paloalto
TECHDOCS

Strata Cloud Manager AIOps

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

- For the most recent version of this guide or for access to 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

February 3, 2025

Table of Contents

AIOps for NGFW

AIOps for NGFW 透過 PAN-OS 裝置遙測收集資料，為您提供新世代防火牆部署的健康狀況和安全性概觀，協助您識別需要改進的領域並彌補安全性差距。AIOps for NGFW 會從裝置的操作狀態相關裝置遙測指標中，獲得健康資訊。針對安全性資訊，AIOps for NGFW 會根據 Palo Alto Networks 最佳做法分析裝置的設定，以指出安全性態勢中的任何潛在差距。

AIOps for NGFW Premium & Strata Cloud Manager

Strata Cloud Manager 僅針對使用 *AIOps for NGFW Premium* 授權的 *NGFW*，提供統一管理與作業。

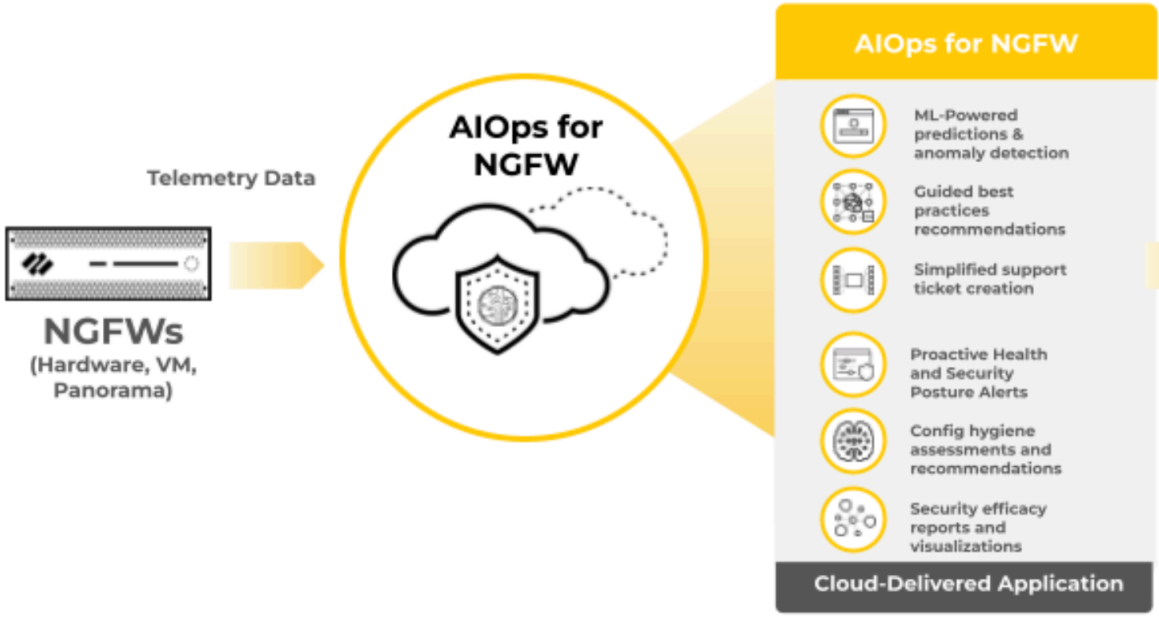
- ***NGFW***（***PAN-OS*** 和 ***Panorama*** 管理）→ 針對使用 *AIOps for NGFW Premium* 授權的 *PAN-OS* 和 *Panorama* 管理的 *NGFWs*，請透過 *Strata Cloud Manager* 來監控您的部署健康和安全性態勢。
- ***NGFW***（雲端管理）→ 透過 *AIOps for NGFW* 授權，您也可以將 *Strata Cloud Manager* 用於 NGFW 的雲端管理。

從 *2024* 年 *10* 月開始，*Strata Cloud Manager* 具有兩個授權層級：*Strata Cloud Manager Essentials* 和 *Strata Cloud Manager Pro*。此統一結構簡化了網路安全產品的部署，包括 *AIOps for NGFW*、自主數位體驗管理 *(ADEM)*、雲端管理功能和 *Strata* 記錄服務。請參閱 Strata Cloud Manager 授權

如果您已經透過 ***AIOps for NGFW Premium*** 授權使用 ***AIOps for NGFW Free*** 應用程式，或是 *Strata Cloud Manager*，您現有的授權不會受到影響，您可以繼續修改、延長或續約。

開始使用：

- Free 和 Premium AIOps for NGFW
- 啟動 AIOps for NGFW
- 開始將裝置遙測傳送到 AIOps for NGFW
- 新功能
- 隨選 BPA 報告
- AIOps for NGFW 事件和警示



適用於 NGFW 的 AIOps 的區域

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	其中一個： ❑ AIOps for NGFW Free或Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium或Strata Cloud Manager Pro

您在啟動 AIOps for NGFW 時選取的區域將會決定 AIOps 處理您資料的具體位置。

Strata Logging Service(SLS) 基礎設施支援的所有區域中並非都有提供 AIOps for NGFW。AIOps for NGFW 部署很快就會擴展至其他區域，以符合遙測資料目的地。目前，如果您將遙測資料傳送到不支援 AIOps 應用程式的區域，您的資料將由 AIOps for NGFW 執行個體在美國 - 美洲地區處理。

當您啟動時 AIOps for NGFW，則會自動套用這些限制。例如，如果您選取德國作為要啟動 AIOps for NGFW 執行個體的區域，則只能將位於德國的 SLS 租戶附加到該執行個體。

支援 *AIOps for NGFW* 的相同區域也支援 *Strata Cloud Manager* 中的 *NGFW*。

請參閱下表，了解各種遙測目標區域的 AIOps 資料處理。

Strata Logging Service 地區	AIOps for NGFW 執行個體處理資料的支援地區
德國	德國
英國	英國
荷蘭 - 歐洲	荷蘭 - 歐洲
義大利 - 歐洲	義大利 - 歐洲
西班牙 - 歐洲	西班牙 - 歐洲
瑞士 - 歐洲	瑞士 - 歐洲
法國 - 歐洲	法國 - 歐洲
波蘭 - 歐洲	波蘭 - 歐洲
韓國	韓國

Strata Logging Service 地區	AIOps for NGFW 執行個體處理資料的支援地區
印尼	印尼
以色列	以色列
臺灣	臺灣
卡達	卡達
新加坡	新加坡
澳大利亞	澳大利亞
印度	印度
日本	日本
加拿大	加拿大
其餘 SLS 區域	美國 - 美洲

免費和高級功能

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	其中一個： ❑ AIOps for NGFW Free或Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium或Strata Cloud Manager Pro

AIOps for NGFW 隨附兩個授權層級：免費和高級。

免費 AIOps for NGFW 的功能可增進您對防火牆部署的理解。

免費功能：

- 評估防火牆的設定，並識別需要改進的地方
- 輕鬆存取防火牆的執行時間和歷史遙測資料
- 檢測系統問題（與檢測方法無關）
- 透過警示/通知工作流程，縮短解決問題的時間
- 為多個安全訂閱提供動態儀表板和圖像資料

您可以透過高級層級授權，使用免費和高級的功能。高級功能著重於確保防火牆的充分利用和極大化安全成果。

高級功能：

- NGFW 的雲端管理

  請連絡您的客戶團隊，以使用 *Strata Cloud Manager* 為 NGFW 啟用雲端管理。

- 使用先進的機器學習技術來促進隨時保持最佳化的安全性態勢，以回應不斷變化的威脅和網路環境，從而減少攻擊
- 為 WildFire 和 IOC 搜尋提供動態儀表板和圖像資料
- 在 Strata Cloud Manager 控管中心與資料互動，並呈現網路上不同事件之間的關係，以發現異常情況或找到增強網路安全的方法

Strata Cloud Manager 有兩個授權層級：*Strata Cloud Manager Essentials* 和 *Strata Cloud Manager Pro*。此統一結構簡化了網路安全產品的部署，包括 *AIOps for NGFW*、自主數位體驗管理 *(ADEM)*、雲端管理功能和 *Strata* 記錄服務。請參閱 Strata Cloud Manager 授權

如果您已經透過 ***AIOps for NGFW Premium*** 授權使用 ***AIOps for NGFW Free*** 應用程式，或是 *Strata Cloud Manager*，您現有的授權不會受到影響，您可以繼續修改、延長或續約。

功能集	Free	Premium（使用 Strata Cloud Manager）
加強安全性態勢	部分	是
• 安全性態勢洞察	是	是
• 功能採用	是	是
• 安全性態勢設定	否。	是
• 軟體升級建議	否。	是
• CDSS 採用	是	是
• 政策分析器	否。	是
• 隨選 BPA 報告	是	是
• Panorama CloudConnector 外掛程式	否。	是
• 功能分析器	否。	是
• NGFW SDWAN 儀表板	否。	是
• 合規摘要儀表板	否。	是
主動解決防火牆中斷	部分	是
• 警示和事件	部分	是
• PAN-OS CVE 儀表板	是	是
• 警示的可能原因分析	否。	是
使用日誌進行疑難排解	是	是
• 在日誌檢視器中查看、查詢和匯出日誌 檢查使用日誌檢視器的授權和其他需求。	是	是
• 匯出中繼資料以進行疑難排解	是	是
• 檢視稽核日誌	是	是
最佳化您的安全投資	部分	是

功能集	Free	Premium（使用 Strata Cloud Manager）
• 基於健康和安全性態勢的裝置排名	是	是
• 除了威脅洞察儀表板外的所有儀表板和報告	是	是
• 威脅洞察儀表板和報告	否。	是
• 搜尋安全性構件	否。	是
• 建立自訂儀表板	否。	是
• Strata Cloud Manager 控管中心	否。	是
通知	部分	是
• 電子郵件通知	是	是
• ServiceNow 整合	否。	是
參與和支援	否。	是
• 針對操作問題的產品內支援票證建立功能 需要具備防火牆上的 *Platinum* 層級支援（電源故障警示除外）	否。	是

產品中所有功能類別的新功能將完全根據 *Palo Alto Networks* 的判斷，指派到 *Free* 和 *Premium* 層級。

如何啟動 AIOps for NGFW

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	其中一個： ❑ AIOps for NGFW Free或Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium或Strata Cloud Manager Pro

