BPA 與 Security Assurance 最佳做法入門

Version 9.1

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page: docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

March 5, 2020

Table of Contents

最佳做法入門

安全性最佳做法可防止已知和未知威脅、減少攻擊面，以及查看流量，因此您知道和控制網路上的應用程式、使用者和內容。當您實作安全性最佳做法時，可以：

- 最大限度降低成功入侵的機會。
- 識別攻擊者的存在。
- 保護重要資料。
- 保護客戶、合作夥伴和員工，進而保護業務信譽。
- 協助達成零信任安全性環境。

若要轉換為安全性最佳做法，您需要先了解目前網路安全性狀態，並識別改善區域。Palo Alto Networks 提供引導式轉換路徑：與安全轉換步驟和最佳做法技術文件相結合的最佳做法評估 (BPA)。

您只要訂用進階 (2019 年 11 月 1 日起) 或白金支援合約，即有機會針對 Security Assurance 做好準備。Security Assurance 可引介 Palo Alto Networks 安全性專家和工具，協助初步事件調查。

- 識別和排定最佳做法優先順序
- 存取和執行 BPA
- Security Assurance

識別和排定最佳做法優先順序

Palo Alto Networks 的最佳做法評估 (BPA) 會使用技術支援檔案來分析 Panorama 和新世代防火牆組態設定，以及比較 Palo Alto Networks 最佳做法的設定。BPA 會顯示最佳做法安全性採用的目前狀態，並建議進行特定變更，讓設定與安全性最佳做法一致。執行 BPA 不僅可讓您了解在何處改善安全性狀態，也會設定基準線供日後比較，提供可顯示如何將 BPA 的建議轉譯為最佳做法設定的技術文件連結。

使用反覆且已排定優先順序的方式，您可以一次一個步驟地將安全性狀態轉換為最佳做法狀態，並依您的速度和舒適程度來測量進度：

STEP 1 | 將技術支援檔案上傳至客戶支援入口網站和存取和執行 BPA給您自己，或聯絡 Palo Alto Networks SE 或合作夥伴以對 Panorama 或新世代防火牆執行 BPA。

如果您自行執行 BPA，則建議您聯絡 Palo Alto Networks SE 或合作夥伴協助解譯結果並討論後續步驟。

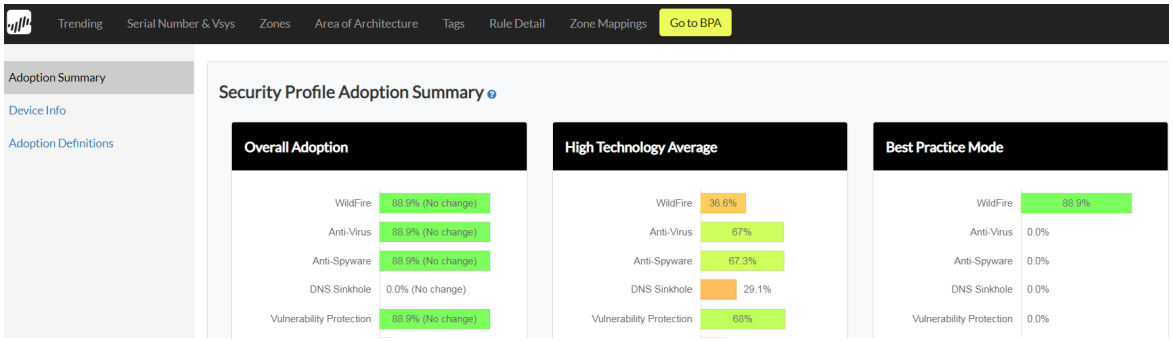
STEP 2 | 識別和排定要開始轉換為最佳做法的第一個改善區域優先順序。

不論是 Palo Alto Networks SE 或合作夥伴執行 BPA 還是您執行 BPA，SE 或合作夥伴都可以協助您制訂已排定優先順序的計畫來安全地逐步進行最佳做法。計劃先從最安全、最簡單且最高影響的變更開始，例如將防毒、反間諜軟體、弱點保護和 WildFire 分析設定檔套用至安全性政策允許規則。

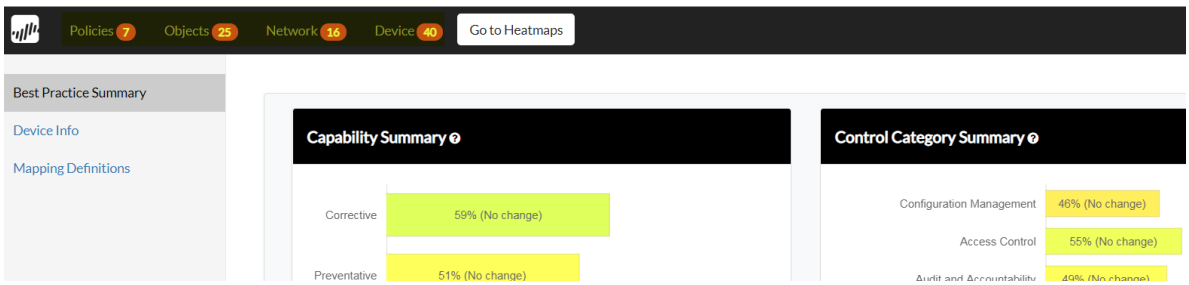
STEP 3 | 使用 BPA 的技術文件連結來設定您已排定優先順序的最佳做法。

下載 BPA 報告會提供 .zip 檔案，其中包含詳細 HMTL 報告、執行摘要以及列出未通過最佳做法檢查的 Excel 試算表。您可以使用兩種方式來連結至技術文件：

