威脅零容忍
智慧做資安

台灣區代理商

鉅晶國際 JJNET

好評見證

連續七年位居領　導者象限 (2012~2018)

唯一具備與國際刑警組織
執行情資交換資格之廠商

惡意攻擊自動化防護技術領導象限廠商

美國國家安全電信諮詢委員會成員

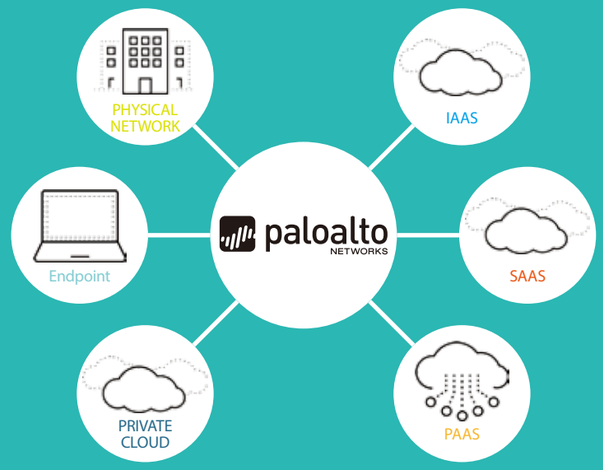
SANS評價最佳新世代防火牆

JD.POWER 全球客戶滿意度認證

全球市場評價
新世代安全平台領導品牌

Palo Alto Networks為各領域之企業、政府及組織提供對抗網路威脅的最佳解決方案，引領著網路安全的新時代。在2005年由創辦人Nir Zuk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，包括進階威脅防護、防火牆、IDS/IPS、URL過濾及SSL加解密功能。所以我們可以保證與傳統的防火牆、UTM或端點威脅檢測產品相比擁有更佳的安全性。

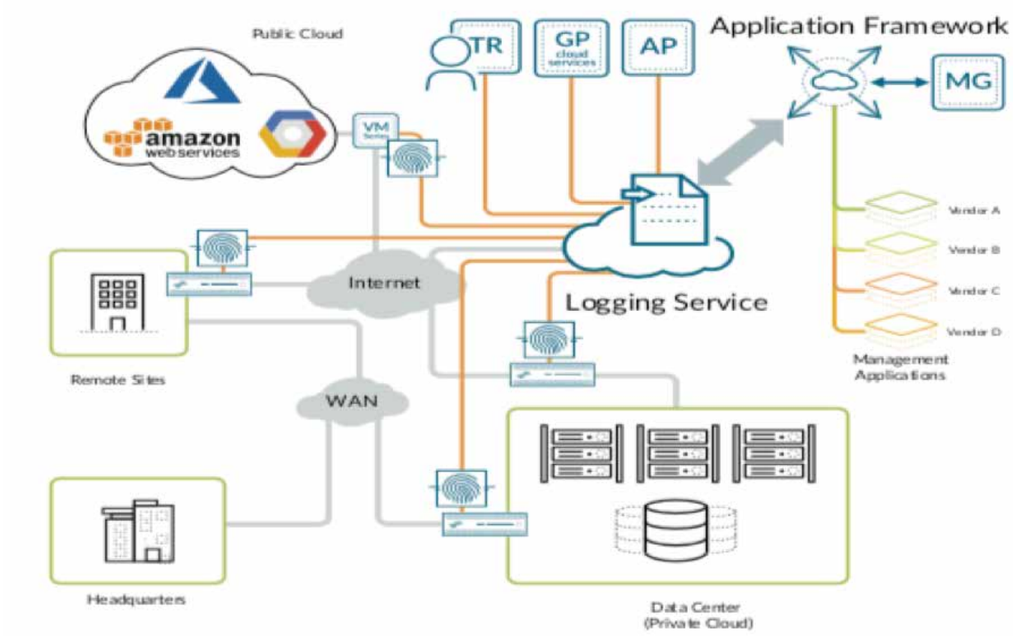
我們持續以獨到的各項先進技術與完善的安全防護平台架構，引領業界進入數位安全新時代，並在全球獲得超過54,000個以上客戶使用，同時在台灣擁有超過2,000位以上客戶的高度評價與肯定，使我們已連續多年蟬連市場上成長最快的資訊安全服務供應商。憑藉我們的平臺，您可以輕易地為所關注的營運服務保駕護航，保持對於環境高度可視性及對於各類風險的可控性，放心地因應業務需求快速擴展所需的服務至各種雲環境並採用各種行動服務的新技術，且免於遭受網路上各種的惡意干擾與攻擊。



安全防護-面面俱到

滿足當今各類型組織的先進資訊安全平台需能夠有效地原生整合各類創新安全技術至單一系統，不但能集中部署安全控制，還能在不同情境 (網路、端點、雲端和 SaaS) 以及攻擊生命週期的各個階段提供一致性的防護能力。

創新資安應用服務框架



應用服務框架(Application Framework)

創新安全平台應用服務框架可滿足以下五項需求

1. 做好準備，阻擋攻擊

首先，您必須擁有網路、端點、雲端和 SaaS 環境的完整可視性，因為您無法保護看不見的地方。有了可視性之後， 您才能夠套用安全政策，並夠針對所有內部網路區段及網路出口點、公司內部及外部所有使用者的網路及端點活動，以及所有存取公司雲端及 SaaS 資源的網路流量，掌握完整的可視性。有了這種可視性，您才能夠套用一致的安全政策，進而保護所有應用程式、使用者及內容。

2. 擁有領先業界的已知威脅防禦

獲得企業環境的完整可視性是必要條件，但對於預防網路攻擊而言還有所不足。有了這樣的可視性後，您的網路安全平台還必須同時擁有領先業界的功能，才能預防好攻擊者為實現目標而在攻擊生命週期中可能發起的每一個已知威脅。這意味著需要採用業界最佳的預防功能來保護您的網路、端點、雲端及 SaaS 環境。

3. 利用相關自動化控制安全功能

業界最佳的預防功能僅能透過原生架構在執行點之間自動進行關聯的範圍內發揮一定作用。當其中一個原生功能發現惡意活動並採取預防措施時，必須以自動化的方式進行溝通和關聯，且據此重寫其他程式，以使每個功能擁有相同的知識基礎。這意味著發現惡意活動並在一個執行點進行預防後，其他所有功能都會自動寫入這個知識。

4. 掌握未知攻擊的能力

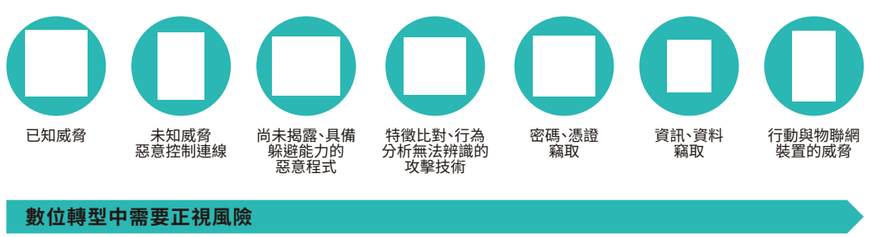
這種集中化控制必須透過多個偵測未知攻擊的技巧來增強。因為不知道攻擊者會從何處出手，所以您必須在企業架構中的所有領域內做好阻止攻擊的準備，同樣您的網路安全架構平台也必須擁有多個偵測未知攻擊的技巧，因為您也不知道攻擊者將會如何發起攻擊。這些技巧必須經過原生整合，才能在發現先前所未知的惡意活動時，將防護機制傳播至每個執行點。

5. 將威脅情報共享至自動化安全

最後，因為沒有組織能真正完整地檢視巨量的惡意活動，因此網路安全平台必須透過全球網路自動追溯威脅情報的來源，並將其和全球網路共享。透過自動化流程及威脅情報共享，網路安全平台能善用強大的網路效應來限制零時差惡意軟體的散播。採用網路安全平台的組織越多，這個網路效應就越強大，因為更多組織能追溯並分享威脅情報，惡意軟體就更難散播。這也能讓工作流程更自動化，減少分析與因應重大資安通報所需的資安人力。

商用科技的不斷演進帶來效率的顯著提升

威脅與風險也跟著進化並以不同的面貌出現



攻擊的手法總是依據各類服務、用戶的行為演進而翻新，並輕易躲避傳統的檢查機制來達成特定的階段性目的，為了避免無止境去異質設備、系統來解決單一問題，最好的策略是先檢視自身環境、關鍵服務及資產等在不同情境下需要被保護的部份，再進一步規劃符合自身需求的技術、擴展需求，同時評估是否能將其整合至單一平台，保有高度的管理效率及風險控制能力。

有效阻絕威脅並做好風險控制的要素

完整的可視性
可以讓您充份了解整體環境中所有的網路活動是否符合預期的管理規劃，同時根據不同情境需求以最直覺的介面進行觀測，更可設計相關自動化的控管機制，提升管理效率。

減少風險曝露
在具備了完整的可視性後，可以透過各類定期事件彙整分析，掌握各項趨勢指標，以此為根據評估相關管理政策之調整與控管機制之優化，積極控制各個可能遭受攻擊的風險。

