Wildfire™

在可擴充的雲端虛擬環境中，WildFire 能透過動態分析識別出未知的惡意程式、零時差入侵和進階持續性滲透攻擊 (APT)。WildFire 能近乎即時的自動佈署保護機制，協助安全團隊應付進階網路攻擊的挑戰。建立在企業級安全性平台上，無論流量來自哪個連接埠或使用 SSL 加密，系統都能自主針對流量（包含威脅和應用程式的流量）進行分類。

- 使用進階的靜態和動態分析技術來識別未知的惡意程式和零時差入侵。
- 針對未知威脅採用雲端動態分析，並對已知威脅與應用程式掌握完整可見度及控制力，雙效結合，確保精確、安全及可擴充的惡意程式分析。
- 真正的內嵌式封鎖具攻擊性與惡意檔案，亦能確實阻擋命令與控制流量。

進階網路攻擊採取狡猾的頑抗方式來閃避傳統的安全措施。若要技巧性地反制此類攻擊，安全團隊需要重新評估其基本設定，如傳統入侵防禦系統、防毒軟體和單一用途沙箱設備是否能應付打擊 APT 的任務。

企業級安全性平台

WildFire 以領先業界的安全性平台為基礎，具有完整掌握網路流量可見度的能力，讓想透過非標準連接埠或 SSL 加密閃避偵測的入侵攻擊都無所遁形。運用威脅防禦機制主動阻擋已知威脅，針對已知入侵、惡意程式、惡意 URL 及命令與控制 (C&C) 活動提供基礎防衛。WildFire 能在可擴充的虛擬沙箱環境中針對未知檔案進行分析，並可在此辨識新型態威脅，自動產生保護機制以立即執行防禦。分析結果具針對性，並能使用封閉式迴路方式來控制網路威脅。首先，系統採用主動式安全性控制來減少攻擊區域、檢查所有流量、連接埠和通訊協定以封鎖所有已知威脅，並在雲端虛擬執行環境中觀察其實際行為以快速偵測出未知威脅，然後立即在前線部署新的保護機制，確保先前的未知威脅已讓所有單位知悉並在所有攻擊鏈上都能加以阻擋。

WildFire

WildFire 具備先進的虛擬惡意程式分析環境，經精密設計，適合執行高精確度的硬體模擬以及可疑樣本的分析。雲端服務不僅能依賴現有的特徵碼，更能觀察流量中的惡意行為，從而偵測並封鎖具針對性的未知惡意程式、入侵和外部 C&C 活動。除了能快速將未知威脅轉化成已知威脅，WildFire 還能在 15 分鐘內產生能全面共用的保護機制。與 Palo Alto Networks® 新一代防火牆緊密整合的安全性服務，在面對網路犯罪者試圖傳送惡意程式或與受感染系統通訊時，協助您全面控管您的網路。

發現行為式網路威脅

為了找出未知的惡意程式和入侵，WildFire 能在 Windows XP、Windows 7 和 Android 作業系統上執行可疑內容，並能針對以下常見的檔案類型，擁有其內容的完整可見度：EXE、DLL、ZIP 檔、PDF 文件、Office 文件、Java、Android APK、Adobe Flash 程式，以及包含高風險的內嵌式 JavaScript、Adobe Flash 檔和圖片的網頁。

paloalto networks

WildFire 能辨識 200 種以上的潛在惡意行為，系統能辨識以下動作來判別出惡意檔案本質：

- **對主機進行變更：**觀察所有針對主機的修改過程，包括檔案、登錄活動、程式碼插入、記憶體 Heap Spray（入侵）偵測、額外的自動執行程式、Mutex、Windows 服務及其他可疑活動等。
- **可疑的網路流量：**針對所有因為後門建立、進階惡意程式、造訪低信評網域和網路勘探等情況而產生的可疑檔案進行網路活動分析。
- **反分析偵測：**監控進階惡意程式用來躲避 VM 分析的技術，例如，偵錯工具偵測、虛擬機管理程序偵測、插入受信賴程序的程式碼、造成主機安全功能停用等技術。