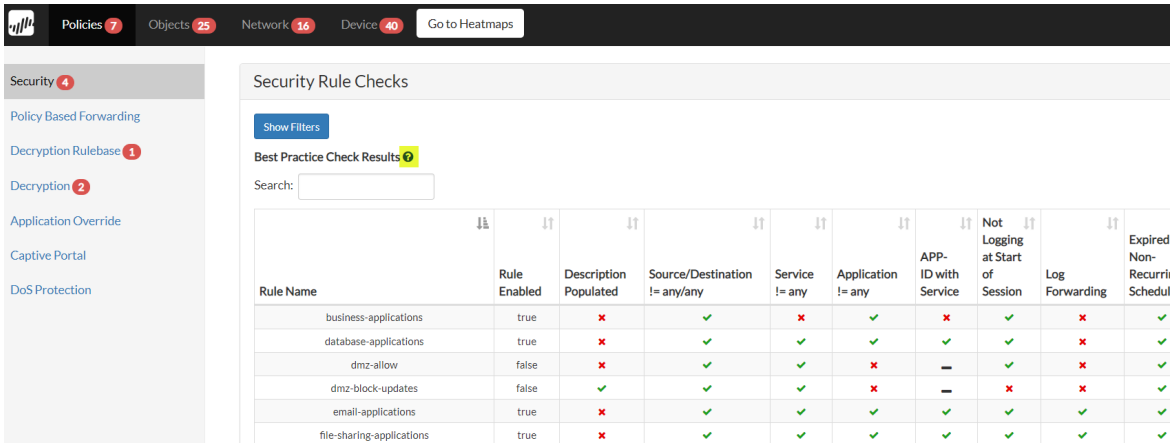
- 從試算表—Documentation（文件）頁籤提供每個失敗檢查的連結。此外，Policies（政策）、Objects（物件）、Network（網路）和 Device（裝置）頁籤的 Check ID（檢查 ID）欄中的識別碼還會直接連結至 Documentation（文件）頁籤上的相關行。
- 從 HTML 報告—當您開啟 HTML 報告時，會看到彙總最佳做法採用的熱圖。**Go to BPA**（移至 **BPA**）以存取報告。



從 BPA 摘要頁面，檢視所選取設定評估的 **Policies (政策)**、**Objects (物件)**、**Network (網路)** 或 **Device (裝置)** 詳細報告。



從詳細報告，按一下加上圓圈的藍色？取得設定檢查的描述和原理以及最佳做法設定的技術文件連結。



針對安全性設定檔（弱點保護、防毒、反間諜軟體、URL 篩選、檔案封鎖），使用安全轉換建議，確定移至最佳做法安全性設定檔的業務關鍵應用程式可用性。

STEP 4 | 在您實作第一組的最佳做法變更之後，請重新執行 BPA 來測量進度，以及協助確認變更如預期運作。

比較第一個 BPA 與下一個 BPA 的輸出，以查看安全性狀態的改善。識別和排定要處理的下一個改善區域優先順序。

STEP 5 | 使用 BPA 的技術文件連結來設定您已排定優先順序的下一組最佳做法。

STEP 6 | 依您自己的速度，重複執行 BPA 的程序以測量進度以及識別和排定後續步驟的優先順序，然後使用技術文件來設定最佳做法。

STEP 7 | 立即開始使用—存取和執行 BPA 或是聯絡 Palo Alto Networks SE 或合作夥伴，並立即開始轉換為更安全的網路！

存取和執行 BPA

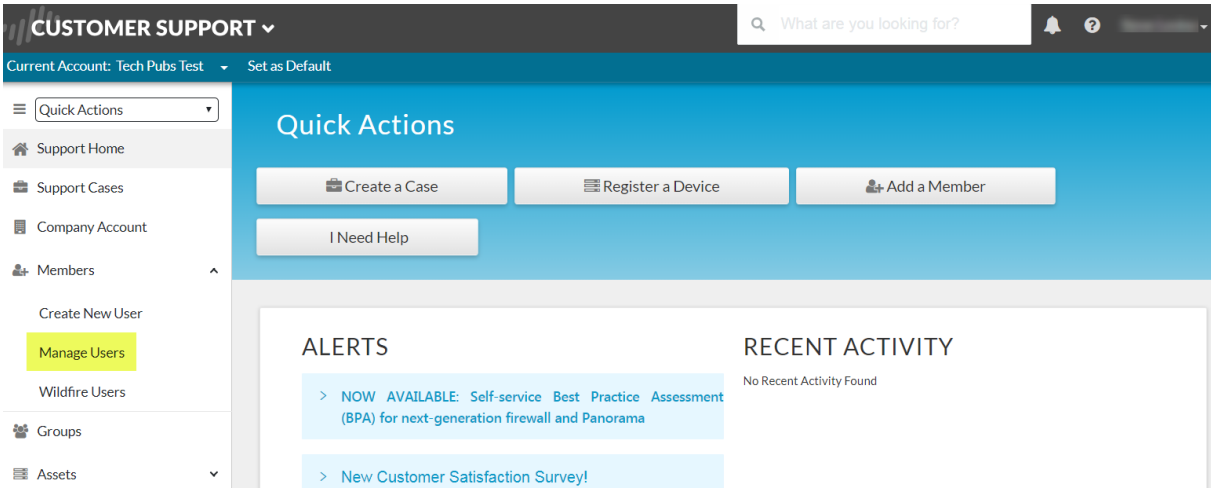
請從客戶支援入口網站存取最佳做法評估 (BPA)。超級使用者帳戶會自動具有 BPA 存取權，而且可以將 *BPA 使用者* 角色指派給標準使用者的設定檔，讓標準使用者可以執行 BPA。此程序顯示超級使用者如何將存取權授與標準使用者，以及如何執行 BPA。您也可以檢視如何執行 BPA 以及如何了解結果的簡短視訊。

此外，您只要訂用進階 (2019 年 11 月 1 日起) 或白金支援合約，即有機會做好準備和啟動Security Assurance。Security Assurance 可引介 Palo Alto Networks 安全性專家和工具，協助初步事件調查。我們大力推薦您 BPA 以度量對於七大安全性功能的採用情形，並且確保您的採用率至少與行業的平均採用率相當，以便給網路更好的保護。進階或白金支援合約的組合加上近期為您顯示七大安全性功能採用率符合行業平均水準的 BPA 度量，能夠自動啟動 Security Assurance。

