

新世代安全平台

防止入侵。提高生產力。保障安全的數位生活。

Palo Alto Networks® 新世代安全平台能讓企業、服務供應商和政府，使用以預防為主的網路安全措施，來保護我們的數位生活方式。我們的平台首先透過讓無論身在何地的使用者或裝置可以使用應用程式，然後在應用程式流量中預防威脅，並將應用程式的使用連結到實體和雲端網路的使用者身分上，使組織可以減少暴露於威脅之中。

Palo Alto Networks 新世代安全平台有 4 個重要的特性，能夠對於網路攻擊達到預防的效果：

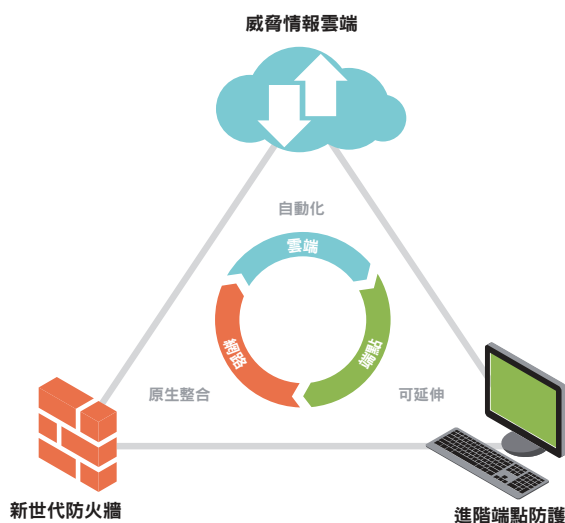
1. 原生整合式技術：

- 運用單通道架構，按照應用程式、使用者和內容來進行積極控制，減少組織攻擊範圍。
- 支援開放性通訊、協調與可見度。
- 維持一致的安全強度，對端點、數據中心、網路、公有和私有雲端以及 SaaS 環境提供相同的防護。

2. 即時在網路、端點和雲端環境中建立和重新設定安全強度，因應新的威脅，讓團隊能夠隨著技術擴張其防禦實力，而非受限於人數，達到**自動**防護的效果。

3. 使用者離開實體網路以及組織擴大並採用新的技術和架構時，能夠保持**延伸性和彈性**，進而獲得一致的防護效果。

4. **威脅情報共享**運用全球社群自動共享防護資訊所帶來的網路效應，提升預防功效，並有效阻止攻擊的擴散。



Palo Alto Networks 安全平台

- **新世代防火牆**：我們的新世代防火牆運用單通道平行處理架構，能夠展現獨步業界的安全功能。這個架構由**實體**和**虛擬**裝置組合實施，涵蓋各種效能和使用案例情境需求，能夠讓組織阻止具有躲避資安檢測能力的網路攻擊。

功能和管理在整個組合中均保持一致。與端點的**GlobalProtect™**網路安全整合，將基於政策的安全擴展到內部部署或遠端的行動裝置。

在 Panorama™ 整合網路安全管理能夠讓您從集中位置控制防火牆的分散式網路。檢視所有防火牆流量、管理裝置組態的所有層面、派送全域政策，並生成流量模式或安全事件報告，全部都可從一個主控台進行。此外，管理員可按照任何日誌欄位篩選日誌，並將相關日誌轉送至適當的收件者，以便讓網路和安全團隊進行跨職能協同作業來管理部署的不同層面。Panorama 的架構能夠取得新世代防火牆以外多個相關來源的日誌來提供執行防禦時的危害指標關聯，例如 Traps™ 進階端點防護日誌，因此會使有迴避能力的威脅現形，並且可搜尋彙總日誌找出攻擊的證據或進行歷史鑑識。

- **進階端點防護：**危害並非無法避免。傳統的端點保護根本跟不上快速演進的威脅形勢，使得企業容易遭受進階攻擊。需要的是新做法，一種能夠在端點安全方面重建信心的做法。Traps 用多重防禦方法取代傳統防毒軟體，以獨特方式結合了針對性的惡意軟體與漏洞防禦措施，可保護使用者與端點免受已知和未知的威脅攻擊。相較於重要資產已經遭到入侵之後的入侵偵測與事件回應，Traps 可防堵安全漏洞。