過濾已知威脅
針對必要的外部連結及服務，首先要利用大數據及雲運算等技術將已被揭露、通報的各種威脅、惡意活動資訊自動更新至所有的防禦政策，免於人工操作造成的失誤及防護空窗期。

預防未知威脅
面對不斷變化及隨機性惡意攻擊（eg.勒索攻擊），防毒、防駭等技術已然過時，需進一步彙整各類先進技術（eg.機器學習、本地分析、實機分析、安全情資通報與利用…），並在大數據及雲運算的優勢基礎上，實現精準防禦並有效破壞惡意攻擊在各個階段的活動。

整合先進科技將安全落實於各種情境

所有對外閘道

您可以藉由重新清點組織內所有與外部連結的邊界，導入我們的安全平台，以獲得前所未有的可視性、有效地依據需求來控制風險，並可進一步阻斷各類可能的威脅。

內部環境、各端點(用戶、裝置)間的通訊

一直以來，內部環境中的用戶、裝置及系統都被視為較安全且不具有威脅性，但隨著不斷爆發的資安事件中，此一風險足以造成組織的營運停擺，並造成重大損失及信譽影響。故充份掌握組織內各類用戶、裝置及系統之間的關係並落實有效的識別與控制(eg.依據職掌）是重要的基礎，並可以進一步執行相關的安全防禦以利在攻擊爆發時進行風險控制。

實體、虛擬資料中心閘道與主機間

採用雲端技術的效益包括提升靈活度、可擴充性，以及因應企業需求的能力。效益相當顯著，不過安全挑戰也相當艱鉅，包括了缺乏應用程式可視性和控制力，無法預防網路攻擊及繁瑣的政策更新程序，導致服務部署和安全政策更新之間出現落差。因此，安全解決方案必須要能識別和控制各種使用的應用程式、依照需求和使用者的認證，控制允許特定使用者進行存取、將安全政策一致性地從網路擴展到雲端和遠端裝置、阻止惡意軟體進入雲端及其帶來的干擾、並在業務需求出現變化時，簡化管理並縮小安全政策更新的落差。

行動裝置

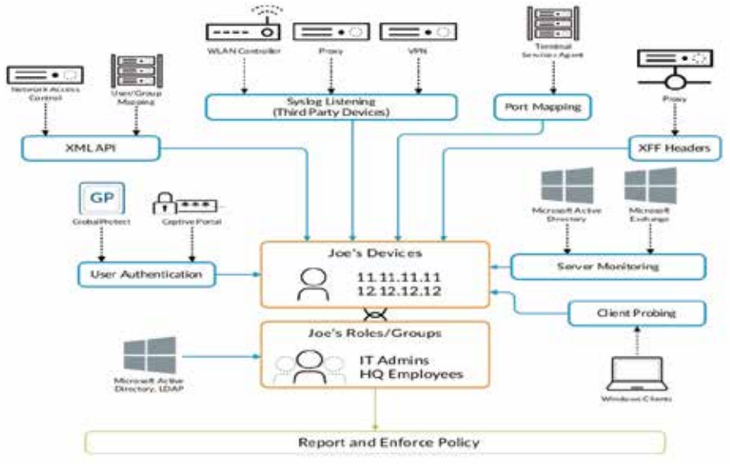
行動工作者需要存取網際網路，以及公共、私人及混合雲端中的應用程式。為保障所有應用程式的存取作業之安全，Global Protect技術能根據您的使用者分布狀態進行部署，還能在人數改變時自動進行調整。各組織能夠部署任何組合形式的硬體、虛擬化或雲端型新世代防火牆，為各種需要支援的應用程式及使用者位置組合提供防護，確保所有用戶在各地都能擁有相同等級的安全防護與高度的服務效率。

公有與私有雲環境及訂閱式商用雲(SaaS)

由於典型 SaaS 的環境對網路管理員而言是不可見的，因此設計用來保護內部資料中心、伺服器及工作站的安全機制便無法有效地保護 SaaS 應用程式或預防資料洩露。Aperture訂閱服務為針對經核准使用的 SaaS 應用程式內的資料和威脅暴露提供了關鍵掌控。並為管理者提供資料分類、共用與存取權限的可見度與威脅防禦，同時保護 SaaS 應用程式內的公司資料免於外部攻擊的威脅和隨之而來的資料洩露或法規違反之問題。

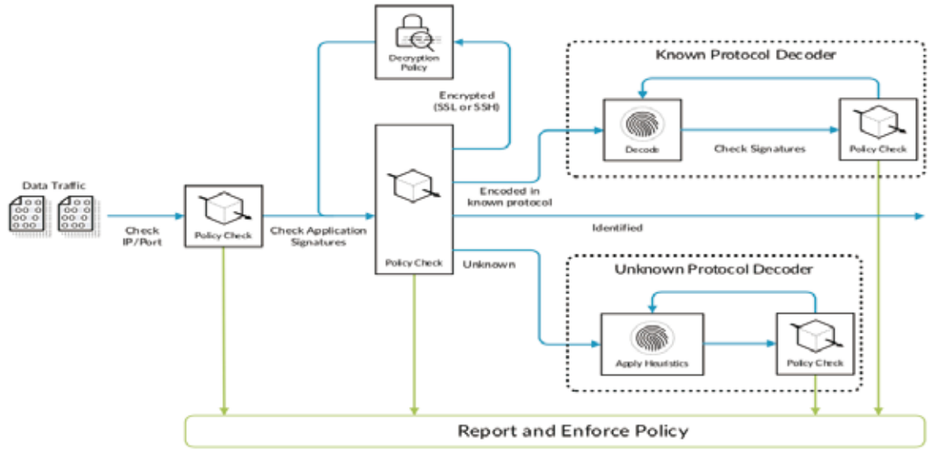
對於環境狀態的完整可視性

業界最完整的用戶識別、管理機制



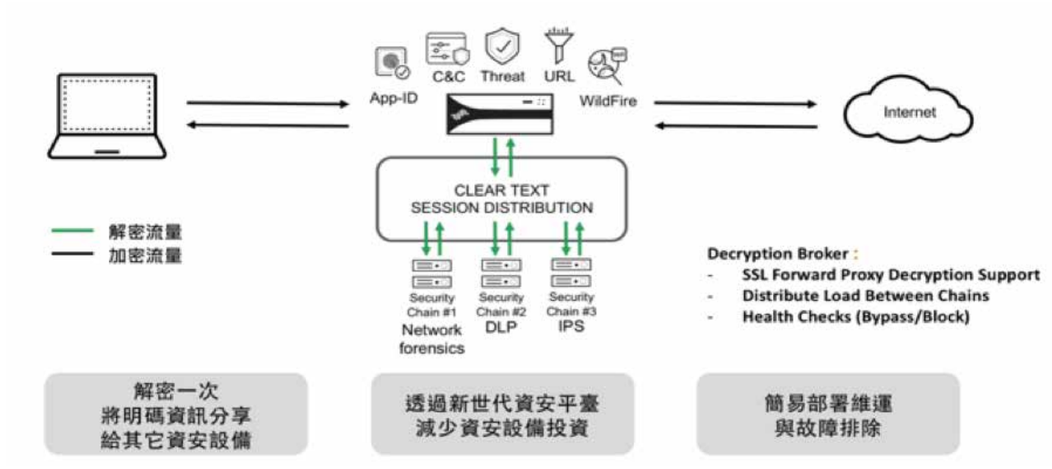
多種主、被動機制協同運行，以符合各種情境需求

精確的應用程式行為識別與控制



應用程式識別技術，擁有完整的可視性，才能實現真正防禦

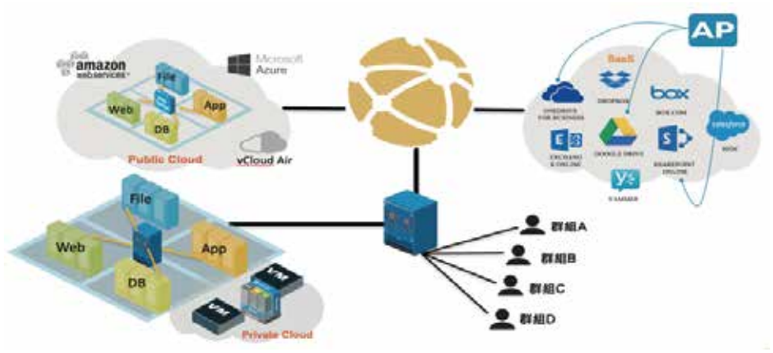
加密流量的識別與控制



簡化SSL加解密部署示意圖

無須額外購買專屬SSL加解密設備, 無須傳統負載平衡器透過三明治架構做SSL加解密增加部署的複雜度，內建SSL加解密排除清單，可彈性依據使用者/IP/IP Subnet/網頁類別等條件做加解密。

減少並有效監控對外曝露



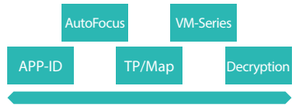
重新識別與盤點所有網路服務
以最嚴謹的思維與先進技術確保用戶安全與關鍵服務正常運行