以下是啟動 AIOps for NGFW 的不同情況：

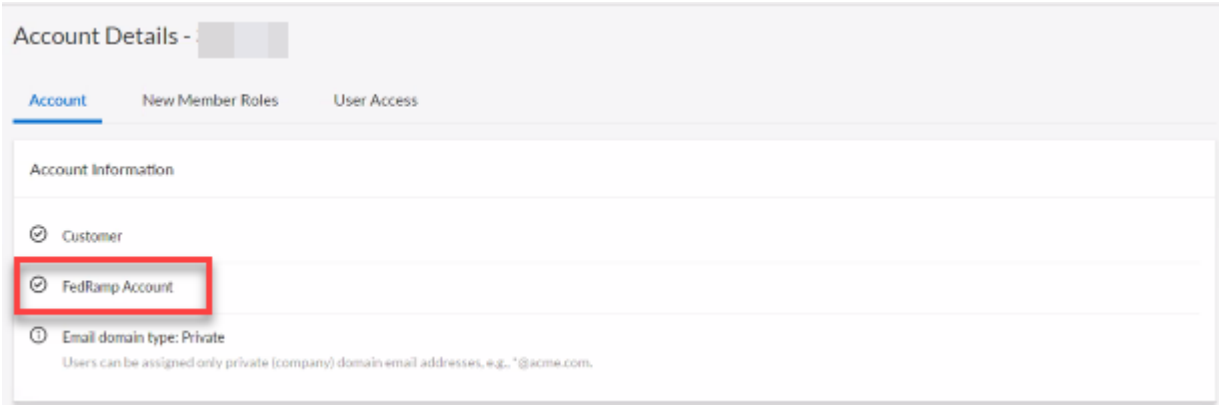
情況	計劃
啟動 AIOps for NGFW Free	啟動 AIOps for NGFW (Free)
啟動 AIOps for NGFW Premium（使用 Strata Cloud Manager 應用程式）	透過常見服務啟動 AIOps for NGFW
將新裝置載入已啟動的 AIOps for NGFW Free 執行個體	將裝置與租用戶建立關聯 在裝置上啟用遙測
將新裝置載入已啟動的 AIOps for NGFW Premium（使用 Strata Cloud Manager 應用程式）	將裝置與租用戶建立關聯 將租戶中的裝置與應用程式建立關聯 在裝置上啟用遙測
啟動 ELA AIOps for NGFW Premium	啟動企業授權合約 (ELA) AIOps for NGFW Premium
使用 Strata Cloud Manager (AIOps for NGFW Premium) 來管理 VM-Series	啟動軟體 NGFW 積分授權合約
將 Strata Cloud Manager (AIOps for NGFW Premium) 用於 Panorama 管理的 VM-Series	針對 Panorama 管理的 VM-Series 啟動軟體 NGFW 積分授權
將 AIOps for NGFW Premium 試用授權轉換為生產	將試用授權轉換為生產
啟動 Strata Cloud Manager Essentials 和 Strata Cloud Manager Pro	• 啟動 Strata Cloud Manager Essentials • 啟動 Strata Cloud Manager Pro

情況	計劃
Strata Cloud Manager Essentials 和 *Strata Cloud Manager Pro* 可在缺乏以下項目的客戶支援入口網站 *(CSP)* 帳戶中啟動：搭配合適儲存空間的 *Strata* 記錄服務、*AIOps for NGFW Free* 或 *Premium*，或是 *Prisma Access*。	

Strata Cloud Manager 僅針對使用 AIOps for NGFW Premium 授權的 NGFW，提供統一管理與作業。繼續使用 AIOps for NGFW Free 應用程式，將 NGFW 載入 AIOps for NGFW Free。

Strata Cloud Manager 可供使用，提供兩個授權層級：Strata Cloud Manager Essentials 和 Strata Cloud Manager Pro 。此統一結構簡化了網路安全產品的部署，包括 AIOps for NGFW、自主數位體驗管理 (ADEM)、雲端管理功能和 Strata 記錄服務。如果您在引入這些新授權層級之前使用 Strata Cloud Manager，則您現有的 AIOps for NGFW Premium 和 AIOps for NGFW Free授權會繼續受到支援。您可以繼續修改、延長或續約這些授權。

FedRAMP 帳戶無法使用 *AIOps for NGFW*。若要檢查這是否適用於您，請登入您的客戶支援入口網站帳戶，然後選取***Account Management***（帳戶管理）***> Account Details***（帳戶詳細資料）。如果您看到列出的 ***FedRamp Account***（***FedRamp*** 帳戶），則無法使用 *AIOps for NGFW*。



啟動 **AIOps for NGFW (Free)**

若要啟動，需要具備帳戶管理員或應用程式管理員角色。

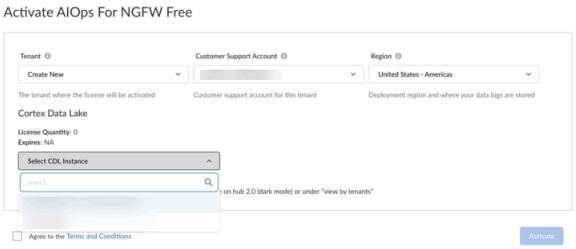
1. 透過以租用戶為中心的檢視，登入中樞。

   如果您在「支援帳戶」檢視中，請將 **View by Support Account**（依照支援帳戶檢視）關閉。

   如果您沒有現有租用戶，請使用支援帳戶檢視登入中樞。

2. 找到 AIOps for NGFW Free，然後選取 **Activate**（啟動）。

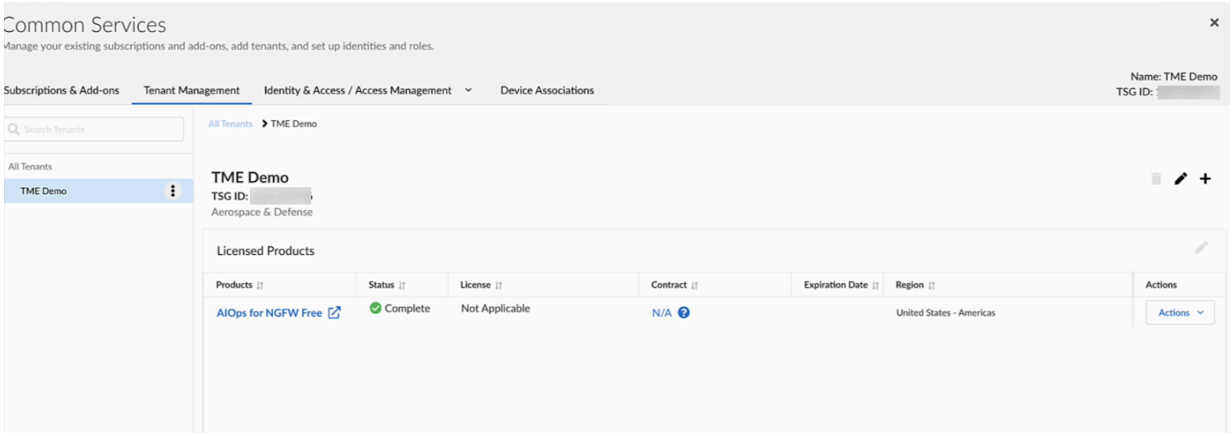
3. 填寫表單。



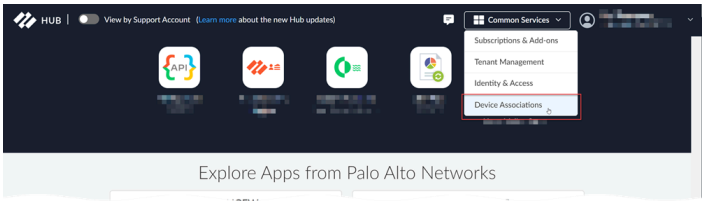
租用戶	選取您要在其中啟動 AIOps for NGFW Free 執行個體的租用戶。如果您沒有現有租用戶，請選取 **Create New**（新建）。
客戶支援帳戶	您的客戶支援入口網站帳戶 ID。
地區	部署區域和儲存資料記錄檔的區域。請參閱 AIOps for NGFW 的區域。
Strata 記錄服務	您要將資料傳送到 AIOps for NGFW Free 的 Strata Logging Service。如果您有記錄 SLS，可以與 AIOps for NGFW Free 建立關聯，否則可以跳過。

4. **Agree to the terms and conditions**（同意條款和條件），然後 **Activate**（啟動）。

5. **Status**（狀態）顯示 **Complete**（完成）後，AIOps for NGFW Free 可供使用。



6. 將裝置與包含 AIOps for NGFW Free 執行個體的租用戶建立關聯。
   1. 登入中樞。
   2. 選取 **Common Services**（常見服務） > **Device Associations**（裝置關聯）。



   3. 選取 **Add Device**（新增裝置）。
   4. 選取一或多個防火牆或 Panorama 設備，然後 **Save**（儲存）。

   如果您正在載入 Panorama 管理的部署，則需要將 Panorama 與包含 AIOps for NGFW Free 的租用戶建立關聯。請務必將 Panorama 管理的所有防火牆與租用戶個別建立關聯。

   您與租用戶建立關聯的裝置將自動新增至 AIOps for NGFW Free。如需詳細資訊，請參閱將裝置與租用戶建立關聯。

   - 針對啟動 *AIOps for NGFW Free*，不需要將應用程式與裝置建立關聯。
   - 如果您已經有現有租用戶，可以在開始啟用時，將裝置與租用戶建立關聯。
   - 例如，如果您要淘汰或傳回防火牆或 *Panorama* 設備，或是要與其他租用戶服務群組 *(TSG)* 建立關聯，可以移除裝置關聯。

7. 在裝置上啟用遙測。
   1. 登入 support.paloaltonetworks.com 以確認裝置已在客戶支援入口網站中註冊，切換到您的帳戶（如有必要），並在 **Assets**（資產） > **Devices**（裝置）中識別您的裝置。
   2. 在您想要載入的裝置上安裝裝置憑證。
   3. 在裝置上啟用遙測共用。

   載入裝置並啟用遙測後，大約需要幾個小時才能在 *AIOps for NGFW* 儀表板上看到第一組洞察。在裝置端產生和傳送遙測資料的過程是分批完成的，每個指標的採樣和收集頻率都已針對指標的使用案例最佳化。此分批過程可能會導致載入防火牆和獲得洞察之間發生延遲。與新載入的裝置相關的所有洞察可能需要幾個小時，才能顯示在 *AIOps for NGFW* 儀表板上。

8. 按一下中樞上的圖示，登入 AIOps for NGFW Free。

我的 AIOps for NGFW 功能在哪裡？

此內容適用於新世代防火牆（搭配 *AIOps for NGFW* 和 *Strata Cloud Manager*）的雲端管理。若要開始管理新世代防火牆（搭配 *PAN-OS*），請按一下這裡。

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	其中一個： ❑ AIOps for NGFW Free或Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium或Strata Cloud Manager Pro

Palo Alto Networks Strata Cloud Manager 是一個全新的 AI 驅動統一網路安全管理平台。現在，您可以使用 Strata Cloud Manager 來互動與管理 AIOps for NGFW，以及您的其他 Palo Alto Networks 產品和訂閱。