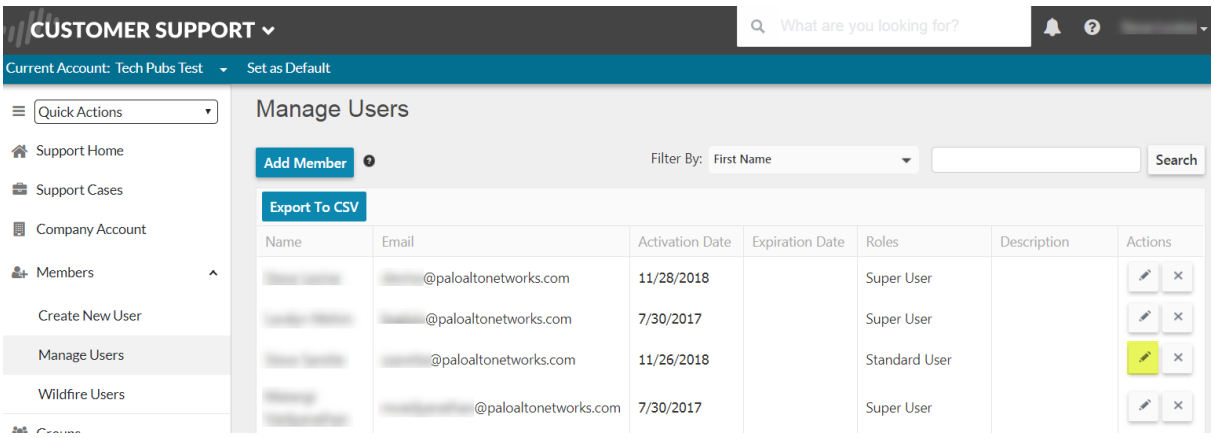
- 從客戶支援入口網站存取 BPA
- 產生及下載 BPA 報告

從客戶支援入口網站存取 BPA

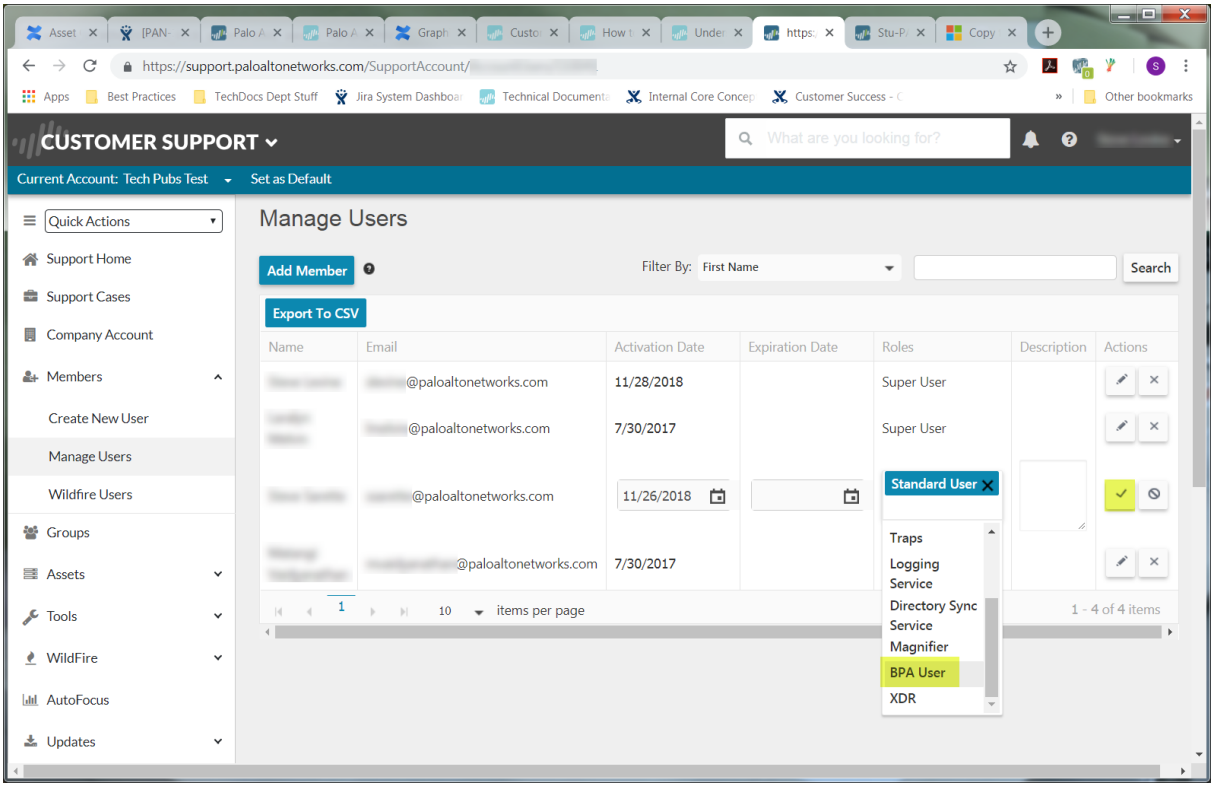
STEP 1 | 從客戶支援入口網站的驗證首頁畫面，選取 **Members (成員)** > **Manage Users (管理使用者)**。