因地制宜設計最適用的管理政策

您可以最簡易、彈性的方式依據不同的用戶、群組(USER-ID)進行所適當的連線行為掌握及控管(APP-ID)，並可視需求進一步針對各種雲應用(SaaS)進行所需的資料內容查核、安全檢測。基於前述功能，可以進一步同時利用各種先進威脅防禦技術(TP/C2)(WF)(Credential protection)(Decryption)確保用戶對外訪問之安全，以有效降低、控制組織可能面臨的風險。

對於僅供組織內用戶存取的服務，其面臨的資安風險往往被低估。您仍可利用(USER-ID)來確保訪問來源用戶的真實性，同時核對用戶本身的安全性是否足夠(GP)。
另外，採用正向表列來規範各種連線請求(APP-ID)也是一個有效降低服務主機被探測、攻擊的方法。最後，同時針對傳輸內容進行對應的威脅防禦功能(TP/C2)(WF)，即可將受駭風險到最低。

用戶之間的感染已成為許多知名惡意攻擊過程的一環，必須打破過時的思維，以零信任(Zero Trust)的概念重塑安全設計，使用(USER-ID)(APP-ID)協助您以最省力的方式來設計依據用戶、群組其屬性、掌職最適當的政策，有效進行各區段的風險控制。相關的威脅防禦機制(TP/C2)(WF)(Credential Protection)則可協助您在攻擊活動潛伏時期獲得即時的通報並進行自動化處置。



各類對外服務一直以來都是惡意攻擊最易展開探測、干擾的對象之一，透過(APP-ID)(MAP)可協助管理者掌握實際連線行為，過濾異常存取並執行正向表列控制，再輔以威脅防禦機制(TP/C2)(Decryption)阻斷各種惡意破壞。
全球資安情報服務(Autofocus)可協助您掌握來自四面八方對組織可能的攻擊意圖，以做好因應策略。另外，當您將服務遷移至各類雲環境中，我們亦提供相同的防禦機制(VM-Series)供您簡易的選用、佈署與管理機制。

自動化威脅防禦

全面性檢測所有(網路、端點、雲)流量不遺漏

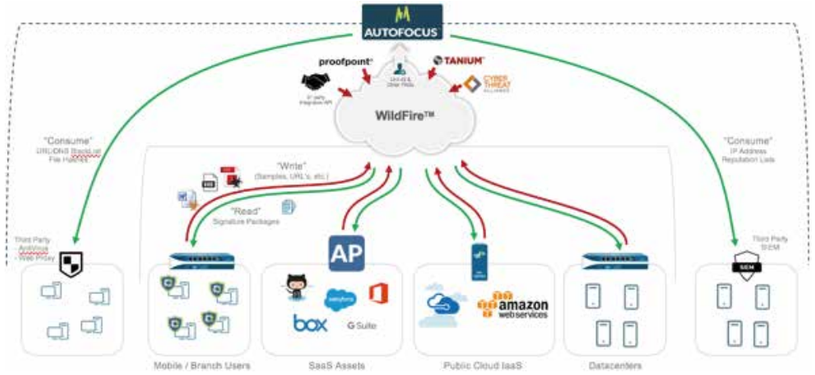
現今網路環境面對各種推陳出新的攻擊手法防不勝防，在傳統資安環境或單一功能資安解決方案拼湊式架構，將會面臨一個很嚴重的問題，專屬資安設備只提供單一功能識別，在駭客技術持續精進之下，很容易規避單一設備檢測，因此需要全面性檢測所有流量資訊從L1至L7(應用服務)執行完整的識別，才能分析裡面的惡意程式碼及攻擊手法，同時自動產生所有和攻擊手法有關的防護資訊並自動更新至資安平臺落實即時防禦，而非僅僅由人工檢視報表後再進行防禦設定。

創新的憑証防護機制

利用帳號竊取資料革命性防護Credential theft

Palo Alto Networks創新技術Credential theft針對現在各種攻擊的起源不外乎透過釣魚郵件裡面夾雜著惡意的釣魚網頁或釣魚網址，而這些郵件或網頁會非常類似你每日常作業所使用的網頁服務，讓使用者無從識別，進而竊取帳號，利用該合法帳號於內部網路搜尋相關機敏性資料，最後將其走加密管道(SSL)匯出，通常使用者都是最後一個才知情的，透過Palo Alto Networks 網頁過濾技術簡合機器學習分析等，我們可以提取email裡的URL連結，即時分析並攔阻，即該帳號被盜時嘗試專取重要系統資料庫時，結合User-ID與MFA(多重認證)來避免，重要系統只要被盜合法帳號存取即所有資料外洩，也避免傳統為了解決帳號被盜問題，耗時耗力耗成本的全面佈建Token解決方案，在預算有限的情況下，可以只針對重要財務、研發資料庫進行Credential theft部署。

創新情資應用與智慧自動聯防



Autofocus智能情資可協助第三方資安廠商快速聯防

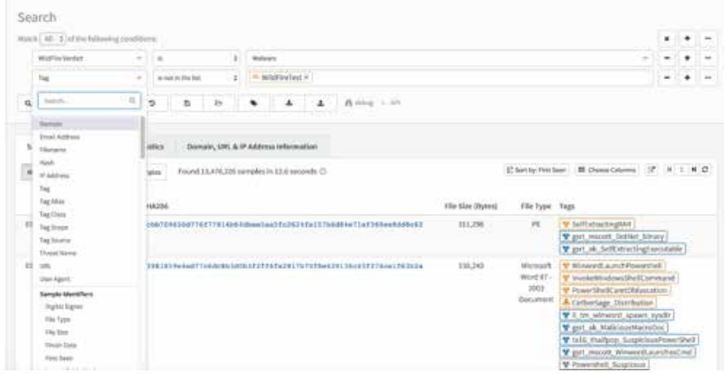
現在資安設備著重於未知攻擊的防禦，多是依靠雲端大數據分析，將流量分析，並即時產生相對應的特徵碼，並更新至資安設備裡，大多數資安廠商由於是單一功能資安設備如AV、IPS、APT、Proxy等，產生的特徵碼也是單一功能為主，無法提供全面性防禦，唯有Palo Alto Networks資安解決方案產生全方位特徵碼(如：AV、IPS、APT、URL、DNS、IP)等，並可設定每5分鐘更新至資安平臺、端點、雲端/資料中心、SAAS等，提供業界最快速即時防禦，落實無邊界的全面防禦，並可將搜尋情資輕易整合至客戶既有SOC或SIEM平臺做即時防禦。

預防未知/零時差新威脅

智慧威脅情報雲(WildFire)全球最即時資安資料庫，每5分鐘更新

WildFire全球最大即時資安資料庫，擁有30億個樣本資料且持續每月新增3億樣本資料快速成長，資料來源源自於Palo Alto Networks全球54,000個客戶，橫跨各種不同產業，從資安平臺(NGFW)、端點防禦(TRAPS)、雲端軟體即服務(Aperture)等各種不同部署位置持續貢獻分析流量與樣本資料，另外還有來自於CTA (Cyber Threat Alliance)APT資安大聯盟資料庫的每天提供的20,000筆最新APT資料及資安相關廠商整合如ProofPoint APT Mail解決方案、TANIUM端點APT IOC專業廠商所餵入APT資料, 還有美國國土安全部(Homeland Security Department)公私部門資安威脅資訊交換與國際刑警組織全球創新總部(INTERPOL Global Complex for Innovation;IGCI)簽署資料交換協定(DEA)等相關最新資安情資，每天新增23萬個獨家最新威脅情資，並可每5分鐘自動更新至資安平臺與端點。

先進資安情報服務(Autofocus)



AutoFocus最新惡意程式及攻擊手法情資即時搜尋

傳統上政府機關或企業都是從新聞或一些相關管道得知哪些單位被駭，無從進一步得知該攻擊的詳細資訊，讓相關單位可以提早預防，避免遭受相同攻擊，如最近的國內常發生的金融業遭受駭客攻擊，造成龐大金融損失，透過Palo Alto Networks AutoFocus智慧情資服務，可以搜尋到特定惡意程式或攻擊手法，透過哪些email及網址造成使用者下載惡意程式，進而植入惡意代碼，透過偽裝成使用者正常連線回報中繼站主機或僵屍網路主機(如DNS查詢)，攻擊手法(Exploits)、攻擊特徵碼(Signatures)、雜臭值(Hash)、機碼、檔案、路徑、C2 IP/DNS等相關資訊皆可即時搜尋，並將搜尋結果匯出至相關資安設備做即時防禦或透過Palo Alto Networks資安平臺和端點TRAPS做即時防禦。