若要啟動 **Strata Cloud Manager:**

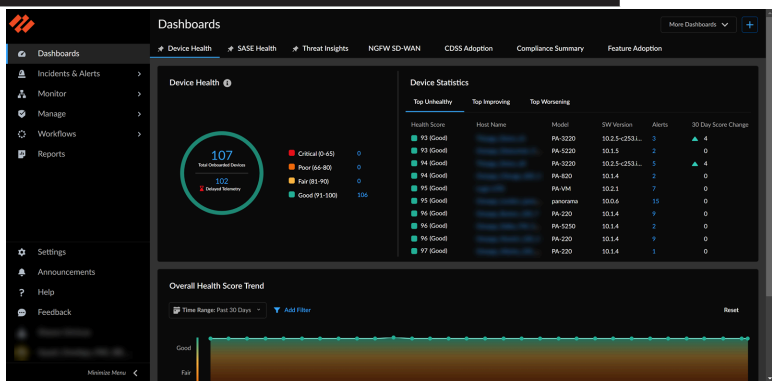
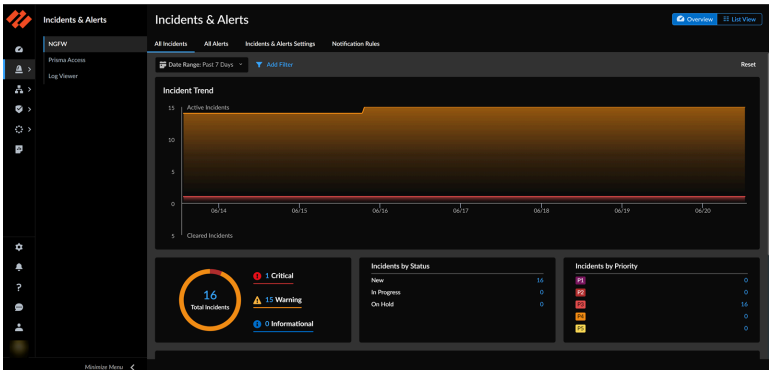
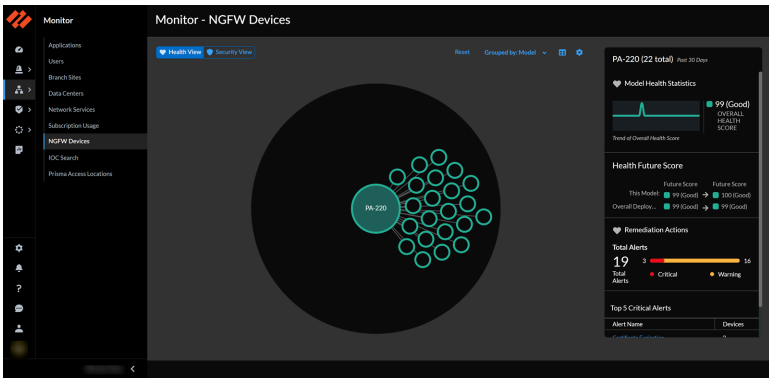
- 請前往中樞並啟動 Strata Cloud Manager 應用程式
- 直接前往 Strata Cloud Manager URL

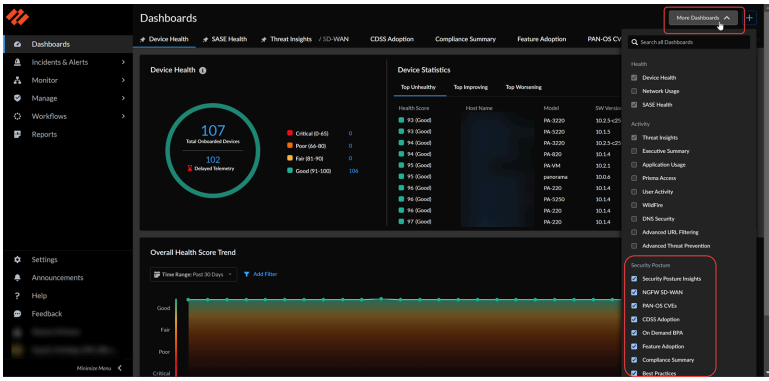
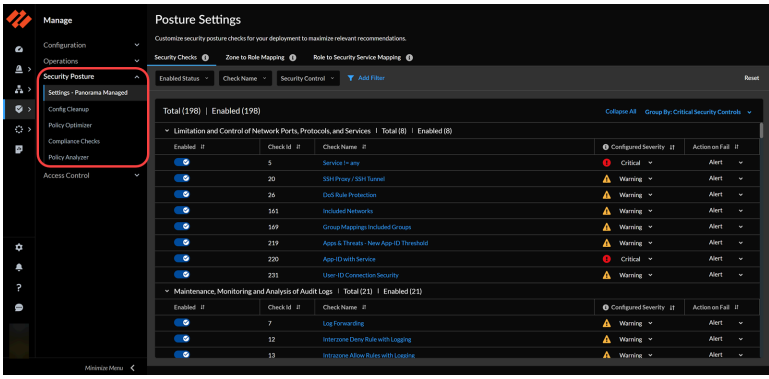
- Strata Cloud Manager 僅針對使用 *AIOps for NGFW Premium* 授權的 *NGFW*，提供統一管理與作業。*AIOps for NGFW*（僅限高級應用程式）中樞上的應用程式圖格名稱現在已變更為 *Strata Cloud Manager*。透過此更新，應用程式 *URL* 也已經變更為 stratacloudmanager.paloaltonetworks.com，您現在也會在左側導覽窗格中看到 *Strata Cloud Manager* 標誌。繼續使用 *AIOps for NGFW Free* 應用程式，將 *NGFW* 載入 *AIOps for NGFW Free*。
- 請連絡您的客戶團隊，以使用 *Strata Cloud Manager* 為 NGFW 啟用雲端管理。

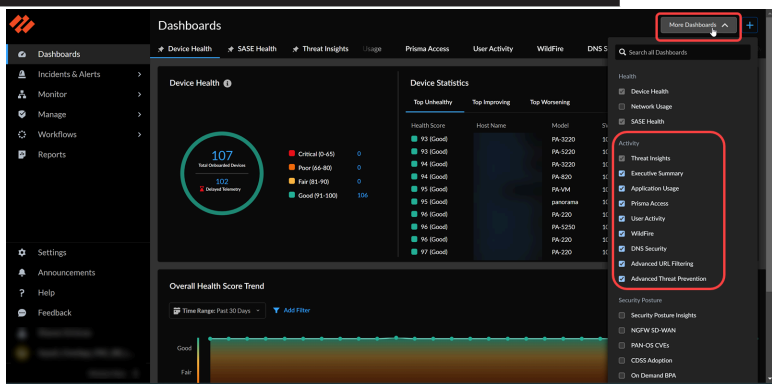
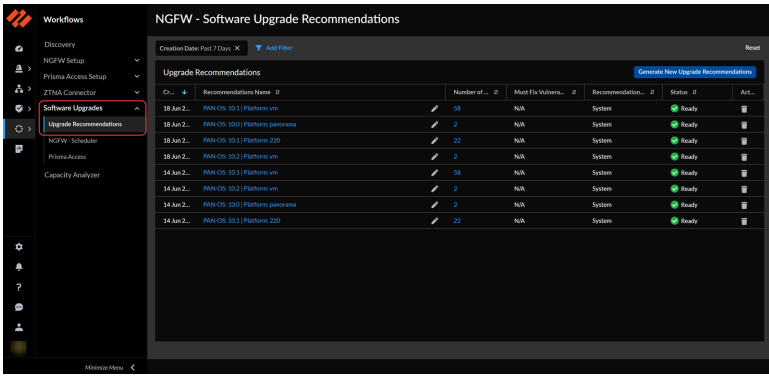
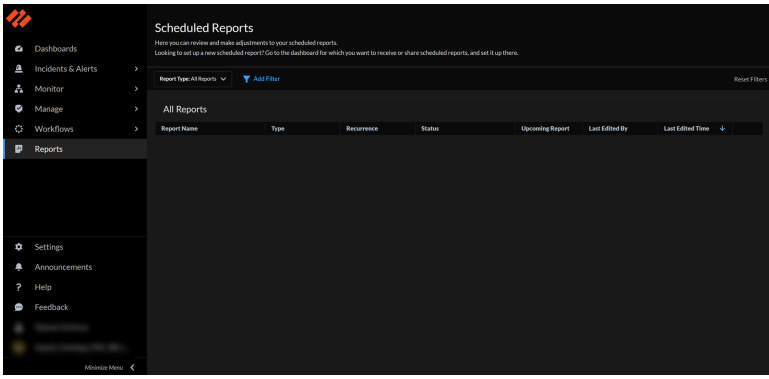
如果您先前使用 AIOps for NGFW 應用程式，您可以在這裡找到 Strata Cloud Manager 中的功能:

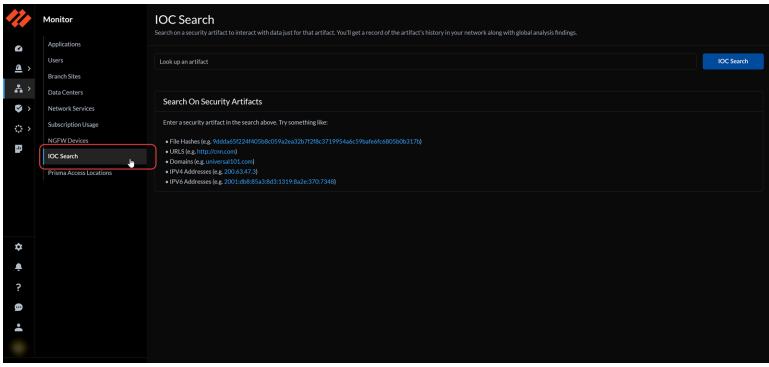
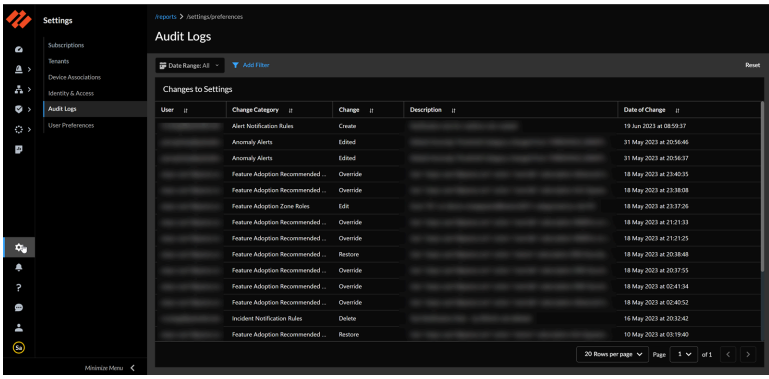
表 **1:**

AIOps for NGFW 應用程式	在哪裡可以找到 **Strata Cloud Manager** 中的這些相同功能**:**
儀表板	→前往→儀表板→裝置健康情況

AIOps for NGFW 應用程式	在哪裡可以找到 Strata Cloud Manager 中的這些相同功能:
	