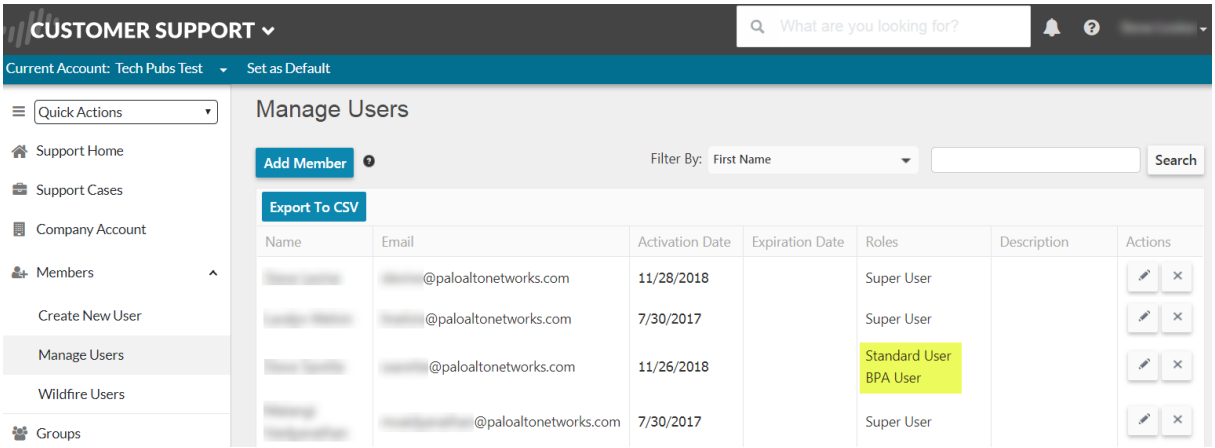
STEP 2 | 按一下鉛筆圖示，以編輯您想要指派 BPA 權限的標準使用者。



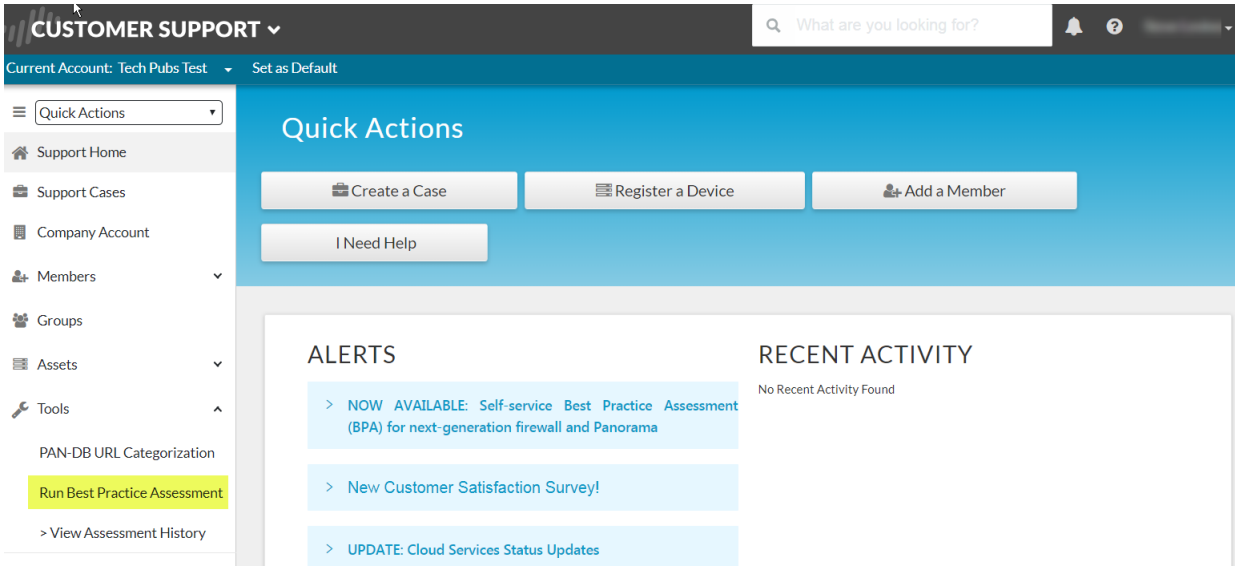
STEP 3 | 選取 **BPA User**（**BPA** 使用者）角色，然後按一下更新核取記號來新增角色。



STEP 4 | 標準使用者這時即擁有「BPA 使用者」角色的權限。



STEP 5 | 具有 BPA 使用者角色的超級使用者和標準使用者可以登入客戶支援入口網站，以存取和執行 BPA（**Tools**（工具）> **Run Best Practice Assessment**（執行最佳做法評估））。



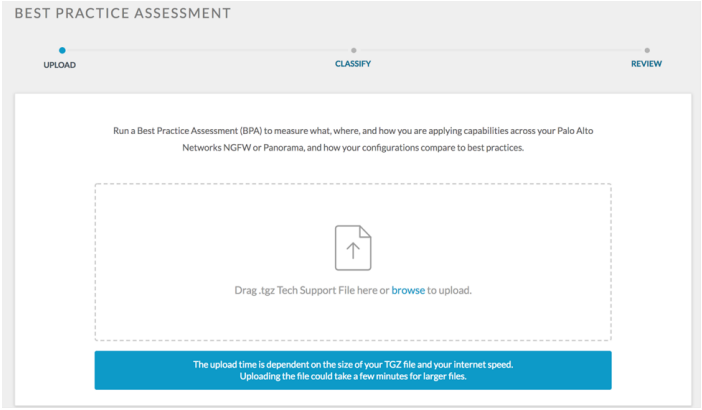
產生及下載 BPA 報告

您取得對 BPA 的存取權之後，可針對 Panorama 設備或新世代防火牆產生 BPA 報告。

如果可能，請為 *Panorama* 設備而非個別的新世代防火牆產生 *BPA* 報告，以一份報告對您環境內的所有防火牆取得完整的可視性。您可以定期產生報告，以度量朝向採用安全性功能和安全性最佳做法的進展。

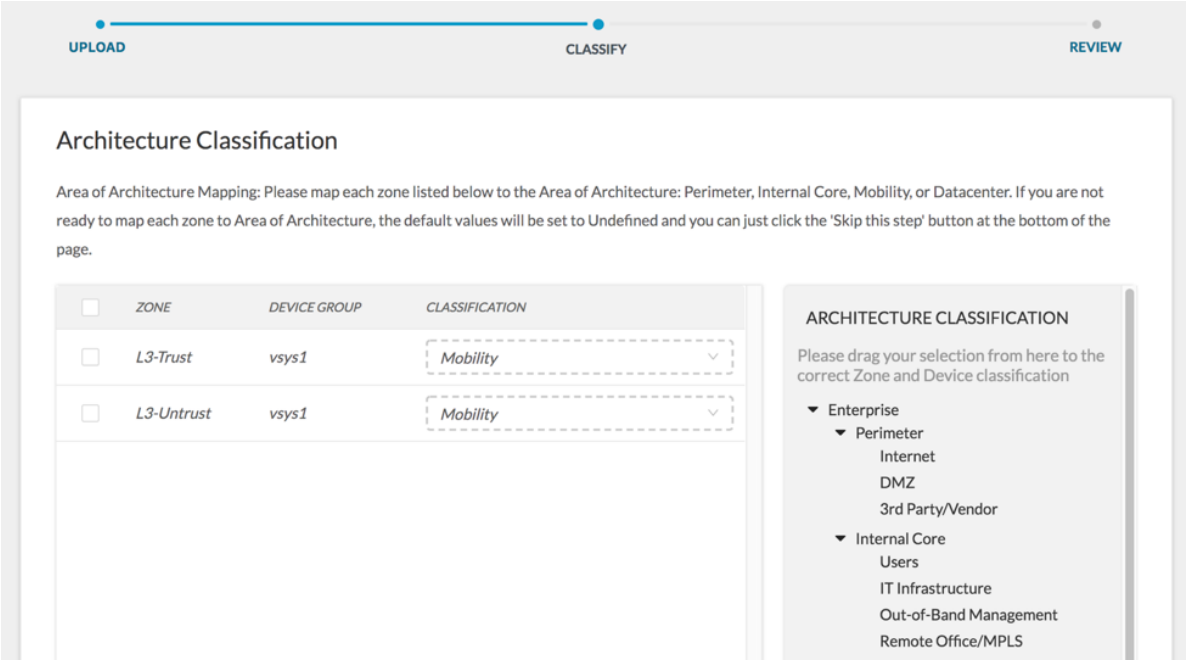
STEP 1 | 在「客戶支援入口網站」視窗中拖曳或放下技術支援檔案 (.tgz 檔案)，或瀏覽技術支援檔案。

