Advanced WildFire

透過內嵌 AI 防護阻止高迴避性惡意軟體

相較於現在的企業，現代威脅行動者有兩個主要優勢：機會和可存取性。隨著採用混合工作、轉移到雲端以及 IoT 和 SaaS 應用程式的快速成長，攻擊範圍已經擴大，威脅行動者有著絕佳機會可以尋找滲透企業的方法。此外，勒索軟體即服務和自動化產品降低部署複雜惡意軟體活動的技術門檻，因此即使是懶散且技術不夠嫻熟的攻擊者也能夠輕易地存取其需要的各種工具來擴大攻擊數量、嚴重性和影響範圍。

雲端支援的內嵌機器學習和內嵌靜態分析超越單純的檔案分析

Palo Alto Networks Advanced WildFire® 是業界最大的雲端惡意軟體防禦引擎，使用獲得專利的機器學習偵測引擎保護企業免於遭受高迴避性威脅，因而達到跨網路、雲端和客戶應用程式端點的自動保護。

Advanced WildFire 分析樣本時，將透過下列分析引擎的組合進行：

- 新世代防火牆上的**輕量級內嵌機器學習模型**可以即時防禦已知惡意軟體和未知變體。
- **雲端支援的內嵌機器學習和靜態分析**可以偵測及防止零時差惡意軟體以防範第一感染源攻擊。
- **靜態分析**會檢查檔案的特徵，同時運用動態解壓縮，對試圖經由封裝工具集規避偵測的威脅進行分析。
- **雲端式機器學習**模型從每個檔案中擷取數千個獨特特徵，這是靜態或動態分析所無法達到的效果。
- **動態分析**在特別建置的防迴避虛擬環境中觀察觸發的檔案，可以偵測先前未知的惡意軟體。
- **智慧型即時記憶體分析**會對於記憶體中的惡意活動拍攝快照並進行即時分析以識別惡意行為，偵測原本無法偵測到的高迴避性惡意軟體。