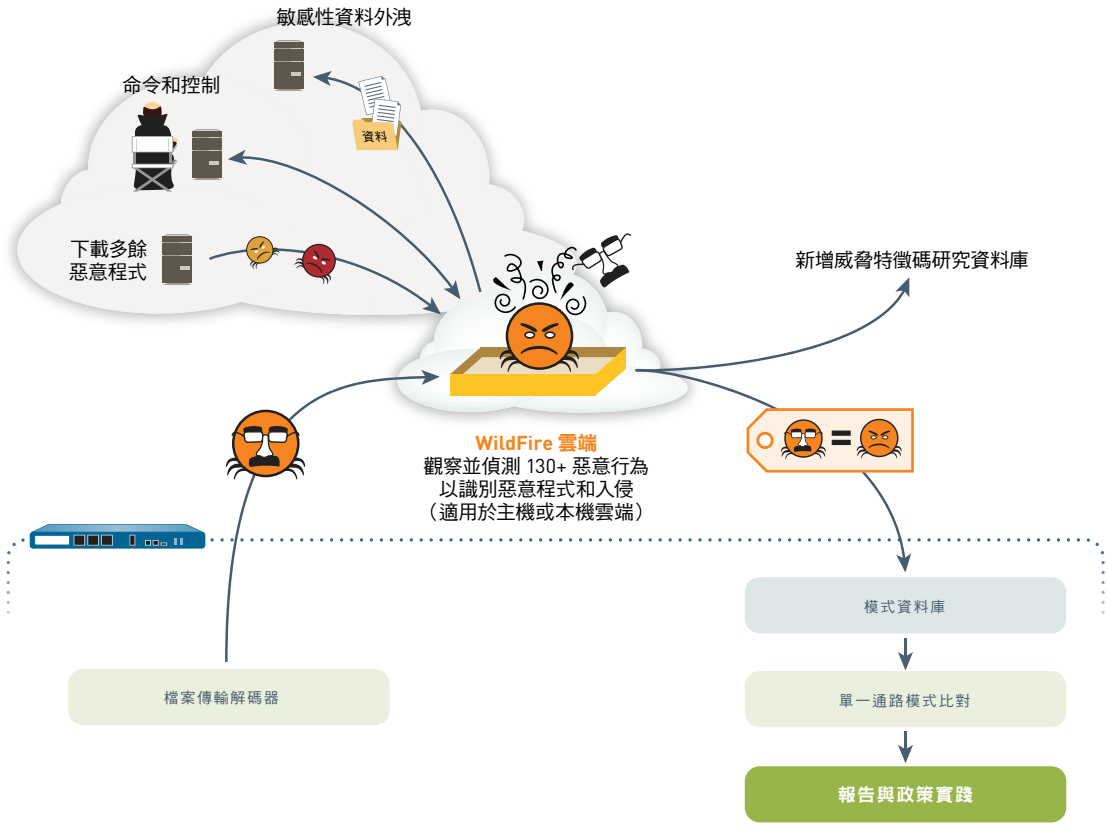
WildFire 拓展了新一代防火牆平台功能，能自主針對數百種應用程式的流量進行分類。無論何種連接埠或加密，WildFire 都能套用此行為分析，還能針對網頁流量、電子郵件通訊協定 (SMTP, IMAP, POP) 及 FTP，提供完整可見度。

以雲端為基礎的偵測架構

為了支援您系統上所有網路的動態惡意程式分析，建立在雲端架構的 WildFire，無須額外硬體就能透過既有的 Palo Alto Networks 新一代防火牆來使用。若因規定或隱私需求無法使用公用雲端基礎結構，也可使用 WF-500 設備來建立內部部署的私有雲端解決方案。無論是公用或私用，WildFire 都提供同等級的最佳可見度，以及簡便、具成本效益的部署。

全面情報共享打造有效的威脅防禦

一旦發現未知威脅，WildFire 能在短短 15 分鐘內自動產生保護機制，在整個網路攻擊鏈上進行封鎖，並與系統上的所有具備此授權之用戶共用這些更新。這些快速更新程式能迅速阻擋惡意程式蔓延，並且無需額外動作或分析，就能針對所有未來變種的繁衍進行識別和封鎖。Palo Alto Networks 客戶的全面情報共享機制，協助我們為阻止網路攻擊邁出成功的一步。



WildFire 運作方式：WildFire 結合新一代防火牆硬體與可擴充的雲端惡意程式分析，提供使用者合理的運用組合。

除了針對惡意及受入侵檔案的防禦機制，WildFire 還能使用反 C&C 特徵碼及 DNS 回撥式特徵碼深入檢查惡意的外部通訊、中斷命令 — 控制活動。這些資訊也會提供給 PAN-DB，新發現的惡意 URL 會在此自動加以封鎖。若要在網路上將進行中的入侵和未來的攻擊加以識別並封鎖，這些相互關聯的資料和內聯的保護機制正是關鍵所在。