超級使用者可以建立技術支援檔案（**Device (裝置)** > **Support (支援)** > **Tech Support File (技術支援檔案)** 或 **Panorama** > **Support (支援)** > **Tech Support File (技術支援檔案)**）。



STEP 2 | 選擇性地將每個區域對應至架構區域，或按一下 **Skip this step**（跳過此步驟）以在未對應區域的情況下執行 BPA。

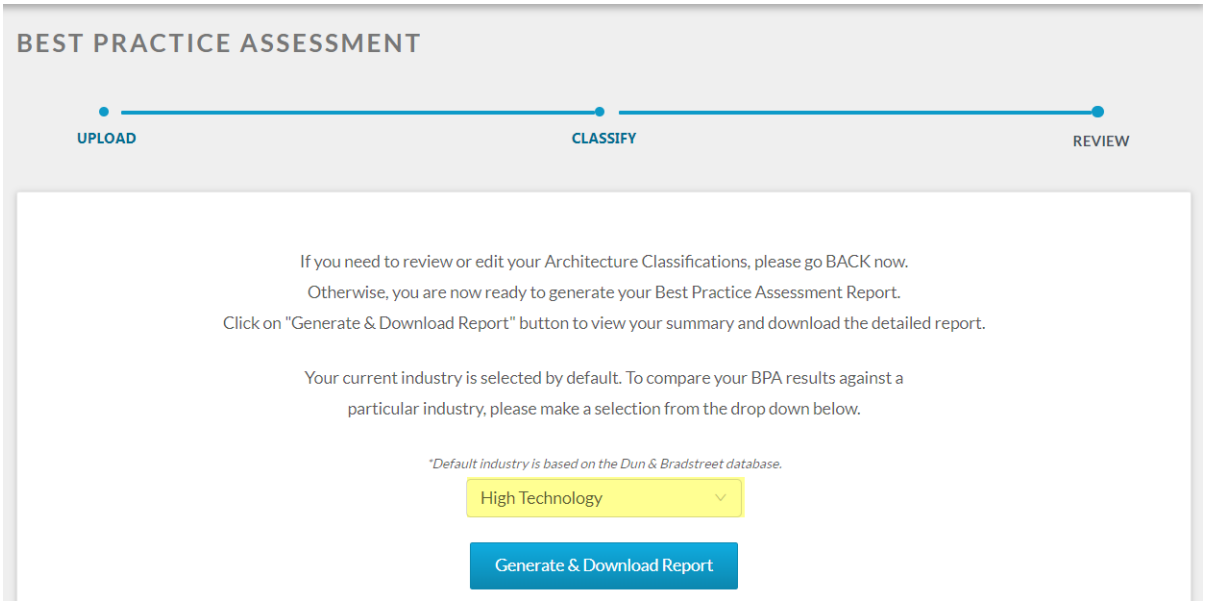
從 Architecture Classification (架構分類) 拖放架構值，使用 **Classification (分類)** 下拉式清單選取值，或使用多個核取方塊選取多個區域，然後一次將值套用至所有選定區域。



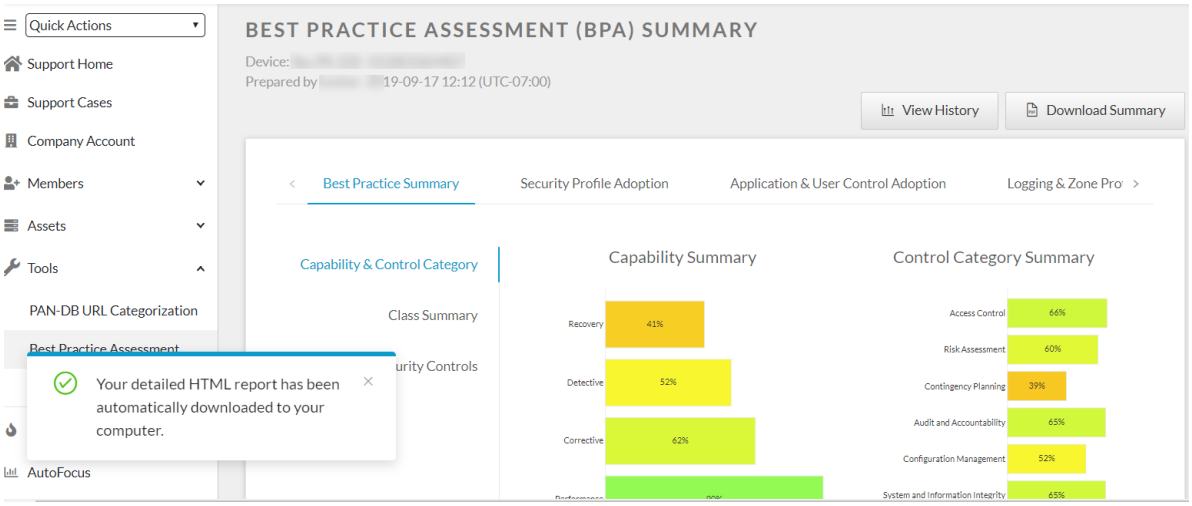
STEP 3 | 識別對應您帳戶的行業，接著產生並下載 BPA 報告 (產生及下載 **BPA** 報告)。