警示	→前往→事件與警示→NGFW 
監控	→前往→監控→裝置→NGFW 
態勢	→前往儀表板查看： • 最佳做法儀表板 • 安全性態勢洞察儀表板 • NGFW SD-WAN 儀表板 • 安全諮詢儀表板 (PAN-OS CVEs) • CDSS 採用儀表板

AIOps for NGFW 應用程式	在哪裡可以找到 Strata Cloud Manager 中的這些相同功能:
	• 隨選 BPA 儀表板 • 功能採用儀表板 • 合規摘要儀表板  →前往→管理→安全性態勢以尋找： • 設定 - Panorama 管理 • 設定清理 • 原則最佳化工具 • 合規性檢查 • 政策分析器 
活動	→前往儀表板查看： • 網路使用情況 • 威脅洞察 • 應用程式使用方式 • 進階 WildFire • DNS 安全性 • 執行摘要 • 使用者活動

AIOps for NGFW 應用程式	在哪裡可以找到 Strata Cloud Manager 中的這些相同功能:
	 →前往 **Reports**（報告），以便為支援的儀表板產生報告。 → 針對 **Log Viewer**（日誌檢視器），前往 **Incidents & Alerts**（事件與警示）。
工作流程	→前往 **Workflows**（工作流程） > **Software Upgrades**（軟體升級），以使用**Upgrade Recommendations**（升級建議）。 
報告	→ 前往 **Reports**（報告）以安排支援的儀表板報告。 

AIOps for NGFW 應用程式	在哪裡可以找到 Strata Cloud Manager 中的這些相同功能:
搜尋	→ 前往 **IoC Search**（IoC 搜尋）的 **Monitor**（監控）。 
設定	→ 前往 **Incidents & Alerts**（事件與警示） > **NGFW** > **Incidents & Alerts Settings**（事件與警示設定），以查看 **Forecast and Anomaly Incidents & Alerts**（預測和異常事件和警示）。 → 前往 **Incidents & Alerts**（事件與警示） > **NGFW**，以設定 **Notification Rules**（通知規則）。 → 前往 **Settings**（設定）以查看： • 稽核日誌 • 使用者偏好設定  → 前往 **Manage**（管理） > **Security Posture**（安全性態勢），以自訂 **Settings - Panorama Managed**（設定 - **Panorama** 管理）。 → 前往 **Help**（說明）→**Export Tenant Metadata**（匯出租用戶中繼資料）。

AIOps for NGFW 應用程式	在哪裡可以找到 Strata Cloud Manager 中的這些相同功能:
–	尋找如何透過 Strata Cloud Manager 管理 NGFW？ 僅支援搭配 AIOps for NGFW Premium 的 Strata Cloud Manager，且不適用於 AIOps for NGFW 應用程式。 → 前往 **Manage**（管理） > **Configuration**（設定） > **NGFWs and Prisma Access**（**NGFW** 和 **Prisma Access**），以及 **Workflows**（工作流程） > **NGFW Setup**（**NGFW** 設定）。

Panorama CloudConnector 外掛程式

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ AIOps for NGFW Premium或Strata Cloud Manager Pro

想要主動檢視您的政策規則是否遵守最佳做法嗎？在推播政策規則後，您不必等到收到警示才解決問題。將 AIOps for NGFW 或 Strata Cloud Manager 連接到您的 Panorama，以便在推播到已受管防火牆之前，根據某些最佳做法檢查來評估您的設定。請參閱主動強制執行安全檢查。

安全性政策規則的更新通常具有時效，需要您快速採取行動。但是，您需要確保對安全性政策規則庫所做的任何更新都符合您的需求，並且不會產生錯誤或設定有誤（例如導致規則重複或衝突的變更）。

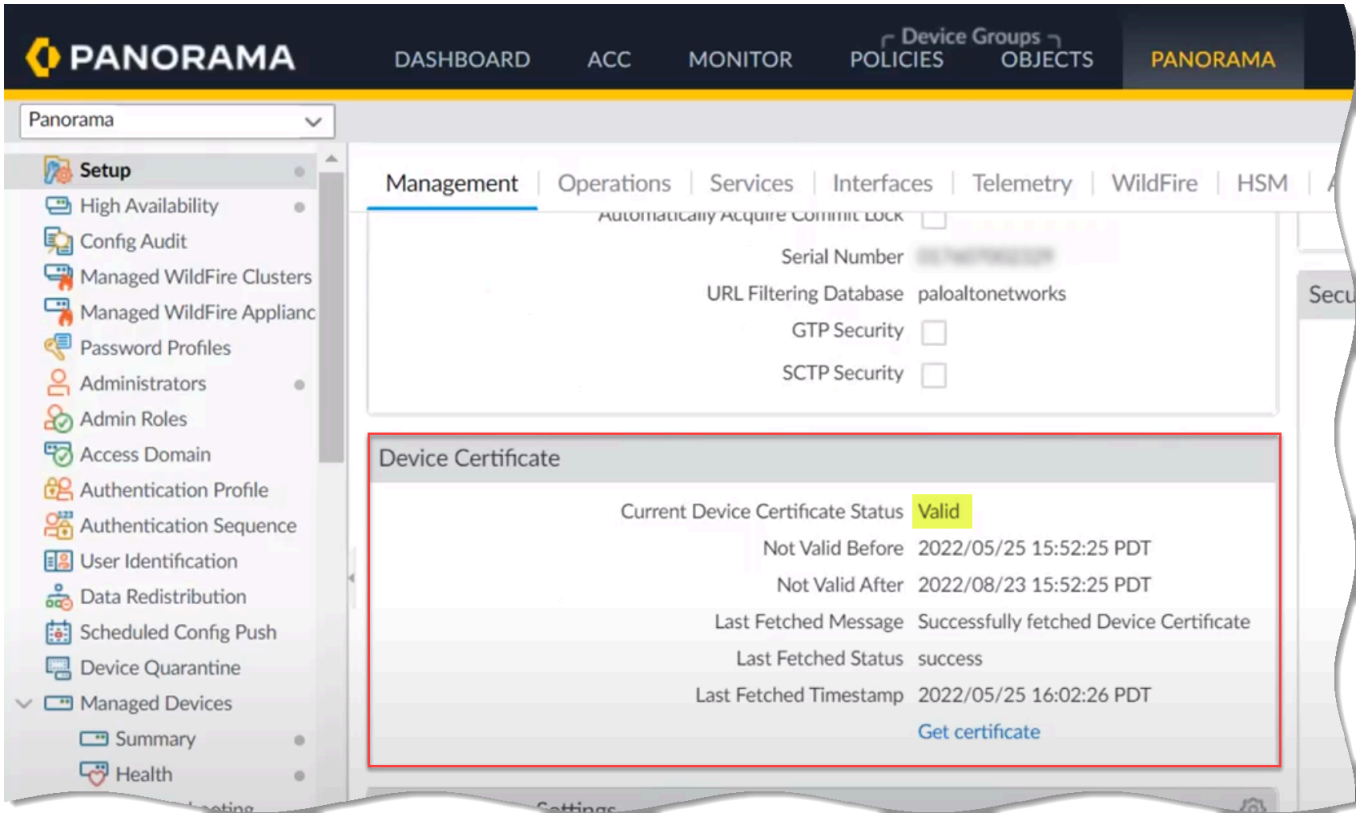
因此，Strata Cloud Manager 中的政策分析器可讓您在實施變更要求時，最佳化時間和資源。政策分析器不僅會分析並提供可能的合併或移除特定規則的建議，以滿足您的意圖，還會檢查規則庫中的異常情況，例如陰影、冗餘、一般化、相關性和合併。

將 AIOps for NGFW 或 Strata Cloud Manager 連接到您的 Panorama，並使用政策分析器來新增或最佳化您的安全性政策規則庫。請參閱政策分析器。

您需要這些才能將 AIOps for NGFW 連接到你的 Panorama：

AIOps for NGFW 或 Strata Cloud Manager 執行個體：您不需要 AIOps for NGFW Premium 授權即可安裝 Panorama CloudConnector 外掛程式。但是，需要 Premium 授權才能使用政策分析器和主動最佳做法評估 (BPA) 等高級功能。

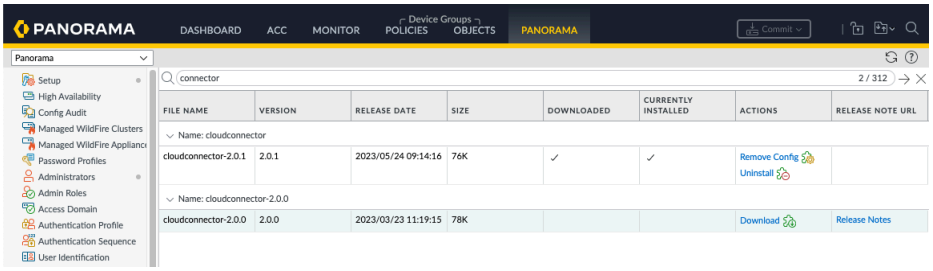
已安裝搭配裝置憑證的 Panorama。



Panorama CloudConnector 外掛程式已安裝在執行 PAN OS 10.2.3 及更高版本的 Panorama 上。

您需要使用以下命令啟用此外掛程式：

```
> 要求外掛程式 cloudconnector 啟用基本功能
```



- 為了協助客戶，我們已在較新的 *Panorama* 版本（*11.0.1* 及更高版本）中預先安裝了此外掛程式。
- 如果您已經安裝 *AIOps* 外掛程式和 *CloudConnector* 外掛程式，請解除安裝 *AIOps* 外掛程式，因為兩者是相同的，只是名稱改變了而已。請確保您只安裝一個外掛程式，應該要是最新版本的 *CloudConnector* 外掛程式。

如果您在 PAN-OS 10.2.3 上安裝了 AIOps 外掛程式，然後升級到 PAN-OS 11.0.1 或更新版本，則該外掛程式的預設版本將隨新的 PAN-OS 版本一起安裝。這會導致這兩個外掛程式都出現在 Panorama 上。在這種情況下，請按照下列步驟操作：

