McAfee Network Threat Response

瞄準網路內進階、持續的惡意軟體

McAfee® Network Threat Response 專門從雞蛋裡挑骨頭：暗中滲透網路的持續性和目標式攻擊。McAfee Network Threat Response 是新一代偵測引擎的架構，專門對付使用者方面的攻擊，一般稱爲進階持續性威脅 (APT)。McAfee Network Threat Response 只會優先選擇呈現需要調查的事件，縮短分析時間。McAfee Global Threat Intelligence™ (McAfee GTI™)、McAfee Network Security Platform 及 McAfee Firewall Enterprise 可讓分析人員解決當今最致命的安全問題：持續性、目標式攻擊。

主要優點

偵測進階的零時差惡意軟體
- 進階持續性威脅 (APT)
- 受感染的 PDF
- 殭屍病毒 (Bot)
- 自動下載
- 社交工程
- 完全針對您公司而來的獨特威脅

縮短回應時間
- 自動尋找惡意軟體
- 加速分析複雜的威脅，不需要花費數週時間，只需要幾分鐘就能決定事件的檢閱優先順序

任何規模之安全小組的進階分析
- 找出其他工具難以察覺的威脅
- 擷取、歸檔和記錄網路流量以供進一步分析
- 加速分析網路封包記錄裝置

彈性的部署選項
- 虛擬感應器
- 偵測速度高達 2 Gbps 的裝置
- 10 以上 Gbps 電信業級的平台，採用 SAIC/CloudShield 裝置

易於部署
- 只需要幾分鐘即可完成 McAfee Network Threat Response 裝置的安裝

揭發他們的詭計

迴避偵測是進階惡意軟體的特點。McAfee Network Threat Response 整合一套工具來對付惡意 PDF、殭屍網路 (Botnet)、自動下載和社交工程，以遏止這些企圖。這些工具包括啓發式 PDF 掃描程式、即時威脅資料庫、檔案類型驗證及隱藏可執行檔的偵測。

McAfee Network Threat Response 不但會針對僞裝情形發出警告，還會解譯流量，讓分析人員深入瞭解其他任何現有工具難以察覺的攻擊。

尋找確鑿證據

想要揪出元兇嗎？證據會說話。以目標式攻擊來說，元兇就是 Shell 程式碼。

Shell 程式碼是惡意軟體用來感染和操弄裝置的說明集。McAfee Network Threat Response 採用正在申請專利的啓發式規則來偵測 Shell 程式碼，無須事先瞭解變化無窮的攻擊承載。

暗中集結

Shell 程式碼會一點一滴滲入網路，等待時機發動攻擊。McAfee Network Threat Response 以獨特的能力揭發這種緩慢、持續性的攻擊，能夠分辨並彙總隨著時間而涓滴滲透的攻擊片段。除此之外，您無力拼湊這種龜速潛入網路的威脅謎團。

Shell 程式碼：保護前後

保護前

保護後

http://w.hack.info/data_theft.exe

縮短分析時間

網路鑑識擷取解決方案可讓分析人員重現歷程流量，以判斷惡意軟體事件的根本原因和後續引發的災情。McAfee Network Threat Response 透過 PCAP 匯入功能來加速這種分析。透過 McAfee Network Threat Response 分析引擎來重現資料時，隱藏的流量就會現出原形，也會浮現關鍵指標。因此，分析人員就有明確的基點可著手調查，而不必浪費許多時間進行分析。

安檢人員發揮最高效率

傳統的安全裝置每天會產生大量事件，但只有一小部分才是目標式攻擊活動的指標。McAfee Network Threat Response 可準確辨別目標式攻擊，讓分析人員在極短時間內完全掌控需要注意的事件。McAfee Network Threat Response 的強大威力，讓每一位分析人員本身形同一支有 20 位惡意軟體調查員的小組。

使用全球情報提供區域安全

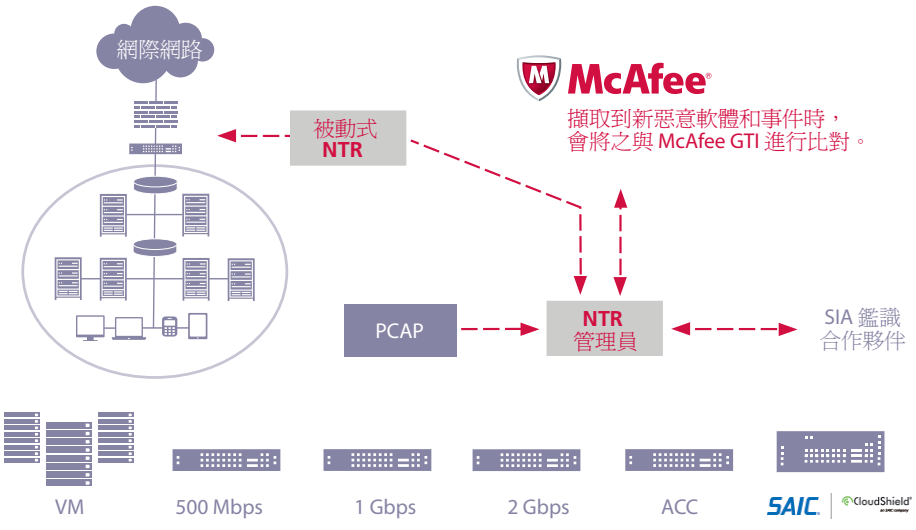
McAfee GTI 收集來自全球數千萬個裝置的資訊。McAfee GTI 超越殭屍網路命令與控制 (C&C) 偵測，能夠找出最初感染階段使用的惡意軟體來源伺服器。McAfee Network Threat Response 運用我們全球龐大的信用評價資料庫，能夠偵測全球各地已知壞蛋的通訊，有助於鎖定潛在的威脅。

