新一代防火牆概觀

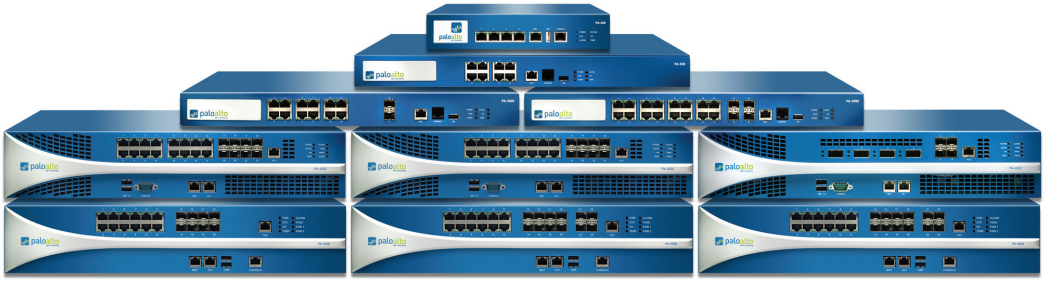
近來，應用程式行為與使用模式的變更正逐漸侵蝕傳統防火牆所提供的保護。使用者通常會從任何位置存取任何應用程式來完成工作。其中許多應用程式會使用非標準連接埠、躍點連接埠或使用加密來簡化使用者存取以及繞過防火牆。然而網路罪犯可以利用這種毫無約束的應用程式使用方式來散佈全新類別的集中目標式現代惡意軟體。結果就是仰賴連接埠和通訊協定的傳統防火牆無法再識別和控制周遊在網路上的應用程式與威脅。

在過去為了重新取得應用程式使用方式的控制權以及保護所有使用者的數位資產，產生了獨立或多種功能拼湊整合之防火牆補強機制 (Firewall Helper) 產業所支援的重複本機和遠端安全性原則。這種方法會造成整體資安政策不一致，而無法解決因為不精確或不完整的流量分類、冗長複雜的管理作業，以及多個導致延遲的掃描程序所造成的可見度和掌控度問題。恢復可見度和掌控度需要採用全新的方法來實現使用各類應用程式的安全性，只有新一代防火牆能夠提供這種方法。

重要的新一代防火牆需求：

- 識別應用程式，而非連接埠。無論使用哪一種通訊協定、加密或規避行為，都能識別應用程式，並且使用這種識別做為所有安全性原則的基礎。
- 識別使用者，而非 IP 位址。針對可見度、原則建立、報告和鑑識調查採用企業目錄中的使用者和群組資訊，無論使用者身處何地都一樣。
- 即時封鎖威脅。抵禦整個攻擊週期，包括危險的應用程式、弱點、惡意軟體、高風險 URL，以及各種惡意檔案與內容。
- 簡化原則管理。透過方便使用的圖形工具和統合原則編輯器，安全地啟用應用程式。
- 啟用邏輯周邊防禦機制。利用從實體周邊延伸到邏輯周邊的一致安全性，保護包括出差或通勤者在內的所有使用者。
- 提供數 GB 以上的傳輸效能。結合特殊用途的硬體和軟體，在啟用所有服務的情況下，達到低延遲與數 GB 的效能。

Palo Alto Networks 新一代防火牆使用三種獨特的識別技術，針對應用程式、使用者和內容提供前所未有的可見度和掌控度，這三種技術是：App-ID™、User-ID 和 Content-ID。這三種識別技術皆運用在每一個 Palo Alto Networks 防火牆中，不但讓企業安全地開放應用程式使用，同時也透過多種創新技術的有效整合大幅減少整體擁有成本。

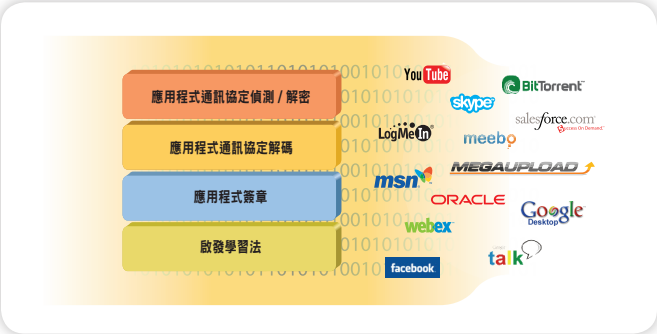


paloalto NETWORKS
the network security company™

App-ID：隨時分類所有的連接埠、所有應用程式

將流量精確分類是任何防火牆最重要的工作，而其成果正是安全性原則的基礎。傳統防火牆是根據連接埠和通訊協定來分類流量，在過去是理想的網路防護機制。但是現今的應用程式可以輕易繞過連接埠防火牆；在連接埠間轉換、使用 SSL 和 SSH、暗中跨過連接埠 80 或使用非標準連接埠。而 App-ID 可以在防火牆看到流量串流之後，在流量串流套用多種分類機制，解決困擾傳統防火牆的流量分類可見度限制，以判斷周遊於網路中各種資料流所代表的應用程式資訊。

