

進階威脅防禦

即時阻止零時差威脅與入侵

現在的網路防禦者面臨的其中一個主要問題是高迴避性和自動化攻擊的肆虐。透過使用複雜的工具集、對抗性即服務產品和常用的紅隊工具可以公開存取版本，惡意行動者已經大幅地提高隱密攻擊的速度和成功率。此外，惡意行動者能夠以輕鬆且低成本的方式找到對於網路威脅而言進入障礙最低的弱點、暴露和其他未知進入點。

重新構思入侵防禦系統 (IPS)

Palo Alto Networks 進階威脅防禦是業界首創、能夠以完全內嵌的方式阻止零時差 C2 攻擊和未知入侵的**入侵防禦系統 (IPS)**。它超越傳統的 IPS 功能，可以提供業界領先的防護能力來防範已知和未知的威脅。進階威脅防禦是進階雲端交付安全服務套件的一部分，適用於包括 VM-Series 和 Prisma® Access 在內的硬體和軟體防火牆。

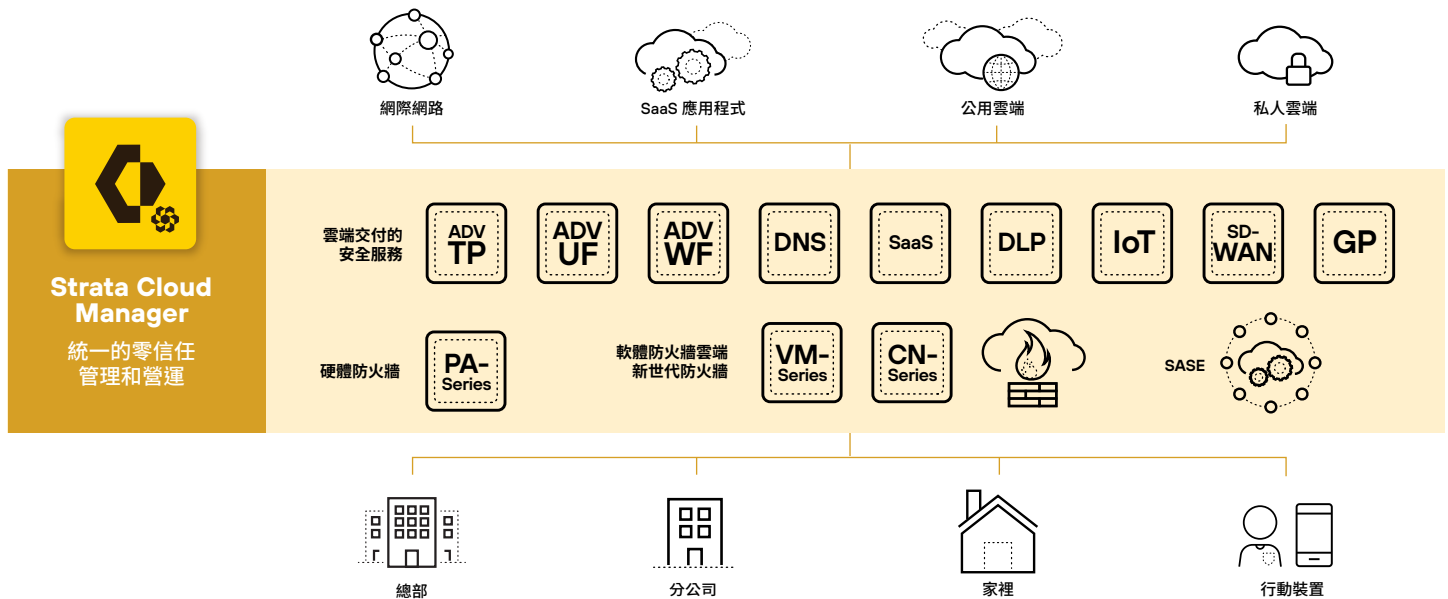


圖 1：Palo Alto Networks 雲端交付安全服務

主要優點

- 針對敵對工具的零時差和已知攻擊進行內嵌防禦。
- 針對已知的入侵和前所未見的弱點進行內嵌防禦。
- 以業界領先的機器學習方式即時偵測 Web 式威脅。
- 提供對於攻擊的全面可視性，檢查所有網路流量以找出威脅。
- 由 Unit 42® 和 Advanced WildFire® 業界領先的威脅情報提供支援。

產品功能

業界領先的進階威脅防禦

進階威脅防禦可以偵測並防止網路和應用程式層的入侵和規避策略。同時採用各種偵測方式以根據所觀察到的特定威脅性質來提供保護，包括特徵碼配對、機器學習和內嵌深度學習模型。我們所有的新世代防火牆 (NGFW) 和 Prisma Access 均提供此功能。

