paloalto networks.

the enterprise security company ™

不斷創新
持續領先

Palo Alto Networks 企業資安領導品牌

全球市場評價 – 新世代防火牆第一領導品牌

Palo Alto Networks 為企業、政府和服務提供者的網路提供保護，對抗網路威脅，引領著網路安全的新時代。在 2005 年由創辦人 NirZuk 成立於美國加州。我們讓企業能安全地使用所有應用服務，並能依照使用者身分，在各種網路、各種裝置上，精準地防禦各種已知與未知的安全威脅。我們的安全平臺天生就融合了所有關鍵的網路安全功能，包括進階威脅保護、防火牆、IDS/IPS，以及 URL 過濾功能。所以我們可以保證與傳統的防火牆、UTM 或威脅檢測產品相比擁有更佳的安全性。

Palo Alto Networks 以獨到的各項技術與完善的安全防護平台架構，再次引領資訊安全業界的新世代，並在全球擁有超過 26,000 位客戶、在台灣擁有超過 800 位客戶的高度評價與肯定，使我們成為市場上成長最快的安全公司。憑藉我們的平臺，公司組織可以安全地為所有應用保駕護航，保持全面的視覺化和可控性，充滿信心地實施雲和移動辦公等新技術專案，保護公司組織免遭網路攻擊。

好評見證

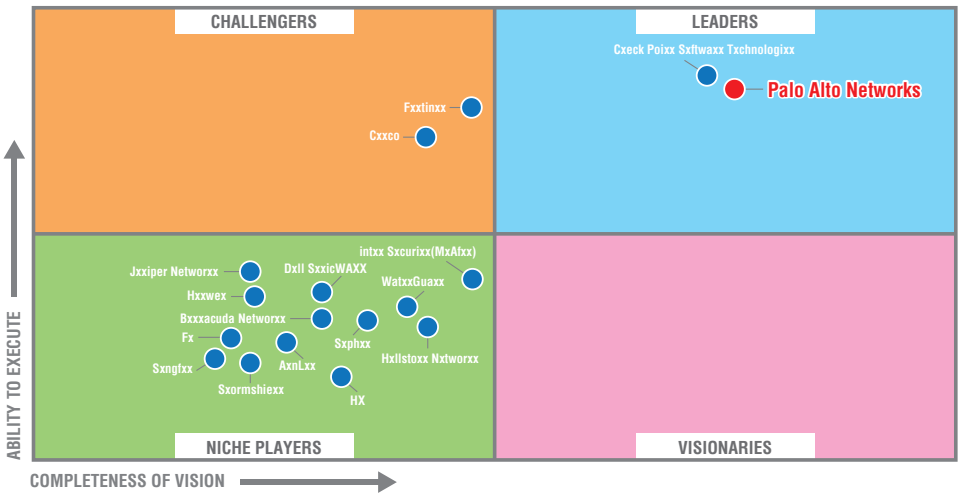
INDUSTRY ENDORSEMENTS

Gartner.	Magic Quadrant for Enterprise Network Firewalls, 4rd time running.
FROST & SULLIVAN	2014 APAC Network Security Vendor of the Year.
Goldman Sachs	2014 Security Outlook: Palo Alto Networks is out favorite Security idea.
IDC	Fastest Growing Security Applance Vendor in CY14. Market Share Growth: Larger than the top 3 players combined.
Deloitte.	Palo Alto Networks named to Deloitte's 2013 Technology Fast 500™.
Morgan Stanley	The state of the network security market: "We favor PANW as a dominart share gainer."
Jefferies	62% of respondents indcated share gains for PANW, which remains wel ahead of other vendors, ... PANW was the vendor cited the most often, 58% of partners, in winning competitive displacement.

跟著資安領導者 成為企業佼佼者

Palo Alto Networks 連續四年蟬聯魔術象限領導地位

Palo Alto Networks 在 2015 年四月份 Gartner 發佈的企業級防火牆魔術象限報告中，連續四年（2012-2015）被評鑑為領導品牌，此一得來不易的肯定與榮耀，再次證明 Palo Alto Networks 是極為重視網路資訊安全，憑藉著多年的資安防護經驗與領先群倫的研發與創新能力，再次將 Palo Alto Networks 新世代防火牆的資安控管能力，提昇至前所未見的新境界！



報告中同時指出：企業級防火牆產品必須能夠支援單一企業防火牆佈署，與大型或複雜的佈署：包含分支機構佈署、多層架構 DMZ 區佈署與日益增多的虛擬化環境，以協助企業因應全球化布局與多樣化應用服務而衍生的各種應用架構，讓您能放心採用各種新興的應用程式來提升競爭力，同時還能讓資訊安全做到滴水不漏！

最後，報告中並對於 Palo Alto Networks 能展現創新能力並勇於挑戰現狀，從而為資訊安全產業帶來令人振奮的轉變，給予高度的評價與肯定！

100% 優異的安全防護能力

NSS 實驗室 2015 新世代入侵防禦系統（NGIPS）測試中針對多種漏洞攻擊程序及規避技術等手法中，對資安防護之效果進行的獨立測試。測試中使用的漏洞評擊程序是利用駭客常使用的偷渡下載的方式來進行傳輸，Palo Alto Networks 是唯一一家 100% 成功攔截了此類漏洞攻擊程序與手法的廠商，並獲得了此項獨一無二的殊榮，展現了其優越的安全防護能力。

資安挑戰以不同的面貌出現在我們的生活中

如何面對如此強大的威脅，你有多少勝算？！

- 在應用服務的層面，你會發現愈來愈難以掌握在網路中各種應用服務的連線行為，因而不易了解環境中真正面臨的各種挑戰與風險。
- 在資安防護的層面，因為新型態惡意程式與零日攻擊的盛行導致傳統防毒、防駭、端點防護等機制（特徵碼比對）的防護效益幾乎喪失。
- 在網路架構的層面，因為虛擬化演進，也讓許多服務主機之間的流量不再受到監控，因此也難以做有效的保護。

攻擊思維與技術的轉變

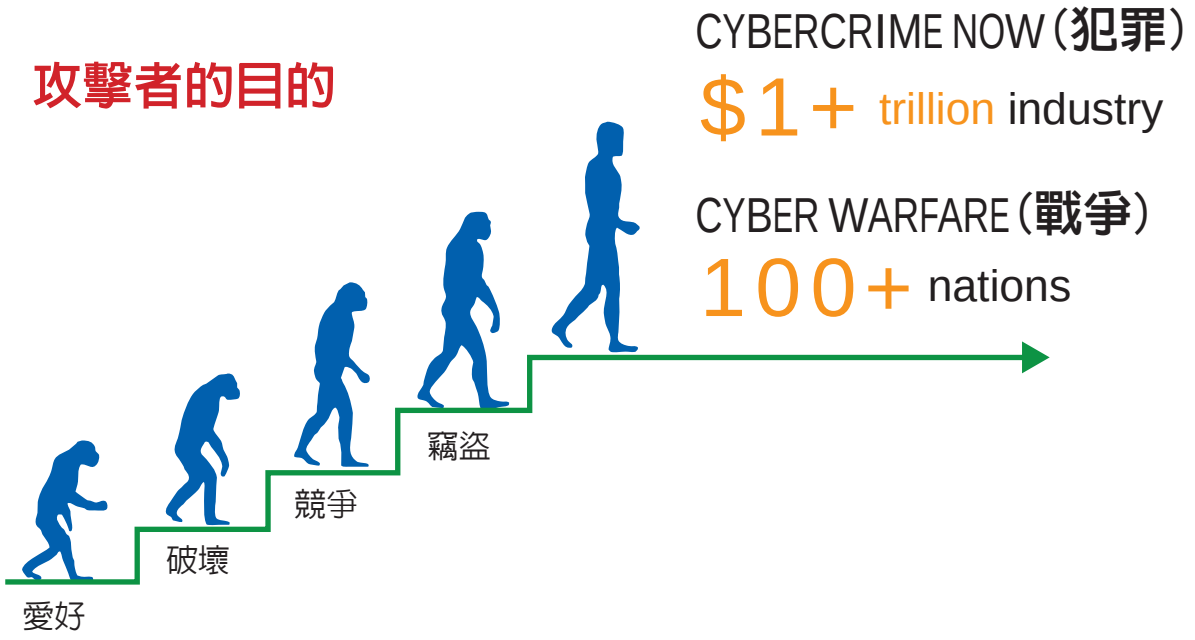
- 從已知威脅轉向未知威脅發展
- 從正規途徑轉向具規避行為的管道
- 從單一形態發展為多樣態攻擊
- 因具經濟價值，未知漏洞的使用日益嚴重
- 一般用戶在不知情的狀況下成為攻擊的幫手
- 基於信任的入侵更為普遍
- 行動裝置成為駭客新寵兒