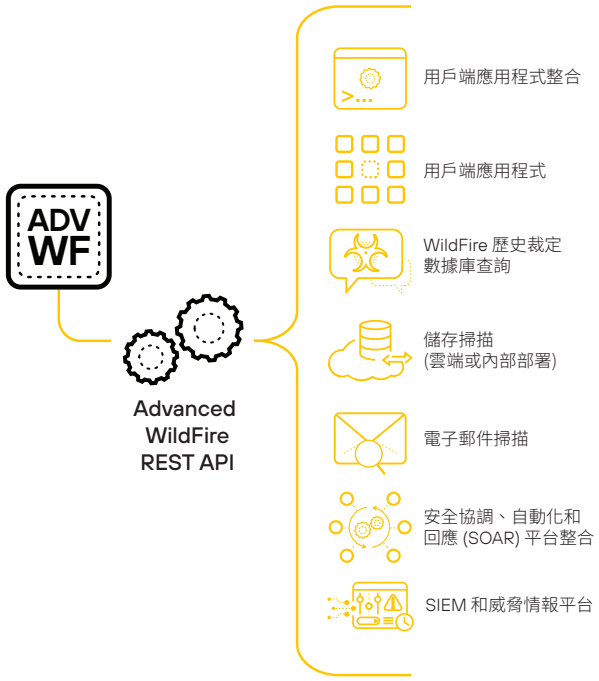


圖 1：Advanced WildFire REST API

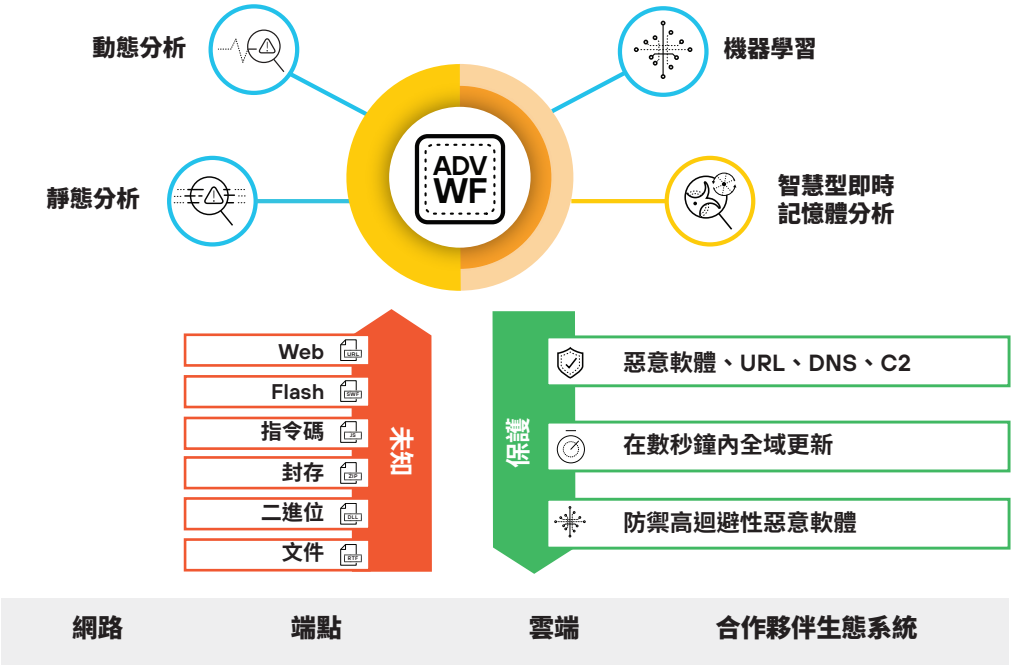
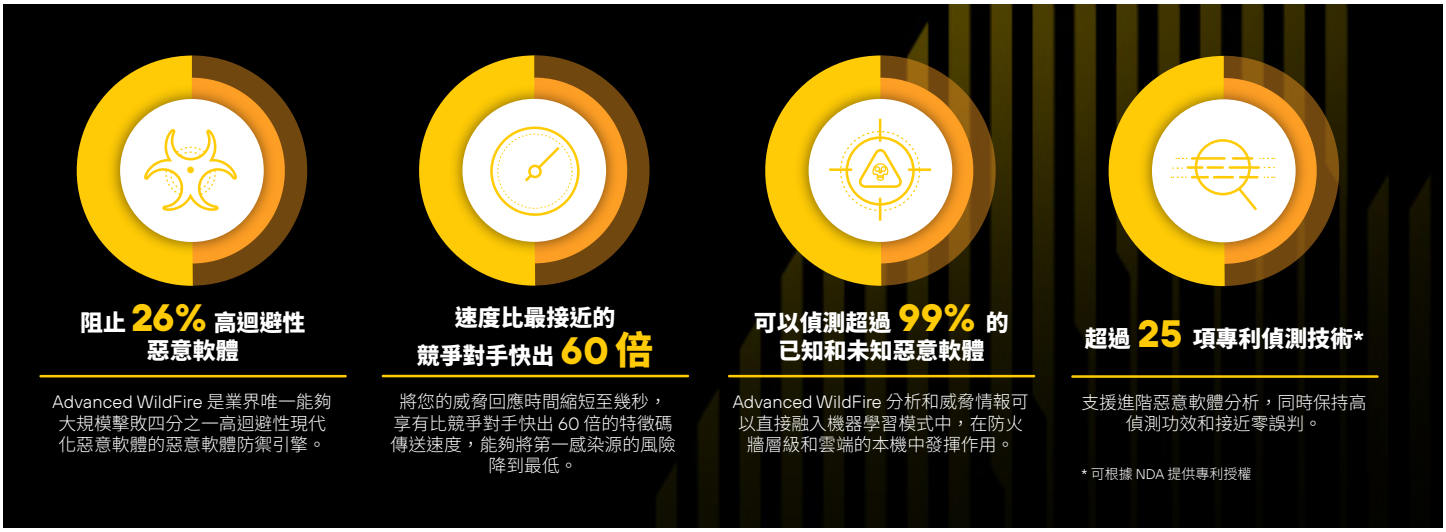