面對不斷進化的攻擊手段須結合雲端上各種新型態偵測預防技術

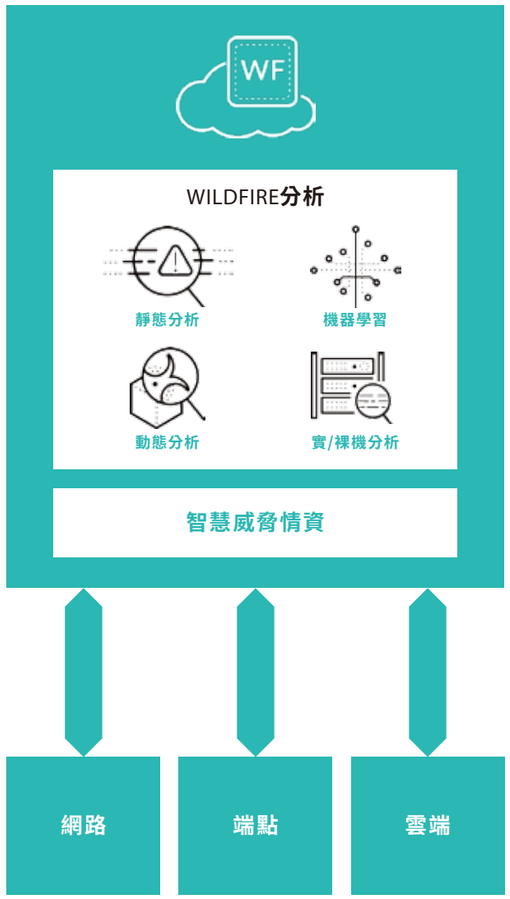
智慧威脅情報雲(WildFire)核心技術 – 偵測未知惡意軟體與攻擊手法

Palo Alto Networks Wildfire雲端威脅分析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核心技術做法，結合:1.靜態分析:檢查數以千計的字串及文件特徵可以快速有效地對已知惡意軟件變種和指標進行分類、2.創新的機器學習技術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、3.動態分析:在客製化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）、4. 突破性的裸機分析環境： 針對規避型威脅會被自動傳送到實際的硬體環境進行觸發，完全解除攻擊者規避VM分析技術的能力。

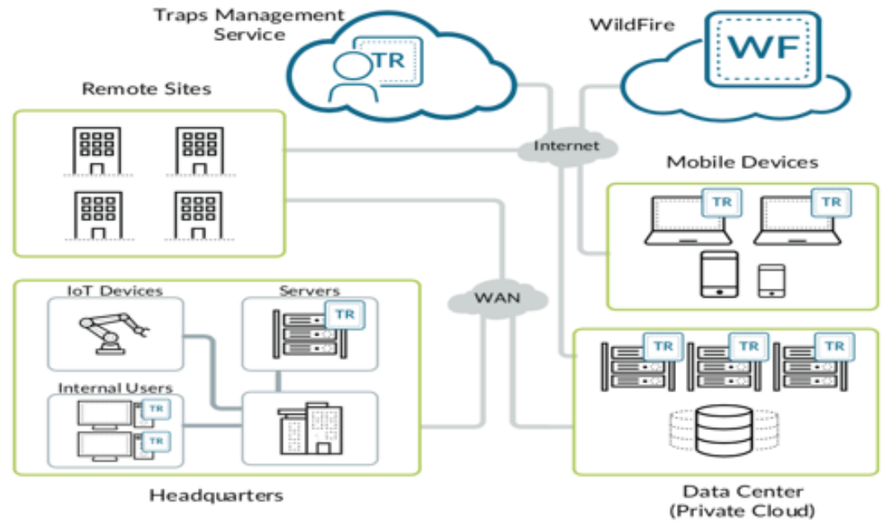
300M WildFire 每個月發現的新惡意軟體樣本

45% Virus Total 從未發現過但WildFire 檢測到的惡意軟體

智慧威脅情資在端點、網路和雲端共享and cloud



端點防禦劃時代創新革命來襲



Traps進階端點防禦部署示意圖

Traps提供端點全方位技術攔阻各種新型態攻擊

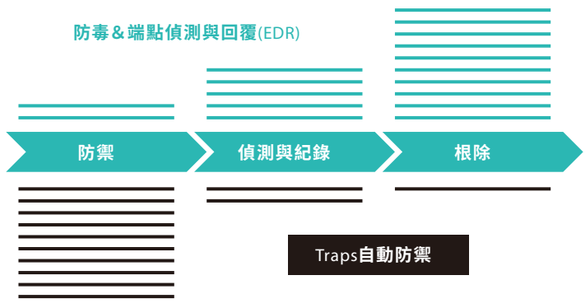
由上圖可以看到傳統端點解決方案功能象限圖，AV主要著重在已知惡意程式偵測，HIPS著重在已知攻擊手法偵測，市場上出現新世代EDR(EndPoint Detection Response)解決方案著重在未知惡意程式事後鑑識分析，記錄完整攻擊軌跡資料，所以即時阻斷功能相對薄弱，唯有Palo Alto Networks Traps提供所有已/未知的惡意程式/攻擊法手法多層次防禦，結合Traps業界獨家行為分析模式，全面阻斷各種攻擊手段。

領先業界的新世代端點多層次創新防禦

Traps提供多層次防禦

傳統AV、新世代AV、EDR(EndPoint Detection and Response)等端點解決方案，九成以上著重在於惡意軟體的防禦，依靠已知特徵碼的比對及攻擊發生後的完整記錄，面對新世代複合型攻擊手法日益推陳出新，除了惡意軟體的防禦，也需針對攻擊手法(Exploits)提供全面性的防禦，因為惡意軟體的攻擊須結合Exploits攻擊手法，Traps新世代端點解決方案，業界唯一提供針對核心攻擊手法(Exploits)技術提供行為模式偵測與防禦，Traps提供多層次的防禦方式，讓各種攻擊手法無所遁形。

端點防禦捨棄過去事後補救換成即時防禦新概念



TRAPS唯一一家著重在攻擊即時防禦而不是事後鑑識分析

傳統端點解決方案依靠特徵碼比對及事後鑑識分析記錄攻擊軌跡，面對新型態攻擊手法常常都是攻擊已經發生後數月後才發現被入侵，此時資料已被竊取，根據統計所有單位被駭時間平均240~280天後，才發現系統已被入侵，傳統端點解決方案重心在攻擊發生後的偵測與清除，對於管理者而言需耗費大量時間蒐集資料與分析並清除，但是由於攻擊手法太先進與複雜，常發生清除不乾淨，最後通常是依靠備份或還原等選項來解決，此時使用者也會備份自己的資料，此時會沿入無止盡的循環，新世代端點解決方案TRAPS是唯一一家著重在攻擊發生時，即時阻斷，避免後續的攻擊手法持續運作，所以對於管理者而言，可以減少大量相關攻擊事件日誌分析，避免駭客於內部網路或系統流竄。

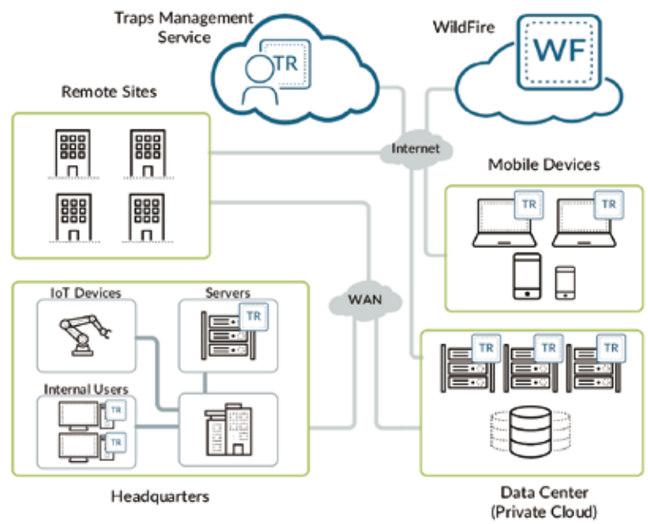
新世代端點防禦Traps獲得NSS實驗室2018進階端點防禦(AEP)最佳推薦

根據 NSS 實驗室的 2018 進階端點防護測試報告，Traps：

- 獲得了 97.7% 的整體安全性效能評分，能阻擋百分之百的入侵和迴避攻擊，誤判率為零。
- 在三年期間內，提供最佳的整體總擁有成本 (包括維護、安裝、警示、監控與維持費用)。

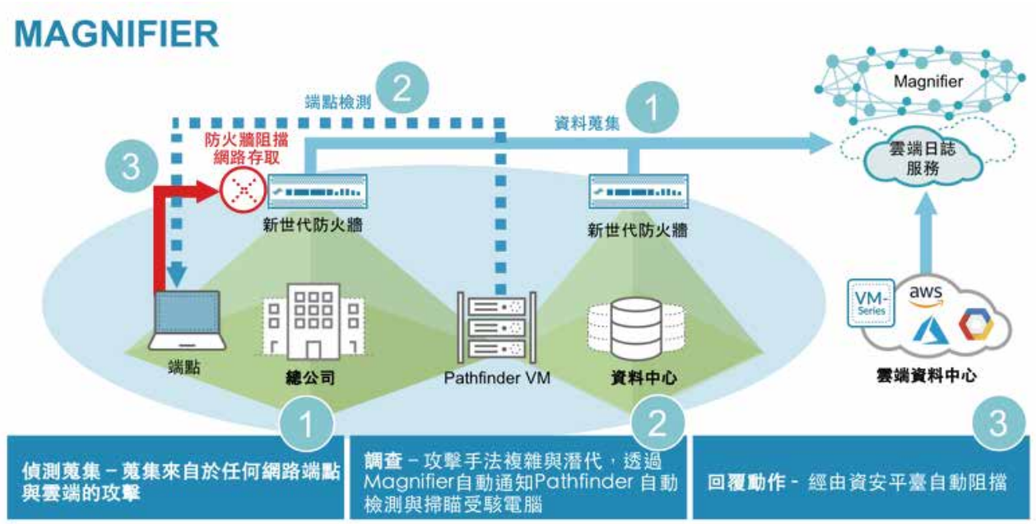
這些結果以及 NSS 實驗室所給予的「推薦」評級，共同印證了 Traps 及其防禦優先做法的實際效能。

