McAfee Deep Defender

超越作業系統的安全，可揭露及消除隱藏的威脅

隱形的惡意軟體已成爲首選的網路犯罪工具，愈來愈多新的和未知的惡意軟體使用 Rootkit 等掩飾的技巧。罪犯依賴這種低階程式碼逃避作業系統 (OS) 型的保護。McAfee® Deep Defender™ 透過 McAfee® DeepSAFE™ 技術支援的業界新一代輔以硬體的安全保護，協助阻擋這些攻擊。這種即時核心作業的行爲監控揭露並移除先進的隱形攻擊。McAfee Deep Defender 與 McAfee ePolicy Orchestrator® (McAfee ePO™) 軟體和 McAfee Global Threat Intelligence™ (McAfee GTI™) 整合，很容易就能夠將系統安全延伸到作業系統 (OS) 之外，確實預防隱藏的零時差威脅。

主要特色

- 核心層級行為監控，可揭露並移除未知威脅（包括 Rootkit），搶先零時差惡意軟體一步
- 與 Intel 前所未有的整合，常駐在記憶體和作業系統之間，執行即時的記憶體和 CPU 監控
- 使用 McAfee ePO 軟體管理，以進行高效率的部署、集中式原則管理、提高的威脅可見性和整合的報告
- 移除傳統作業系統型保護偵測不到的低階威脅，降低重新製作映像和修補成本，以及增強整體安全
- 隱形惡意軟體正逐漸增加：McAfee Labs™ 每一季發現將近 110,000 個獨特的新 Rootkit

企業端點很容易遭到隱形惡意軟體的危害，隱形惡意軟體能夠巧妙避開防毒和其他作業系統型的防禦。罪犯設計這種低階惡意軟體來入侵作業系統固有的安全弱點、隱藏本身的存在，讓系統在開機時似乎一切正常。

隱形的惡意軟體可隨心所欲地散播感染、停用對策，以及竊取網路認證或機密資訊。還原受危害的端點需要完整重新製作映像，每次事件都要 IT 和一般使用者暫停生產性工作數小時。

超越作業系統

McAfee 和 Intel 合作，使用在 CPU 和作業系統之間作業的輔以硬體的保護來打擊這些攻擊，保護常駐在實體記憶體中的元件。McAfee Deep Defender 會在驅動程式和其他軟體運作時獲得可靠的檢視，而且可以偵測和清除在作業系統之前、期間和之後載入的威脅。

即時記憶體和 CPU 監控

McAfee Deep Defender 運用 McAfee DeepSAFE® 技術 (在 VMX 根模式執行的記憶體軟體層)，提供即時核心記憶體和 CPU 事件防護，將效能影響降至最低。

此一低階可見性可讓 McAfee Deep Defender 辨識隱形惡意軟體使用的難以捉摸的技術，並讓管理員得以即時檢視記憶體處理程序、執行可設定的封鎖或拒絕動作。如果 Rootkit 或隱形惡意軟體作用中，McAfee DeepSAFE 會捕獲修改核心的嘗試。

真正的零時差保護

McAfee Deep Defender 不需要事先學習 Rootkit 相關知識，就能偵測它的存在。McAfee Deep Defender 會識別其惡意行爲，提供真正的零時差防護。

McAfee Deep Defender 會在 Rootkit 還來不及隱藏惡意軟體之前即提供保護。它的核心和記憶體保護包括：

- 預防和記錄寫入系統中斷描述表 (IDT) 和系統服務配送表 (SSDT) 的嘗試
- 防止變更處理程序系統轉換表
- 預防修改直接核心物件操作 (DKOM) 清單和執行緒
- 消除核心模式驅動程式的惡意附件
- 禁止惡意內嵌攔截核心程式碼區段與主要裝置驅動程式
- 防止惡意修改驅動程式的匯入位址表 (IAT) 攔截

「關於 *Stuxnet* 和 *Zeus* 等隱形惡意軟體，其中一件最應該瞭解的重要事項是，它真正擁有它所接管的電腦。透過在使用者和核心與韌體層級作用的 *Rootkit*，惡意軟體可以隱藏、複製、保護自己防止被覆寫及停用防毒和其他防禦。」

