McAfee Network Threat Behavior Analysis

取得網路行為與威脅的完整分析報告

McAfee® Network Threat Behavior Analysis 提供網路基礎架構的即時分析報告。它會運用 Cisco 網路流量資料，在比入侵預防系統 (IPS) 涵蓋範圍更廣範的範圍中，識別並刻畫出威脅的特徵。McAfee Network Threat Behavior Analysis 在分析來自 Cisco 交換器與路由器的流量後，即可準確指出在網路中特定點遇到的危險行爲，並有效地預防內部與外部威脅。McAfee Network Threat Behavior Analysis 可快速查詢檢視透過各種媒介傳播的複雜攻擊和混合型威脅。它可完整評估網路層級的威脅、識別每個網路元素的整體行爲，以及能夠即時找出潛在的異常或攻擊類型，包括分散式阻絕服務 (DDoS)、殭屍網路 (Botnet) 或蠕蟲病毒。

McAfee Network Threat Behavior Analysis 裝置配備完整的四核心處理器、RAID 磁碟陣列及超高速乙太網路連線，並且提供離線的儲存區域網路 (SAN) 連線。由於它所允許的流量較大，因此可以處理大量的網路流量，加快流量分析。

McAfee Network Threat Behavior Analysis 可與 McAfee Network Security Platform IPS 緊密整合，這有助於透過 McAfee Network Security Manager 進行 McAfee Network Threat Behavior Analysis、McAfee Network Access Control (McAfee NAC) 與 IPS 偵測器的一般管理。

McAfee Network Threat Behavior Analysis 可藉由分析未經授權的應用程式使用和使用者行爲事件，更嚴格地落實法規遵循。它會驗證是否符合重要的 PCI DSS 需求並大幅加強「稽核信心」。

合併使用 McAfee Network Security Manager 與 McAfee ePolicy Orchestrator® (McAfee ePO™) 軟體的話，還可將整個網路上的威脅資訊進行交互關聯。McAfee Network Threat Behavior Analysis 有助於維護全方位且高效率的網路安全基礎架構，同時又注意不產生太多人力與物力成本。

主要優點

最大程度地降低 IT 與商業風險

- 主動的行爲式威脅偵測
- 有效偵測不明的威脅
- 利用網路流量分析來監控及報告異常的網路行爲
- 偵測攻擊以免其滲透到網路中
- 快速識別及回應未經授權的應用程式使用活動
- 透過與 McAfee Network Security Platform、McAfee ePO 和 McAfee Vulnerability Manager 的整合，協助確保遵循法規

大幅提升保護涵蓋範圍和價值

- 提供符合成本效益的全網路分析報告
- 毫不費力地分類及分析網路流量
- 省去手動診斷網路相關流量問題的麻煩
- 準確指出有問題的區段
- 針對零時差攻擊、垃圾郵件、殭屍網路 (Botnet) 和偵查攻擊進行異常偵測

強化競爭優勢

- 提供額外一層安全保護
- 避免網路威脅及入侵問題中斷營運作業
- 快速有效地執行分析工作
- 提供企業級效能及確保可靠性
- 簡化威脅與特徵碼管理的相關作業
- 提高網路效能、可擴充性和彈性
- 協助您制定即時的安全決策

主要功能

搭載完整的高效能配備

- 每個 McAfee Network Threat Behavior Analysis 裝置都包含：
  - » 四核心處理器
  - » RAID 磁碟陣列
  - » 超高速乙太網路連線
  - » 離線的 SAN 儲存空間
  - » 允許較大的流量
- 滿足現今不斷演進的安全與網路需求
- 提供經濟可靠的網路級效能

無可比擬的網路分析能力和洞見

- 透過單一的 McAfee Network Threat Behavior Analysis 偵測器收集整個網路的流量，以提供符合成本效益的全網路分析報告
- 透過流量分析監控及報告異常的網路行爲
- 透過行爲式演算法以識別威脅
- 刪除重複的 NetFlow
- 分析主機與應用程式的行爲
- 檢查網路是否有蠕蟲病毒、殭屍網路 (Botnet) 或垃圾郵件的相關行爲
- 探測零時差威脅和偵查攻擊

輕鬆進行整合和原則強制作業

- 與 McAfee Network Security Platform IPS 整合，將網路入侵活動造成的任何異常網路行爲交互關聯
- 與 McAfee ePO 軟體和 McAfee Vulnerability Manager 軟體緊密整合
- 與 Cisco 的交換器/路由器 (NetFlow v5 或 v9) 相容
- 有助於透過 McAfee Network Security Manager 進行 McAfee Network Threat Behavior Analysis、McAfee Network Access Control 與 IPS 偵測器的一般管理
- 促進內部與法規原則的強制作業

規格	T-200	T-500
處理器	1xE5540	2xE5540
記憶體	6x2 GB DDR3 1,333 MHz	6x2 GB 與 6x1 GB DDR3 1,333 MHz
硬碟	2x73 GB 與 4x300 GB 2.5 英吋的可熱交換序列連接 SCSI	2x146 GB 與 4x600 GB 2.5 英吋的可熱交換序列連接 SCSI
NIC	4 個銅連接埠	2 個銅連接埠和 2 個光纖連接埠
其他	備援電源供應	備援電源供應
	免工具滑軌	免工具滑軌
每秒流量	25,000	50,000
Cisco NetFlow	v5 與 v9	v5 與 v9

McAfee

邁克菲台北辦公室
台北市 104 南京東路三段
132 號 4 樓 A2 室
886-2-2721-7766
www.mcafee.com/tw

31000ds_nt-behavior-analysis_0811_fnl_ETMG