進階端點防禦全面性部署



Traps部署示意圖

新世代使用者行為分析Magnifier

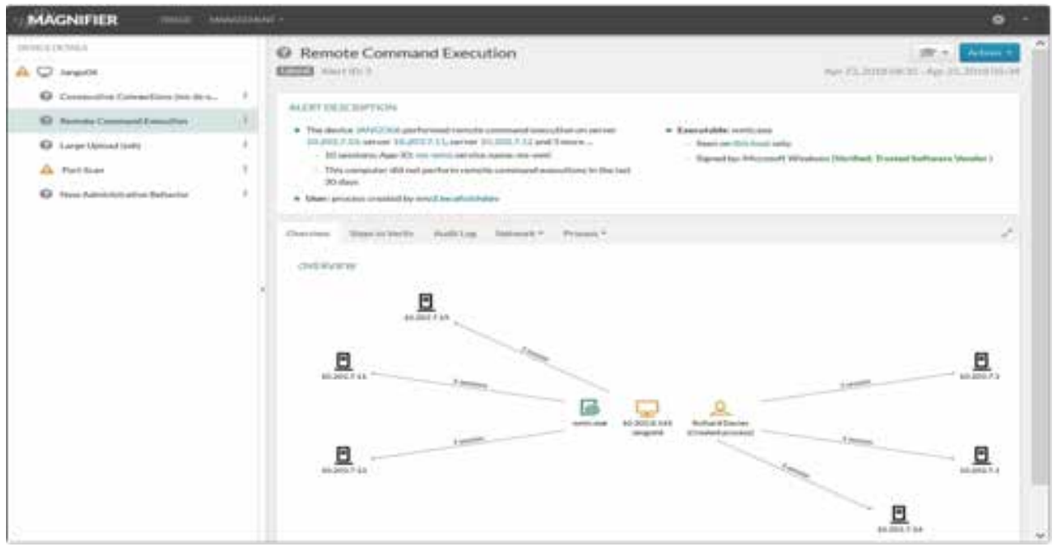


Magnifier運作模式

新世代使用者行為分析(UBA/UEBA)協助客戶快速找出潛伏於網路的惡意軟體與駭客，無須大量部署Sensor，即可透過現有Palo Alto Networks新世代防火牆資安平臺蒐集來自於網路相關線索，經由Magnifier運算分析相關網路日誌，即自動啟發Pathfinder針對可疑與異常行為之端點/伺服器主機執行掃瞄與檢測，透過Magnifier儀表板圖形化介面呈現所有可疑主機之有問題的網路存取行為透過關聯性分析讓你清楚透析攻擊全貌，並可透過新世代防牆自動阻擋。

使用者行為分析演算框架

Magnifier輕鬆分析出潛伏的惡意/異常連線行為



Magnifier直覺化圖形介面

Magnifier提供自動化作業方式，將最好的行為分析能力整合到Palo Alto Networks新世代安全平台以預防網路攻擊。它將協助負荷繁重的安全團隊改善資安同時節省金錢與時間，運用機器學習並且自動辨識潛在威脅以預防網路攻擊。

Magnifier行為分析提供多項創新能力，包括：

精確與效率

Magnifier分析來自新世代防火牆和Pathfinder端點分析服務的資料，建立使用者與裝置行為模式。由於Magnifier的偵測演算法是針對新世代安全平台傳送的日誌(logs)量身訂製，可以運用精確的機器學習和攻擊偵測演算法，因此和仰賴檢查日誌檔以預防威脅的方法相比能夠產生數量較少且精確度高的有效預警。

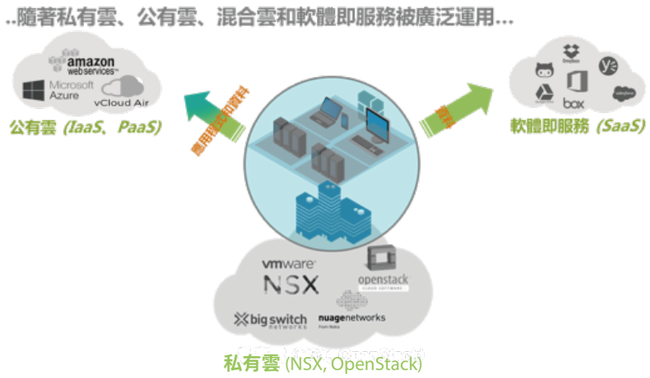
自動調查

Magnifier藉由自動質詢可疑的端點以判斷是否有那些程序涉及攻擊行為，提供精簡而有效率的威脅搜尋。然後，它會運用Palo Alto Networks WildFire®雲端威脅分析服務，分析上述可疑程序以判斷其是否惡意。Magnifier的端點分析和詳細的預警提供完整的偵查細節，讓安全分析師能夠立即檢視並做出回應。

延展、敏捷、容易部署

Palo Alto Networks客戶只需要啟用Magnifier應用和Palo Alto Networks Logging Service就能簡單的建置行為分析能力，並使用他們既有的Palo Alto Networks防火牆作為感測器從遠距收集他們的網路資料，而無需採購和維護額外的網路裝置或部署昂貴的on-premise日誌伺服器。

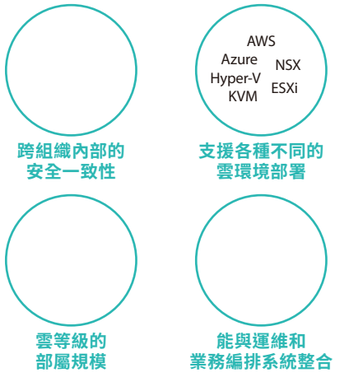
基於各類雲環的安全整合趨勢



隨著雲時代的快速進化，安全需求更需要強化，在人力不增加的狀況下，又可以快速配合與增減虛擬主機的變動，以下三項條件，是虛擬化在運作中必須要的考量。

1.企業等級的防護　　**2. 預防、應變與重新加固**　　**3. 高度整合與自動化**

雲時代的安全需要全面性的通盤考量



	雲平臺內建安全功能	基於雲的安全服務	新一代虛擬防火牆
功能特性	基於IP位置和四層網路層通訊（Layer 4）埠的存取控管和流量過濾	僅能提供如入侵偵測或入侵防預之單一功能，且多基於端點	基於應用和使用者資訊的存取控管和流量過濾，並能預防威脅入侵
優勢	免費且易於部屬，提供基本的存取控管	基於端點的入侵偵測或入侵防御功能，對現有管理平臺影響較小	提供基於應用層可視性，控管及威脅入侵預防
弱項	無法有效防護高危應用；缺乏威脅預防機制；不能針對特殊檔案位置進行控制	受限於已知威脅資料庫，但經常更新會使運維流程變得複雜	需要透過網路配置變更進行部屬，不易融入DevOps 的流程

藉由原生雲服務構建安全，可擴展，及高可用的應用部署環境

PAN-OS 對數據平面的優化

充分運用例如
PCI-PT，SR-IOV 及 DPDK 等 I/O新技術

支援資料平面橫向擴展的設計
(性能可能伴隨運算資源線性擴張)

在軟體架構上完美呈現 PAN-OS 的 Single Pass Architecture

專為私有雲和公有雲需求設計的 VM-Series 次世代防火牆

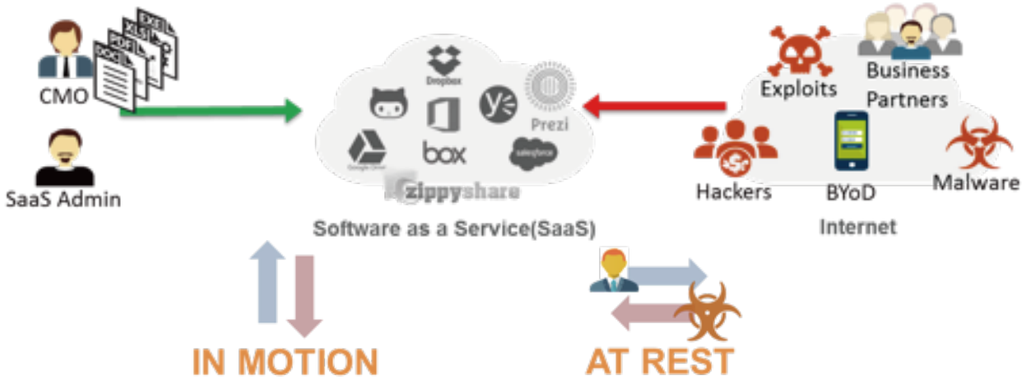
提供完整可視性	降低攻擊管道	防禦已知威脅	防禦未知威脅
・識別所有應用程式、使用者、內容 ・識別加密流量 ・識別雲端流量、軟體即服務SaaS流量 ・識別憑證、身份與主機配置資訊	・允許單位業務應用程式 ・阻檔非法應用程式 ・限制應用程式功能 ・限制檔案種類存取 ・阻檔網站	・惡意程式/惡意軟體 ・攻擊手法 ・中繼站主機連線 ・惡意與非法網站 ・惡意網域名稱 ・憑証竊取	・動態沙箱分析 ・靜態分析 ・機器學習分析 ・攻擊者核心手法分析 ・裸/實機分析 ・異常行為分析

