

McAfee Network Security Platform

獨家網路安全性智慧型解決方案

主要優點

無與倫比的威脅防護

- 新一代架構
- 進階殭屍網路偵測
- 行為分析

全方位惡意軟體防護

- 無特徵碼進階惡意軟體分析
- 惡意軟體調查儀表板
- 透過 McAfee GTI 預先偵測惡意軟體

Security Connected

- 透過 McAfee ePO 軟體即時偵測主機相關內容
- McAfee GTI
- 整合鑑識分析

效能及可用性

- 輸送量高達 20 Gbps
- 領先業界的可靠度
- 主動-主動式高可用性

智慧型安全管理

- 可擴充的 Web 管理
- 智慧型警示優先順序
- 漸進式揭露工作流程

可見性及控制

- 應用程式識別資料
- 使用者識別資料
- 裝置識別資料

McAfee® Network Security Platform 是一項獨家智慧型安全性解決方案，能夠找出網路上設計複雜的威脅並加以封鎖。這項產品採用先進的威脅偵測技術，從單純的模式比對進步到絕對精準的隱性攻擊防禦系統，而其採用的新一代硬體平台仍可在單一裝置上以超過 20 Gbps 的速度執行，滿足嚴格的網路使用需求。與即時 McAfee Global Threat Intelligence™ (McAfee GTI™) 包含有關使用者、裝置和應用程式、內容豐富的資料摘要結合，Security Connected 安全管理方法簡化了安全性作業，並可針對來自網路的攻擊做出更快更準確的回應。

防範當今的隱性威脅

您的網路正面臨魔高一丈的隱性攻擊，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。遺憾的是，大多數的組織都缺乏財力與營運資源，無法採用及管理提供適當防禦的系統所需的工具和技術。

McAfee Network Security Platform 是一款整合式的網路安全性解決方案，它結合了新一代威脅防禦和直覺式安全管理功能，藉此提升偵測準確度並簡化安全性作業。它提供了業界首屈一指的服務範圍，舉凡惡意軟體、零時差威脅、阻絕服務攻擊和殭屍網路，全都涵蓋在防禦範圍內。

無與倫比的威脅防護

McAfee Network Security Platform 是以新一代檢查架構做為設計藍圖，可針對網路流量執行深入檢查，同時仍能維持線路速率。此產品結合了多種進階檢查技術，包括完整的通訊協定分析、威脅信用評價、行為分析和進階惡意軟體分析，藉此偵測並防範網路上已知的攻擊和零時差攻擊。

全方位抵禦惡意軟體

沒有任何一種惡意軟體偵測技術足以抵禦所有的攻擊，因此 McAfee Network Security Platform 當中包含了多種進階惡意軟體分析技術，如此才能阻止不需要的惡意軟體大肆破壞您的網路。它具備 McAfee GTI 的檔案信用評價功能、可透過 JavaScript 偵測技術深入分析檔案，同時採用進階的反惡意軟體引擎，可偵測零時差威脅、自訂惡意軟體和其他隱性攻擊。

Security Connected

取得所需的資料再輕鬆不過了。McAfee 透過 McAfee® ePolicy Orchestrator® (McAfee ePO™) 軟體和 McAfee Enterprise Security Manager 提供即時整合功能，針對所有相關來源的網路事件提供即時關聯。與 McAfee ePO 軟體及 McAfee Enterprise Security Manager 整合後，McAfee Network Security Platform 更能精準掌握威脅，因為這些威脅與裝置和使用者有所關聯，而這些威脅就是組織最大的風險。這項解決方案包含了裝置詳細資料、使用者資訊、端點安全性狀況、弱點評估及其他豐富資訊，可協助組織瞭解威脅嚴重性及業務風險因素。



McAfee Network Security Platform 可協助您：

- 封閉安全性漏洞
- 封鎖惡意軟體網路活動
- 防禦隱性攻擊
- 偵測進階惡意軟體

減少管理方面的困擾

- 自動排定事件優先順序
- 簡化調查工作流程
- 避免沒有必要的調校

適用於網路

- 1 GigE、10 GigE、40 GigE 連線能力
- 可擴充至 80 Gbps
- 主動-主動式高可用性

效能及延展性

兩全其美—安全性與高效能兩者兼顧。McAfee Network Security Platform 結合了只需執行一次的通訊協定式檢查架構及專門建構的電信業者等級的硬體設備，以滿足使用者在單一裝置上以超過 20 Gbps 的速率連線的需求。不論您如何設定所需的安全性，它的超高效率架構仍能維持極佳效能，但如果採用其他的 IPS 解決方案，您可能就會因為「安全性優先，效能其次」的原則而遇到輸送量暴跌達 50% 的窘境。

可見性及控制

掌握充足的資訊，對您網路中的應用程式和通訊協定做出明智的決策。McAfee Network Security Platform 是唯一一款最先將進階威脅防禦系統及應用程式感知功能納入單一安全性決策引擎的 IPS 解決方案。我們將威脅活動與應用程式使用狀況相互關聯，其中包含超過 1,500 項應用程式和通訊協定的第 7 層可見性，讓您能夠掌握更充足的資訊，決定哪些應用程式可在您網路上運作。除了應用程式識別資料以外，McAfee Network Security Platform 也提供使用者及裝置的可見性。並且會找出異常網路行為，優先偵測風險較高的主機和使用者 (包括使用中的殭屍網路)。

