

McAfee Network Security Platform

以新一代入侵防禦最佳化網路防護

McAfee 是全球網路入侵防禦系統 (IPS) 的領導品牌，提供前所未有的安全等級，同時提供可協助您最佳化網路投資的彈性部署選項。只有 McAfee® Network Security Platform 提供同類最佳的安全效力、有規模彈性的 In-Line 效能及新一代 IPS 控制，能夠確定無疑地執行網路安全管理。橫跨實體和虛擬環境的統一網路安全管理、精簡安全操作，及防護您的企業避免最新的惡意軟體、零時差攻擊、殭屍網路 (Botnet)、阻絕服務 (DoS) 嘗試與進階定位攻擊。

主要優點

快速、準確的威脅防禦

- 檢查可設定狀態的流量
- 由 McAfee GTI 提供的可預測威脅情報
- 惡意軟體、零時差、DoS/DDoS、殭屍網路 (Botnet)

效能和可用性

- 輸送量超過 10 Gbps
- 領先業界的可靠性
- 容錯移轉和故障開啟

整個網路的可見性

- 新一代的應用程式可見性
- 行為式殭屍病毒 (Bot) 偵測
- 流量型網路行為分析

集中的安全管理

- 可擴充的網路安全管理
- McAfee ePO 軟體整合
- 主機 IPS/病毒/間諜軟體事件可見性

操作簡便

- 動態智慧型封鎖
- 多種威脅關聯
- 整合式弱點掃描

病毒環境檢查

- 檢查虛擬機器間流量
- 隔離惡意虛擬機器
- 適用於實體和虛擬管理的單一主控台

領先業界的防護

談到網路安全工作時，讓 McAfee 為您分憂解勞。McAfee Network Security Platform 在大幅調整後，提供遠比大多數網路 IPS 解決方案所能達成的更佳現成安全效能。在全球部署了數萬個偵測器，McAfee Network Security Platform 是業界最可靠的網路 IPS。防禦範圍包括惡意軟體、零時差威脅、阻絕服務攻擊和殭屍網路 (Botnet)。

數 GB 的效能

在安全和高效能雙方面取得雙贏。McAfee Network Security Platform 將單次操作、以通訊協定為基礎的檢驗架構結合定製的業者級硬體，能夠以單一裝置達成 10 Gbps 以上的實際應用檢驗。其超高效率的架構無論安全設定為何均可保留效能，而其他 IPS 解決方案在「安全重於效能」的原則下，可能會發生輸送量降低 50%。

可預測的威脅情報

利用預測的威脅情報，大幅改進安全效能。McAfee Network Security Platform 結合 McAfee Global Threat Intelligence™ (McAfee GTI™)，可動態影響傳統及新興攻擊的 In-Line 防禦能力。McAfee GTI 會根據遍佈全球各地的數十億個唯一的檔案、IP、URL、通訊協定和地理位置資料之信用評價，來評估網路通訊的信用評價。

應用程式感知與控制能力

掌握足夠的情報，正確判斷您網路上的應用程式和通訊協定。McAfee Network Security Platform 是第一套，也是唯一一套將進階威脅防護與應用程式感知結合到單一安全決策引擎中的 IPS 解決方案。我們將威脅活動與應用程式的使用方式連結起來，包括 1,100 種以上應用程式和通訊協定的 7 級可見性，讓您掌握足夠的情報，足以正確決定在您的網路上允許哪些應用程式和通訊協定。

無可比擬的網路可見性

提供前所未有的網路深入洞察力。透過網路異常偵測功能，讓您清楚瞭解系統、應用程式和使用者行為。McAfee Network Security Platform 會分析企業中任何地方的交換器和路由器流出的資料，大幅擴展傳統網路 IPS 的範圍，輕易識別網路上的殭屍病毒 (Bot) 和其他惡意活動。