所有網路位置

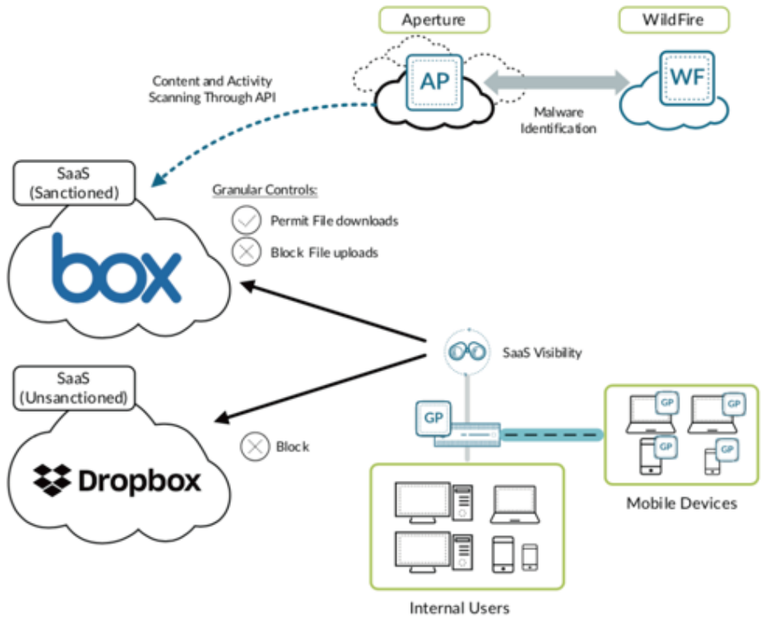
為公有雲、私有雲及混合雲環境量身打造的新一代安全防護

基於各類雲環境的安全整合趨勢 Aperture

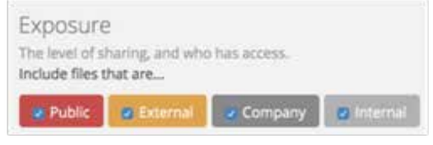
SAAS的安全挑戰

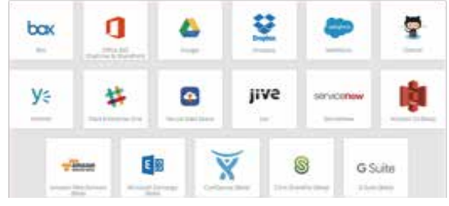


當使用者便利的使用雲的應用程式時，相關的漏洞與惡意攻擊產生在雲端，也會讓駭客組織有機會入侵滲透，需要雙管齊下的策略與解決方案。



Aperture 雲端服務(SaaS)安全示意圖



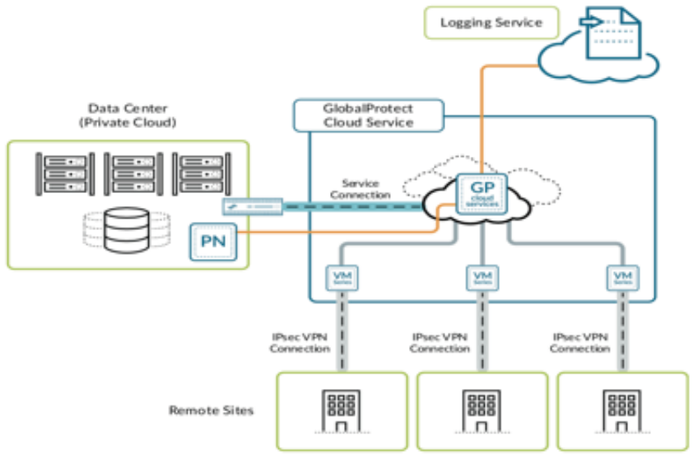


便利的雲端存取時，安全的防禦機制，必須符合以下的幾個條件

1. 稽核資料的存取 : 必須要記錄著每份文件的使用者傳遞過程與檔案內容
2. 阻斷惡意程式的入侵 : 雲端沙箱快速過濾每份檔案的內容
3. 保護公司憑證與機密文件 : 防禦憑證竊取機制、使用者二次認證與應用程式的辨識
4. 保護程式原始碼 : 防禦程式原始碼被竄改或是植入惡意程式
5. 阻檔不信任的使用者存取 : 辨識使用者的身份與檢查硬體設備的安全性

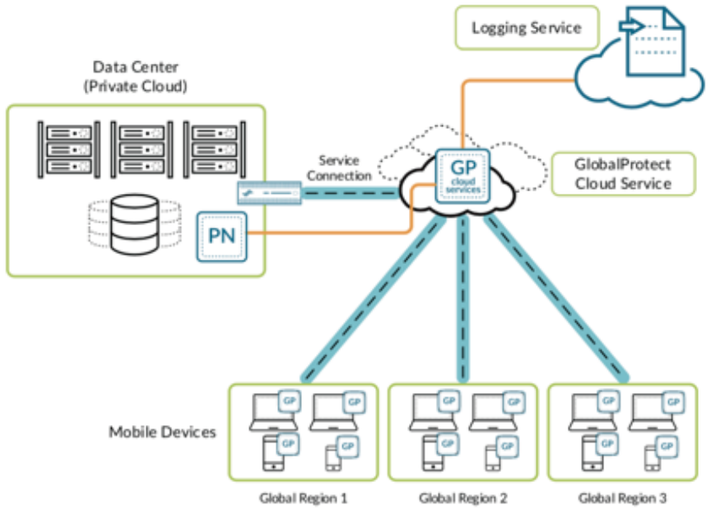
雲端應用程式支援種類不斷的增加，快速提供全球客戶群的使用度，遍及美國、歐洲與亞洲，讓全球用戶都可享用Palo Alto Networks Aperture的保護機制。

行動用戶安全雲服務



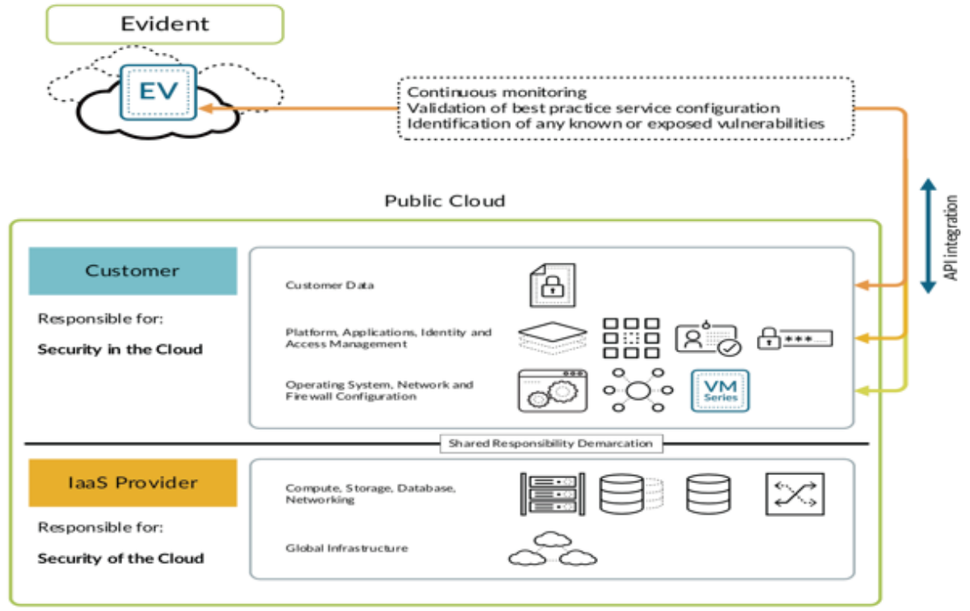
GobalProtect雲服務對於分公司遠端加密存取示意圖

因應目前網路使用的便利趨勢，可以在全球各地雲端上安全的存取總公司的資料，可透過各地分公司的網路設備，也可使用行動裝置設備存取，並可達成硬體設備安全的檢查，確認使用者的身份與分配應用程式存取。