遏止 APT 的一切行為

McAfee Network Threat Response 是業界中打擊網路 APT 最頂尖的技術。這套威脅揭發和鑑識架構可執行進階惡意軟體偵測、頻外流量檢查，以及辨別其他所有安全技術都無法應付的最新、未知的攻擊。它可以揭發 APT、殭屍網路、特洛伊木馬程式、指令碼和 Shell 程式碼，擷取承載並執行深入分析，充分瞭解其出處、感染徑途及目標式弱點。McAfee Network Threat Response 可解讀已編碼的承載和刻意躲藏且已重組的切割式攻擊。

如此準確地全盤瞭解威脅 (從最初滲透到資料外洩)，自然能夠遏止一切攻擊行爲。此外，這番瞭解也可讓您制訂全方位的防護策略，防止未來可能危及企業的威脅。

McAfee Network Threat Response 運用一套可擴充的調查架構，可隨著攻擊技術演進而進化。這套架構以提供最先進的實用解決方案爲設計重點，不但節省時間，還可隨著您的網路而調整。



McAfee Network Threat Response 硬體規格

型號	A50VM	A50	A100	A200	ACC
角色	偵測器虛擬機器裝置	偵測器裝置	偵測器裝置	偵測器裝置	管理主控台裝置
效能輸送量	200 Mbps	500 Mbps	1 Gbps	2 Gbps	最多 10 個偵測器
連接埠					
10/100/1000 乙太網路偵測器連接埠	—	4	3	5	—
10/100/1000 管理連接埠	—	1	1	1	1
作業模式					
McAfee Network Security Platform M 系列連線	是	是	是	是	—
SPAN 埠監視	是	是	是	是	—
虛擬機器	是	—	—	—	—
硬體					
Intel 伺服器	—	SR1630HGPRX	SR1625URSAS	SR1625URSAS	SR1625URSAS
CPU 核心	—	4	4	8	8
CPU	—	1	1	2	2
記憶體	—	2 G	6 G	12 G	12 G
硬碟機	—	500 GB	2 x 300 GB	4 x 300 GB	4 x 300 GB
作業系統	—	RHEL 5	RHEL 5	RHEL 5	RHEL 5
高可用性					
備援電源	—	否	是	是	是
RAID 層級	—	SATA	RAID 1	RAID 10	RAID 10
實體					
外觀尺寸	虛擬機器	1 U	1 U	1 U	1 U
機箱尺寸	—	4.31 公分 (高) x 43 公分 (長) x 64.79 公分 (寬)	4.31 公分 (高) x 43 公分 (長) x 66.54 公分 (不含纜線管理支架) (寬)	4.31 公分 (高) x 43 公分 (長) x 66.54 公分 (不含纜線管理支架) (寬)	4.31 公分 (高) x 43 公分 (長) x 66.54 公分 (不含纜線管理支架) (寬)
配送尺寸	—	59.18 公分 (寬) x 106.17 公分 (長) x 21.84 公分 (高)	59.18 公分 (寬) x 106.17 公分 (長) x 21.84 公分 (高)	59.18 公分 (寬) x 106.17 公分 (長) x 21.84 公分 (高)	59.18 公分 (寬) x 106.17 公分 (長) x 21.84 公分 (高)
重量	—	約 19.73 公斤	約 24.72 公斤	約 25.4 公斤	約 25.4 公斤
消耗功率	最多兩個 650-W 電源供應器模組				
電源輸入	自動切換 110-220 VAC				
運作中溫度	+10° C 至 +35° C，最大變化率不超過每小時 10° C				
非運作溫度	-40° C 至 +70° C				

接續下頁。

McAfee Network Threat Response 硬體規格

非運作濕度	90%，35° C 時不結霜
產品安全規範	UL60950 - CSA 60950 (美國 / 加拿大)、EN60950 (歐洲)、IEC60950 (國際)、CB Certificate and Report、IEC60950 (報告含括所有國家 / 地區誤差)、GS Certification (德國)、GOST R 50377-92 - Certification (俄羅斯)、Belarus Certification (白俄羅斯)、Ukraine Certification (烏克蘭)、CE - Low Voltage Directive 73/23/EEE (歐洲)、IRAM Certification (阿根廷)
產品 EMC 規範 - A 級規範	FCC/ICES-003 - Emissions (美國 / 加拿大) Verification、CISPR 22 - Emissions (國際)、EN55022 - Emissions (歐洲)、EN55024 - Immunity (歐洲)、EN61000-3-2 - Harmonics (歐洲)、EN61000-3-3 - Voltage Flicker (歐洲)、CE - EMC Directive 89/336/EEC (歐洲)、VCCI Emissions (日本)、AS/NZS 3548 Emissions (澳洲 / 紐西蘭)、BSMI CNS 13438 Emissions (台灣)、GOST R 29216-91 Emissions (俄羅斯), GOST R 50628-95 Immunity (俄羅斯)、Belarus Certification (白俄羅斯)、Ukraine Certification (烏克蘭)、KCC Certification (EMI) (韓國)

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

31101ds_ntr_1011