圖 2：用於保護整個企業的整合式安全性

根據分析，自動化防禦是 Advanced WildFire 的優勢所在。它可在邊緣、數據中心、雲端、軟體即服務 (SaaS) 應用程式以及端點上套用快速且一致的防護。Advanced WildFire 超越傳統的沙箱方法，可以在雲端中防禦未知和高迴避性惡意軟體。



主要優點

Advanced WildFire 解決方案可讓您：

- 利用「無限制」特徵碼儲存庫並存取所有已知的 AV 特徵碼。
- 在符合合規性要求的同時達到全面保護。
- 減少可採取動作的事件和 SOC 的工作負載。
- 與 Palo Alto Networks 平台進行原生整合。
- 利用機器學習式引擎以內嵌方式阻止惡意檔案類型。

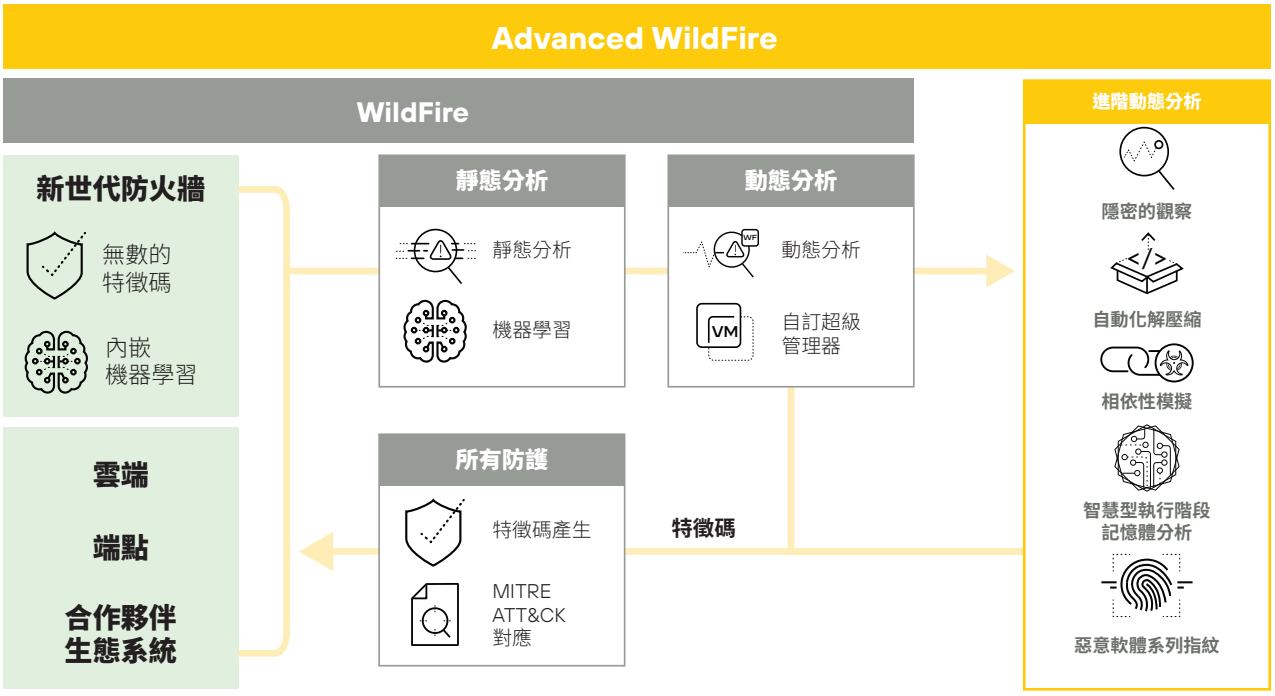


圖 3：Advanced WildFire 偵測引擎

產品功能

偵測惡意行為

Advanced WildFire 會識別具有潛在惡意行為的檔案，然後透過套用威脅情報、分析和關聯性以及進階功能，依據檔案的動作做出判斷，其中包括：

- **完整的惡意行為可視性**能夠在數百個應用程式中識別所有流量的威脅，其中包括 Web 流量以及例如 SMTP、IMAP 和 POP 等電子郵件通訊協定。
- **可疑網路流量分析**會評估可疑檔案產生的所有網路活動，例如後門建立、進階惡意軟體下載等等。
- **無檔案攻擊/指令碼偵測**可以識別潛在惡意指令碼 (例如 JScript 和 PowerShell) 何時周遊於網路，並轉送到 Advanced WildFire 進行分析和執行。

