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 是 McAfee Network Security Platform 的整合式元件，屬於 McAfee 產品系列的一部分，可讓您即時掌握網路基礎架構的狀態並保護其免於威脅侵擾。McAfee Network Threat Behavior Analysis 在分析來自交換器和路由器的流量後，即可準確指出網路中的危險行為，有效預防潛在隱形攻擊。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為，以及能夠即時找出潛在的異常或攻擊類型，包括惡意軟體、零時差攻擊、殭屍網路和蠕蟲病毒。McAfee Network Threat Behavior Analysis 也可裝備部分 McAfee Network Security Platform 的進階引擎，包括不須簽章即可識別惡意軟體的即時模擬引擎。

今日潛在隱形攻擊的情報分析能力

您的網路正面臨進階的隱性攻擊，它們會規避傳統偵測方法，讓您的網路暴露在弱點入侵和網路中斷的風險中。McAfee Network Threat Behavior Analysis 在分析來自交換器和路由器的網路流量後，可以智慧地監視及報告不尋常的行為，以便讓您識別及快速回應網路上的攻擊。

McAfee Network Threat Behavior Analysis 裝置使用 NetFlow 和 J-Flow 資料來識別一般入侵防禦系統 (IPS) 周邊以外的威脅。它是配備完整的裝置，具有四核心處理器、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。

無可比擬的網路分析能力和洞見

McAfee Network Threat Behavior Analysis 可讓您掌握充足的資訊，對網路中的應用程式和通訊協定做出明智的決策。它可監視及報告不尋常的網路行為，並透過行為式演算法識別威脅。它可透過分析主機和應用程式行為，針對零時差攻擊、垃圾郵件、殭屍網路及事前勘查攻擊進行異常偵測。具備全面流量分析功能，可以識別未經授權的應用程式使用狀況，並準確指出有問題的網路區段。

主要優點

保護網路的分析能力

- 利用網路流量分析來監控及報告異常的網路行為。
- 主動的行為式威脅偵測。
- 有效偵測不明的威脅。
- 針對零時差攻擊、垃圾郵件、殭屍網路和事前勘查攻擊進行異常偵測。

全方位惡意軟體防護

- 使用惡意檔案即時模擬來阻止惡意軟體入侵。
- 在網路間使用進階關聯以偵測殭屍網路活動。
- 提供網路流量與事件的端點情報和關聯。

控制及防止惡意軟體爆發

McAfee Network Threat Behavior Analysis 與 McAfee Network Security Platform 一起使用，可以提供進階檢查和封鎖可疑檔案的即時模擬。即時模擬引擎會掃描可疑檔案，以偵測及封鎖惡意行為。McAfee Network Threat Behavior Analysis 具備多個 IPS 和網路裝置的進階關聯，可以找到規避傳統簽章式防護的潛在隱形攻擊。使用 McAfee Endpoint Intelligence Agent，可以偵測及控制將惡意流量偽裝成合法網路流量來傳輸的受危害端點。基於信用評價的端點活動分析可以減少資料外洩及防止惡意軟體爆發。

簡化安全性作業及節省成本

McAfee Network Threat Behavior Analysis 提供符合需求的實際洞見，提升安全性管理的成本效益。裝置可以加快事件反應時間，簡化網路程序來增進效能，同時避免網路威脅及入侵問題中斷企業營運。

其他功能

- 透過整合 McAfee Global Threat Intelligence (McAfee GTI) 增強安全性。
- 使用虛擬版本以讓實作符合成本效益。
- 整合 McAfee ePolicy Orchestrator® (McAfee ePO™) 軟體、McAfee Enterprise Security Manager 及 McAfee Vulnerability Manager 軟體以擴大分析和關聯範圍。
- 毫不費力地分類及分析網路流量。
- 每一流量的中繼資料 (應用程式 ID、檔案及 URL) 儀表板。
- 使用完整隔離選項提高安全性狀態。
- 具備外部主機分析能力，可以為主機威脅因素詳細分級。
- 與 Cisco (NetFlow v5 與 v9) 和 Juniper (J-Flow v5 與 v9) 交換器與路由器相容。

資料工作表

	NTBA T-600	NTBA T-1200
規格		
每秒流量	最多 60000 個	最多 100000 個
Cisco NetFlow	v5 與 v9	v5 與 v9
Juniper J-Flow	v5 與 v9	v5 與 v9
處理器	1x Xeon E5-2658	2 x Xeon E5-2658
記憶體	46 GB	96 GB
可用儲存區	4.4 TB / Raid 10	8.8 TB / Raid 10
網路介面	x4 銅線 10/100/1000	x4 銅線 10/100/1000
環境		
外型規格	1U	2U
寬度	438 公釐	438 公釐
長度	709.37 公釐	707.8 公釐
高度	43.2 公釐	87.6 公釐
最大重量	14.96 公斤	21.6 公斤
預估插入口電源使用率 (最糟的情況)	402W	667W
備援電源供應	750W	750W
系統冷卻裝置需求 (BTU/小時)	1370	2280
運作中溫度	+10°C 至 +35°C，最大變化率不超過每小時 10°C	

虛擬 NTBA 規格	T-VM	T-100VM	T-200VM
建議的 RAM	16 GB	8 GB	16 GB
建議的 CPU	4	4	4
每秒流量	最多 25,000 fps	最多 10,000 fps	最多 25,000 fps

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