傳統資安防護技術已無法解決全新的挑戰

攻擊的目的已和過去大不相同

- 取得個人私密或有價值的資料或資訊
  已達成特定心理或勒索之目的
- 攻占企業及各類組織網路
  以竊取重要商業秘密、敲詐或進行跳板攻擊
- 入侵重要政府組織網路、系統
  已達成特定軍事、政治、經濟等目的

正在發生的轉變



以創新思維定義資安防護新標準

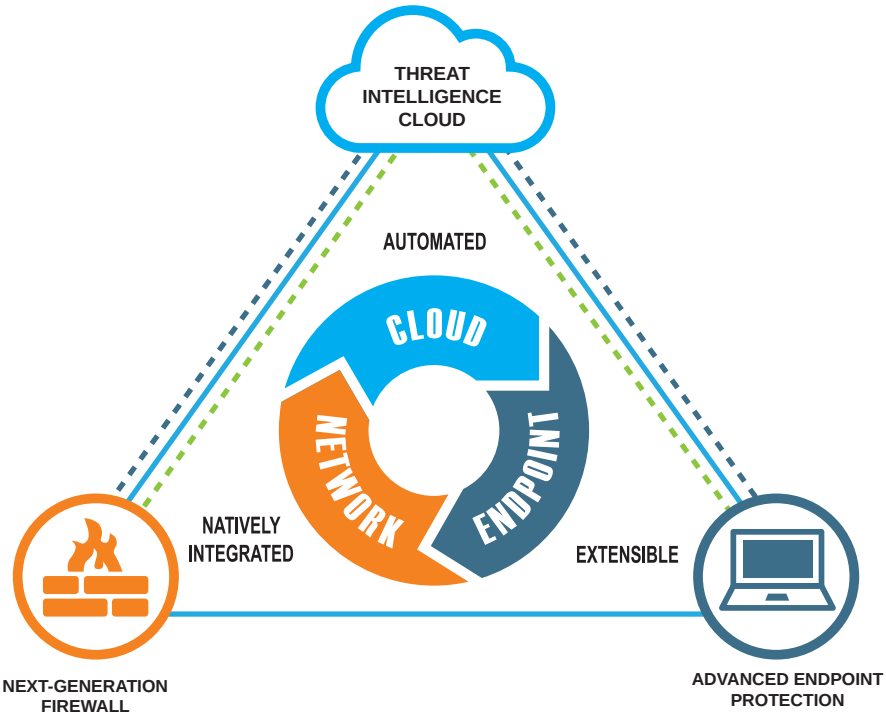
Palo Alto Networks 新世代資安防護平台

Palo Alto Networks 新世代資安防護平台，建構在舉世聞名的新世代防火牆之上，同時更有效利用雲端運算能力來提供高強度的防護品質與效率，同時更整合了新世代終端防護技術，讓資訊安全從此面面俱到。

Palo Alto Networks 新世代資安防護平台，包含三項重要防護核心，分別是：

- 新世代防火牆
  - 檢查所有流量中的應用程式加強可視性
  - 阻擋已知的威脅
  - 未知的威脅傳送至雲端進行分析與阻擋
  - 防禦機制可以延伸到行動裝置與虛擬化的運用
- 新世代雲端威脅偵測
  - 匯集了網路與端點的威脅
  - 定期的分析與威脅關聯的情報提供給用戶
  - 傳播威脅的網路與端點的資訊更新並及時更新到全球用戶
- 新世代端點安全控管
  - 檢查所有啓用中程式與檔案
  - 防禦已知與未知的威脅
  - 整合雲端的服務以防禦已知與未知的惡意程式

此三項防護核心，彼此協同運作、高度整合，讓您利用 Palo Alto Networks 新世代資安防護平台，輕鬆控管日趨複雜的資安威脅，不用購置多廠牌的設備、耗費時間學習管理，真正實現一站式資安管理！



五大核心技術 –
匝道到端點提供全面防護

精準的應用程式識別（App-ID）

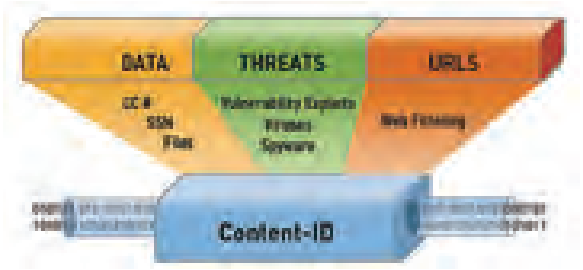
採用第七層的應用程式識別技術，能夠正確地分析出應用程式行為，讓您在導入新興應用服務與上網行為控管間，更加得心應手！

一清二楚的使用者識別（User-ID）

隨著 IPv6 時代的來臨，您將無法像以往般輕鬆利用 IP 位址來記錄與追蹤用戶。Palo Alto Networks 持續創新的用戶識別能力，讓您即使在 IPv6 環境中，依然能輕鬆整合各種用戶資料庫 (如：微軟 AD 帳號、電子郵件帳號…)，不用再管理難以理解的 IP 位址。

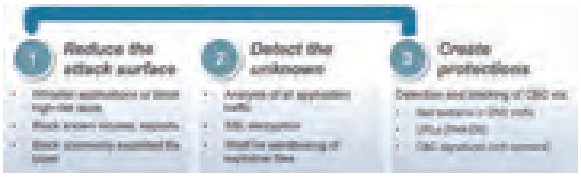
防範未然的內容識別（Content-ID）

擁有「即時威脅防禦」、「不良網站過濾」及「傳輸檔案類型識別」這些能力，讓您能專注於工作，不須費心於病毒及駭客入侵防範。



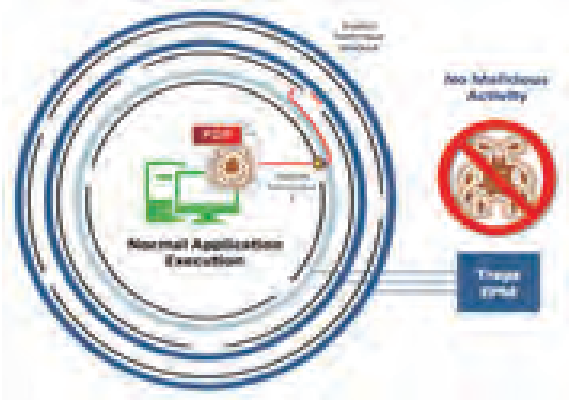
一氣呵成的 APT 防禦技術（Wildfire）

我們所創造的 ATP 防禦技術是一個可以大幅簡化企業應對惡意程式無孔不入的安全解決方案，除了自動檢測未知的惡意程式，並迅速阻止威脅的組織受到損害之前。不同於傳統的安全解決方案，野火（Wildfire）迅速識別並停止這些先進的攻擊，而無需事後手動人工干預，讓採樣、分析、防禦一氣呵成。