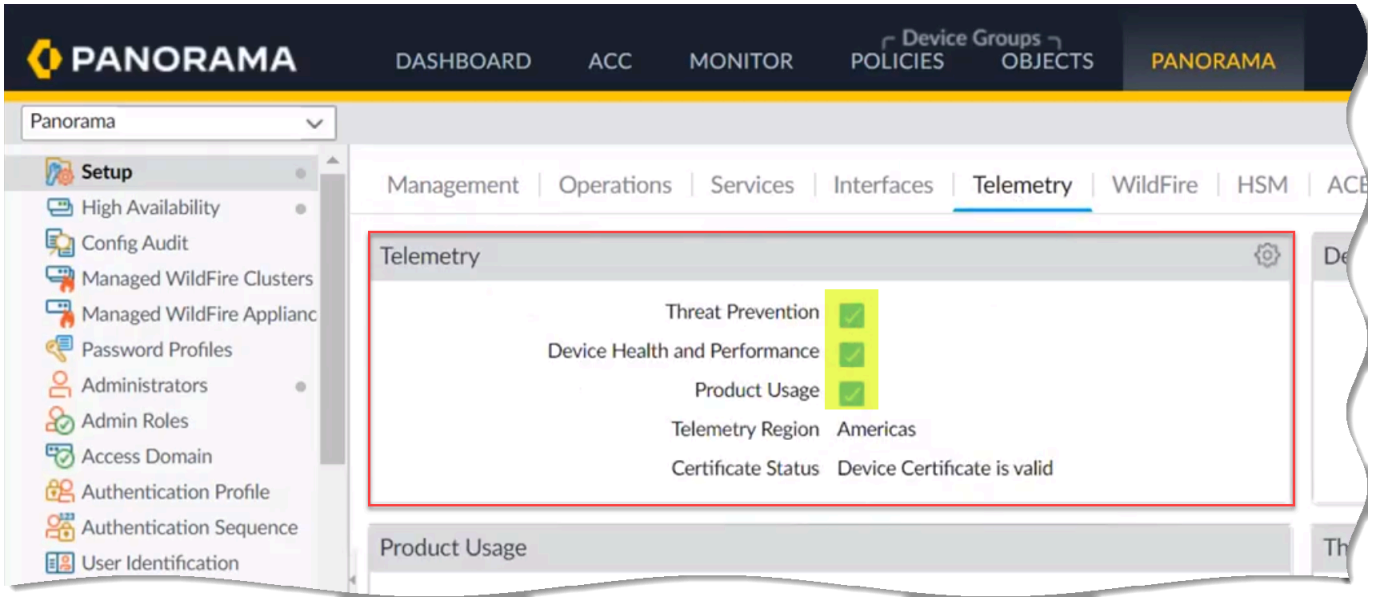
1. 在 Panorama 網頁介面中，選取 **Panorama > Plugins**（外掛程式）並 **Uninstall**（解除安裝）AIOps 外掛程式。
2. 啟用 CloudConnector 外掛程式：

   ```
   > 要求外掛程式 cloudconnector 啟用基本功能
   ```

CloudConnector 外掛程式 2.2.0 支援來自 Panorama 的 Proxy 配置設定。這些設定僅在提交後生效。以下是情況：

- 配置 Proxy 設定：當您配置 Proxy 設定並執行提交時，CloudConnector 外掛程式在此提交期間將無法識別新的 Proxy 設定。提交後，外掛程式將使用 Proxy 設定進行將來與雲端的互動。
- 移除 Proxy 設定：當您移除 Proxy 設定並執行提交時，CloudConnector 外掛程式將無法在提交期間識別已移除的 Proxy 設定。提交後，外掛程式將無法再使用 Proxy 設定進行將來與雲端的互動。

裝置遙測已在您的 Panorama 上啟用。



安全性政策規則，允許 Panorama 和對應到您 Strata Logging Service 主機區域的 FQDN 之間進行通訊：

美洲 (americas)	https://prod.us.secure-policy.cloudmgmt.paloaltonetworks.com/
澳州 (au)	https://prod.au.secure-policy.cloudmgmt.paloaltonetworks.com/
加拿大 (ca)	https://prod.ca.secure-policy.cloudmgmt.paloaltonetworks.com/
歐洲 (europe)	https://prod.eu.secure-policy.cloudmgmt.paloaltonetworks.com/
FedRAMP (gov)	https://prod.gov.secure-policy.cloudmgmt.paloaltonetworks.com/
德國 (de)	https://prod.de.secure-policy.cloudmgmt.paloaltonetworks.com/
印度 (in)	https://prod.in.secure-policy.cloudmgmt.paloaltonetworks.com/
日本 (jp)	https://prod.jp.secure-policy.cloudmgmt.paloaltonetworks.com/
新加坡 (sg)	https://prod.sg.secure-policy.cloudmgmt.paloaltonetworks.com/
英國 (uk)	https://prod.uk.secure-policy.cloudmgmt.paloaltonetworks.com/

取得警示通知

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	其中一個： ❑ AIOps for NGFW Free或Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium或Strata Cloud Manager Pro

將 Strata Cloud Manager 整合到您現有的操作中，涉及設定主動警示，使您能夠在潛在問題升級為嚴重複雜的問題之前，及早偵測和管理潛在問題。這些警示可以根據您的營運團隊的案例管理通訊協定量身打造，例如常用的 P1 或 P2。

例如，您可以設定一個警示系統，其中代表最嚴重問題的嚴重警示會即時升級到您的安全團隊，以供其立即處理。另一方面，緊告類警示的緊急程度較低，但仍然具有重要性，可以安排每日審查。這種安排可確保高效率的事件管理，同時保持營運的順利運作。

另一種選擇是根據團隊路由警示；某些類別的警示，甚至特定的警示，可以路由到最有能力處理這些問題的不同團隊。您可以定義通知偏好設定，例如哪些警示觸發通知、接收通知的方式以及接收通知的頻率，來建立通知規則。

以下影片示範如何建立通知規則。

STEP 1 | 選取 **Incidents & Alerts**（事件和警示） > **Incident & Alert Settings**（事件和警示設定） > **Notification Rules**（通知規則） > **+ Add Notification Rule**（+ 新增通知規則）

STEP 2 | 輸入名稱及說明。

STEP 3 | **Add New Condition**（新增條件）以指定將觸發通知的 `Rule Conditions`（規則條件）。

例如，若要建立硬體警示通知，請選取 **subCategory**、**Equals**（等於）和 **Hardware**（硬體）。

STEP 4 | 選擇通知的通知類型和收件者。

1. 如果選取 **Email**（電子郵件），請選取一個電子郵件群組（接收電子郵件通知的使用者群組），或 **Create a New Email Group**（建立新電子郵件群組）。
   1. 若要建立新的電子郵件群組，請輸入電子郵件群組名稱，然後開始輸入要新增至群組的電子郵件地址。填寫完每個電子郵件地址後，按下 Return 鍵。
   2. 選取 **Next**（下一步）。
   3. 選取您要傳送這些通知的頻率：
      - 立即
      - 每 4 小時分組傳送一次
      - 每天分組傳送一次
2. 如果選擇 **ServiceNow**，請輸入 `ServiceNow URL`、用戶端憑證、ServiceNow 憑證和 `ServiceNow API` 版本。
   1. **Test**（測試）您的連線以確保整合正常運作。
   2. 選取 **Next**（下一步）。

STEP 5 | **Save Rule**（儲存規則）。

針對 NGFW 連線和政策強制執行異常進行疑難排解

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ AIOps for NGFW Premium或Strata Cloud Manager Pro ❑ 需要「Strata 記錄服務」的授權，才能進行記錄 ❑ 如果您擁有 Prisma Access 授權，則可以使用資料夾管理來檢視預先定義的資料夾，並為資料夾啟用網路安全

從 Strata Cloud Manager 對 NGFW 進行疑難排解，且無需在各種防火牆介面之間移動。如果您在部署和設定 NGFW 後遇到連線問題，您可以取得路由和通道狀態的彙總視圖，並深入了解具體情況，以查找異常和有問題的設定。

對基於身分的政策規則和動態定義的端點進行疑難排解。您可以檢查特定 NGFW 的狀態，並揭示您期望政策運作的方式與其實際執行行為之間可能存在的不符情況。

Troubleshooting（疑難排解）可讓您深入了解這些網路和身分功能中可能出現的問題 - 追蹤並解決連線問題或政策執行異常：

網路疑難排解

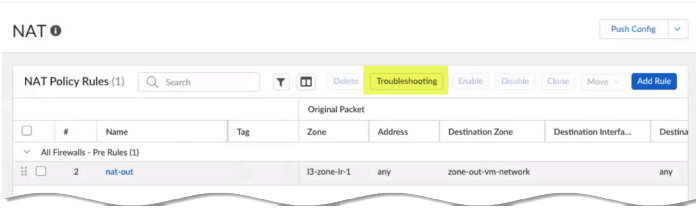
- NAT
- DNS Proxy

身份和政策疑難排解

- 使用者群組
- 動態位址群組
- 動態使用者群組
- 使用者 ID

防火牆疑難排解

- 工作階段瀏覽器



前往 **Manage**（管理）> **Configuration**（設定）> **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**）> **Operations**（操作）> > **Troubleshooting**（疑難排解）> **Session Browser**（工作階段瀏覽器），以針對您的防火牆開始進行疑難排解。

或者，您可以前往要疑難排解的功能，然後選取 **Troubleshooting**（疑難排解）按鈕以開始。

按狀態、操作、搜尋目標和時間戳記，檢視和排序您已執行的疑難排解作業。

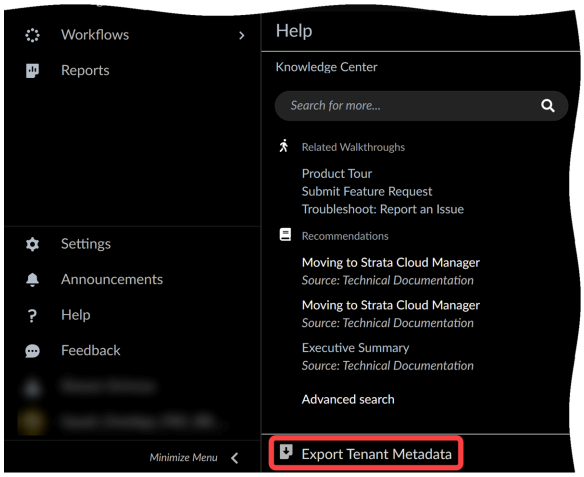
功能	功能位置	可用動作	操作範圍	工作輸出組織依據：
工作階段瀏覽器（防火牆）	管理 > 組態設定 > **NGFW** 和 **Prisma Access** > 操作人員 > > 疑難排解 > 工作階段瀏覽器	篩選依據： • 防火牆 • 規則名稱 • 來源區域 • 來源位址 • 來源使用者 • 來源連接埠 • 目的地區域 • 目的地位址 • 目的地連接埠 • App-ID	您指定的防火牆	• 工作階段 ID • 開始時間 • 地區 • 來源 • 目的地 • 連接埠 • 通訊協定 • 應用程式 • 進入 • 輸出 • 位元組
DNS Proxy（網路）	管理設定 > **NGFW** 和 **Prisma Access** > 裝置設定 > **DNS Proxy**	• 顯示 DNS Proxy 快取 • 搜尋 DNS Proxy 快取	您指定的防火牆	• 域名 • IP 位址 • 類型 – IPv4 Address Record (A)、IPv6 Address Record (AAAA)、Canonical Name Record (CNAME)、Mail Exchange Record (MX) 和 Pointer to a canonical name (PTR) • 類別：Internet (IN TCP/IP)、Chaos (CH) 和 Hesiod (HS) • time-to-live (存留時間 -