透過內嵌機器學習在防火牆層級阻止威脅

Advanced WildFire 由持續在雲端中強化的威脅模型提供支援，並透過我們的硬體和虛擬機器學習式新世代防火牆部署內嵌機器學習式引擎。這種創新的無特徵碼功能可在常見的檔案類型中偵測危險內容 (例如可攜式執行檔和源自 PowerShell 的無檔案攻擊)，這是一種完全內嵌的功能，不需要進行雲端分析、不破壞內容，而且不會降低使用者的工作效率。

防禦高迴避性惡意軟體

使用下列主要功能抵禦現代惡意軟體迴避技術：

- **隱密的觀察**：如果惡意軟體認為本身是在沙箱環境中，則會進行環境檢查並停止觸發攻擊。它使用自訂強化的超級管理器，其中分析元件存在於訪客虛擬機器 (VM) 外部。
- **自動化解壓縮**：Advanced WildFire 可在分析過程中獲得檔案內容的完全可視性，並在封裝的承載中產生特徵碼。
- **相依性模擬**：運用全新的相依性模擬功能，沙箱環境將滿足惡意軟體執行所需的所有外部相依性，因此分析引擎能夠觀察惡意行為。
- **智慧型執行階段記憶體分析**：偵測基礎結構可支援智慧型執行階段記憶體分析，因而能夠在觀察到惡意行為時在記憶體中的關鍵點拍攝快照。
- **惡意軟體系列指紋比對**：使用獲得專利的惡意軟體系列指紋偵測將新威脅與已知惡意軟體系列相關聯，藉此以大規模的方式防禦迴避性惡意軟體。

數秒內完成整個 Advanced WildFire 生態系統的全球防禦

Advanced WildFire 應用強大的雲端式分析，可針對內嵌機器學習式防禦無法阻止的高度自訂威脅提供跨網路、雲端和端點的防禦。此外，還可部署支援 Advanced WildFire 的感應器，可在針對大多數新威脅進行初步分析後的幾秒內提供全球防禦。

使用特徵碼而不是雜湊

Advanced WildFire 使用內容特徵碼進行防禦，而不是使用雜湊值來透過單一特徵碼識別更多惡意軟體，因此可以防範單一惡意軟體多達數百萬個多型態變體。

在相容且安全的雲端架構中進行部署

系統會將檔案提交至 Advanced WildFire 全球雲端，進而提升速度和規模。客戶可以開啟該服務，其中包括硬體和虛擬機器學習式新世代防火牆、公有雲產品、新世代 CASB 和 Cortex XDR® 代理程式的使用者。此外，Palo Alto Networks 遵循業界標準的安全性和機密性最佳實務，透過定期的 SOC 2 合規性稽核直接管理 Advanced WildFire 基礎結構。如需詳細資訊，請參閱 Advanced WildFire 隱私權型錄和認證網頁。

與現有安全工具及自訂應用程式緊密整合

在朝向雲端與數位轉型的快速發展過程中會面臨安全挑戰，因此需要新世代防火牆或傳統控制點以外的快速、有效且隨需的惡意軟體分析。客戶可以利用 Advanced WildFire 領先業界的惡意軟體分析功能來與現有的 SOAR 工具整合、保護自訂應用程式 (例如企業對消費者的 Web 入口網站)、以及在雲端移轉之前掃描檔案共用與儲存位置是否存在惡意內容等多種動作。此外，新世代防火牆的 Advanced WildFire 訂閱可以解鎖對固定數量提交和查詢的 API 存取。

獨立 WildFire API

獨立 WildFire API 訂閱可讓您查詢 WildFire 雲端威脅數據庫以取得有關潛在惡意內容的資訊，並根據企業的特定要求使用 WildFire 的進階威脅分析功能提交檔案進行分析。