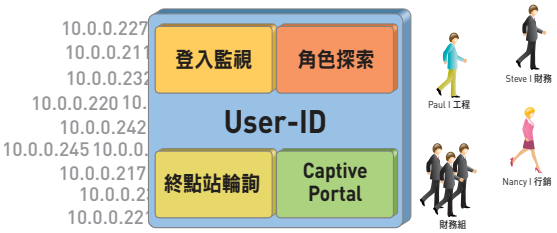
每一個 App-ID 都會自動使用多達四種流量分類機制來識別應用程式，這一點完全不同於過去仰賴 IPS 掃描機制只進行特徵比對的作法，在連接埠型分類之後再實作的附加元件不同。App-ID 會持續監視應用程式狀態，並且重新分類流量以及識別目前所使用的不同功能。安全性原則會判斷如何處理應用程式：封鎖、允許還是安全地啟用（掃描是否有內嵌式威脅並加以封鎖、檢查是否有未獲授權的檔案傳輸和資料模式，或者利用 QoS 進行頻寬控管）。



User-ID：根據使用者和群組來啟用應用程式

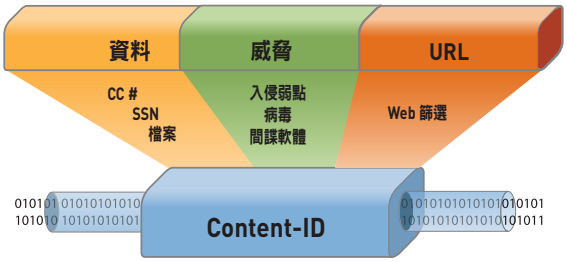
以往是根據 IP 位址加以套用，但是隨著使用者和運算作業的性質趨向動態，光靠 IP 位址已經無法有效監視和控制使用者活動了。User-ID 可讓組織將以使用者或群組為基礎的應用程式啟用原則擴及 Microsoft Windows、Apple Mac OS X、Apple iOS 和 Linux 使用者。

使用者資訊可從企業目錄 (Microsoft Active Directory、eDirectory 和 Open LDAP) 以及終端機服務產品 (Citrix 和 Microsoft Terminal Services) 取得，而 Microsoft Exchange、Captive Portal 和 XML API 的整合可讓組織將原則擴及通常位於網域外部的 Apple Mac OS X、Apple iOS 和 UNIX 使用者。



Content-ID：保護允許的流量

現今許多應用程式可提供重大優勢，不過也會成為現代惡意軟體和威脅的傳遞工具。Content-ID 與 App-ID 兩者結合可以提供系統管理員一套雙管齊下的解決方案，以便保護網路。當系統管理員使用 App-ID 來識別並封鎖不需要的應用程式之後，就可以防止入侵弱點、現代惡意軟體、病毒、殭屍網路和其他惡意軟體在網路上傳播（不論連接埠、通訊協定或規避方法為何），進而安全地啟用允許的應用程式。而讓 Content-ID 所提供之控制元素更加完備的，是控制網路瀏覽和資料篩選功能的全方位 URL 資料庫。



安全的應用程式啟用作業

App-ID、User-ID 和 Content-ID 的完美整合，讓組織建立了一致的應用程式啟用原則（在很多情況下還會進一步執行更細微的控管），遠超過基本的允許或拒絕。透過 GlobalProtect™，您可以將保護公司總部使用者所用的原則，延伸到所有的使用者（無論他們身在何處），而為身在網路外的使用者建立邏輯防護邊界。