功能	功能位置	可用動作	操作範圍	工作輸出組織依據：
				TTL)，以毫秒為單位 • Hits – 自上次重新啟動以來要求記錄的次數
NAT（網路）	管理設定 > **NGFW** 和 **Prisma Access** > 網路政策 > **NAT**	顯示 NAT 規則 IP 集區	您指定的防火牆	• rule • 類型 • 已使用 • 支持 • 記憶體大小比例
使用者群組（身分）	管理設定 > **NGFW** 和 **Prisma Access** > 身分服務 > 雲端識別引擎	• 顯示使用者群組 • 搜尋使用者群組	您指定的防火牆	• 使用者名稱 • 群組
動態位址群組（身分）	管理設定 > **NGFW** 和 **Prisma Access** > 物件 > 位址 > 位址群組	• 顯示所有動態位址群組 • 搜尋動態位址群組（從清單中選擇）	您指定的防火牆	• 名稱 • 篩選 • 會員
動態使用者群組（身分）	管理設定 > **NGFW** 和 **Prisma Access** > 物件 > 動態使用者群組	• 按動態使用者群組搜尋 • 按使用者名稱搜尋	您指定的防火牆	• 成員（使用者名稱）和/或動態使用者群組
使用者 ID（身分）	管理設定 > **NGFW** 和 **Prisma Access** > 身分服務 > 身分重新分配	• 顯示所有使用者的 IP 對應 • 搜尋使用者 IP 對應	您指定的防火牆	• ip • 使用者 • 從 • 閒置逾時 • 逾時上限

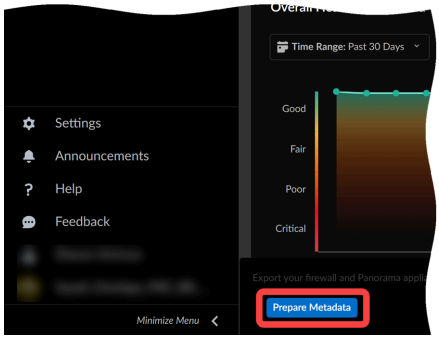
匯出中繼資料以進行疑難排解

為了向技術支援團隊提供他們需要的資訊，以進一步協助您，AIOps for NGFW 可讓您將部署資料匯出到本機。該資料以 JSON 檔案形式傳送，並以 gzip 格式壓縮。

1. 選取 **Help**（說明）**> Export Tenant Metadata**（匯出租用戶中繼資料）。



2. **Prepare Metadata**（準備中繼資料）。



3. **Download**（下載）您的中繼資料檔案。

   中繼資料檔案名稱包含您的客戶支援入口網站 (CSP) ID、您的 AIOps for NGFW 租用戶 ID，以及匯出的時間戳記：*<csp-tenant-timestamp>*.gzip。

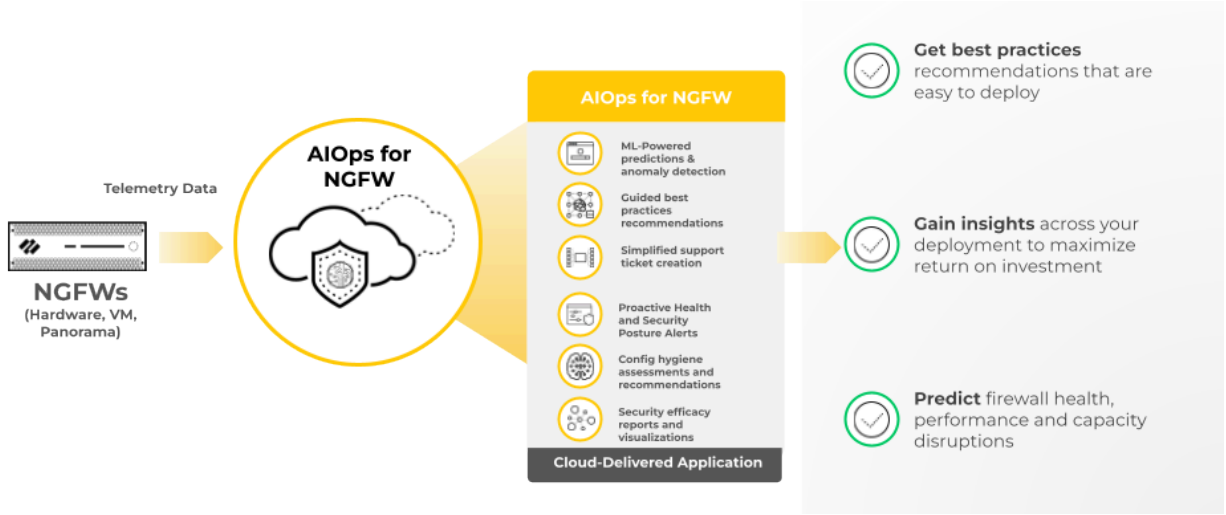
AIOps for NGFW 的裝置遙測

我可以在哪裡使用這個？	我需要哪些內容？
• ，包括由軟體 NGFW 積分資助的項目	其中一個： ❑ 或 ❑ 或

AIOps for NGFW 透過分析 PAN-OS 裝置傳送到 Strata Logging Service 的遙測資料，來評估部署中的防火牆健康狀況。若要傳送此資料，您必須在裝置上啟用裝置遙測。

設定遙測後，您的新世代防火牆會將原始遙測資料傳送到 Strata Logging Service（在固定間隔傳送）。Strata Logging Service 會解析並翻譯這些原始資料，以便 AIOps for NGFW 可以為您提供裝置狀態、圖像資料和警示。

載入您的裝置，以開始將裝置遙測資料傳送到 AIOps for NGFW。



在裝置上啟用遙測

請依照以下步驟，將 AIOps for NGFW 與您的 PAN-OS 裝置搭配使用。

如果您的輸出流量會通過 Proxy，請確保您已允許 AIOps for NGFW 所需的網域。

如果您要載入 *Panorama* 管理的部署，則需要在 *AIOps for NGFW* 上載入 *Panorama*。

1. 登入 support.paloaltonetworks.com 以確認裝置已在客戶支援入口網站中註冊，切換到您的帳戶（如有必要），並在 **Assets**（資產） > **Devices**（裝置）中識別您的裝置。
2. 在您想要載入的裝置上安裝裝置憑證。
3. 在裝置上啟用遙測共用。

載入裝置並啟用遙測後，大約需要幾個小時才能在 *AIOps for NGFW* 儀表板上看到第一組洞察。在裝置端產生和傳送遙測資料的過程是分批完成的，每個指標的採樣和收集頻率都已針對指標的使用案例最佳化。此分批過程可能會導致載入防火牆和獲得洞察之間發生延遲。與新載入的裝置相關的所有洞察可能需要幾個小時，才能顯示在 *AIOps for NGFW* 儀表板上。

AIOps for NGFW 所需的網域

我可以在哪裡使用這個？	我需要哪些內容？
• ，包括由軟體 NGFW 積分資助的項目	其中一個： ❑ 或 ❑ 或

如果來自您裝置的輸出流量通過 Proxy，請確保您已允許以下 FQDN，才能成功使用 AIOps for NGFW。

要存取 **AIOps for NGFW** 的網域

無論地理區域為何，允許這些網域以存取 AIOps for NGFW 應用程式。

- *.prod.di.paloaltonetworks.cloud
- *.paloaltonetworks.com
- *.prod.di.paloaltonetworks.com
- *.prod.reporting.paloaltonetworks.com
- *.receiver.telemetry.paloaltonetworks.com
- https://storage.googleapis.com

用於傳送遙測資料的 **App-ID** 和網域

請查看 Strata Logging Service 所需的 TCP 通訊埠和 FQDN，以了解您必須在 Palo Alto Networks 防火牆上允許的 App-ID 和通訊埠，以便成功將遙測資料傳送至 AIOps for NGFW。

在您的 Proxy 伺服器上，除了允許所需的 通訊埠和 FQDN，也允許與您的地理區域對應的網域，以便裝置將遙測資料傳送到 AIOps for NGFW。

地區	網域
US	http://br-prd1.us.cdl.paloaltonetworks.com/
歐洲	http://br-prd1.nl.cdl.paloaltonetworks.com/
英國	http://br-prd1.uk.cdl.paloaltonetworks.com/
加拿大	http://br-prd1.ca1.ne1.cdl.paloaltonetworks.com/
新加坡	http://br-prd1.sg1.se1.cdl.paloaltonetworks.com/

地區	網域
日本	http://br-prd1.jp1.ne1.cdl.paloaltonetworks.com/
澳大利亞	http://br-prd1.au1.se1.cdl.paloaltonetworks.com/
德國	http://br-prd1.de1.ew3.cdl.paloaltonetworks.com/
印度	http://br-prd1.in1.as1.cdl.paloaltonetworks.com/

最佳化安全性態勢

我可以在哪裡使用這個？	我需要哪些內容？
• ，包括由軟體 NGFW 積分資助的項目	其中一個： ❑ 或 ❑ 或

除了協助您保持防火牆功能健全之外，AIOps for NGFW 也會協助驗證防火牆是否為您提供針對安全威脅的有效防護。

安全性態勢評估目前不支援多個虛擬系統；設定處理期間僅考慮預設虛擬系統 *(vsys1)*。

- 監控安全性態勢洞察：根據載入 NGFW 裝置的安全性態勢，了解部署的安全狀態和趨勢。
- 監控功能採用：檢視您在部署中使用的安全功能。
- 監控安全性訂閱：檢視建議的雲端交付安全服務 (CDSS) 訂閱，及其在您的裝置中的使用情況。
- 評估弱點：檢視影響特定防火牆和 PAN-OS 版本的弱點，協助您做出是否需要升級的決策。
- 監控合規性摘要：檢視過去 12 個月內進行的安全檢查變更歷史記錄，依照網際網路安全中心 (CIS) 和美國國家標準技術研究所 (NIST) 架構分組。
- 主動強制執行安全檢查：透過封鎖未通過特定最佳做法檢查的提交，針對次優設定採取主動措施。
- 政策分析器：取得分析和建議，以便進行特定政策規則的可能整合或移除，以滿足您預期的安全性態勢，並檢查規則庫中的異常情況，例如陰影、冗餘、一般化、關聯和整合。