最後一哩路的防護（TRAPS）

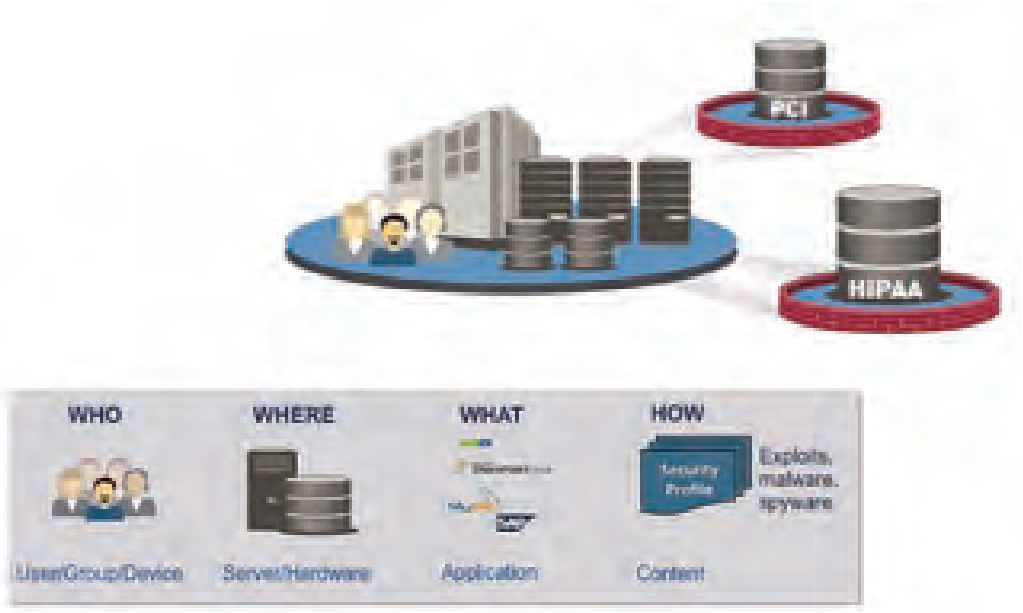
Palo Alto Networks Traps 為企業網路終端設備提供全面安全防護，Traps 僅利用極少常駐系統資源及特有多個入侵防護模組，針對駭客所能使用的入侵技術，逐一移轉或封鎖。此外，Traps 將收集詳細的鑑識資訊並回報該資訊端端點安全管理系統（ESM）。由於入侵的鏈結特性使然，僅需禁止鏈結中的一項技術即可封鎖整個攻擊。



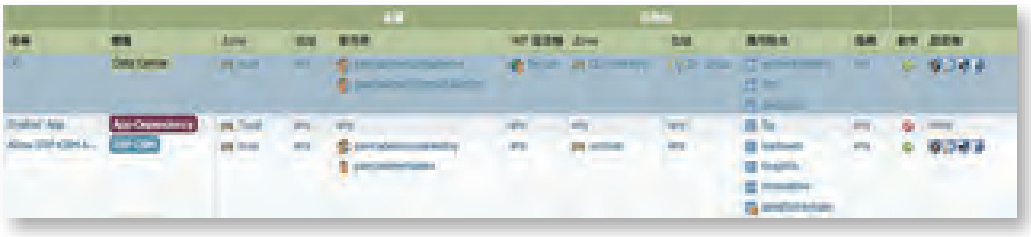
匠心獨具的內網安全管理機制

Palo Alto Networks 是唯一真正讓您能有效發揮正向管理機制效益的新世代資安防護平台，除了可以落實創新的區段管理（Network segmentation）概念外，更新符合各類資安規範中對於重要資源存取控制上最低授權的目標與精神。

Palo Alto Networks 以其優異的創新技術，讓您在劃分網路用戶的部門時，能直接以用戶身分而非 IP 位址來實現，如此一來，無論用戶使用何種裝置，您都能輕鬆掌握其身分與部門別，並以此給予相應的網路使用權限，從而避免內部網路用戶，因疏忽或惡意查探行為，而致企業網路陷入資安攻擊或機密外洩的危機。



Palo Alto Networks 新世代防火牆，只需在單一資安政策上執行各種正向管理控制，真正讓管理人以簡御繁並提升管理效益。



最高等級的資料中心安全機制

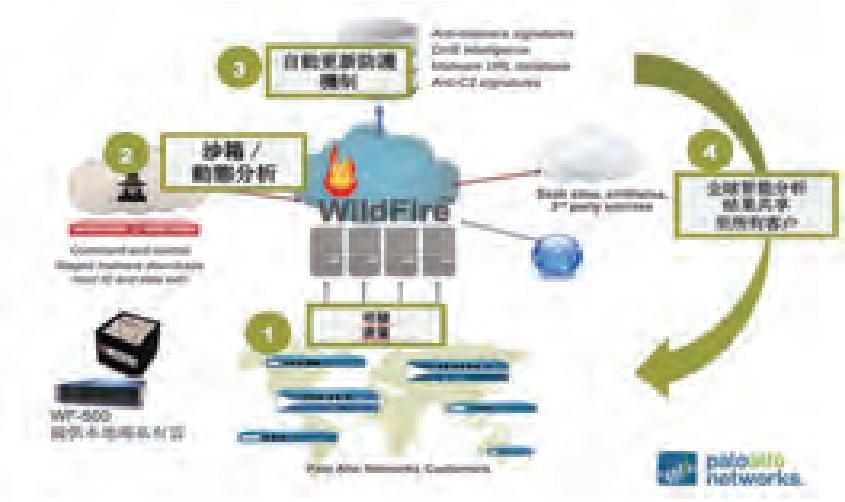
您可以善用 Palo Alto Networks 的創新技術（用戶與行為識別）在資料中心實現新一代正向防禦的策略；以有效杜絕各種可能的未知惡意探測或零日攻擊。

在不同的行業別中，我們更支援了各種專用系統的應用服務識別，所以你可以利用這個優勢來保護企業關鍵服務不受各種惡意存取，以確個營運的永續性。

天羅地網般的資安威脅防護

WildFire 讓進階持續性滲透攻擊，就此止步

Palo Alto Networks 新世代防火牆，特別推出精心設計的 WildFire 防護機制，藉由獨到的運作架構，讓您在面對新型態惡意程式攻擊，亦即所謂的 APT (Advanced Persistent Threat) 攻擊時，不僅能淡定以對，還能藉由 WildFire 防護機制的運作，輕鬆掌握內部的各種 APT 攻擊資訊，從而制定更加完善的資安防護政策。



WildFire 具有極富創意的雲端沙箱環境，讓您的 Palo Alto Networks 新世代防火牆，能輕鬆的分析惡意程式，而且絲毫不會降低設備處理效能。當 Palo Alto Networks 新世代防火牆發現網路上傳遞的檔案 (例如：Office 文件、PDF、可執行檔及 Android APk 等) 時，便會利用 WildFire 雲端沙箱環境執行動態行為分析，透過目前已可識別 250 餘種的惡意行為分析模組，來分析是否包含惡意的攻擊行為。雲端沙箱環境的設計，讓您不必擔心惡意攻擊行為被引爆於您的網路中，同時，還能明確得知可執行檔案的安全與否且不受惡意檔案刻意更換其特徵（例如：更改檔名及傳輸途徑等）來干擾分析效率。雲端沙箱技術，簡單，卻一點也不簡單！