智慧型安全管理

您可透過智慧型網路安全管理，讓您的安全性投資發揮最大效益。McAfee Network Security Manager 提供具延展性的 Web 管理，不論您的組織只有兩部網路安全性設備，或是擁有多達數百部的網路安全性設備，都可使用。它提供直覺式的漸進式揭露工作流程，可將管理員導向相關警示，以及易於使用且可根據警示嚴重性和相關性自動排列事件優先順序的安全性儀表板。McAfee Network Security Platform 整合了 McAfee ePO 軟體，為您的組織提供整個企業的詳實風險與符合性資訊，包括根據系統弱點、網路防禦及端點安全性等級所做的最新風險基礎架構評估。

McAfee Network Security Platform 裝置功能

進階入侵防禦功能

- 狀態式流量檢查 (IP 重組與 TCP 資料流重組)
- 異常偵測
- 支援 McAfee 定義、使用者定義、開放原始碼等各種特徵碼
- 信用評價式偵測 (McAfee GTI)
- 第 7 層通訊協定檢查
- 主機隔離
- 進階規避防護

殭屍網路防護

- 啓發式殭屍病毒 (Bot) 偵測
- 多個攻擊關聯
- 命令與控制資料庫

進階惡意軟體防護

- 惡意軟體程式碼模擬
- 透過 JavaScript 分析檢查檔案
- 惡意軟體調查儀表板
- GTI 檔案信用評價

阻絕服務 (DoS) 及分散式阻絕服務 (DDoS) 防護

- 閾值與啓發式偵測
- 主機式連線限制
- 以設定檔為基礎的自我學習型偵測

端對端可見性

- 應用程式、裝置和使用者可見性
- 弱點關聯
- 主機 IPS 警示
- 虛擬環境檢查
- 擷取封包以供鑑識分析整合
- 流量式行為分析 (透過 McAfee Network Threat Behavior Analysis 進行)

細部控制

- 應用程式與子應用程式控制
- 地理位置與識別資料型 ACL 規則
- 連線限制
- 主機隔離
- 系統健康狀態型存取控制

Network Security Platform 規格



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
最高輸送量 (UDP 1,512 位元組封包)	最多 20 Gbps	最多 10 Gbps	最多 4 Gbps	最多 2.5 Gbps	最多 1.5 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
每秒新增連線數	120,000	60,000	36,000	18,000	15,000	10,000	4,000	2,000
SSL 加密輸送量 (以 10% SSL 流量為準)	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
已匯入 SSL 金鑰	64	64	64	64	64	64	不適用	不適用
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 Gigabit 超高速乙太網路	12	8	4	4	—	—	—	—
專屬回應埠 (RJ45)	1 (1 Gbps/100 Mbps/10 Mbps)	1 (1 Gbps/100 Mbps/10 Mbps)	1 (1 Gbps/100 Mbps/10 Mbps)	1 (1 Gbps/100 Mbps/10 Mbps)	1 (1 Gbps/100 Mbps/10 Mbps)	1 (1 Gbps/100 Mbps/10 Mbps)	1 (1 Gbps/100 Mbps/10 Mbps)	1 (1 Gbps/100 Mbps/10 Mbps)
專屬管理埠 (GigE)	1 (1 Gbps/100 Mbps/10 Mbps)	1 (1 Gbps/100 Mbps/10 Mbps)	1 (1 Gbps/100 Mbps/10 Mbps)	1 (1 Gbps/100 Mbps/10 Mbps)	1 (1 Gbps/100 Mbps/10 Mbps)	1 (1 Gbps/100 Mbps/10 Mbps)	1 (1 Gbps/100 Mbps/10 Mbps)	1 (1 Gbps/100 Mbps/10 Mbps)
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 42,54 cm x 7,75 cm x 76,20 cm	2RU 機架掛載式 42,54 cm x 7,75 cm x 76,20 cm	2RU 機架掛載式 42,54 cm x 7,75 cm x 76,20 cm	2RU 機架掛載式 42,54 cm x 7,75 cm x 76,20 cm	2RU 機架掛載式 40,34 cm x 8,38 cm x 62,23 cm	2RU 機架掛載式 40,34 cm x 8,38 cm x 62,23 cm	1RU 機架掛載式 44,12 cm x 4,19 cm x 34,29 cm	1RU 機架掛載式 44,12 cm x 4,19 cm x 34,29 cm
重量	42.6 kg (2 x 21.3 kg)	21.3 kg	21.3 kg	21.3 kg	18.1 kg	18.1 kg	5.4 kg	5.4 kg
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)			
相對溼度 (不結霜)					運作中： 10% 至 90% 非運作中： 5% 至 95%			
海拔					0 至 3,000 m			
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)			

McAfee GTI

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

高可用性

- 主動-主動型的狀態式容錯移轉
- 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

- Web 管理
- 層級管理架構 (高達 1,000 個偵測器)
- 多種預先定義的 IPS 安全性原則範本
- 高達 1,000 項的「虛擬 IPS」原則 (限指定機型)
- 整合式使用者驗證 (Radius、LDAP 及 TACACS)
- 自動容錯移轉與容錯回復
- 重要組態資料嚴重損壞復原
- 集中原則控制的階層管理

整合式解決方案

- McAfee ePO 軟體
- McAfee Enterprise Security Manager
- McAfee Network Threat Behavior Analysis
- McAfee Vulnerability Manager
- 第三方鑑識