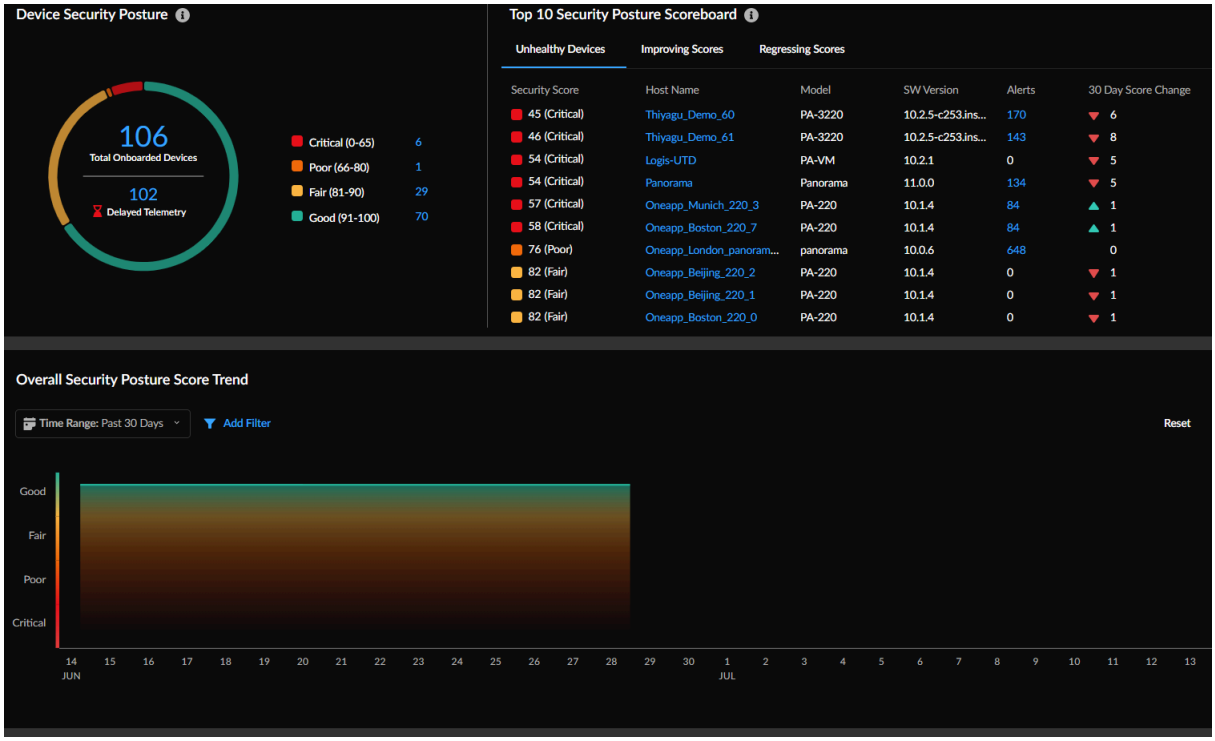
監控安全性態勢洞察

我可以在哪裡使用這個？	我需要哪些內容？

• ，包括由軟體 NGFW 積分資助的項目	• 其中一個：
	  ❑ 或
	  ❑ 或
	• 有權檢視儀表板的角色

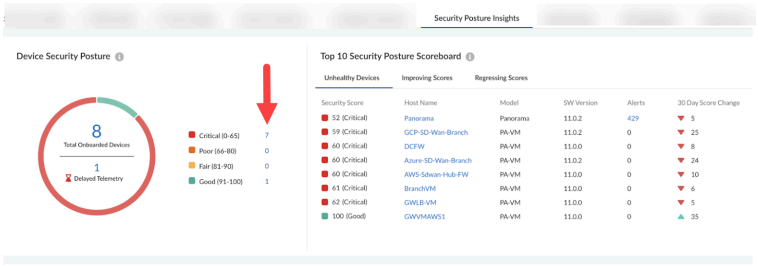
您可以使用 **Security Posture Insights**（安全性態勢洞察）儀表板，根據已載入 NGFW 裝置的安全性態勢，來了解部署的安全狀態和趨勢。安全評分 (0-100) 的嚴重性及其相應的安全等級（良好、一般、差、嚴重）決定了裝置的安全性態勢。安全評分是根據開放警示的優先順序、數量、類型和狀態來計算。

1. 瀏覽至 **Dashboards**（儀表板）> **Security Posture Insights**（安全性態勢洞察）即可開始。



2. 使用 **Device Security Posture**（裝置安全性態勢）檢視裝置的健康狀況。您可以檢視下列內容：
   - 已載入的 NGFW 總數。
   - 超過 12 小時未傳送遙測資料的裝置數量。
   - 部署中載入裝置的安全評分優先順序。按一下數字連結即可了解裝置詳細資料和安全統計資料。

   例如，您可以檢視所有裝置的 7 個嚴重風險。



   在這種情況下，您可以按一下嚴重警示，並查看產生警示的裝置。您可以進一步深入查看，可以看到防火牆上尚未啟用「使用者憑證保護」。您可以在所有裝置上解決此問題，以避免網路釣魚攻擊。

3. 檢查過去 30 天內最不健康且安全評分下降的裝置。您可以檢視裝置的健康狀況，包括其運作狀態、軟體版本和其他重要指標。

   您也可以留意某些裝置是否正在執行過時的軟體版本。在這種情況下，您可以計畫升級到最新推薦版本，您可以透過升級建議找到該版本。

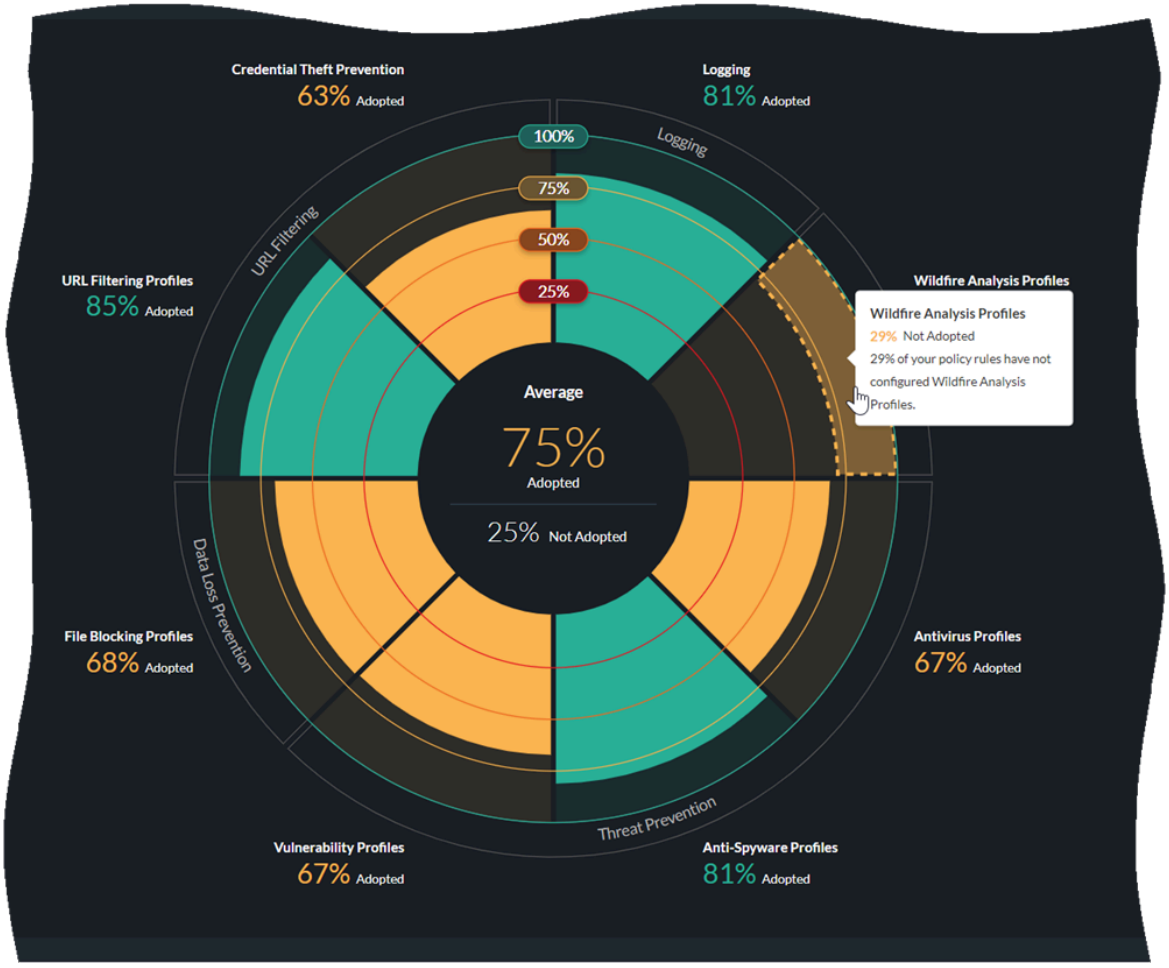
4. 檢查所選時段內部署的安全性態勢趨勢。將滑鼠懸停在觸發點上即可了解計入安全性態勢趨勢的裝置和作用中警示。您可以檢視按主機名稱、型號或軟體版本篩選的一或多個裝置趨勢。

如需更多詳細資訊，請參閱儀表板：安全性態勢洞察。

監控功能採用

我可以在哪裡使用這個？	我需要哪些內容？
• ，包括由軟體 NGFW 積分資助的項目	• 其中一個： ❑ 或 ❑ 或 • 有權檢視儀表板的角色

在 **Dashboards**（儀表板） > **Feature Adoption**（功能採用）中，您可以檢視您在部署使用的安全功能。這有助於您確保能充分利用 Palo Alto Networks 安全訂閱和防火牆的功能。

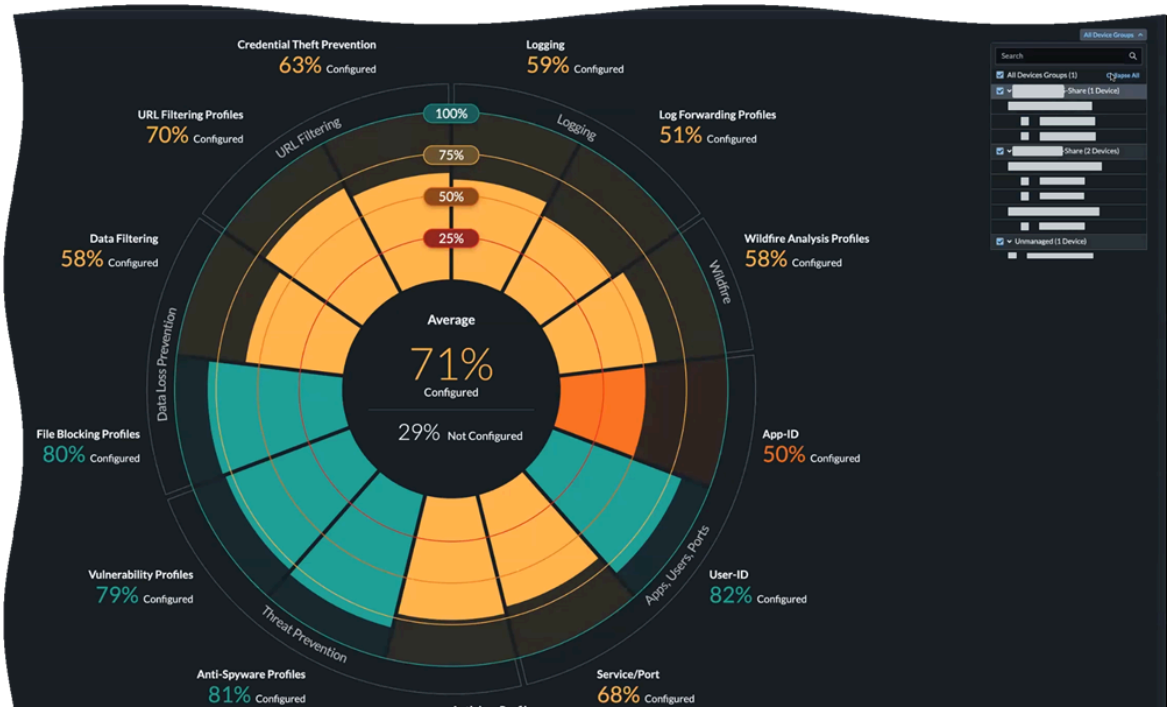


此儀表板顯示安全性政策強大的地方，以及您可以專注於改進的功能採用差距。若要看到最多流量以及獲得最大程度的攻擊保護，請設定安全性功能採用的目標，並使用下列建議作為最佳做法基準線。根據基準來評估您目前的狀態，以識別安全性政策功能採用中的差距。

