WILDFIRE

自動預防高迴避能力的零時差入侵和惡意軟體

Palo Alto Networks® WildFire™ 雲端威脅分析服務是業界針對高迴避能力零時差入侵和惡意軟體而言最先進的分析和預防引擎。該服務運用獨特的多重技術做法，結合動態和靜態分析、創新的機器學習技術和突破性的裸機分析環境，能夠偵測並預防最有迴避能力的威脅。

WildFire 威脅分析和預防服務：

- 使用動態和靜態分析、創新的機器學習技術以及領先業界的裸機分析環境的獨特組合，偵測規避型零時差入侵和惡意軟體。
- 世界任何地方第一次發現未知威脅後的 300 秒內，協調對於威脅的自動化預防，不需要手動因應。
- 運用 14,000 多個訂戶共享的即時情報，發揮對於未知惡意軟體和入侵的集體免疫能力。
- 運用 AutoFocus™ 環境威脅情報服務提供高相關性威脅分析和脈絡。

現今的組織必須對付整個惡意軟體和入侵市場，這些惡意軟體和入侵開發人員向所有類型的攻擊者販售或出租惡意工具。同時，進階迴避技術已經商品化，能夠讓攻擊者規避舊式偵測做法。現在，即使低技能的攻擊者都能夠發動獨特的攻擊，迴避傳統的威脅識別和預防做法需要人力介入才能處理，但是人力無法針對現今大量的未知威脅進行調整。

WildFire 改變了攻擊者佔居的優勢，將每個 Palo Alto Networks 平台部署轉化為分散式感應器和強制執行點來阻止零時差惡意軟體和入侵，以免擴散並成功發動攻擊。在 WildFire 環境中，只要世界任何地方第一次發現威脅，就會在 300 秒內觸發威脅並擷取情報，然後自動在 Palo Alto Networks 新世代安全平台協調預防措施。

運用獨特的多重技術做法尋找未知威脅

WildFire 突破偵測未知威脅的傳統做法，結合 4 種獨立的技術進行高擬真度防迴避發現，其中包括：

- **動態分析：**在特別設置的防迴避虛擬環境中觀察觸發的檔案，以便使用數百種行為特性偵測零時差惡意軟體和入侵。
- **靜態分析：**高效率偵測嘗試迴避動態分析的惡意軟體和入侵，並立即識別現有惡意軟體的變體。
- **機器學習：**從每個檔案擷取數千個特徵，訓練預測性機器學習模型識別新的惡意軟體，這是單獨使用靜態或動態分析所無法達到的效果。

- **裸機分析：**規避型威脅會被自動傳送到實際的硬體環境進行觸發，完全解除攻擊者對抗 VM 分析技術的能力。

這四種獨特的技術能夠讓 WildFire 有效發現並預防未知的惡意軟體和入侵，達到近乎零誤判的成效。

預防的自動協調

WildFire 使用者在世界任何地方第一次發現零時差入侵或惡意軟體時，服務會在 300 秒內為所有 WildFire 訂戶自動協調進行高度擬真的防迴避保護。這些保護會擴及 14,000 多位 WildFire 使用者，形成業界最大的分散式感應器網路，專門偵測和預防未知威脅。WildFire 也會成為 Palo Alto Networks 新世代安全平台的中央預防協調點，以便實施新的控制：

- **Threat Prevention** 封鎖惡意軟體、入侵，以及命令與控制 (防 C2 和 DNS 型回呼) 活動。
- **URL 篩選**結合 PAN-DB，可預防新發現的惡意 URL。
- **AutoFocus™** 環境威脅情報服務，能夠擷取、關聯和分析高關聯性並脈絡的威脅情報。
- **Traps™** 進階端點防護和 **Aperture™** SaaS 安全服務，發揮即時裁定和威脅預防的效用。
- 與技術合作夥伴整合，使用第三方服務與 WildFire API 進行裁定。