- David Marcus，McAfee Labs 與 Thom Sawicki，Intel，隱形犯罪軟體的新現實，http://www.mcafee.com/tw/resources/white-papers/wp-reality-of-stealth-crimeware.pdf

系統需求與規格

- 支援 Intel® Core i3、i5 和 i7 處理器
- 支援 Microsoft Windows 7 (32 位元和 64 位元)
- 2 GB RAM (32 位元) 或 4 GB RAM (64 位元)
- 由 McAfee ePO 軟體 4.5 或以上版本管理
- 在 BIOS 中啟用 Intel 虛擬化技術 (VT, Virtualization Technology)
- 國際化與當地語系化，以部署至全球

通過測試，可與下列 McAfee 產品相容：

- McAfee VirusScan Enterprise 8.7 或以上版本
- McAfee Application Control 5.x
- McAfee Endpoint Encryption for PC 5、5.2.6、5.2.9 和 6.1
- McAfee Host DLP 9.x
- McAfee Host Intrusion Prevention 8.x
- McAfee Network Access Control 3.2

- 防止惡意修改核心匯出位址表 (EAT)
- 防止來自裝置驅動程式的惡意 I/O 呼叫
- 偵測惡意變更驅動程式配送常式

運用 McAfee GTI 偵測及刪除已知和未知的威脅

McAfee Deep Defender 會報告、封鎖、隔離和移除核心中已知和未知的惡意軟體。您現有的 McAfee VirusScan® Enterprise 防惡意軟體運用 McAfee Deep Defender 的清除功能，完全清潔受影響的使用者模式元件。

針對可疑或未知的惡意軟體，McAfee Deep Defender 會傳送程式碼的指紋至 McAfee GTI 網路，以報告及確認其身分。已確認的惡意軟體指紋會加入 McAfee GTI 資料庫，將立即防護延伸至其他 McAfee GTI 已啓用端點，包括您的場所的其他端點。

使用 McAfee ePO 集中管理

McAfee Deep Defender 可在不增加管理費用的情形下加強您現有的防護。現在執行 McAfee 端點軟體的個人電腦和筆記型電腦可以使用現有的 McAfee ePO 代理程式和管理基礎架構，在整個企業內支援的系統上部署 McAfee Deep Defender。

熟悉的 McAfee ePO 主控台使得部署 McAfee Deep Defender 即時記憶體動作的原則變得相當簡便。安裝 McAfee Deep Defender 之後，McAfee ePO 儀表板和報告即可提供隱藏性威脅的可見性。

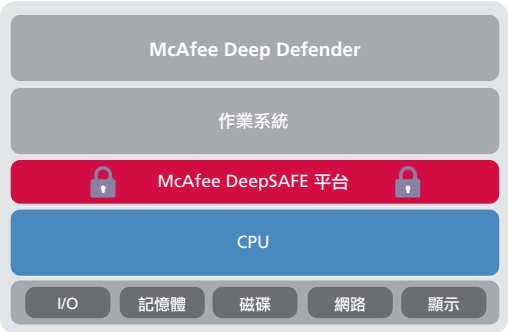

圖 1. McAfee Deep Defender 運用常駐在 CPU 和作業系統之間的 McAfee DeepSAFE 技術，在面 對威脅時佔有新的優勢。

立即開始揭露隱形惡意軟體

只在作業系統中起作用的防禦無法偵測或揭露現今老練的網路罪犯使用的先進規避技巧。McAfee Deep Defender 使用重大的增量防護輔助傳統的端點安全，以抵禦這些威脅。

採用相當容易，因爲 McAfee Deep Defender 利用便利的集中式 McAfee ePO 管理環境，並強化 McAfee VirusScan 防惡意軟體引擎和 McAfee GTI 網路提供的防護。

若要深入瞭解，請至 www.mcafee.com/tw/products/deep-defender.aspx。

McAfee
104 台北市
南京東路三段 132 號 4 樓 A2 室
886-2-2721-7766
www.mcafee.com/tw

35301ds_deep-defender_1011_fnl_ETMG