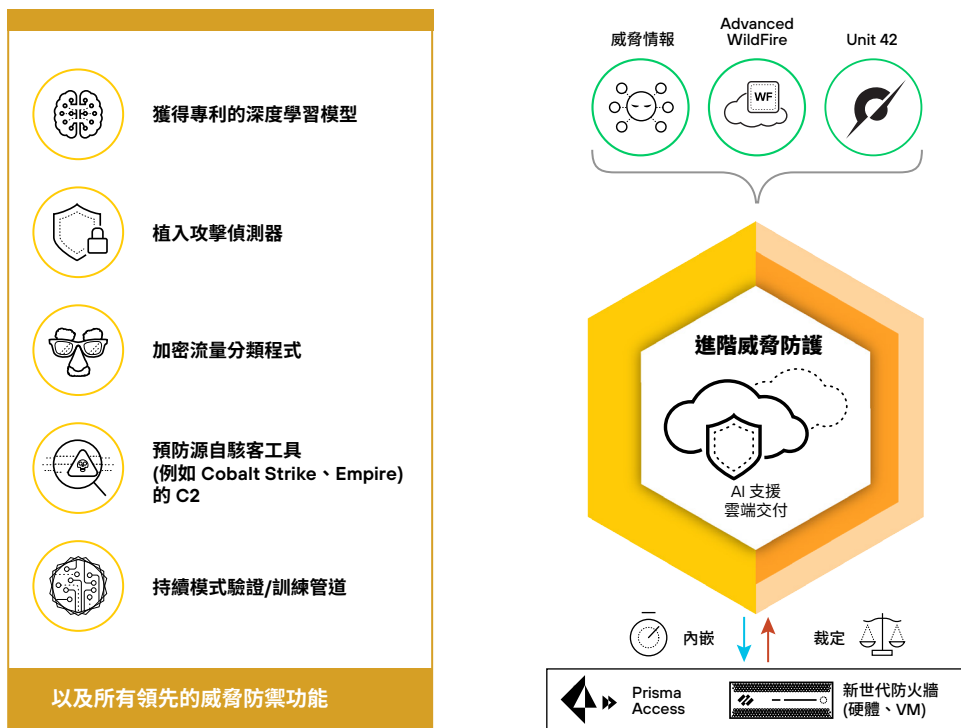


圖 2：Palo Alto Networks 進階威脅防禦

命令與控制 (C2) 偵測

進階威脅防禦使用專利的內嵌深度學習模型，可以阻止來自常見紅隊工具 (例如 Cobalt Strike 和 Empire) 的未知和迴避性 C2 流量。這些模型會持續在雲端更新以防止各種新興攻擊。進階威脅防禦還可以防止未知的 Web 式攻擊。在與特徵碼式偵測相互結合後，此功能還可以提供強大防禦來防止對手攻擊。

入侵防禦

進階威脅防禦使用雲端式機器學習模型，並且定期透過最新的訓練數據集進行更新，以防止未知的命令植入和 SQL 植入攻擊。其中包括對於數千個已知弱點的特徵碼式防禦，並針對各大廠商極為嚴重或高度嚴重的 CVE 提供業界領先的回應時間。

惡意軟體防禦

進階威脅防禦可以透過內嵌特徵碼式偵測阻止網路層的惡意軟體攻擊，並且結合 Advanced WildFire，可以提升防護層級以避免已知和未知的變體入侵目標主機。

關鍵的反惡意軟體功能包括：

- 防範隱藏在常見檔案類型中的惡意軟體。
- 針對隱藏在壓縮檔與網路內容中的惡意軟體防護功能。
- 來自我們 [Unit 42 威脅研究團隊](#) 的高真實性數據庫和情報。
- 由 Palo Alto Networks 收集的數十億個樣本產生的特徵碼。



96%

防禦 Web 式 Cobalt Strike C2。

此外，偵測到的迴避性 C2 流量多出 **48%**。*

*根據 Palo Alto Networks 測試的結果。

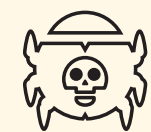


99%

防禦 Empire 傳播的 C2。

此外，ATP 能比傳統解決方案多阻止 **43%** 的未知 Empire C2 攻擊。*

*根據 Palo Alto Networks 測試的結果。



90%

防禦 SQLi 等植入攻擊。

此外，偵測到的零時差植入攻擊多出 **60%**。*

*根據 Palo Alto Networks 測試的結果。

核心入侵防禦服務

除了上述防護以外，我們的核心入侵防禦技術還提供：

- 自訂特徵碼以及與 Snort 和 Suricata 規則的相容性。
- 針對軟體弱點以及命令與控制攻擊量身打造的特徵碼。
- 啟發式分析、通訊協定解碼器式分析、基於通訊協定異常的防護，以及易於設定的自訂弱點特徵碼。
- 對流量進行檢查和分類，同時偵測及阻止單一通道中的惡意軟體和弱點入侵。
- 彙整的 IP 位址封鎖清單。

類別定義的網路威脅防禦						
威脅類別	 弱點	 暴力破解	 防毒軟體	 命令與控制	 檔案識別	 惡意 IP
	防範	• 內嵌雲端分析  • 入侵嘗試 • 弱點 • 迴避技術 • 混淆嘗試	• 連接埠掃描 • 緩衝區溢位 • 通訊協定拆分	• 以內容為基礎而不是以雜湊為基礎的特徵碼 • 已知的惡意軟體和未知的變體	• 內嵌雲端分析  • 命令殼層 • 惡意網域 • 承載檢驗 • DNS 沉洞	• 已知的惡意或高風險檔案類型 • 識別受保護的密碼

圖 3：進階威脅防禦功能