您可以使用下拉式清單變更 BPA 將結果與之比較的行業。在您產生報告之前若想變更任何資料，亦可返回進行變更。

產生及下載報告可下載詳細的 BPA 報告、執行摘要報告以及試算表，其中顯示您所存取和執行 BPA 之系統失敗的最佳做法檢查。



STEP 4 | 所產生的 BPA 可顯示執行摘要，並且告知您詳細的 HTML 報告已下載至您的電腦。



STEP 5 | 既然您已知道如何執行 BPA，請立即前往客戶支援入口網站並試用（或聯絡 Palo Alto Networks SE 或合作夥伴執行 BPA）以開始轉換為更安全的網路。

若您訂用進階 *(2019 年 11 月 1 日起)* 或白金支援合約，請使用 *BPA* 為安全性狀態做好準備，以利用 Security Assurance，協助您進行初步的事件調查。

Security Assurance

若您察覺網路中有可疑活動，Security Assurance 能在您最需要的時候提供 Palo Alto Networks 給予的額外協助。Security Assurance 提供：

- Palo Alto Networks 安全性專家及其專門的威脅情報工具和威脅搜索做法。
- 進階日誌和入侵指標 (IOC) 分析。
- 設定評估，包括自訂產品安全性的建議。
- 下一步是建議加快移轉至您的事件回應 (IR) 廠商，以利處理和解決事件。

為利用 Security Assurance，您必須訂用進階支援合約 (2019 年 11 月 1 日起) 或白金支援合約。

欲走向 Security Assurance，第一步應當執行最佳做法評估 (BPA)，以度量您對於以下七大安全性功能的採用情形：WildFire、防毒、反間諜軟體、DNS Sinkhole、URL 篩選、弱點保護和記錄。我們建議您，確保這些安全性功能的採用率至少與業界的平均採用率相當。

執行 BPA 及採用更高層級的主要安全性功能，能給您網路更好的保護，也協助避免事件發生。BPA 也度量許多其他安全性功能的採用層級，例如應用程式ID 和使用者 ID、區域設定、其他安全性設定檔，例如檔案封鎖和 DoS 保護設定檔，BPA 還會就如何改善您的安全性狀態提出建議。

定期執行 *BPA (*例如每月或每季*)* 以度量主要安全性功能的採用、瞭解網路安全性的狀態，及排列改善安全性的優先順序。

當您訂用進階支援合約 (2019 年 11 月 1 日起) 或白金支援合約並且執行 BPA，若其顯示您對於七大安全性功能的採用率符合業界平均，Security Assurance 會自動啟用。若您需要協助以使對於這些主要功能的採用率符合行業平均，請聯絡 Palo Alto Networks 銷售代表協助您定義需求、提供合理論證準則等。如果業務原因使您無法採用這般層級的主要安全性功能，請與 Palo Alto Networks 銷售代表一同研究如何享有 Security Assurance 帶來的益處。

應採用的七大安全性功能

我們大力推薦採用下列七大安全性功能的理由如下：

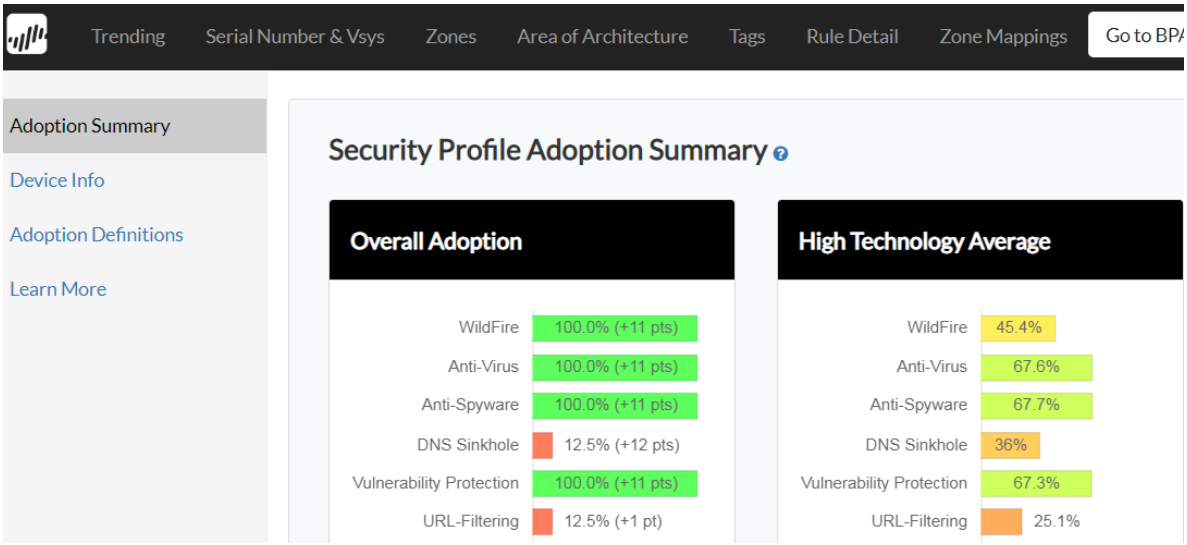
- **WildFire**—將 WildFire 安全性設定檔附加到安全性政策規則，允許流量保護網路，避開新的未知威脅。WildFire 是對抗進階持續性威脅 (ATP) 的強大防禦功能。
- 防毒—將防毒安全性設定檔附加到安全性政策規則，允許流量封鎖已知惡意檔案，例如惡意軟體、勒索軟體、機器人和病毒。
- 反間諜軟體—將反間諜軟體安全性設定檔附加到安全性政策規則，允許流量偵測從伺服器或端點上執行的惡意程式碼所啟動的命令與控制流量 (C2)，並防止遭入侵的系統從您的網路建立輸出連線。
- **DNS Sinkhole**—設定反間諜軟體安全性設定檔的 DNS Sinkhole 部分，其附加到允許流量的安全性政策規則。DNS Sinkhole 可透過追蹤主機並防止它們存取這些網域，以找出嘗試進入可疑網域、可能遭到入侵的主機。
- **URL** 篩選—將 URL 篩選設定檔附加到安全性政策規則，允許流量防範存取有風險的網頁內容 (可能含有惡意內容的網站)。URL 篩選設定檔與 URL 類別可供您精細掌控允許您存取的網站類型。
- 弱點保護—將弱點保護安全性設定檔附加到安全性政策規則，允許流量防範攻擊者入侵用戶端和伺服器端的弱點，傳遞惡意承載至您的網路和使用者，並且防範攻擊者使用弱點在您的網路內橫向移動。