Traps 使用獨特的嶄新方式來預防入侵。Traps 不專注於數以百萬計的單次攻擊以及其所利用的軟體漏洞，而專注在所有入侵式攻擊中所使用的核心入侵或技巧。Traps 能使用獨特的多重防禦措施預防惡意執行檔，不但有著最大的惡意軟體防禦範圍，還能減少可能被攻擊的範疇，並增加惡意軟體偵測的準確度。Traps 也能夠運用與取自 WildFire™ 雲端威脅分析服務的威脅情報進行原生整合，自動進行重新設定，以便自動進行預防。

- **威脅情報雲：**威脅的複雜度、速度和數量大幅增加。攻擊者利用商品化的迴避技術隱身而不被偵測。為了確實跟上進自動化攻擊者的步伐，必須在機器層面防範威脅。對於已知和未知威脅，我們透過 Threat Prevention、URL 內容過濾和 WildFire 服務提供以雲服務為基礎的進階的雲端防護。Palo Alto Networks 運用威脅數據的機器學習，對命令與控制活動大規模提供研究人員等級的保護。WildFire 結合全新的自訂超管理器與裸機擬真主機執行，能夠偵測並預防具有躲避資安檢測能力的威脅。透過與 Palo Alto Networks 新世代安全平台的原生整合，以及能夠與可自訂的第三方情報反饋整合的能力，這些服務在網路、端點和雲端環境全面發揮進階威脅偵測和預防的效用，可以在 5 分鐘內向全球的所有訂戶自動共享防護機制。

雲端的進階偵測和預防由因 AutoFocus™ 脈絡威脅情報服務得到進一步強化。隨著組織轉而採用我們平台以預防為導向的做法，對於必須因應的攻擊，AutoFocus 為安全團隊提供優先處理且可據以採取行動的安全防護情報，並提供可針對重要威脅立即採取行動的脈絡。透過 AutoFocus 的 MineMeld 應用程式，安全團隊能夠將任何第三方情報來源連結到新世代平台，達到對於新的預防控制加以強化的效果。AutoFocus 能夠武裝加強威脅情報，因此能夠更快速有效調查獨特的目標攻擊。

- **雲端安全：**組織必須更靈活改變開發、部署和採用應用程式的方式。隨著組織愈來愈採用雲端進行虛擬化，應用程式和數據愈來愈分散，因此可能遭受危害的機率愈來愈高。組織需要一致的做法來防護任何這些環境，預防愈來愈多的風險、增加的營運複雜度和外洩。對於私有、公有和混合雲端運算環境，VM-Series 提供完整的新世代防火牆安全和進階的威脅預防。藉由 VM-Series，組織能夠一致掌握從生產到開發的任何雲端部署，並預防已知和未知的威脅。我們的原生雲端服務提供以雲端為中心的安全、可擴充、彈性架構，相當容易協調和管理，而且我們的雲端中立性能夠自由運用任何雲端環境。

- **Aperture：**當組織的每個業務單位都已採用 SaaS 應用程式提高生產力和成功率。IT 和數據監管團隊發現難以追蹤愈來愈多的新 SaaS 應用程式之運用。應用程式可以大量獲得、採用並儲存數 TB 的敏感數據，因而威脅面範圍明顯擴大。Aperture 擴展新世代安全平台保護 SaaS 環境，掌握哪些使用者使用哪些應用程式，對於愈來愈多受支援的應用程式強化安全政策，並能夠隔離或刪除雲端上資產來自動進行風險補救。

注重預防

愈來愈便宜的運算能力成本的缺點是網路罪犯和攻擊者能夠以愈來愈低的成本自動發動精密攻擊。現在發動成功的網路攻擊所需的成本愈來愈低，導致惡意活動大規模爆發，並對於企業營運和創新優勢之關鍵數位系統的信任基礎構成威脅。

資訊安全的最終目標便是讓您的事業能夠欣欣向榮，並讓您的組織不會成為網路入侵頭條新聞的主角。這意味著需要降低攻擊成功的可能性。Palo Alto Networks 新世代安全平台注重預防，能使網路安全風險降低到可控的程度，也讓各組織能夠區隔出最嚴重的威脅，專注在業務運作上。