安全啟用原則的第一步是由 App-ID 判斷應用程式識別，接著再以 User-ID 對應到相關的使用者，同時由 Content-ID 掃描流量內容，看看有無威脅、檔案、資料模式和網路活動。這些結果會顯示在應用程式控管中心 (ACC)，讓系統管理員即時了解網路發生的狀況。這時，原則編輯器在 ACC 中檢視而得的應用程式、使用者和內容等相關資訊就可以轉變成適當的安全性原則，以便封鎖不需要的應用程式，同時安全地允許並啟用其他應用程式。同樣地，最後您也可以使用應用程式、使用者和內容做為基礎，執行所有詳細的分析、報告或鑑識。

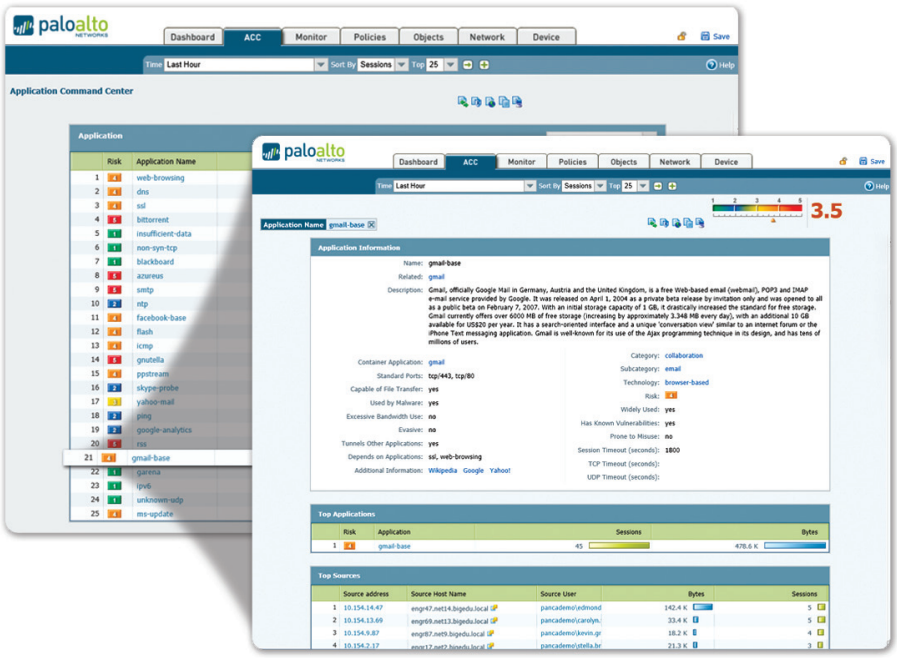
應用程式控管中心：知識就是力量

應用程式控管中心 (ACC) 會以圖形方式摘要列出記錄資料庫，以便強調周遊在網路上的應用程式、這些應用程式的使用者，以及它們的潛在安全性影響。ACC 會使用 App-ID 執行的連續流量分類進行動態更新。如果應用程式變更了連接埠或行為，App-ID 還是會繼續查看流量，並在 ACC 中顯示結果。如果 ACC 中出現全新或不熟悉的應用程式，您只要按一下就會顯示該應用程式的描述、重要功能、行為特質，以及目前正在使用它的使用者，方便您快速進行調查。其他 URL 類型、威脅和資料的可見度會提供您一份完整且全面的網路活動記錄。在 ACC 的協助下，系統管理員可以很快的深入了解周遊在網路上的流量，然後將這項資訊轉換為更詳實的安全性原則。