- 記錄—啟用所有流量的記錄 (允許與拒絕) 以針對系統事件和網路流量事件提供具有時間戳記的稽核記錄。日誌能為調查事件提供關鍵資訊。日誌轉送可讓您從所有防火牆傳送日誌到 Panorama 或至外部以彙總日誌進行分析。

採用這些主要功能可大幅改善安全性的狀態、減少攻擊面、增加對網路流量的可視性、防範已知和新的攻擊，並且保護對您的網路最寶貴的資料、資產、應用程式和服務。

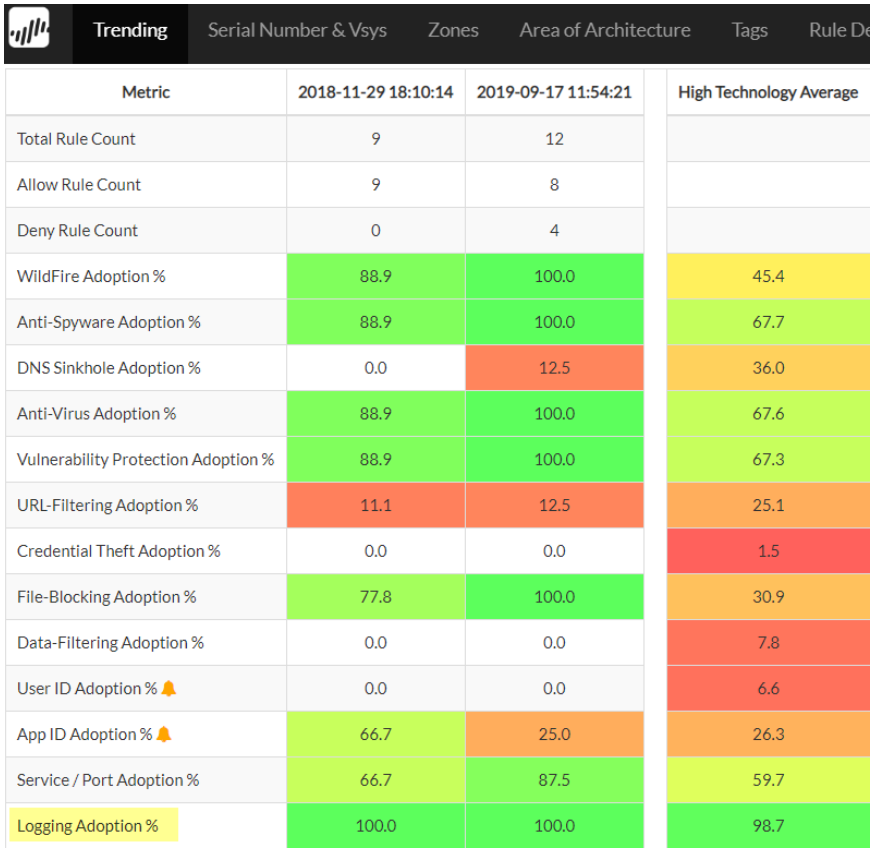
檢查七大安全性功能的採用

在您產生並下載 BPA 結果後收到的詳細 BPA 報告 (HTML 格式) 中，請至採用摘要頁面查看六個安全性設定檔 (WildFire、防毒、反間諜軟體、DNS Sinkhole、弱點保護和 URL 篩選) 功能的整體採用情形，以及您所屬行業對這些功能的平均採用率 (記錄是另外的檢查)。「採用摘要」頁面可顯示您與所屬行業相較之下的安全性功能採用情形，協助您識別採用上的差距。例如，假設您所屬的產業是高科技：



結果顯示，設定符合四項功能的行業平均採用率：WildFire、防毒、反間諜軟體及弱點保護設定檔。結果亦顯示，設定未達到兩項功能的行業平均採用率：DNS Sinkhole 和 URL 篩選。這指出下一波行動：設定反間諜軟體設定檔中的 DNS Sinkhole，然後套用 URL 篩選至網際網路流量。

在詳細的 HTML BPA 報告中，前往趨勢頁面以查看您在於記錄功能的整體採用情形，以及所屬行業的記錄功能平均採用率。



Trending | Serial Number & Vsys | Zones | Area of Architecture | Tags | Rule De

Metric	2018-11-29 18:10:14	2019-09-17 11:54:21	High Technology Average
Total Rule Count	9	12	
Allow Rule Count	9	8	
Deny Rule Count	0	4	
WildFire Adoption %	88.9	100.0	45.4
Anti-Spyware Adoption %	88.9	100.0	67.7
DNS Sinkhole Adoption %	0.0	12.5	36.0
Anti-Virus Adoption %	88.9	100.0	67.6
Vulnerability Protection Adoption %	88.9	100.0	67.3
URL-Filtering Adoption %	11.1	12.5	25.1
Credential Theft Adoption %	0.0	0.0	1.5
File-Blocking Adoption %	77.8	100.0	30.9
Data-Filtering Adoption %	0.0	0.0	7.8
User ID Adoption %	0.0	0.0	6.6
App ID Adoption %	66.7	25.0	26.3
Service / Port Adoption %	66.7	87.5	59.7
Logging Adoption %	100.0	100.0	98.7

此頁除顯示您與所屬行業相較的採用程度之外，也顯示與您上次執行 BPA 相較的採用程度。這是安全性長時間改善的度量；若您的結果指出安全性不如所希望的如此嚴密，則也是一種行動呼籲。