從網路到雲端再到端點的一致性安全架構

在採用新的行動、SaaS、公有或私有雲端技術帶來更多生產力時，安全性不該成為當中的阻礙。貴組織應該能夠防範網路攻擊，對於應用程式和數據所在地點或使用方式自動因應風險進行調整。只有透過原生整合的安全平台，並在持續演化的技術環境中提供各式組件，才能持續性地防止新一代攻擊者對於目標利用新的攻擊媒介和安全漏洞。Palo Alto Networks 新世代安全平台採用原生工程技術，運用單通道預防架構，按照應用程式、使用者和內容來進行積極控制。其結果就是可以縮小攻擊範圍、提升可見度，並保持從網路到雲端和端點的一致安全等級防護。

靈活度和安全性：為什麼選擇？

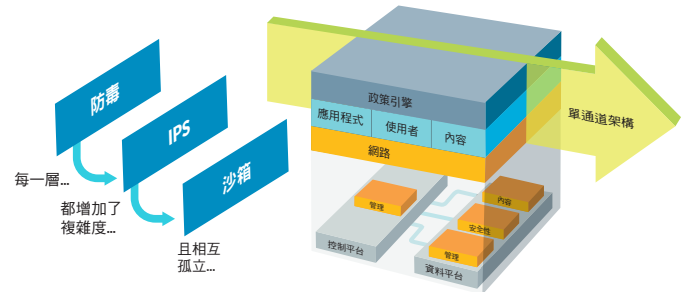
缺乏彈性又複雜的安全防護會對採用的新技術造成主要阻礙，例如提升組織靈活度的雲端運算和 SaaS 應用程式。在此情況下，安全性和靈活度成為犧牲品，最終失去提高生產力的機會，或隨著使用者規避嚴格的安全控制而導致組織面臨風險。

我們的平台能夠對任何位置的應用程式、使用者和內容將所有流量分類，一致實施安全政策，包括對實體和虛擬環境的威脅進行偵測和進階情報分析。採取這些措施後，平台即可安全地採用提高生產力的新技術，例如公有和私有雲以及 SaaS 應用程式。

改善的安全措施

多個單一功能產品組成的防護措施無法整合防護，徒留漏洞造成組織遭受攻擊。現今的攻擊透過許多步驟達到目的，預防攻擊需要自動分享多種來源的資訊並據以採取行動。孤立的工具無法彼此充分聯繫，且當其中一個工具為了因應新威脅而必須進行變更時，需要手動調整其他所有工具，才能反映變更。

以原生技術整合式的 Palo Alto Networks 新世代安全平台能夠充分掌握所有流量，按照應用程式、使用者和內容層級將流量分類，並提供實施安全政策以及使所有日誌與其他安全相關事件產生關聯所需的脈絡，提供詳細的威脅情報和分析。偵測未知的攻擊並建立保護機制，同時自動重新設定安全基礎設施，能夠隨著機器擴充其防禦實力，而非受限於人工操作。



舊式與新世代安全措施

提高效率 – 降低成本和複雜度

採用多個廠商的多種單一功能產品所形成的安全防護導致環境變得複雜而且耗費成本，不僅需要設備投資、多重授權訂閱和服務成本，而且需要耗費心力操作並維護這些產品。部署的單一功能產品增加後，企業的安全架構變得更加複雜，環境也變得更加複雜，安全團隊很容易就會在部署時出錯。管理不相關聯的點安全產品組合也會導致無法有效運用安全人員的時間，安全人員愈來愈發現自己忙於處理大量警示和繁雜的手動程序。

我們的安全平台能夠按照應用程式、使用者和內容將所有流量分類並加以判別，因此能夠運用脈絡和分析隔離獨特的目標攻擊，有助於安全人員釐清作業的輕重緩急，更有效地處理作業。整合式平台也能夠在偵測到未知的攻擊時自動重寫程式，建立並散播保護機制，完全不需要人為介入。Palo Alto Networks 新世代安全平台能夠整合多種產品的投資，降低複雜度，達到更高的可用性，並減少資金與作業支出。



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

© 2017 Palo Alto Networks, Inc. Palo Alto Networks 是 Palo Alto Networks 的註冊商標。您可在以下網址檢視我們的商標清單：<http://www.paloaltonetworks.com/company/trademarks.html>。本文提及的所有其他標誌皆為其各自公司所擁有之商標。next-generation-security-platform-ds-011117