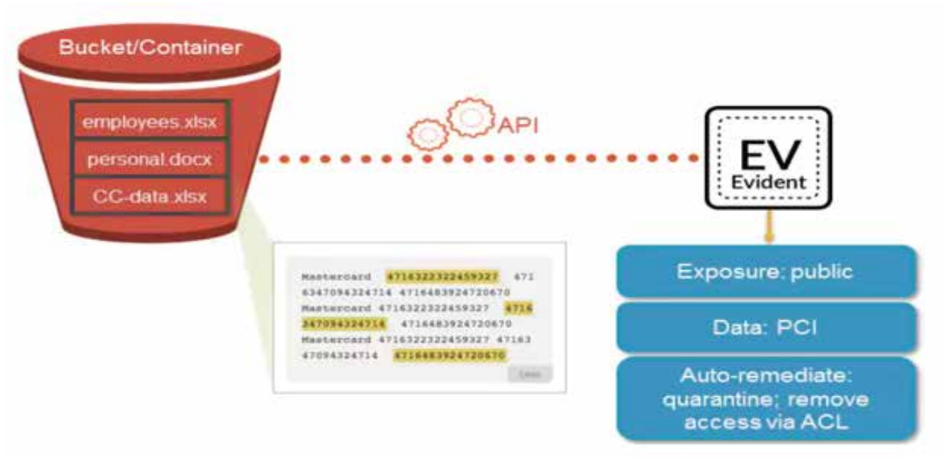
GobalProtect雲服務對行動使用者遠端加密存取示意圖

公有雲監控與稽核風險服務



Evident雲端基礎架構保護示意圖

Evident儀表板一目了然各種公有雲服務的資安風險



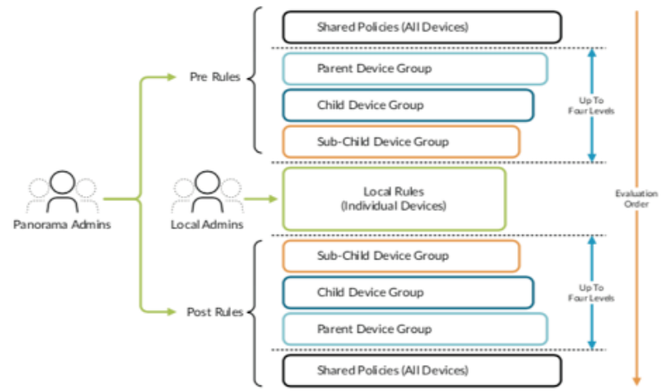
Palo Alto Networks Evident公有雲跨平臺監控與稽核機敏資料外洩與合規性。

Evident提供安全性針對公有雲基礎設施服務與一目了然的資安法規報告，使您能夠自信地部署應用程式，知道公有雲的設定為符合與滿足您組織的安全需求。

Palo Alto Networks Evident公有雲跨平臺監控與稽核機敏資料外洩與合規性。

針對大型環境下完善的管理平台

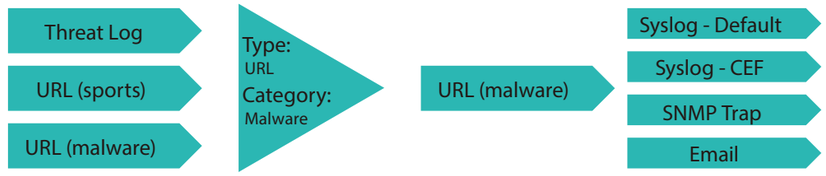
彈性的政策佈署派送至不同的次世代防火牆



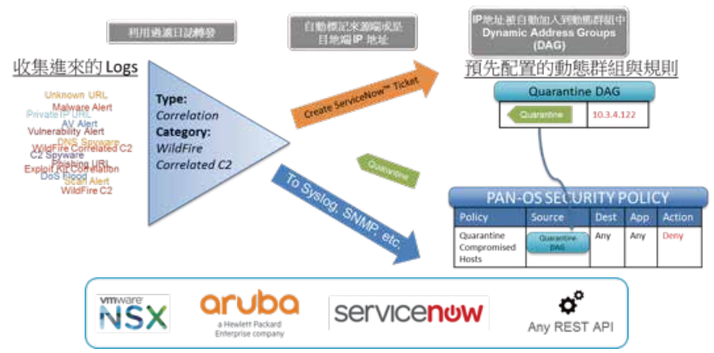
Panorama logs

檔案的收集可以選擇篩選條件與轉送後的格式

收集進來的logo　客製化的篩選條件　篩選後的logo　轉送的格式



自動化的工作流程



預先定義好動態群組與規則，當收集到預先篩選記錄的條件時，自動啟動標記來源端或是目地端隔離機制，在規則上自動隔離有異常的IP位址，可迅速在未擴散或是爆發前，阻斷與攔截異常的來源端與目地端。
並可使用Http log轉送方式，整合至客戶端目前的工作派單流程(create ticket)，也可使用API達到程式語法的整合。

隨時可針對您的環境進行安全風險評估

1. 評估網路流量中的應用程式風險

以Tap Mode方式收集由外往內與內往外的網路流量，進而分析使用者往外的應用程式連線存取風險，也可再深入分析ServerFarm前進出的應用程式流量，可視性使用者的是否正確存取與濫用。

2. 未知連線與加密連線

從報表分析中更可以細部的看到未知的連線(unknown tcp or unknown udp)，由哪些用戶端或是主機上所發起的，進而做後續處理但可先用規則攔截未知連線存取；甚至SSL的加密連線屏蔽掉管理者的管控，透過加解密的方式發覺駭客連線隱藏在其中，竊取或是存取重要機密文件。

3. 已知的Malware與Exploits

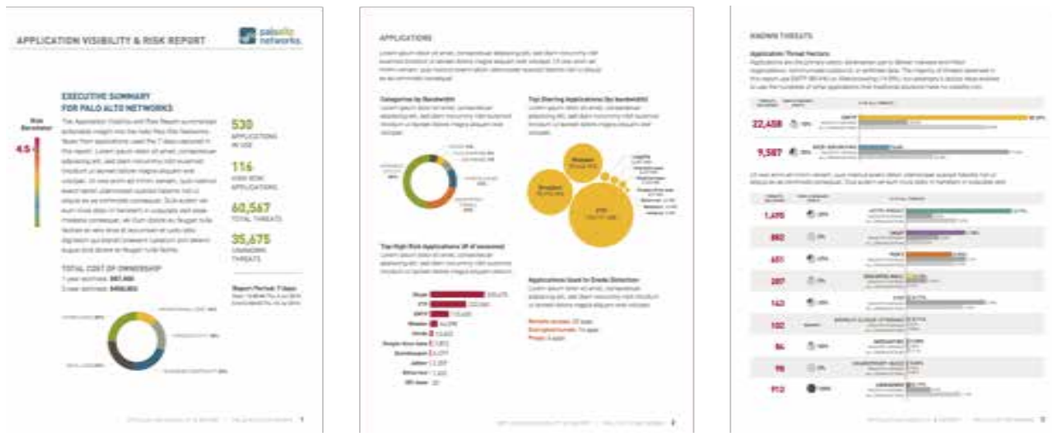
已知的Malware與Exploits: 既然是已知的Malware與Exploits，更應該在用戶端詢問DNS時或是存取(C2 Networks)當下，就可以直接阻斷掉這些惡意連線，所以每分鐘的大數據資料庫更新，取決於樣本數量多(1.5億)與更新的速度(每分鐘)，讓及時的探詢或是攻擊連線都可被比對顯示於報表中。

4. Zero-day Malware與APT

透過雲端沙箱檢視檔案後，把相關的軌跡資訊更新至大數據中，從雲端中使所有用戶都可以更新，並可防禦新形態的攻擊手法。

5. Command and Control Traffic

C2 Networks惡意中繼站的大本營，當企業內部網路中有很多Botnet時，會隨著需要更新惡意中繼站資訊，透過正常網路連線(DNS、Http、SMTP)或是加密連線(Https)做更新，操控著Botnet並發出大量的對外攻擊連線，甚至於成為駭客的跳板，竊取企業資訊或是控制著權限較高的帳號，盜轉資金或是盜賣機密資料。



全面性的進階威脅檢測報告，只需要一週的時間，以簡易架構(Tap Mode)就可提供評估企業網路內部流量的可視化，解析藏在應用程式通道中的威脅，在攻擊爆發前找出受駭的用戶端，讓未來的資安規劃更輕鬆。

Performance and Capacities[1]	PA-7080 System[2]	PA-7050 System[2]	PA-5280	PA-5260	PA-5250	PA-5220
Firewall throughput (App-ID)	200 Gbps	120 Gbps	68 Gbps	68 Gbps	39 Gbps	18 Gbps
Threat prevention throughput	100 Gbps	60 Gbps	30 Gbps	30 Gbps	20 Gbps	9 Gbps
IPSec VPN throughput	80 Gbps	48 Gbps	24 Gbps	24 Gbps	16 Gbps	8 Gbps
New sessions per second	1,200,000	720,000	462,000	462,000	348,000	171,000
Max sessions	40,000,000/80,000,000[3]	24,000,000/48,000,000[3]	64,000,000	32,000,000	8,000,000	4,000,000
Virtual systems (base/max[2])	25/225	25/225	25/225	25/225	25/125	10/20