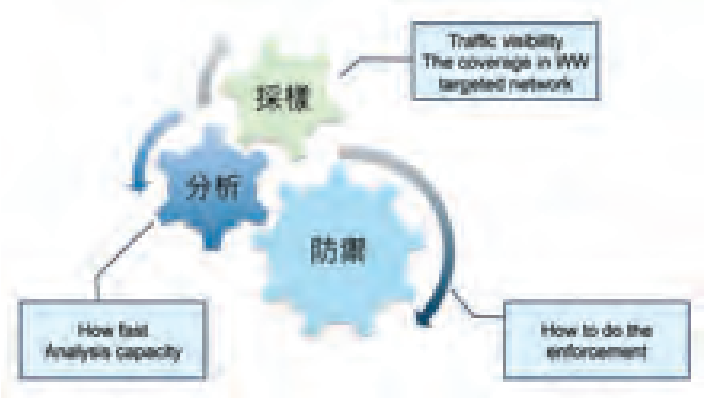
阻斷攻擊才是關鍵 分秒必爭的全自動防護機制

APT 攻擊的手法變幻莫測，往往在一日之內即可變化多種攻擊手法，為了有效遏止攻擊的持續，我們無法再透過漫長的等待，苦候各種傳統防護機制 (例如：入侵偵測、防毒牆等) 發佈更新的特徵碼。

Palo Alto Networks 新世代防火牆的 WildFire 防護機制，能在雲端沙箱環境中發現惡意程式後，立即自動產生針對該惡意程式所有活動行為之防護特徵碼，並在 15 分鐘內，主動下載至您所擁有的 Palo Alto Networks 新世代防火牆，讓您的資安防護真正具備零日攻擊 (Zero-Day Attack) 或各種未知攻擊手法的防護能力。

新世代 APT 滲透攻擊防護機制 – 迴路式防禦機制

Palo Alto Networks 在面對進階持續性滲透攻擊 (APT attack) 時，藉由新世代資安防護平台架構，提出了嶄新的「迴路式防禦機制」，從惡意程式的採樣、分析到防禦一氣呵成，讓 IT 管理人員不再疲於奔命！



行動裝置的資安控管機制

行動運算是資訊科技中最具影響力的技術之一。行動運算大大改變了員工的工作模式和地點型態，執行工作的工具也發生了變革。行動裝置不僅用來存取公司電子郵件等既有的應用程式，行動平台更開啓了全新的商務應用新思維。

組織因此必須針對行動裝置所面臨的安全性風險提出管理方案。為了能全面了解行動能力的優點並安全啓用行動裝置，企業必須採取下列方法：

管理裝置

- 為裝置進行適當的安全性設定，以確保裝置能安全啓用。提供電子郵件帳戶等一般設定，或採用憑證來進行認證等方式，簡化部署及設定。

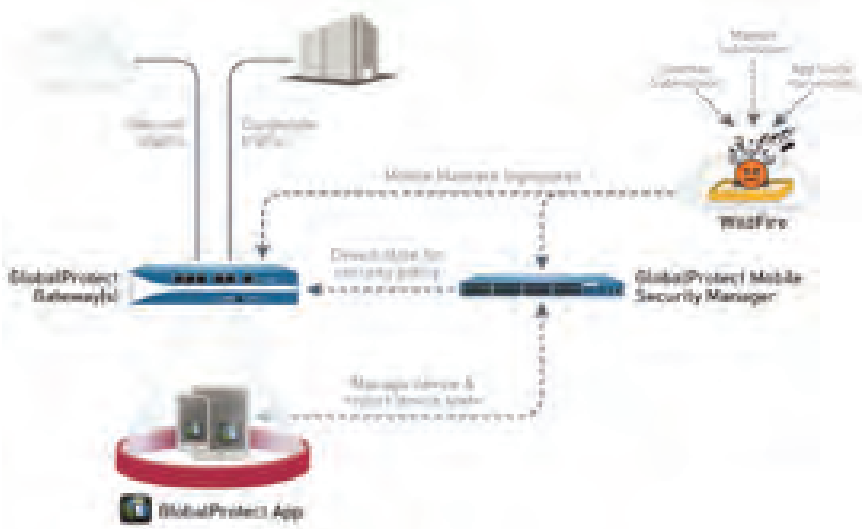
保護裝置

- 保護行動裝置免於入侵和惡意程式威脅。保護行動裝置也是保護資料很重要的一環，因為裝置一旦遭到入侵，裡面的資料也就不再安全。

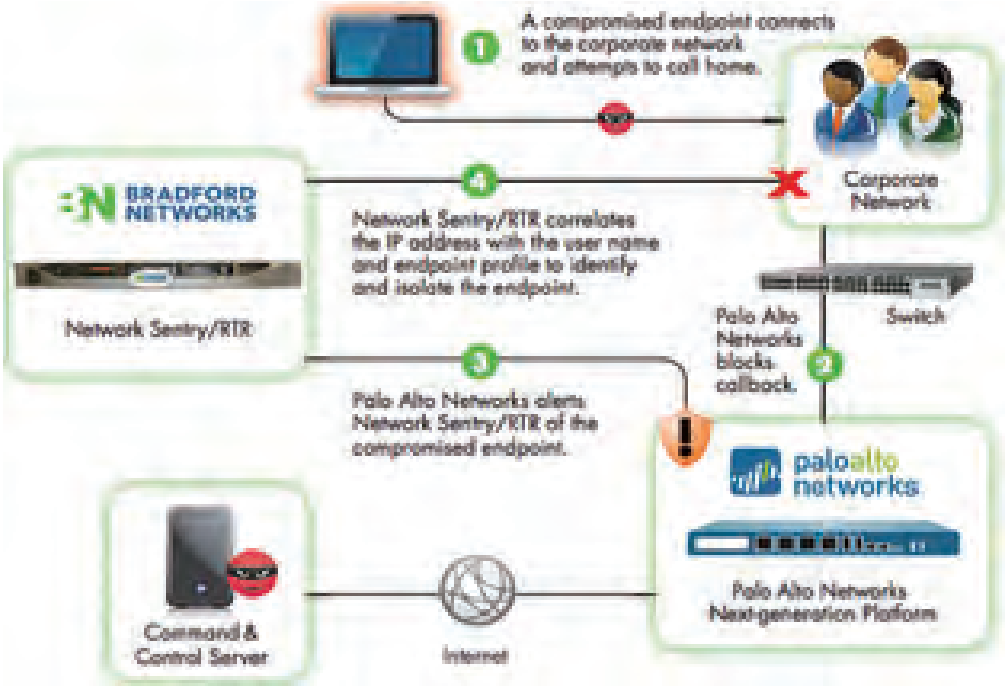
控管資料

- 控管資料的存取，以及應用程式間的資料活動。建立政策，針對能存取敏感應用程式的人員進行定義，並定義能使用的特定裝置類型。

Palo Alto Networks 推出的 GlobalProtect 能針對裝置管理、保護及資料控管等問題，提供專屬的的解決方案，讓您能安全地啓用行動裝置，無虞地進行商務使用。GlobalProtect 結合必要科技和情報資訊，為行動安全性提供全方位解決方案，協助組織阻擋行動威脅、落實安全性政策並保護網路不受入侵、防禦非法行動裝置的侵害。