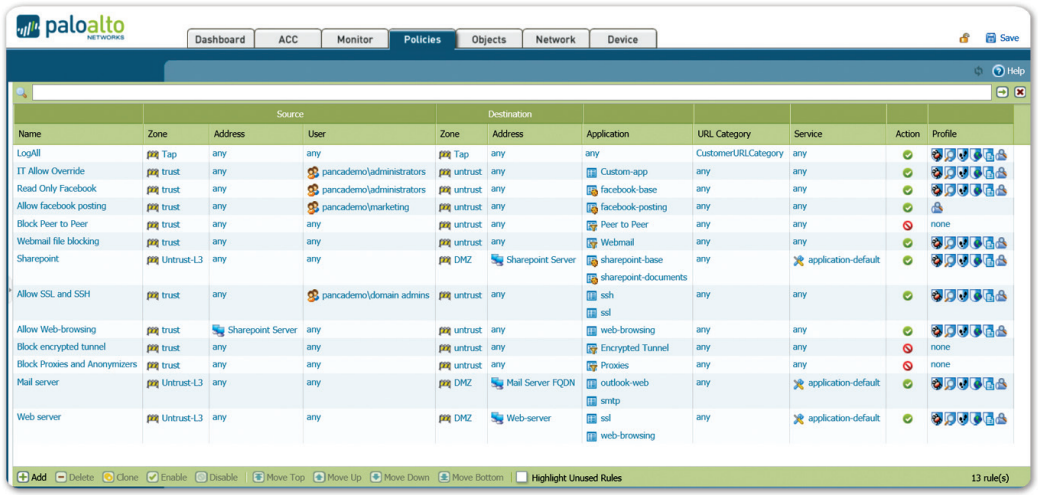
原則編輯器：將知識轉換為安全的啟用原則

哪些應用程式正在網路上周遊、哪些人正在使用這些應用程式，以及有哪些潛在的安全性風險等知識，讓系統管理員得以條理分明、小心謹慎地快速部署以應用程式、應用程式功能和連接埠為基礎的啟用原則。原則回應的範圍有開放式（允許）、中度（啟用某些應用程式或功能，接著是掃描或塑造、排程等），以及封閉式（拒絕）。其範例如下：

- 僅將存取權交給財務組、強迫流量經由標準連接埠，以及檢查流量是否有應用程式弱點，藉此保護 Oracle 資料庫。
- 只讓 IT 群組固定使用一組經由其標準連接埠的遠端管理應用程式（例如 SSH、RDP 或 Telnet）。
- 定義並強制執行允許和檢查特定網路郵件和即時訊息使用情況，但是封鎖其個別檔案傳輸功能的公司原則。
- 只允許系統管理小組使用 Microsoft SharePoint Administration，但允許所有其他使用者存取 Microsoft SharePoint Documents。
- 部署網路啟用原則，以便允許並掃描企業相關網站的流量，同時封鎖存取明顯非工作相關的網站，並且透過自訂的封鎖網頁「引導」存取其他網站。



應用程式可見度
以清楚、容易閱讀的格式，檢視應用程式活動。新增和移除篩選器，以進一步了解應用程式、其功能及其使用者。



統合原則編輯器
熟悉的外觀與操作，可讓您快速建立和部署控制應用程式、使用者和內容的原則。

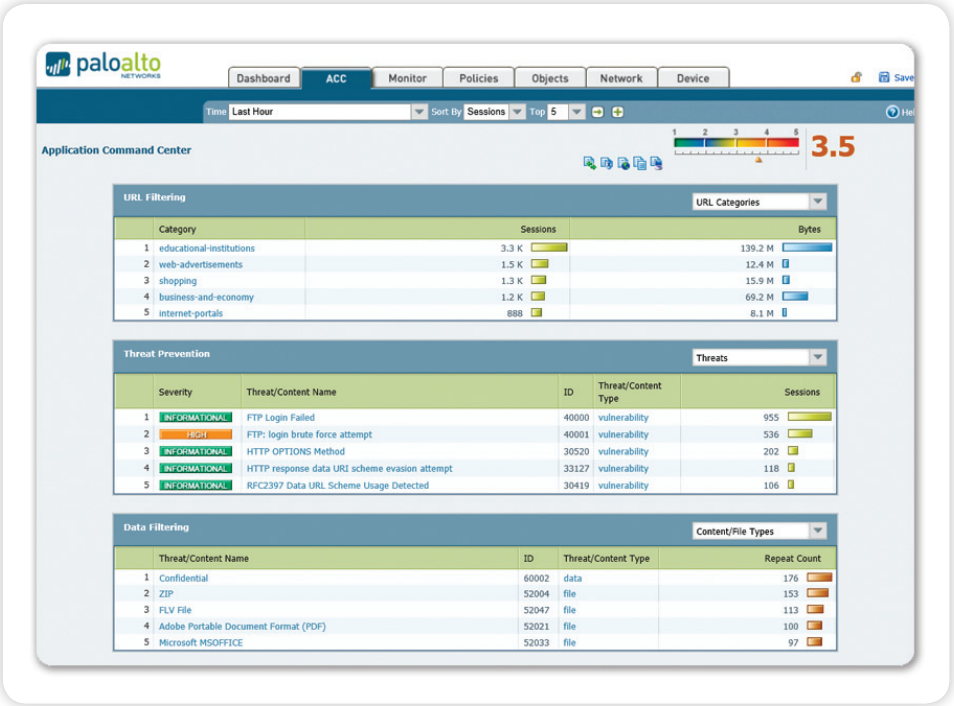
- 實作 QoS 原則，以便允許使用耗用大量頻寬的媒體應用程式和網站，但限制它們對 VoIP 應用程式可能造成的影響。
- 解析社交網路和網路郵件網站的 SSL 流量，並且掃描是否有惡意軟體和入侵程式。
- 只有當使用者確認之後，才允許從未分類的網站下載可執行檔，防止經由零時差入侵進行偷渡式下載 (Drive-by Download)。
- 拒絕所有來自特定國家的流量，或者封鎖不需要的應用程式，例如 P2P 檔案共用、規避管控之工具和外部 Proxy。