整合式記錄、報告和鑑識

WildFire 使用者會接收來自管理介面、Panorma、WildFire 事件的整合式記錄、分析，讓安全團隊能快速進行調查，並在網路中觀察到的事件中找出關聯性。這讓安全團隊成員能迅速找出需要即時調查及做出事件回應的資料位置。透過記錄分析與自訂特徵碼，就能進行主機式及網路式的危害分析。

WildFire 還提供以下功能協助安全與 IR 工作人員找出受感染的主機：

- 針對來自多種作業系統環境（包括主機式與網路式活動），傳送至 WildFire 的每個惡意檔案進行詳細分析
- 與傳送惡意檔案相關的工作階段資料，包括來源、目的地、應用程式、User-ID™ 及 URL 等。
- 存取原始惡意程式樣本以進行逆向工程及動態分析工作階段的完整封包採集。
- 開放式 API，能與同等級最佳的 SIEM 工具（例如適用於 Splunk 的 Palo Alto Networks 應用程式）以及市場主流終端用戶安全程式進行整合。

此分析提供廣泛的資料危害分析 (IOC)，能套用在所有 APT 攻擊鏈上。

維護您檔案的隱私性

WildFire 能運用直接受 Palo Alto Networks 管理的公用雲端環境。所有可疑檔案都能安全的透過加密連線在防火牆和 WildFire 資料中心間傳輸，並透過 Palo Alto Networks 在兩邊登入。所發現的檔案若無害即予以銷毀，惡意程式檔則保存以供進一步分析。

WildFire 程式需求：

- 需要 PAN-OS™ 4.1+ 以使用 WildFire
- PDF、Java、Office 及 APK 分析需要 PAN-OS 6.0+
- Adobe Flash 及網頁分析需要 PAN-OS 6.1+

授權資訊：

使用 PAN-OS 4.1 或更高版本的系統都能在所有平台上執行基本 WildFire 標準功能。

- Windows XP 和 Windows 7 分析用之映像檔
- EXE 和 DLL 檔案類型，包含壓縮 (zip) 和加密 (SSL) 內容
- 自動提交可疑檔案至 WildFire
- 每隔 24-48 小時，自動透過定期威脅防禦內容更新（需要威脅防禦授權）來提供保護機制。

WildFire 功能授權針對進階威脅新增近乎即時的保護機制，提供下列新功能：

- 針對全球所偵測到的新種惡意程式，每隔 15 分鐘就自動更新 WildFire 特徵碼。
- 增強檔案類型支援，包括：PE檔（EXE、DLL及其他）、所有 Microsoft Office 檔案類型、Portable Document Format (PDF) 檔、Java小程式（JAR和CLASS）、Android Application Package (APK)、Adobe Flash 小程式（SWF 和 SWC），以及網頁。
- 支援 WF-500。
- WildFire API 程式每日可提交多達 1,000 項樣本，以及 10,000 次報告查詢。

WF-500

WF-500 是選用的硬體設備，能支援選擇將 WildFire 部署為私用雲端以滿足資料隱私的需求。WF-500 為多數中大型規模網路量身打造，當流量增加或需要在各地建置網路時，提供可部署額外設備的選擇。

WF-500 規格

處理器
- 採用超執行緒技術的 Dual 6-Core Intel 處理器

記憶體：
- 128 GB RAM

系統磁碟
- 120GB SSD

硬體規格

I/O
- 4x10/100/1,000
- DB9 主控台序列埠、USB

儲存空間
- 2TB RAID1：4 x 1TB RAID 受認證 HDD for 2 TB 的 RAID 儲存空間

電源供應：
- Dual 920W 熱交換、多餘組態電源供應器

最大消耗電源
- 510 瓦

機架安裝（尺寸）
- 2U, 19" 標準機架 (3.5"H x 21"D x 17.5"W)

最高 BTU/HR
- 1,740 BTU/hr

輸入電壓（輸入頻率）
- 100-240VAC (50-60Hz)

最大消耗電流
- 11A@100VAC

安全性
- UL, CSA, CB

EMI
- FCC Class A, CE Class A, VCCI Class A

環境
- 操作溫度：華氏 32~95 度，攝氏 5~35 度
- 不可操作溫度：華氏 -4~158 度，攝氏 -40~65 度

請登入 **www.paloaltonetworks.com/products** 以取得 WF-500 安全性等相關功能的更多資訊

paloalto networks
the enterprise security company™

4401 Great America Parkway
Santa Clara, CA 95054

主要電話： +1.408.753.4000
銷售專線： +1.866.320.4788
支援專線： +1.866.898.9087

www.paloaltonetworks.com