最先進的惡意軟體分析環境

WildFire 經過 4 年的突破創新，推出業界最先進的分析環境，能夠對於現今的未知威脅進行最準確的防迴避偵測。WildFire 引擎由 2 個主要元件組成：

- **自訂超管理器：**WildFire 超管理器經過全新設計，避免使用很容易迴避的常用開放原始碼模擬軟體，能夠破解迴避傳統惡意軟體分析環境偵測的商品化對抗 VM 分析技術。自訂超管理器也提供彈性架構，未來可持續將進階偵測和防迴避功能加入 WildFire 中。
- **裸機分析：**最精密的威脅即使在最先進的虛擬環境中也可能會觀察到本身被檢查，而無法被完全觸發。為了因應這種新型攻擊，WildFire 能夠在實際的硬體系統中使用裸機分析引擎自動分析進階威脅。現在，即使最有迴避能力的威脅最終能夠加以識別和預防。

在惡意軟體分析環境中，WildFire 會執行 Windows® XP、Windows 7、Android™ 和 macOS™ 作業系統中可疑的內容，充分掌握通常遭入侵的檔案格式，包括：EXE、DLL、ZIP、PDF、Microsoft® Office 文件、Java® 檔、Android APK、Adobe®Flash®小程式，以及電子郵件訊息中的連結。WildFire 能辨識數百種潛在惡意行為，依據檔案動作來判別出惡意檔案本質：

- **全面的惡意行為可見度：**識別數百個應用程式的所有流量中的威脅，包括網路流量、電子郵件通訊協定 (SMTP、IMAP、POP) 和 FTP，無論使用何種連接埠或加密。
- **對於主機的變更：**觀察對於主機進行修改的所有程序，包括入侵跡象、持續性機制、資料加密 (勒索軟體) 或系統破壞技術。
- **可疑網路流量：**分析可疑檔案產生的所有網路活動，包括後門建立、下載進階惡意軟體、造訪低信評網域和網路偵察。
- **反分析偵測：**監控進階惡意軟體用來躲避 VM 分析的技術，例如，偵錯工具偵測、超管理器偵測、插入受信賴程序的程式碼、造成主機型安全功能停用等技術。

威脅情報、分析和關聯

組織能夠結合 WildFire 使用 AutoFocus 偵測高關聯性和脈絡的最具針對性的威脅。AutoFocus 能夠搜尋從 WildFire 擷取的所有資料，並且使用 Unit 42 威脅研究團隊的人工智慧比對危害指標 (IoC) 和樣本。WildFire 和 AutoFocus 完整呈現鎖定貴組織和產業的未知威脅，而且能夠讓您運用情報進行處理，完全不需要配置專門處理的安全人員。

安全、可擴充的雲端架構

WildFire 的獨特雲端架構支援網路、端點和雲端的大規模未知威脅偵測和預防。客戶能夠運用 Palo Alto Networks 新世代安全平台提供的服務，完全不會對防火牆造成效能影響。WildFire 有多種部署模式可供使用，能夠滿足當地最嚴格的隱私權或法規需求，包括：

- **全球雲端交付：**檔案提交到 WildFire 全球雲端，達到擴大規模並提升速度的效果，能夠讓 Palo Alto Networks 的任何客戶迅速啟動服務，包括新世代防火牆、VM-Series、公共雲端服務、Aperture 和 Traps。
- **私人雲端交付：**本機內部部署裝置 WF-500 可進行所有威脅觸發、情報擷取和防護產生活動，而且可對於有隱私權或法規需求的客戶持續接收來自全球雲端的更新。
- 混合雲端交付：您可以結合全球雲端與私人雲端的優點，選擇將機密檔案傳送到私人雲端，而由全球雲端分析其他內容。
- **歐盟 (EU) 地區雲端交付：**對於需要使用 WildFire 但是由於法規而無法將內容傳送到當地以外地區的組織，檔案不會離開歐洲資料中心。使用者仍然可獲得全球雲端提供的保護。