根據使用者和群組來控制應用程式，以及掃描所允許的流量中是否有各種威脅存在，這兩種功能如果能密切整合，將可大幅減少公司部署的原則數量，以及每日發生的員工新增、移動和變更數量。

原則編輯器：保護啟用的應用程式

安全地啟用應用程式，是指先允許存取應用程式，然後再套用特定的威脅防禦，以及檔案、資料或 URL 篩選原則。Content-ID 所包含的每一個元素都可以針對個別應用程式設定。

- **入侵防禦系統 (IPS)：**弱點保護整合了一組完整的入侵防禦系統 (IPS) 功能，可封鎖網路和應用程式層入侵弱點、緩衝區溢位、DoS 攻擊以及連接埠掃描。
- **網路防毒軟體：**串流式防毒防護機制可封鎖數百萬種惡意軟體變化，包括 PDF 病毒以及隱藏在壓縮檔或網路流量中的惡意軟體 (壓縮的 HTTP/HTTPS)。原則式 SSL 解密可讓組織抵禦在 SSL 加密應用程式之間傳遞的惡意軟體。
- **URL 篩選：**一套完全整合的可自訂 URL 篩選資料庫可讓系統管理員套用精細的網路瀏覽原則，彌補應用程式可見度和掌控度原則的不足，以及使企業免於法律、規定和生產力風險的全面困擾。
- **檔案與資料篩選：**資料篩選功能可讓系統管理員制定相關原則，減少與檔案和資料傳輸有關的風險。您可以查看檔案內容 (相對於僅查看副檔名) 來控制檔案的傳輸與下載，判斷是否應該允許進行。一般在偷渡式下載 (Drive-by Download) 中的可執行檔都可加以封鎖，讓網路免於受到看不見的惡意軟體傳播之害。最後，資料篩選功能可以偵測並且控制機密資料模式 (信用卡和身分證號碼) 的流程。



內容與威脅的可見度
以清楚、容易閱讀的格式，檢視 URL、威脅與檔案 / 資料傳輸活動。新增和移除篩選器，以進一步了解個別元素。

新一代惡意軟體偵測與防護

惡意軟體已經發展成可擴充的網路應用程式，讓攻擊者能夠在目標網路內部進行前所未有的存取和控制。由於現代惡意軟體的能力逐漸增加，所以企業必須能夠立即偵測這些威脅，甚至在威脅具有定義的特徵碼之前加以偵測。Palo Alto Networks 新一代防火牆將為組織提供一種多面向方法，這種方法會直接分析可執行檔和網路流量來保護其網路，甚至在特徵碼可用之前提供防護。

- **WildFire™：**使用雲端架構方法的 WildFire 會直接在安全的虛擬化環境中觀察可執行檔的行為，藉以揭露以往傳統資安設備看不見的惡意可執行檔。WildFire 會在 Microsoft Windows 可執行檔中尋找惡意動作，例如變更登錄值或作業系統檔案、停用安全性機制，或是將程式碼插入執行中的處理序。這種直接分析可快速且正確地識別惡意軟體，即使沒有任何防護機制可用也一樣。其結果將立即傳遞給系統管理員以進行適當的回應，而且系統會自動開發特徵碼並透過下一個可用的內容更新傳遞給所有客戶。
- **以行為模式為依據的殭屍網路偵測技術：**App-ID 會分類所有應用程式層級的流量，因而公開網路上的任何未知流量，而這通常表示惡意軟體或其他威脅活動。行為型殭屍網路報告會分析指出殭屍網路感染的網路行為，例如重複造訪惡意軟體網站、使用動態 DNS、IRC 和其他可能可疑的行為。其結果會以可能受感染之主機的清單格式顯示，而這些主機就可以當成殭屍網路可能的成員來加以調查。