如果設定檔和記錄結果顯示您對於所有七項功能的採用皆符合行業平均，就會自動啟用 Security Assurance。若您需要協助以使對於這些主要功能的採用率符合行業平均，請聯絡 Palo Alto Networks 銷售代表協助您定義需求、提供合理論證準則等。如果業務原因使您無法採用這般層級的主要安全性功能，請與 Palo Alto Networks 銷售代表一同研究如何享有 Security Assurance 帶來的益處。

改善七大安全性功能的採用

您可使用 BPA 搭配 Palo Alto Networks 技術文件以識別需要改善的安全性功能，並且進行所需的改善，尤其在於七大安全性功能。改善安全性的狀態有助於防護使用者，以及您寶貴的裝置、資產、應用程式和服務。

- **WildFire**—將 WildFire 設定檔安全地轉換為最佳做法，然後實作 WildFire 最佳做法。WildFire 設定檔的最佳做法是預設設定檔。
- 防毒—將防毒設定檔安全地轉換為最佳做法，然後實作防毒最佳做法 (或是對資料中心略為更加嚴格的防毒最佳做法)。
- 反間諜軟體和 **DNS Sinkhole**—DNS Sinkhole 設定位在反間諜軟體安全性設定檔中的 **DNS** 特徵碼頁籤。將反間諜軟體設定檔安全地轉換為最佳做法，然後實作反間諜軟體最佳做法 (或是對資料中心略為更加嚴格的反間諜軟體最佳做法)。
- **URL** 篩選—將 URL 篩選設定檔安全地轉換為最佳做法，然後實作 URL 篩選最佳做法。
- 弱點保護—將弱點保護設定檔安全地轉換為最佳做法，然後實作弱點保護最佳做法 (或是對資料中心略為更加嚴格的弱點保護最佳做法)。
- 記錄—安全性政策規則預設是在工作階段結束時記錄。

此外，BPA 和技術文件可向您指出如何改善許多其他安全性功能，例如應用程式 ID、使用者 ID、檔案封鎖設定檔、DoS 和區域保護，及認證盜竊保護。部分主要資源為：

- BPA 入門—向您指出如何使用 BPA 檢視安全性功能的採用，並識別採用上的差距、評估您的設定，包括政策、物件、網路和裝置以及 Panorama 設定，並將變更排列優先順序，包括強化裝置管理狀態、改善對流量的可視性，及實作初步控制的最佳做法。
- 解密最佳做法—向您指出如何提高可視性，作法包括將您的業務模型的所有流量解密、隱私考量並且法規允許，讓您能檢查最大流量，保護網路，免受加密威脅。
- DoS 和區域保護最佳做法—向您指出如何採取分層方式以防禦企圖破壞您的網路的拒絕服務 (DoS) 攻擊，並且防護您的網路周邊、區域及個別裝置。
- 應用程式與威脅內容更新的最佳做法—以對您的業務需求而言最佳的方式部署內容和應用程式更新，可確保您的網路能夠防範最新威脅並且識別最新應用程式。

您可從最佳做法入口網站和移轉至最佳做法頁面找到所有這些文件和其他更多資訊。

如何啟用 Security Assurance

若您遇到可疑的活動，當您啟用 Security Assurance 時，必須提供關於疑似事件的特定資料集，以便 Palo Alto Networks 的專家能對該活動進行調查。

- 啟用 Security Assurance 之前需收集的資料
- 啟用 Security Assurance

啟用 *Security Assurance* 之前需收集的資料

Palo Alto Networks 的專家至少需要疑似活動的下列相關資訊，方能開始診斷該項可能的問題。請收集此份資料之後再啟用 Security Assurance。

關於疑似活動的基本詳細資料：

- 疑似攻擊向量和類型：是疑似活動的什麼證據警示您的管理或回應團隊？
- 時間軸：
  - 疑似初步攻擊的日期和時間 (若知道)。
  - 您識別可能問題的時間。
- 事件詳細資料：
  - 已知的受害系統 IP 位址。
    - 透過 NAT 公用的受害主機 IP 位址。
    - 能使系統成為目標的關鍵服務，例如資料庫、網頁服務、遠端存取 (RDP、Citrix 等) 伺服器。
  - 與攻擊可能相關的已知或疑似 IP 位址。
  - 受危害使用者帳戶的使用者 ID (若有)。
- 拓樸圖或概覽：防火牆相對於受害主機的位置。(不需要完整的網路網路拓樸圖。)
- 惡意軟體和入侵指標：
  - 範例。
  - 雜湊。

防火牆資料：

- 技術支援檔案：
  - 於疑似活動發生時從可能受害裝置路徑上的防火牆產生並上傳技術支援檔案。
  - 若您使用 Panorama 管理防火牆，請產生並上傳 Panorama 技術支援檔案。
- 防火牆日誌：從防火牆和 Panorama 設備匯出自疑似活動前起的兩小時日誌。在您匯出日誌之前，請確認 CSV 列設定為以 65535 列為最大值（**Device (裝置)** > **Setup (設定)** > **Management (管理)** > **Logging and Reporting Settings (**日誌記錄與報告的設定**)**）。若值較低，請提高到最大 65535 列。依照 IP 位址資訊和時間戳記詳細資料，為下列各種基本日誌類別匯出日誌 (如果啟用日誌) (您可篩選日誌以基於 IP 位址和時間顯示日誌項目)：

- 資料過濾日誌
- 流量日誌
- 威脅日誌
- URL 篩選日誌
- 使用者 ID 日誌 (若您懷疑涉及橫向移動)
- WildFire 提交日誌

務必瞭解您部署項目的記錄留存政策和記錄留存容量，以確保沒有相關資料未受檢查。管理員可能需要採取更多行動，例如從防火牆或其他記錄伺服器匯出資料，以確保調查期間資料的連續與完整。

識別疑似活動的有意義相關資料的更多方式：

- 使用應用程式控管中心 (ACC)。ACC 可向您指出疑似活動發生前、中、後的流量峰值、異常和改變。
- 使用威脅監控報告檢視疑似活動之前、中、後期間的主要威脅。

啟用 *Security Assurance*

在您就疑似活動收集資料以確保適時分析相關資訊之後，即可啟用 Security Assistance。啟用 Security Assistance 的方式有兩種：

- 登入客戶支援入口網站。按一下建立案例以開立支援案例。填妥表單後，選擇威脅。
- 您的銷售工程師 (SE) 能代您開立支援案例。