整合式記錄、報告和鑑識

Advanced WildFire 使用者可以透過 PAN-OS® 管理介面、Panorama® 網路安全管理、Strata™ Cloud Manager、Cortex XDR 或 Cortex XSOAR® 獲得整合式記錄、分析和對惡意事件的可視性，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。

表 1：功能和授權摘要

	透過連線至新世代防火牆的 Advanced WildFire 訂閱而啟動的功能
檔案支援	PE 檔案 (EXE、DLL 等等)、所有 Microsoft Office 檔案類型、Mac OS X 檔案、Linux (ELF) 檔案、Android Package Kit (APK) 檔案、Adobe Flash 和 PDF 檔案、封存 (RAR 和 7-Zip) 檔案、指令碼 (BAT、JS、VBS、PS1、Shell 指令碼和 HTA) 檔案、電子郵件訊息中的連結分析以及加密 (TLS/SSL) 檔案。
通訊協定支援	SMTP、POP3、SMB、FTP、IMAP、HTTP 和 HTTPS。加密版本也支援先前提到的通訊協定。
每日檔案分析	每天分析超過 8000 萬個唯一檔案。
特徵碼類型	• 依據在 Web 流量 (HTTP/HTTPS)、電子郵件通訊協定 (SMTP、IMAP 和 POP) 和 FTP 流量中發現的全新/零時差惡意軟體。 • 根據樣本的惡意軟體承載產生特徵碼，而且測試特徵碼的準確性與安全性。
未知惡意軟體的防護功能更新	數秒之內，對於連線的新世代防火牆使用零延遲特徵碼。*
區域雲端位置	澳大利亞、加拿大、德國、印度、日本、荷蘭 (歐盟地區雲端)、新加坡 (亞太地區雲端)、英國、美國 (全球雲端與美國政府雲端)。區域雲端。
WildFire API 金鑰	新世代防火牆的 Advanced WildFire 訂閱包含 Advanced WildFire API 的存取權，可將 Advanced WildFire 整合至其他應用程式。此 API 有檔案提交和雜湊查詢的每日限制。
整合	• 與 Palo Alto Networks 整合，包括所有雲端交付的安全訂閱、Cortex XDR、Cortex XSOAR、Prisma Access、Prisma Cloud 和 SaaS 安全性。 • 與技術合作夥伴整合，使用第三方服務與 Advanced WildFire API 進行裁定。
管理與報告	Palo Alto Networks Panorama 以及 WebUI、API 和 AIOps。

表 1：功能和授權摘要 (續)		
	透過連線至新世代防火牆的 Advanced WildFire 訂閱而啟動的功能	
鑑識	• 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 Advanced WildFire 的每個惡意檔案進行詳細分析。 • 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。	
信任與隱私權	Palo Alto Networks 擁有嚴格的隱私權與安全性控制措施，以防止在未獲授權情況下存取機密或個人可識別資訊。我們會套用業界標準的最佳實務提供安全性和機密性。您可在我們的隱私權型錄中找到進一步的資訊。	
	Advanced WildFire 功能	PAN-OS 需求
需求†	WildFire 雲端式檔案分析	任何支援的 PAN-OS
	Advanced WildFire 雲端式檔案分析	任何支援的 PAN-OS
	新世代防火牆內嵌機器學習 (PE、ELF、PS1、PS2、Office)	10.1+
	Advanced WildFire 即時特徵碼交付	10.1+
	Advanced WildFire 內嵌第一感染源防護	11.1
建議的環境	Palo Alto Networks 新世代防火牆可以部署在任何位置，因為內部和外部來源都可能會將檔案型威脅引入到網路中。	

* 需要 PAN-OS 10.1。

† 客戶可以購買任何 PAN-OS 版本的 Advanced WildFire，並在升級後獲得額外功能。若要使用 Palo Alto Networks Advanced WildFire 訂閱的功能，您必須符合此處所示的 PAN-OS 要求。

諮詢熱線：0800666326
網址：www.paloaltonetworks.tw
郵箱：contact_salesAPAC@paloaltonetworks.com

Palo Alto Networks 台灣代表處
11073 台北市信義區松仁路 100 號 6F-1

strata_ds_advanced-wildfire_032624