流量監視：分析、報告和鑑識

安全性最佳作法規定系統管理員必須在主動與被動之間取得平衡，主動是為了保護公司資產而持續學習與適應；被動則是調查、分析與報告安全性事件。您可以使用 ACC 和原則編輯器，主動套用應用程式啟用原則，而公司則可以使用一組完整監視和報告工具所提供的必要方法，針對流經 Palo Alto Networks 新一代防火牆的應用程式、使用者和內容進行分析與報告。

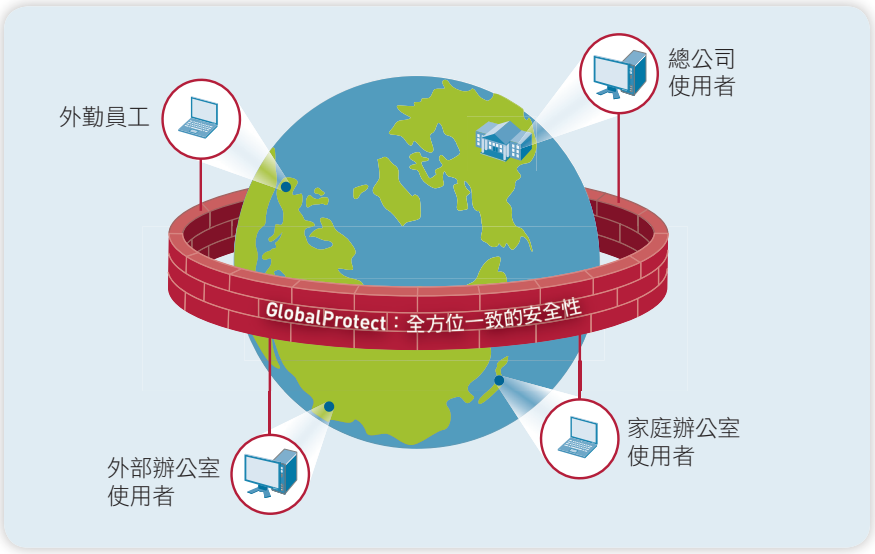
- **應用程式範圍：**應用程式範圍會提供動態、可由使用者自訂的長時間流量、應用程式與威脅活動檢視，可彌補 ACC 提供之內容與應用程式即時檢視的不足。
- **報告：**預先定義的報告可以配合特定需求依現狀使用、自訂或組合為一份報告。所有報告都可以匯出成 CSV 或 PDF 格式，而且可以按照排程執行以及用電子郵件寄出。
- **記錄：**即時記錄篩選可以快速針對周遊於網路的每一個工作階段進行鑑識調查。記錄篩選結果可以匯出至 CSV 檔案，或傳送至 syslog 伺服器，以供離線封存或其他分析。
- **追蹤工作階段工具：**透過集中式相互關聯的檢視，加速對所有記錄進行鑑識或事件調查，看看是否有與某個個別工作階段相關的流量、威脅、URL 和應用程式。

GlobalProtect：全方位一致的安全性

應用程式並非企業變革的唯一動力。 越來越多使用者只想要使用他們所選擇的任何裝置，從任何位置連線和工作。因此，IT 小組必須努力將安全性擴及這些可能遠離企業傳統周邊防禦機制的裝置和位置。GlobalProtect 完全符合這項挑戰的需要 因為它可將一致的安全性原則擴及所有使用者，不論其所在位置和使用的裝置為何。

首先，GlobalProtect 會使用支援各種裝置 (包括 Microsoft Windows、Apple Mac OS X 和 Apple iOS) 的透明 VPN，確保所有使用者的連線安全。一旦連線之後，防火牆就會分類所有流量、套用啟用原則、掃描流量看看是否有威脅，並且保護網路和使用者。

此外，GlobalProtect 可以根據使用者裝置的狀態套用其他控制。例如，如果裝置的防毒軟體過期或者沒有啟用磁碟加密，系統可能會拒絕使用者存取特定應用程式或網路的機密區域。這樣可讓 IT 人員安全地在各種使用者裝置類型之間啟用應用程式使用方式，同時保持一致的新一代安全性方法。



GlobalProtect
針對所有使用者強制執行一致的安全應用程式啟用原則，不論其所在位置為何。

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

主要連絡電話：+1.408.573.4000
銷售部門： +1.866.320.4788
客戶支援： +1.866.898.9087

www.paloaltonetworks.com