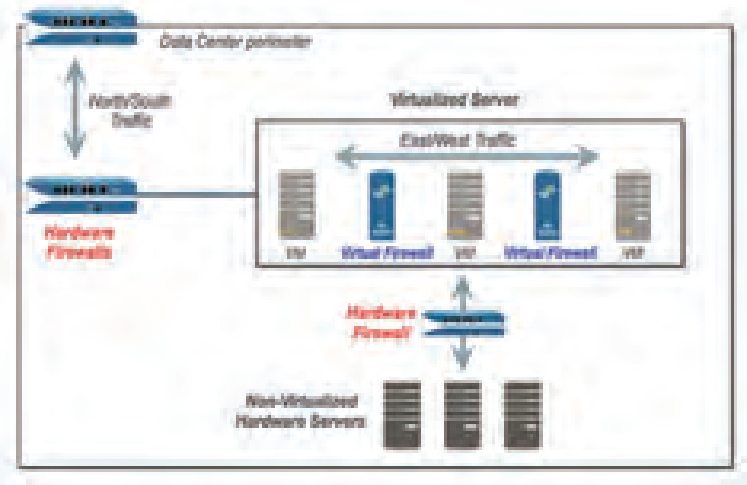


行動裝置：無線與 NAC 的廠商透過整合方式，快速辨識出使用者，從規則中管理使用者的行為，進而後續達到 BYOD 彈性整合。

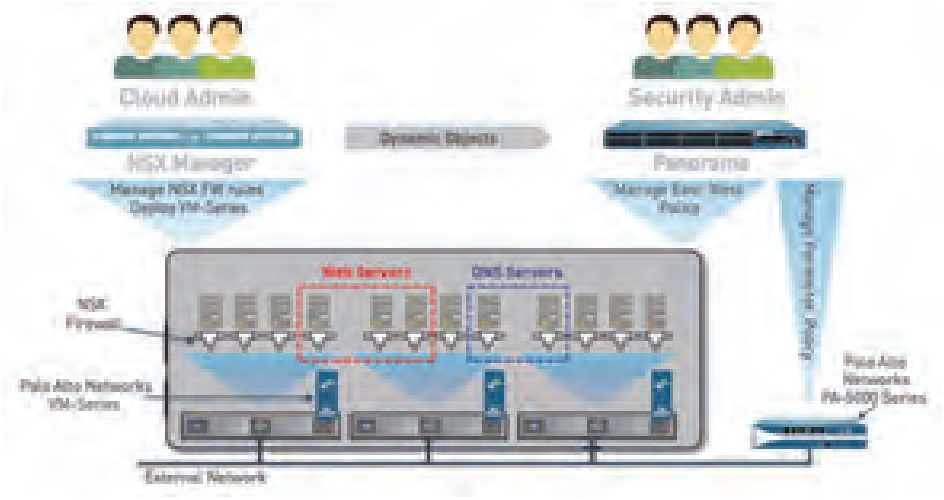


深得您心的虛擬化安全機制

Palo Alto Networks 更進一步針對虛擬化平台 (Hypervisor) 與雲端服務環境提供完整的資安防護技術。不僅擁有 Palo Alto Networks 新世代防火牆的完整功能，還能在虛擬化平台中，識別與控管應用程式行為，讓您輕鬆的掌握虛擬機器間 (Virtual machine) 透過虛擬交換器傳輸的各種流量，同時在控管各個虛擬機器的資安威脅時，一樣能擁有與管理實體網路時，同樣強大的控管能力。如此一來，以往流竄於虛擬機器間的資安威脅，將能有效被發現與攔截，在雲端資料中心提供服務時，能更為安全、更讓用戶安心。

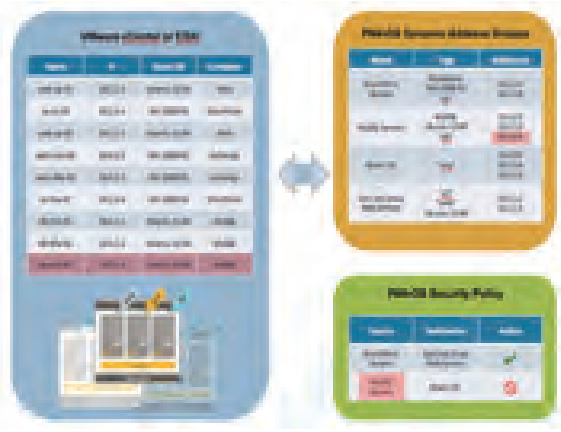


虛擬化：在 Web UI 上直接整合 VMware 的環境，跟著 VMware 快速變動下，以監控與不變動規則的方式達到 VMware 整合，另外已經都支援 Public Cloud 的廠商，可以直接選購與設定。

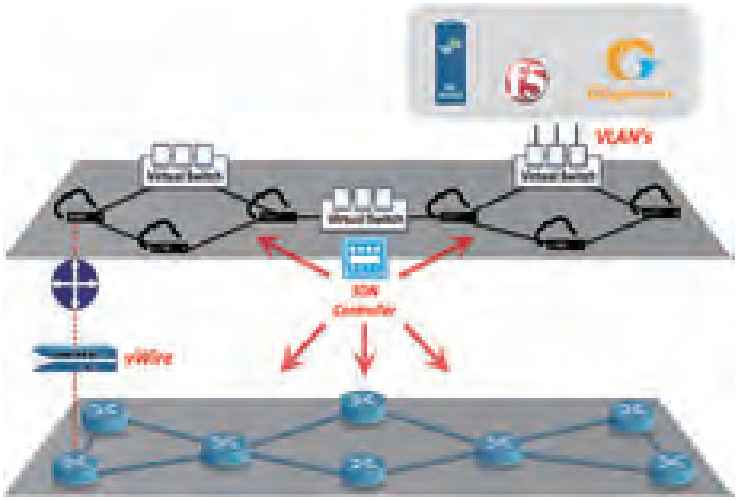


隨您所用的動態資安控管機制

在雲端服務資料中心內，因應前端服務用量而來的資源動態配置是非常頻繁且即時的，因此虛擬機器的異動（新增、移除、遷移）是極為常見的情形，Palo Alto Networks，特別針對這樣的需求，提供動態位址物件 (Dynamic Object) 及豐富 XML API 介面，讓資安管理能與虛擬化平台管理系統自動地協同作業，即時了解虛擬機器的變化，並隨之調整資安政策，讓資安防護無縫接軌，減輕管理負擔，一切都能自動完成，不勞您費心。

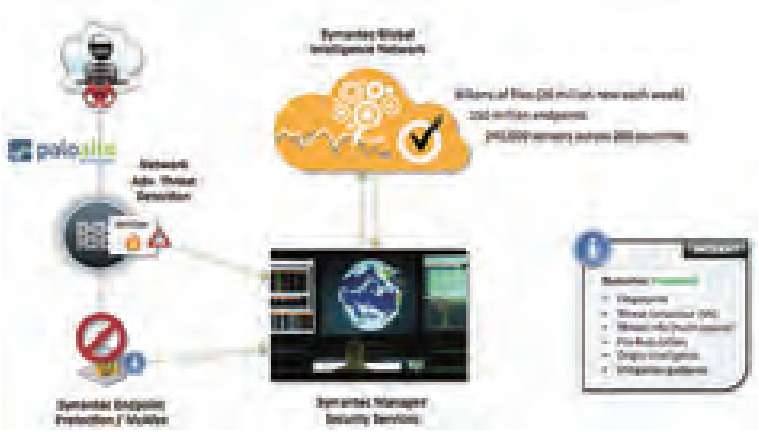


軟體定義網路：透過整合各交換器領導廠商，以達到大型網路下的整合，讓管理者可以快速的管理、監控與佈署。



風險分析：許多知名的安全分析廠牌均已支援 PaloAlto Networks 的各類事件分析，有利於提升整體環境狀況之掌握。

安全聯防：提供未知威脅分析結果供各家防毒廠商免費參考以利加速製作相關防護疫苗執，強化防護強度。



專家服務讓您掌握全局

在過去，您可能為了做好資安防護而投入了大量的資源，但到最後可能往往不容易從各種分析報告與巨量的事件統計中了解你的單位或企業網路真正的風險系數有多高，以及有哪在潛在的攻擊行為在在發生中，尤其是在目標式攻擊當道的今天，很可能因此錯失了發現藏在細節中的魔鬼（駭客攻擊）的先機。