Hardware Specifications	PA-7080 System	PA-7050 System	PA-5280	PA-5260	PA-5250	PA-5220
Interfaces supported NPC option 1[4]	Up to (20) QSFP+, (120) SFP+	Up to (12) QSFP+, (72) SFP+	(4) 100/1000/10G Cu, (16) 1G/10G SFP/SFP+, (4) 40G/100G QSFP28			(4) 100/1000/10G Cu, (16) 1G/10G SFP/SFP+, (4) 40G QSFP+
Interfaces supported NPC option 2[4]	Up to (120) 10/100/1000, (80) SFP, (40) SFP+	Up to (72) 10/100/1000, (48) SFP, (24) SFP+				
Management I/O	(2) 10/100/1000, (2) QSFP+ high availability, (1) 10/100/1000 out-of-band management, (1) RJ45 console		(2) 10/100/1000 Cu, (1) 10/100/1000 out-of-band management, (1) RJ45 console			
			(1) 40G/100G QSFP28 HA			(1) 40G QSFP+ HA
Rack mountable?	19U, 19" standard rack	9U, 19" standard rack or 14U, 19" standard rack with optional Airduct kit	3U, 19" standard rack			
Power supply	4x2500W AC (2400W / 2700) expandable to 8	4x2500W AC (2400W / 2700W)	2x1200W AC or DC			
Redundant power supply?	Yes		Yes			
Disk drives	2TB RAID1		System: 240GB SSD, RAID1. Log: 2TB HDD, RAID1			
Hot swap fans	Yes		Yes			

Performance and Capacities[1]	PA-3260	PA-3250	PA-3220	PA-3060	PA-3050	PA-3020
Firewall throughput (App-ID)	8.8 Gbps	6.3 Gbps	5 Gbps	4 Gbps	4 Gbps	2 Gbps
Threat prevention throughput	4.7 Gbps	3 Gbps	2 Gbps	2 Gbps	2 Gbps	1 Gbps
IPSec VPN throughput	4.8 Gbps	3.2 Gbps	2.5 Gbps	500 Mbps	500 Mbps	500 Mbps
New sessions per second	135,000	94,000	58,000	50,000	50,000	50,000
Max sessions	3,000,000	2,000,000	1,000,000	500,000	500,000	250,000
Virtual systems (base/max2)	1/6	1/6	1/6	1/6	1/6	1/6

Hardware Specifications	PA-3260	PA-3250	PA-3220	PA-3060	PA-3050	PA-3020
Interfaces supported[4]	(12) 10/100/1000, (8) 1G/10G SFP/SFP+,(4) 40G QSFP+	(12) 10/100/1000, (8) 1G/10G SFP/SFP+	(12) 10/100/1000, (4) 1G SFP, (4) 1G/10G SFP/SFP+	(8) 10/100/1000, (8) SFP, (2) 10 SFP+	(12) 10/100/1000, (8) SFP	
Management I/O	(1) 10/100/1000 out-of-band management port, (2) 10/100/1000 high availability, (1) 10G SFP+ high availability, (1) RJ-45 console port, (1) Micro USB			(1) 10/100/1000 out-of-band management,(2) 10/100/1000 high availability, (1) RJ-45 console		
Rack mountable?	2U, 19" standard rack			1.5U, 19" standard rack	1U, 19" standard rack	
Power supply	Redundant 650-watt AC or DC			Redundant 400W AC	250W AC	
Redundant power supply?	Yes			Yes	No	
Disk drives	240GB SSD			120GB SSD		
Hot swap fans	No			No		

Performance and Capacities[1]	PA-850	PA-820	PA-220	PA-220R
Firewall throughput (App-ID)	1.9 Gbps	940 Mbps	500 Mbps	500 Mbps
Threat prevention throughput	780 Mbps	610 Mbps	150 Mbps	150 Mbps
IPSec VPN throughput	500 Mbps	400 Mbps	100 Mbps	100 Mbps
New sessions per second	9,500	8,300	4,200	4,200
Max sessions	192,000	128,000	64,000	64,000
Virtual systems (base)	1	1	1	1

Hardware Specifications	PA-850	PA-820	PA-220	PA-220R
Interfaces supported[4]	(4) 10/100/1000, (4/8) SFP, (0/4) 10 SFP+	(4) 10/100/1000, (8) Gigabit SFP	(8) 10/100/1000	(6) 10/100/1000, (2) SFP
Management I/O	(1) 10/100/1000 out-of-band management, (2) 10/100/1000 highavailability, (1) RJ-45 console, (1) USB, (1) Micro USB console		(1) 10/100/1000 out-of-band management, (1) RJ-45 console, (1) USB, (1) Micro USB console	(1) 10/100/1000 out-of-band management, (1) RJ-45 console, (1) USB, (1) Micro USB console
Rack mountable?	1U, 19" standard rack		1.62"H X 6.29"D X 8.07"W	2.0"Hx8.66"Dx9.25"W
Power supply	Two 500W AC. One is redundant.	200W power supply	Dual redundant 40W	Dual DC Power Suuply
Redundant power supply?	Yes	No	Yes (optional)	Yes (optional)
Disk drives	240GB SSD		32GB EMMC	64GB EMMC
Hot swap fans	No		No	No

Performance and Capacities[1]	VM-50	VM-100/VM-200	VM-300/VM-1000HV	VM-500	VM-700
Firewall throughput (App-ID)	200 Mbps	2 Gbps	4 Gbps	8 Gbps	16 Gbps
Threat prevention throughput	100 Mbps	1 Gbps	2 Gbps	4 Gbps	8 Gbps
IPSec VPN throughput	100 Mbps	1 Gbps	1.8 Gbps	4 Gbps	6 Gbps
New sessions per second[1]	3,000	15,000	30,000	60,000	120,000

PANORAMA	Central Management Appliance				Central Management Virtual			
	M-100	M-200	M-500	M-600	N/A	Vmware ESX	MicroSoft Hypervisor	Cloud Amazon AWS
I/O	(4) 10/100/1000, [1] DB9 consolese rial port, (1) USB	(4) 10/100/1000, [1] DB9 console serial port, (1) USB port	• (4) 10/100/1000, (1) DB9 console serial port, (1) USB port,(2) 10 GigE ports	• (4) 10/100/1000, (1) DB9 console serial port, (1) USB port,(2) 10 GigE ports	Management Only Mode		8 CPUs	t2.xlarge m4.2xlarge
Storage	Maximum configuration: RAID: 8 x 2 TB RAID Certified HDD for 8 TB of RAID storage	Maximum configuration: RAID: 4 x 8 TB RAID Certified HDD for 16 TB of RAID Storage	• Maximum configuration: RAID: 24 x 2TB RAID Certified HDD for 24TB of RAID storage	• Maximum configuration: RAID: 12 x 8 TB RAID Certified HDD for 48 TB of RAID storage	Panorama Mode		32 GB	m4.2xlarge m4.4xlarge
Power Supply/Max Power Consumption	500W/500W	• Dual Power Supplies, hot swap redundant configuration • 750W/300W	• Dual power supplies, hot swap redundant configuration • 1200W/493W (total system)	• Dual Power Supplies, hot swap redundant configuration • 750W/486W (total system)	Log Collector Mode		2 TB to 24 TB log storage	m4.4xlarge c4.8xlarge
Max BTU/hr	1,705BTU/hr	1,114 BTU/hr	• 1,681 BTU/hr	1,803 BTU/hr				
Input Voltage (Input Frequency)	100-240 VAC (50-60Hz)	100-240 VAC (50-60Hz)	100-240 VAC (50-60Hz)	100-240 VAC (50-60 Hz)				
Max Current Consumption	10A@100 VAC	9.5A@110 VAC	4.2A @ 120 VAC	4.5A @ 220 V				
Mean Time Between Failures (MTBF)	14.5 years	10 years	6 years	8 years				
Rack Mount (Dimensions)	1U,19" standard rack (1.75"Hx23"Dx17.2"W)	1U, 19" standard rack (1.7"H X 29"D X 17.2" W)	2U, 19" standard rack (3.5" H x 21" D x 17.5" W)	2 U, 19" standard rack (3.5"H X 28.46"D X 17.2"W)				
Weight	26.7 lbs	26 lbs	42.5 lbs.	36 lbs				
Safety	UL, CUL, CB	UL, CUL, CB	UL, CUL, CB	UL, CUL, CB				
EMI	FCC Class A, CE Class A, VCCI Class A	FCC Part 15, EN 55032, CISPR 32	FCC Class A, CE Class A, VCCI Class A	FCC Part 15, EN 55032, CISPR 32				
Environment	• Operating Temperature: 40° to 104° F, 5° to 40° C • Non-operating Temperature: -40° to 149° F, -40° to 65° C	• Operating temperature: 41° to 104° F, 5 to 40° C • Non-operating temperature: -40° to 140° F, -40° to 60° C	• Operating temperature 50° to 95° F, 10° to 35° C • Non-operating temperature -40° to 158° F, -40° to 65° C	• Operating temperature: 41° to 104° F, 5 to 40° C • Non-operating temperature: -40° to 140° F, -40° to 60° C				