內容感知的安全

積極執行網路安全，但不會增加誤報的風險。McAfee 將許多來源 (McAfee GTI、弱點掃描、應用程式行為及系統行為) 的資料建立關聯，以確定地識別網路攻擊，並能在許多情況下自動預防惡意活動。例如，可以根據特徵碼型攻擊定義和威脅來源 IP 信用評價的即時關聯，將低可信度的「僅警示」事件動態升級至最高可信度的「封鎖」事件。



McAfee Network Security Platform 可協助您：

保護您的企業

- 預防攻擊，同時縮短停機時間
- 保護您的資料與基礎架構
- 滿足法規遵循計劃的需求

保護您的系統

- 主動保護未修補的系統
- 主動防禦零時差攻擊
- 內容感知的入侵防禦

保護您的網路

- 應用程式可見性與控制能力
- 可調整速率限制
- 特定主機的連線限制

保障您的安全投資

- 原生 10 GB 超高速乙太網路
- 網路級硬體
- 領先業界的使用壽命

內建存取控制

加入選用的網路存取控制 (NAC) 軟體，並將 McAfee Network Security Platform 轉變為 NAC 裝置，以提供許可前後控制力、識別型存取控制，外加主機隔離與可強制執行之存取原則。

整合式安全管理

透過整合式安全和風險管理，充分發揮您的安全投資效益。Network Security Platform 整合了 McAfee® ePolicy Orchestrator® (McAfee ePO™) 軟體，提供整體企業的風險與法規遵循完整面貌，包括根據系統弱點、網路防禦和端點安全層級的有風險基礎架構之最新評估。

所有 McAfee Network Security Platform 裝置均提供下列功能：

進階入侵防禦

- 可設定狀態的流量檢查 (IP 重組與 TCP 資料流重組)
- 異常偵測
- 特徵碼型偵測 (McAfee 定義、使用者定義、開放來源)
- 信用評價型偵測 (McAfee GTI)
- 啓發式殭屍病毒 (Bot) 偵測
- 多種攻擊關聯
- 7 級通訊協定偵測
- 主機隔離
- 進階規避防護

阻絕服務 (DoS) 及分散式阻絕服務 (DDoS) 防禦

- 閾值型與啓發式偵測
- 連線限制
- 以設定檔為基礎的自我學習型偵測

網路可見性

- 應用程式可見性
- 系統資訊
- 弱點關聯
- 主機 IPS 警示
- 病毒環境檢查
- 封包擷取以供鑑識分析整合
- 流量型行為分析 (透過 NTBA)

細部控制

- 應用程式與子應用程式控制能力
- 地理位置型 ACL 規則
- 連線限制
- 主機隔離 (透過 IPS 或 NAC)
- 識別型存取控制
- 系統健康型存取控制

McAfee GTI

- 檔案信用評價
- IP 信用評價
- 應用程式和通訊協定信用評價
- 地理位置

高可用性選項

- 可設定狀態的完整容錯移轉
- 外部故障開啓 (主動與被動)
- 內建故障開啓 (僅限銅線埠)

支援通道通訊協定

- IPv6
- V4-in-V4、V4-in-V6、V6-in-V4 及 V6-in-V6 通道
- MPLS
- GRE
- Q-in-Q 雙 VLAN

McAfee Network Security Manager

- 永不間斷的管理
- 數十個預先定義的 IPS 安全原則範本
- 高達 1,000 個「虛擬 IPS」原則 (限特定機型)
- 整合式使用者驗證 (Radius、LDAP 和 TACACS)
- 自動化容錯移轉和容錯回復
- 關鍵組態資料的嚴重損壞復原
- 集中式原則控制的分層管理

整合式解決方案

- McAfee ePolicy Orchestrator 軟體
- McAfee Network User Behavior Analysis
- McAfee Network Access Control (附加軟體)
- McAfee Network Threat Response
- McAfee Vulnerability Manager
- 協力廠商鑑識