Palo Alto Networks® 提供了一個全新的專家分析服務平台，並具備了三大特色：

- 彙整所有事件進行透過狀態與專家分析來了解所面臨的攻擊來源、手法。
- 協助客戶有效識別最重要的攻擊行為及其所造成的影響評估。
- 提供分析平台的使用者介面，供客戶進行客製化搜尋與分析。

高度的設計彈性創造最大整合效益

身為資安防護領導品牌的 PaloAlto Networks 一直以來採取彈性、開放的態度，致力與各領域主流供應品牌進行合作。從虛擬化、軟體定義網路、行動裝置、風險分析與安全聯防，提供所有客戶最佳解決方案之整合效益。

端點防護的最後一哩路（TRAPs）

Palo Alto Networks® Traps 提供進階威脅防護，可避免複雜的弱點入侵及惡意程式碼式攻擊。Traps 透過可高度擴充、輕量的常駐程式來實現此目標，此常駐程式使用創新方式來防禦攻擊，無須事先了解威脅。透過此方式，Traps 即可為組織提供強大工具，可保護主機或裝置免於目標式攻擊

Palo Alto Networks® Traps 採用多個入侵防護模組，針對駭客所能使用的入侵技術，逐一移轉或封鎖。這些模組以「陷阱」方式運作，插入使用者所使用的各種程序，當攻擊者嘗試入侵時，就會立即觸發並封鎖入侵技術。當應用程式開啓時，Traps 即會將防護模組作為透明、靜態的「陷阱」無縫地插入程序。在模組插入程序後，該程序即可免於任何入侵。若使用可用的技術之一嘗試入侵，Traps 將立即封鎖技術、終止程序並通知使用者及管理員已防禦攻擊。此外，Traps 將收集詳細的鑑識資訊並回報該資訊至端點安全管理系統 (ESM)。由於入侵的鏈結特性使然，僅需禁止鏈結中的一項技術即可封鎖整個攻擊。

Traps 架構

Traps 提供 3 層管理結構，包括主機或裝置安全性管理員、主機或裝置連線伺服器及主機或裝置常註程式。此模組可提供極高的水平擴充能力，同時維護原則、鑑識等內容的集中組態及資料庫。

主機或裝置安全性管理員

主機或裝置安全性管理員提供管理計分板以供管理安全性活動、主機或裝置健康狀況及原則規則。ESM 也可在傳送雜湊以供檢查時處理與 WildFire 的通訊。

端點安全管理系統包括儲存管理資訊、安全性原則規則、主機或裝置記錄及其他安全性活動相關資訊的集中資料庫。資料庫透過 MS-SQL 平台管理。

除了在內部儲存其本身記錄以外，端點安全管理系統可將記錄寫入至外部記錄平台，例如安全性資訊和活動管理 (SIEM)、服務組織控制 (SOCs) 或系統日誌。指定外部記錄平台可讓您彙總檢視所有主機或裝置伺服器的記錄。

端點安全管理系統伺服器

會定期將安全性原則發佈至所有常註程式，並管理所有安全性活動相關資訊。

特色與效益

特色		效益
應用程式識別	• 正確識別與控管超過 2,000 種以上應用程式。 • 提供使用者自行定義應用程式識別能力。	• 擁有了全方位的應用程式識別能力，管理各種新興服務，將變得無比簡單。還能利用自行定義應用程式識別功能，做到對自行開發應用服務的控管，一切盡在掌握之中。
使用者識別與控管	• 可在同一時間與各類使用者資料庫 (Microsoft Active Directory , Microsoft-Exchange, Microsoft-Terminal service, LDAP , RADIUS, Novell eDirectory, API, UAC, Syslog) 緊密整合，並在其間逐一比對使用者資訊。 • 除了 IPV4，在 IPv6 環境中，一樣能整合。	• 您可以直接在資安政策中，直接選用者帳戶及群組來進行管制，讓您的安全控管更加周全。 • 可動態將使用者 IP(IPV4/V6) 位址對應至使用者名稱及群組資訊，並以這些資訊做為設定各類政策 (資安、頻寬控管、政策路由、SSL 解密) 之依據，以獲得高度的管理彈性。
威脅防禦	• 擁有多達 100 萬筆以上病毒特徵碼比對能力。 • 高達 10,000 多筆以上 IPS 特徵碼偵測防護能力 (包括：7,300 餘筆 Vulnerability 漏洞攻擊特徵檢測與 3,400 餘筆 Spyware 惡意程式檢測)。 • 可識別與控管 40 種以上的檔案類型。 • 在 IPv6 環境中，一樣能提供完整的防禦能力。 • 可制定規則以針對任一網路服務埠及特定目的地網址之 HTTPS 等加密連線之傳輸內容進行解密，執行資安檢測與防護功能 (包含：入侵防禦、惡意程式檢查及病毒掃描)。	• 2015 NSS Lab 指名推薦，擁有優於型錄載明的防護效能。對於 NSS Lab 測試的各種 Evasion (規避行為) 更是能夠完全偵測與阻擋。 • 隱藏在應用服務中的病毒、蠕蟲、間諜程式，一樣能毫不費力的揪出來，讓您不再操心。 • 能依據國家別資訊，在資安政策及阻斷式攻擊 (DoS / DDoS) 政策中進行管控，並具備最大即時連線數控管之能力 (同時針對特定來源、目的地)，以避免遭受攻擊時對網路服務造成影響。 • 可整合外部系統自動讀取黑名單資訊並阻斷其與內部網路之連線。 • 通過 2014 年 ICSA Lab 之 Firewall 認證。
新型態惡意程式攻擊防護 (APT attack Protection)	• WildFire 防護機制，能於 15 分鐘內偵測出惡意程式行為，並立即產生防護特徵碼，主動下載回設備上。 • 具備雲端沙箱機制 (Sandbox)，在沙箱中執行設備上發現的可疑惡意程式，讓惡意程式無所遁形。 • 提供手動上傳惡意程式樣本分析功能。 • 提供下列分析資訊與功能： A. 來源 / 目的 (IP, 使用者), 服務連接埠 , 應用程式名稱。 B. 惡意程式檔案名稱、雜湊值 (MD5, SHA256)。 C. 利用檔案之雜湊值 (SHA256) 與其他全球 40 家以 上資安廠商 (Virus Total) 進行資訊比對以利進階分析。 D. 惡意程式行為彙總資訊。 E. 惡意程式網路活動記錄。 F. 惡意程式在受感染主機內之活動記錄 (eg.Registry key/ value/Action, Process activity) 與活動歷程 (Event timeline)。 G. 惡意程式樣本檔案、側錄封包及報表匯出匯出功能。 H. 誤判回報機制。	• 透過雲端沙箱機制，檢測惡意程式更為完整準確，既不用擔心洩漏機密，又不影響設備效能，功能與效能兼備。 • 具備完善的報表功能，可製作詳細的分析報表，協助資安政策的強化，有憑有據。 • 可從分析報告中取得惡意程式樣本及側錄封包做進一步的分析。 • 使用 Wildfire 授權後即可每 15 分鐘取得一次各資安防禦資料庫之更新 (Vulnerability , Virus , Spyware, URL filtering)。
疆屍網路行為分析功能	• 提供可疑疆屍網路活動行為分析日誌以掌握可疑的受駭用戶端資訊，以利進一處置。 • 針對遭受病毒、惡意程式感染之用戶端與駭客惡意中繼站的連線請求進行過濾與反制 (DNS Sinkhole)，以利找出真正的受駭用戶端主機。	• 透過各種異常行為分析模組有利於提前察覺各種可能的駭客攻擊活動行為並同時找到佈署在內部網路中的受駭主機，以利早期預警與處置。 • DNS Sinkhole 功能，有助於查找真正受駭用戶端主機，並真正阻斷惡意中繼站查詢請求之連線 (不通過防火牆)。
惡意網址過濾	• 具備 PANDB 資料庫，提供多達 59 種以上的網頁類別 (IPV4/ IPV6) 及超過 2,000 萬筆的網站名單，並可自訂網址類別。 • 每週更新不良網站及中繼站資料庫。 • 可將網址類別套用至資安政策、頻寬管理及網頁存取驗証等各種政策中。	• 不再擔心用戶瀏覽色情、賭博等網頁，資源不被濫用。 • 免除用戶不慎連結至中繼網站所產生的資安風險，防患未然。 • 設定資安政策時，能簡化複雜度，讓管理更有彈性。

