McAfee Network Security Platform

全方位的網路安全性智慧型解決方案

McAfee® Network Security Platform (McAfee NSP) 是新一代入侵防護系統 (IPS)，能夠找出網路上設計複雜的惡意軟體威脅並加以封鎖。這項產品採用先進的偵測及模擬技術，從單純的模式比對進步到高度精準的隱性攻擊防禦系統。此平台可在單一裝置以超過 40 Gbps 的速度執行，以滿足嚴格的網路使用需求。整合式 McAfee 解決方案產品組合會將即時 McAfee Global Threat Intelligence 摘要與有關使用者、裝置和應用程式的豐富內容相關資料結合，藉此簡化安全性作業，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，讓您的應用程式和資料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 NSP 是一款整合式的網路安全性平台，它結合了智慧型威脅防護和直覺式安全性管理功能，藉此提升偵測準確度並簡化安全性作業。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 NSP 將多個特徵碼及無需特徵碼的偵測引擎分層，如此才能協助阻止不需要的惡意軟體大肆破壞您的網路。它運用多種進階檢查技術的組合，包括完整的通訊協定分析、威脅信用評價和行為分析來偵測及抵禦惡意軟體回呼、阻絕服務 (DoS)、零時差攻擊和其他進階威脅，藉此針對網路流量執行深度檢查。

整合式安全性

McAfee Network Security Platform 與結合了深層靜態程式碼分析、動態分析 (惡意軟體沙箱作業) 與機器學習的 McAfee Advanced Threat Defense 整合，可偵測零時差威脅偵測，包括利用規避技術和勒索軟體的威脅。此外，McAfee NSP 結合了 McAfee Global Threat Intelligence 中的檔案信用評價，並透過 McAfee® ePolicy Orchestrator® 軟體和 McAfee Enterprise Security Manager 提供整合功能，針對所有相關來源的網路事件提供即時關聯。此種混合式解決方案包含了裝置詳細資料、使用者資訊、端點安全性狀態、弱點評估及其他豐富資訊，可協助組織更充分地瞭解威脅嚴重性及業務風險因素。

主要優勢

- 快速偵測及封鎖威脅，藉此保護應用程式和資料的安全
- 高效能且可擴充的解決方案，能適應瞬息萬變的環境
- 集中式管理讓您掌握和控管情況
- 進階偵測功能，包括免特徵碼的惡意軟體分析
- 入埠及出埠 SSL 解密功能，可檢查網路流量
- 高可用性及嚴重損壞復原保護
- 同時適用於虛擬裝置
- 與 McAfee 解決方案產品組合整合，提供裝置到雲端的安全性

NSS LABS RECOMMENDED

與我們聯絡

效能及可用性

McAfee Network Security Platform 能兼顧安全性與高效能，可謂兩全其美。本產品將單次操作、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 40 Gbps 以上的實際應用檢驗。不論您如何設定所需的安全性，它的高效率架構仍能維持極佳效能，但如果採用其他 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。

此外，McAfee NSP 提供主動-主動及主動-被動的狀態式容錯移轉，讓您符合高可用性 SLA 的要求，同時避免出現裝置效能遲緩或獨立解決方案負荷過重的瓶頸。

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，使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 NSP 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)。

智慧型且可擴充的安全性管理

您可透過智慧型網路安全性管理，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。本產品提供直覺的漸進式揭露工作流程，可將管理員導向相關警示，以及導向至易於使用的安全性儀表板，該儀表板會根據警示嚴重性和相關性自動排列事件優先順序。

其他功能

進階威脅防護

- 入埠安全通訊端層 (SSL) 解密會利用代理程式型的共用重要解決方案，支援 Diffie-Hellman (DH) 及 Elliptic-Curve Diffie–Hellman (ECDH) 加密，而不會影響到偵測器的效能 (專利審核中，適用於 NS 系列)
- 出埠 SSL 解密 (NS 系列)
- McAfee Gateway Anti-Malware 模擬引擎
- PDF JavaScript 模擬引擎
- Adobe Flash 行為分析引擎
- 進階規避防護
- 行動威脅信用評價及雲端分析

殭屍網路和惡意軟體回呼保護

- DNS/DGA Fast Flux 回呼偵測
- DNS Sinkholing
- 啟發式殭屍病毒 (Bot) 偵測
- 多重攻擊關聯
- 命令與控制資料庫

進階入侵防護

- IP 重組與 TCP 資料流重組
- McAfee、使用者定義、開放原始碼等各種特徵碼
- 針對 Snort 特徵碼提供原生支援(NS 系列)
- 支援 Structured Threat Information eXpression (STIX) (NS 系列) 中的黑/白名單增強功能
- 主機隔離及速率限制
- 虛擬環境檢查
- 與 McAfee Advanced Threat Defense 整合
- HTTP 回應解壓縮支援

DoS 與 DDoS 防護

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

McAfee Global Threat Intelligence

- 檔案及 IP 信用評價
- 應用程式與通訊協定信用評價
- 地理位置
- 依據 McAfee Global Threat Intelligence 類別建立白名單

高可用性

- 主動-主動及主動-被動的狀態式容錯移轉
- 外部故障開啟 (主動)
- 內建故障開啟

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 雙重 VLAN

McAfee Network Security Manager

- 層級管理 (高達 1,000 個偵測器)
- 使用者驗證 (RADIUS 及 LDAP)
- 自動容錯移轉與容錯回復
- 重要組態資料嚴重損壞復原
- 集中的階層原則管理
- 記憶體儀表板詳細說明了裝置的記憶體使用率

深入瞭解

如需詳細資料及實體裝置選項，請參閱 **McAfee Network Security Platform 規格表**。

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