Network Security Platform 規格

10 GB 超高速乙太網路連線能力



偵測器硬體元件	M-8000	M-6050	M-4050	M-3050	M-2950	M-2850/M-2750	M-1450	M-1250
效能								
實際輸送量	10 Gbps	5 Gbps	3 Gbps	1.5 Gbps	1 Gbps	600 Mbps	200 Mbps	100 Mbps
最大輸送量 (UDP 1512 位元組封包)	最多 20 Gbps	最多 10 Gbps	最多 4 Gbps	最多 2.5 Gbps	最多 1 Gbps	最多 1 Gbps	最多 300 Mbps	最多 150 Mbps
同時連線數量上限	4,000,000	2,000,000	1,500,000	750,000	750,000	750,000 / 250,000	80,000	40,000
每秒新增連線	120,000	60,000	36,000	18,000	15,000	10,000	4,000	2,000
含 SSL 解密的輸送量 (根據 10% SSL 流量)	8.8 Gbps	4.4 Gbps	2.7 Gbps	1.3 Gbps	900 Mbps	550 Mbps	不適用	不適用
SSL 流量計數上限	400,000	200,000	150,000	75,000	25,000	25,000	不適用	不適用
匯入的 SSL 金鑰	64	64	64	64	64	64	不適用	不適用
設定檔								
虛擬 IPS 系統數目	1,000	1,000	1,000	1,000	100	100	32	16
DoS 設定檔數量上限	5,000	5,000	5,000	5,000	5,000	300	120	100
ACL 規則	1,000	1,000	1,000	1,000	1,000	400	100	50
連接埠								
超高速乙太網路 - 固定銅線埠	—	—	—	—	8	8 / —	8	8
超高速乙太網路 - SFP 連接埠	16	8	8	8	12	12 / 20	—	—
10 GB 超高速乙太網路	12	8	4	4	—	—	—	—
專屬回應埠 (GigE)	1	1	1	1	1	1	1	1
專屬管理埠 (GigE)	1	1	1	1	1	1	1	1
內建故障開啓功能的連接埠	—	—	—	—	8	8 / —	8	8
適用於外部故障開啓套件的控制埠	14	8	6	6	6	6 / 10	—	—
實體								
尺寸	2x 2RU 機架掛載式 一個 16.75 (長) x 3.05 (高) x 30.00 (寬)	2RU 機架掛載式 16.75 (長) x 3.05 (高) x 30.00 (寬)	2RU 機架掛載式 16.75 (長) x 3.05 (高) x 30.00 (寬)	2RU 機架掛載式 16.75 (長) x 3.05 (高) x 30.00 (寬)	2RU 機架掛載式 15.88 (長) x 3.3 (高) x 24.5 (寬)	2RU 機架掛載式 15.88 (長) x 3.3 (高) x 24.5 (寬)	1RU 機架掛載式 17.37 (長) x 1.65 (高) x 13.5 (寬)	1RU 機架掛載式 17.37 (長) x 1.65 (高) x 13.5 (寬)
重量	94 磅 (2 x 47)	47 磅	47 磅	47 磅	40 磅	40 磅	12 磅	12 磅
消耗功率	900 W (2 x 450 W)	450 W	450 W	450 W	450 W	450 W	120 W	120 W
使用 DC 電源	可選	可選	可選	可選	可選	可選	否	否
電源	100 - 240 VAC (50/60 Hz)							
溫度	0 °C 至 35 °C (運作中) - 40 °C 至 70 °C (非運作中)				0 °C 至 40 °C (運作中) - 40 °C 至 70 °C (非運作中)			
相對溼度 (不結霜)	運作中：10% 至 90% 非運作中：5% 至 95%							
海拔	0 到 10,000 英尺							
安全認證	UL 1950、CSA-C22.2 No. 950、EN-60950、IEC 950、EN 60825、IEC 60825、21CFR1040 CB 授權與報告 (涵蓋所有國家/地區誤差)。							
EMI 認證	FCC Part 15、Class A (CFR 47) (美國) ICES-003 Class A (加拿大)、EN55022 Class A (歐洲)、CISPR22 Class A (國際)							