特色		效益
資安政策	• 單一資安政策 (Security Policy) 中，可以同時依據 IP(IPV4/IPV6)、使用者帳戶 / 群組、國家別、應用程式及網址類別執行各種連線行為控管與資安檢測。	• 透過簡易的操作介面，就可同時完成各種情境條件之設定進行靈活的控管與資安防護。 • 防火牆規則的動作支援 Allow, Deny, Drop, Reset Client, Reset Server, Reset Both 的不同設定。
工作模式	• 具備在單一系統 (VSYS or VDOM or Virtual Firewall or Context) 功能下在可同時佈署旁接、透通、路由、轉址等多種工作模式。且可在透通、路由模式下，執行 IP 轉址 (NAT) 功能。	• 多用途的工作模式有助於您應用於各種環境，像是：對外安全閘道、資料中心及檢測內部網路問題，通通一台搞定，真正落實資安防禦縱深的目標。
系統日誌	• 提供資料流、威脅事件、網頁瀏覽、檔案傳輸及設定檔變更等日誌記錄。	• 所有日誌都詳實記錄各種資訊，例如：用戶帳號名稱、日期與時間、應用程式名稱、檔案名稱等，確保所有行為都有跡可循。 • 支援 Syslog over SSL 與 suite-b cipher。 • 整合無線的 Syslog 紀錄，辨識無線的使用者。
用戶端安全存取	• 透過 GlobalProtect(Agent Base SSL VPN) 功能，將資安政策落實於各個用戶端設備，無論用戶身處何處，都必須遵循相同的資安政策。	• 用戶端的安全性，可藉由 HIP 機制 (Host Information Profile)，即時得知並做為資安政策的控管條件。同時，還能區分用戶的設備不同，給予不同的使用權限。 • SSL VPN 支援使用者可自動派發與自訂哪個使用者配發固定。
關聯式分析	• 完善的關聯式分析能力，可以迅速分析所有日誌資料，快速找出問題發生原因。 • 提供頻寬用量排行 (Top N) 顯示功能，顯示來源位址 / 目的位址連線資訊排行、事件排行、用戶端網址類別之連線時間、介面流量歷史記錄圖表等狀態顯示。	• 利用關聯式分析引擎整理為數龐大的系統日誌後，讓您在單一畫面看到所有應用程式的傳輸資料量、Session 數量。 • 搭配威脅防禦功能，還能顯示所有病毒威脅、漏洞攻擊、惡意程式攻擊及內部攻擊者與被受害者名稱，您不會遺漏一絲一毫。 • 支援客製化監控 Dashboard, 以圖型或是趨勢圖顯示。
流量地圖	• 在世界地圖上，清楚顯示進出世界各國的網路傳輸量與風險等級。 • 資安政策、DoS 防護政策與加密連線分析政策，都能依據來源與目的國家別做控管。	• 想知道網路流量是去了哪裡，不再是天大的難題。只要滑鼠一按，所有國家的流量盡在您眼前，如此輕而易舉。 • 依照國家別設定管理政策，不僅創新，還能給您大大的便利。 • 具備網路流量地圖功能，可於世界地圖上顯示所有對內與對外網路傳輸流量所屬國家的資訊，能清楚顯示每個國家的傳輸量是由哪些應用程式、個別應用程式的傳輸資料量、來源使用者 IP address、目的使用者 IP address 及所造成的資安威脅事件名稱、資安威脅事件數量等資訊。
報表系統	• 內建 30 種以上的豐富中、英文報表，還有完善的自定報表能力。	• 內建 30 種以上的豐富中、英文報表，還有完善的自定報表能力。
設定檔稽核	• 可以記錄超過 100 萬份的設定檔，還能呈現每個版本的不同。	• 誰做過資安政策的修改，從此不再查無此人。凡改過必留下痕跡，才能符合資安稽核與安全規範的要求。
資安政策稽核	• 顯示設備開機後沒有執行過的資安政策。	• 顯示設備開機後沒有執行過的資安政策。
NetFlow 流量資料	• 設備內建可產生 NetFlow v9 流量資料至外部收集器。	• NetFlow v9 能提供應用程式統計資訊及用戶識別資料 (IPV4/IPV6)，讓您進行流量分析時更能面面俱到。
支援外部硬體式憑證管理設備 (HSM)	• Palo Alto Networks 設備與 HSM 用戶端整合，能夠增強 SSL/TLS 解密 (SSL 轉送 Proxy 與 SSL 輸入檢查) 中所使用私密金鑰的安全性，您可以使用 HSM 將設備主要金鑰加密。	• 硬體安全性模組 (HSM) 是管理數位金鑰的實體設備。HSM 能夠安全地儲存與產生數位金鑰，同時提供邏輯與實體方法保護這些材料免遭未經授權的使用與潛在對手的危害。

特色		效益
VM 系列防火牆	● 將各種令人稱道的安全防護功能，完美延伸至虛擬化環境，讓您在規劃雲端資料中心時，依然享有與實體環境一模一樣的安全防護。 ● 動態位址物件，讓您輕易地完成聯防動作。 ● 資安政策可動態整合外部 IP 列表 (IPV4/IPV6) 執行自動化管制。 ● 完整的 API 功能大幅降低管理、維護負擔。	● 今後，您將能輕鬆管理虛擬主機之間的傳輸行為與資安防護。 ● 利用動態定址物件 (Dynamic Object) 及 XMP API，輕鬆與各虛擬化管理系統整合，以即時了解虛擬機器的 IP 位址變化，隨時自動調整資安政策。 ● 透過 API 可進行各類政策 (資安、頻寬控管、政策路由、SSL 解密) 與物件 (IP 位址) 之新增、異動、刪除等作業。 ● 可有效與 VMware(ESX, NSX), Citrix, Arista 等虛擬化領導廠進行整合以利提升其環境之安全強度。
分權管理功能	● 可依據不同管理人員設定其帳戶並可個別授予各種管理功能： • 防火牆系統資訊與即時負載查詢。 • 事件關聯分析查詢。 • 流量記錄查詢。 • 資安事件查詢。 • 系統事件查詢。 • 設定異動查詢。 • 報表查詢。 • 製作客製作報表。 • 資安政策設定。 • 各類物件設定。	● 創新的平行授權概念，有別於以往由上到下的繼承授權機制，能夠真正做到權責分立的目的並符合各種稽核工作與資安規範的要求。
管理平台	● 提供獨立實體管理埠以保障管理效率。 ● 具備網頁式 (HTTP and HTTPS) 管理與指令式設定 (Console / Telnet / SSH) 介面。 ● 擴充相關授權時，可在不需重啓設備與重建連線下進行各類資料庫 (防毒、防駭) 更新。 ● 提供完整自動化管理與維護機制 (API) • Device configuration： Retrieve / Get / Set / Edit / Delete / Reporting / Packet capture • Object： Address / Address group / Application / Application group / Security rule / NAT rule / Dos rule / QoS rule / Schedule(for rule) ● 內建於設備的獨立管理平台（含報表系統）提供以下多種語系的操作介面： • 中文繁體。 • 中文簡體。 • 英文。 • 日語。	● 新一代的硬體設計架構有效地將管理與流量處理資源進行最佳化配置具互不影響，有利於在網路異常狀況發生時快速進行問題分析與排除。 ● 新一代的軟體平台提供管理者前所未有的整合彈性及自動化管理之效益。 ● 提供多種語系的操作介面有利於管理者依據其所熟悉的語言進行各種所需的資安控管與分析。
其他特色	● 無使用人數限制。 ● 同時執行 Layer4 至 Layer7 之流量檢查。 ● 加密連線分析與檢查。 ● 資料進階分析。	● 同時具備連線狀態檢測技術 (Stateful inspection) 外，更同時進行第七層應用程式連線識別與控管以利交互運作並達到最好的防護效果。 ● 設備須內建或透過外加設備 / 模組能針對加密連線 (eg. SSH) 執行解密功能，並可設定針對特定目的地網址加密連線 (HTTPS) 進行解密之功能 (Inbound & Outbound)，以提升對資料流之控制與資安防護能力。 ● 除可針對加密連線之資料進行資安檢測外，亦可將原始資料提供至第三方系統進行稽核、存查等各種需求之分析 (PA3000 以上)。