整合式記錄、報告和鑑識

WildFire 使用者可透過 PAN-OS® 安全性作業系統管理介面、Panorama™ 網路安全管理、AutoFocus 或 WildFire 入口網站獲得整合式記錄、分析和可見度，讓團隊能快速進行調查，並在網路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並採取行動，包括：

- 針對在多種作業系統環境 (包括主機式與網路式活動) 中傳送至 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™ 使用者識別技術、URL 和其他屬性。
- 存取原始惡意軟體樣本以進行逆向工程及動態分析工作階段的完整封包擷取 (PCAP)。
- 與第三方安全工具整合的開放式 API，例如安全性資訊和事件管理 (SIEM) 系統。

新世代安全平台

WildFire 以 Palo Alto Networks 新世代安全平台為基礎，能夠預防已知和未知威脅造成危害，包括：

- **充分掌握**所有網路流量，包括隱密嘗試迴避偵測，例如使用非標準連接埠或 SSL 加密。
- 運用主動安全控制主動消除感染途徑，達到縮小攻擊範圍的效用。
- 運用新世代防火牆、Threat Prevention、URL 篩選、Traps 和 Aperture 自動預防已知威脅，防範已知入侵、惡意軟體、惡意 URL 以及命令與控制 (C2) 活動。
- 運用 WildFire 進行未知威脅偵測和預防，包括透過 AutoFocus 服務進行高關聯性和脈絡的威脅分析。

結果是獨特的封閉迴路式做法，藉以避免網路威脅，並確保這些威脅已被公告週知，而且在攻擊生命週期中予以封鎖。

維護您檔案的隱私性

客戶資料的安全和隱私是我們的首要重點。WildFire 基礎設施直接由 Palo Alto Networks 管理，運用安全性和機密性的業界標準最佳實務，而且針對 SOC 2 合規性定期接受稽核。您可以在 **WildFire 隱私權資料表**找到詳細資訊。

WildFire 程式需求：

- PAN-OS 4.1 以上版本
- PDF、Java、Office 及 APK 分析需要 PAN-OS 6.0 以上版本
- Adobe Flash 及網頁分析需要 PAN-OS 6.1 以上版本

授權資訊：

WildFire 全球雲端訂閱提供：

- Windows XP、Windows 7、macOS 和 Android OS 虛擬分析環境。
- 對於任何 WildFire 訂戶發現並將樣本提交到 WildFire 全球雲端的零時差惡意軟體和入侵，每 300 秒 (5 分鐘) 提供自動化特徵碼更新。特徵碼包含檔案型防毒特徵碼、網域 (DNS) 特徵碼，以及 URL 特徵碼。URL 特徵碼需要 PAN-DB 訂閱。
- 支援 PE 檔 (EXE、DLL 等等)、所有 Microsoft Office 檔案類型、PDF 檔、Flash 檔，以及 Java 小程式 (JAR 和 CLASS)、Android APK、MacOS 二進位檔案 (mach-O、DMG、PKG 和應用程式套件組合)，以及對於電子郵件訊息內的連結進行的分析。這包括支援壓縮 (zip) 和加密 (SSL) 內容。
- 分析裸機分析環境中的特定樣本，由 WildFire 系統決定。
- 在執行 PAN-OS 4.1 (含) 以上版本的 Palo Alto Networks 中，Basic WildFire 功能是所有 Palo Alto Networks 客戶可用的標準功能，能夠啟用有限的 WildFire 功能，包括：
  - Windows XP 和 Windows 7 虛擬分析環境。
  - 僅自動提交 EXE 和 DLL 檔案類型，包含壓縮 (zip) 和加密 (SSL) 內容。
  - 透過每隔 24 小時的定期威脅防禦內容更新 (需要 Threat Prevention 授權) 來自動提供保護機制。

4401 Great America Parkway
Santa Clara, CA 95054

總部辦公室： +1.408.753.4000
銷售專線： +1.866.320.4788
支援專線： +1.866.898.9087

www.paloaltonetworks.com