境中執行，但可透過解壓縮與全靜態程式碼分析加以偵測。

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。本產品採用靜態程式碼分析，不僅能夠在高階檔案屬性以外區域尋找異常狀況，更可分析所有屬性和指令集，藉此判斷預期行為。

McAfee Advanced Threat Defense 結合靜態程式碼和動態分析，完整而詳盡地評估可疑惡意軟體。

intel Security

整合式解決方案

- McAfee Email Gateway
- McAfee Enterprise Security Manager
- McAfee ePolicy Orchestrator
- McAfee Network Security Platform
- McAfee Next Generation Firewall
- McAfee Threat Intelligence Exchange
- McAfee Web Gateway

目標鎖定式沙箱作業可提高偵測準確性

管理員可透過自訂虛擬機器或金級圖像集合上傳與分析物件，讓組織在面對實際主機設定檔 (而不是憑藉一般印象) 的情形下分析威脅，進而提供更精準的風險評估。

由於組織可能在同一網路中擁有多個主機設定檔，因此 McAfee Advanced Threat Defense 會先查詢 McAfee ePolicy Orchestrator® (McAfee ePO™) 軟體，判斷主機的作業系統和應用程式清單，接著再分析目標主機下的可疑檔案。

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 可以透過兩種方式進行整合，其一是直接整合特定安全性解決方案，其二是透過 McAfee Threat Intelligence Exchange 間接整合。

直接整合之後，一旦 McAfee Advanced Threat Defense 判定檔案懷有惡意，Intel Security 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。

尋找及修正受到入侵的系統

若要修復攻擊，組織需要的解決方案必須要能提供全面且清晰的情報，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 Enterprise Security Manager、McAfee Endpoint Protection 和 McAfee Threat Intelligence Exchange 可協同運作，提供組織需要的防護。

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。這能監視端點事件基準，對重大偏差和既定閥值隨時採取行動，同時調整使用者和資產風險。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 與 McAfee Threat Intelligence Exchange 有助於採取各種更正動作，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。

部署

McAfee Advanced Threat Defense 是採取集中部署的進階惡意軟體分析裝置，可與您現有的 McAfee 安全性投資完美整合。McAfee Advanced Threat Defense 可當作多個 Intel Security 裝置之間的共用資源，以符合成本效益的方式在網路中擴充。安全性運作中心與惡意軟體分析師也能使用 McAfee Advanced Threat Defense 的手動輸入選項執行各種調查。有了強大的解壓縮功能，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。McAfee Advanced Threat Defense 的摘要報告有助於廣泛瞭解威脅資訊與行動的優先順序，而解析輸出、圖形式功能呼叫流程圖，以及內嵌或外顯的檔案資訊等其他詳細報告，則能提供分析調查所需的重要資訊。

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

McAfee Advanced Threat Defense 規格	ATD-3000	ATD-6000
外觀尺寸	1U 機架安裝	2U 機架安裝
效能	每天最多 150,000 個物件	每天最多 250,000 個物件
偵測	ATD-3000/ATD-6000	
支援的檔案/媒體類型	PE 檔案、Adobe 檔案、Microsoft Office 套件檔案、封存檔、Java、Android 應用程式封裝	
分析方法	McAfee Anti-Malware Engine、McAfee GTI 檔案信用評價、Gateway Anti-Malware (模擬與行為分析)、動態分析 (沙箱作業)、靜態程式碼分析	
支援的作業系統	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 2003、Windows Server 2008 (64 位元)；Android	

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