技術規格

型號	PA-200	PA-500	PA-3020	PA-3050	PA-3060	PA-5020	PA-5050	PA-5060	PA-7050 (Chassis Base)
網路介面	4 x10 / 100 / 1000	8 x10 / 100 / 1000	12 x 10 / 100 / 1000 + 8 x 1000-SFP		8 x 10 / 100 / 1000 8 x 1000-SFP 2 x 10G-SFP+	12 x 10 / 100/1000 8 x 1000-SFP	12 x 10 / 100 / 1000 8 x 1000-SFP 4 x 10G-SFP+		4 SFP+ (10 Gig) 8 SFP (1 Gig) 12 copper gigabit / Per NPC Max : NPC X6
Firewall 效能 (Layer 7)	100 Mbps	250 Mbps	2 Gbps	4 Gbps	4 Gbps	5 Gbps	10 Gbps	20 Gbps	120 Gbps
Threat Prevention 效能 (AV, IPS, Spyware)	50 Mbps	100 Mbps	1 Gbps	2 Gbps	2 Gbps	2 Gbps	5 Gbps	10 Gbps	96 Gbps
VPN 效能	50 Mbps	50 Mbps	500 Mbps	500 Mbps	500 Mbps	2 Gbps	4 Gbps	4 Gbps	24 Gbps
New Sessions / Second	1,000	7,500	50,000	50,000	50,000	120,000	120,000	120,000	720,000
MAX Concurrent Session (Layer 7)	64,000	64,000	250,000	500,000	500,000	1,000,000	2,000,000	4,000,000	24,000,000
GlobalProtect 同時用戶數	25	100	1,000	2,000	2,000	5,000	10,000	20,000	120,000
Virtual Routers	3	3	10	10	10	20	125	225	225
Virtual Systems (Base/Max)	N/A	N/A	1/6	1/6	1/6	10/20	25 / 125	25 /225	25 /225
Security Zones	10	20	40	40	40	80	500	900	4,000
Security Policies	250	1,000	2,500	5,000	5,000	10,000	20,000	40,000	80,000
High Availability	Y	Y	Y	Y	Y	Y	Y	Y	Y
Temperature (Operating)	32 to 104 ˚F 0 to 40 ˚C	32 to 122 ˚F 0 to 50 ˚C	32 to 122 ˚F 0 to 50 ˚C	32 to 122 ˚F 0 to 50 ˚C	32 to 122 ˚F 0 to 50 ˚C	32 to 122 ˚F 0 to 50 ˚C	32 to 122 ˚F 0 to 50 ˚C	32 to 122 ˚F 0 to 50 ˚C	32 to 122 ˚F 0 to 50 ˚C
Temperature (Non-operating)	-4 to 158 ˚F -20 to 70 ˚C	-4 to 158 ˚F -20 to 70 ˚C	-4 to 158 ˚F -20 to 70 ˚C	-4 to 158 ˚F -20 to 70 ˚C	-4 to 158 ˚F -20 to 70 ˚C	-4 to 158 ˚F -20 to 70 ˚C	-4 to 158 ˚F -20 to 70 ˚C	-4 to 158 ˚F -20 to 70 ˚C	-4 to 158 ˚F -20 to 70 ˚C
Environmental Conditions (Humidity)	10-90%								
Certificate	UL, CUL, CB,FCC class B, CE class B, VCCI class B, TUV								

型號	VM-100	VM-200	VM-300	VM-1000-HV
Firewall 效能 * (Layer 7)	1 Gbps	1 Gbps	1 Gbps	1 Gbps
Threat Prevention 效能 * (AV, IPS, Spyware)	600 Mbps	600 Mbps	600 Mbps	600 Mbps
VPN 效能 *	250 Mbps	250 Mbps	250 Mbps	250 Mbps
New Sessions / Second*	8,000	8,000	8,000	8,000
MAX Concurrent Session (Layer 7)	50,000	100,000	250,000	250,000
GlobalProtect （SSL VPN) 同時用戶數	25	200	500	500
Virtual Routers	3	3	3	3
Security Zones	10	20	40	40
Security Policies	250	2,000	5,000	10,000

* VM 系列產品效能取決於配置之 CPU 核心數而有所不同，本表所列為配置 4 個 CPU 核心之效能數據。

訂購資訊

產品型號	產品敘述
PAN-PA-200	Palo Alto Networks PA-200
PAN-PA-500	Palo Alto Networks PA-500
PAN-PA-3060	Palo Alto Networks PA-3060
PAN-PA-3020	Palo Alto Networks PA-3020
PAN-PA-3050	Palo Alto Networks PA-3050
PAN-PA-5020	Palo Alto Networks PA-5020
PAN-PA-5050	Palo Alto Networks PA-5050
PAN-PA-5060	Palo Alto Networks PA-5060
PAN-PA-7050	Palo Alto Networks PA-7050
PAN-VM-100	Palo Alto Networks VM-100
PAN-VM-200	Palo Alto Networks VM-200
PAN-VM-300	Palo Alto Networks VM-300
PAN-VM-1000-HV	Palo Alto Networks VM-1000-HV
PAN-WF-500	Palo Alto Networks WF-500
PAN-GP-100	Palo Alto Networks GP-100, 500 Devices, 1TB RAID storage. 管理裝置數量可以購買授權方式增加，最多可管理 10 萬部裝置
PAN-PRA-25	Panorama central management software, 25 devices
PAN-M-100	Palo Alto Networks M-100, 1TB RAID storage (2 1TB RAID certified drives preinstalled). Rack mount rails included.
PAN-M-P-25	Panorama central management software license, 25 devices or log collector for the M-series
PAN-M-100	Panorama central management (Hardware appliance)

Threat Prevention 使用授權 (含 Anti-Virus、IPS、Anti-Spyware)
依設備型號選擇相應之授權

WildFire 使用授權
依設備型號選擇相應之授權

PANDB URL filtering 使用授權
依設備型號選擇相應之授權

GlobalProtect Gateway 使用授權
依設備型號選擇相應之授權

paloalto networks.

the enterprise security company™

Palo Alto Networks
新世代資安防護平台

面面俱到的防護範圍　天羅地網的資安防護

paloalto networks.

the enterprise security company ™

Westcon Solutions

新加坡商威寶康科技－台灣分公司
台北市內湖區洲子街 112 號 4 樓
TEL：(02) 8751-8026
FAX：(02) 8751-8022

Email：wstw@westcon.com
www.tw.westcon.com
www.westconsolutions.com