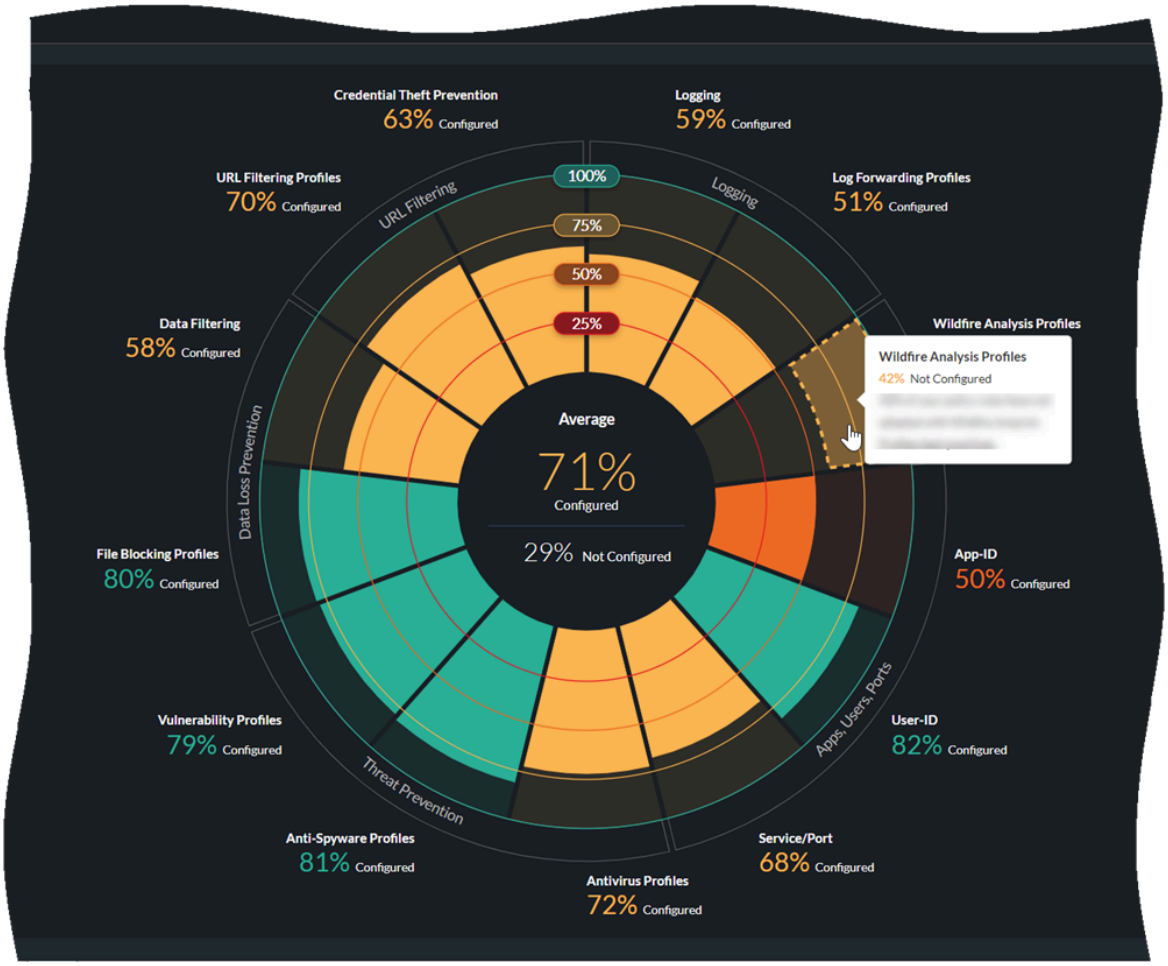
採用摘要有助於識別您可以改善安全性政策功能採用的裝置、區域和領域。您可以依裝置群組、序號和 Vsys、區域、架構區域、標籤、規則詳細資料和區域對應來檢閱採用資訊。在裝置群組上進行篩選，以縮小範圍並識別差距。

在 **Feature Adoption**（功能採用）中，您也可以透過選取 **Best Practices**（最佳做法），來檢視安全功能是否根據 Palo Alto Networks 最佳做法加以設定。

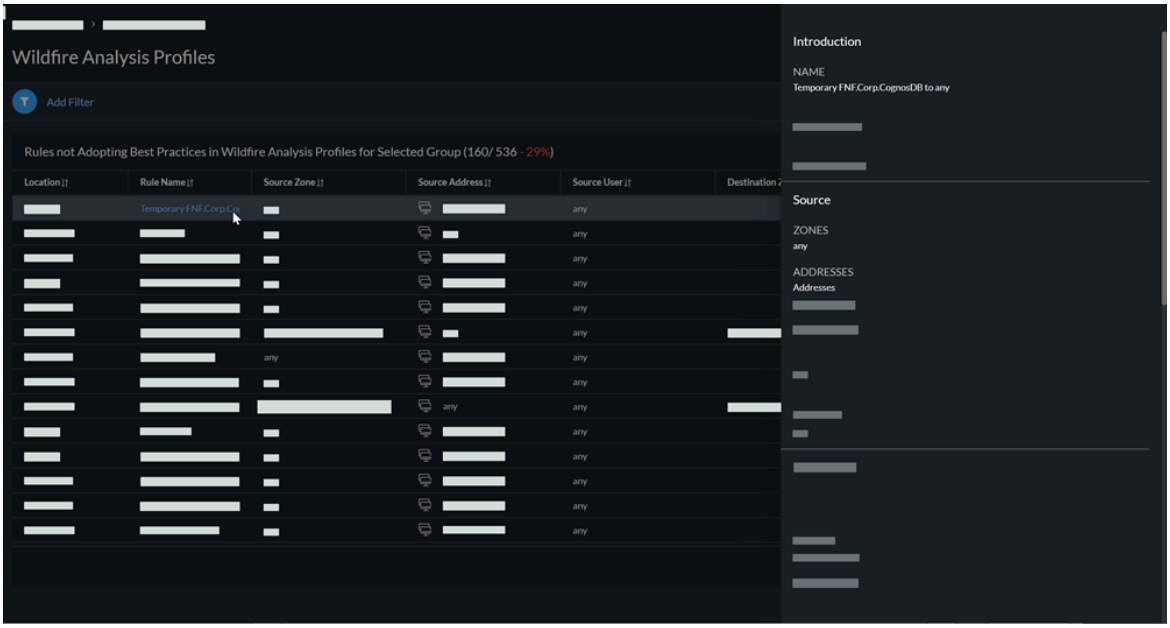
若要專注於特定一組防火牆的最佳做法合規性，您可以根據裝置群組篩選圖表。



選取圖表上某個功能的區段，以檢視有哪些政策規則可以改進。



選取規則即可檢視其詳細資料，而無須離開應用程式。



如需更多詳細資訊，請參閱儀表板：功能採用。

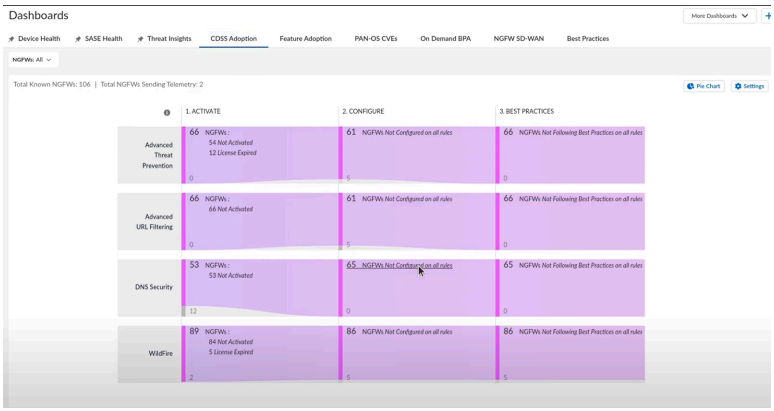
監控安全性訂閱

我可以在哪裡使用這個？	我需要哪些內容？
• ，包括由軟體 NGFW 積分資助的項目	• 其中一個： ❑ 或 ❑ 或 • 有權檢視儀表板的角色

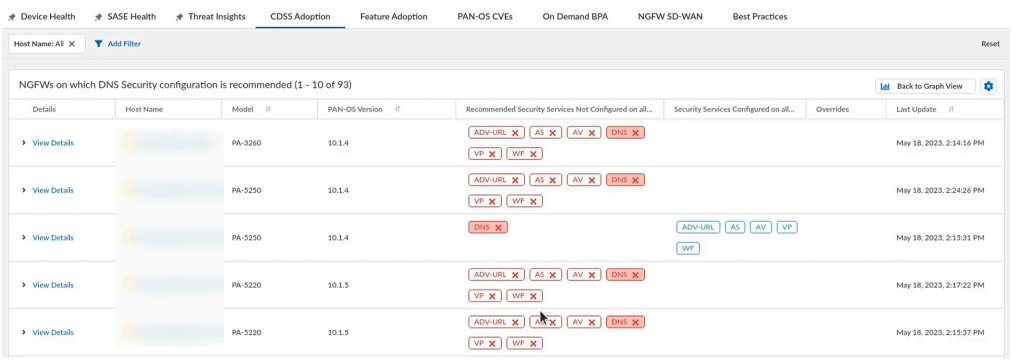
在 **Dashboard**（儀表板） > **Posture**（態勢） > **CDSS Adoption**（**CDSS** 採用）中，您可以檢視建議的雲端交付安全服務 (CDSS) 訂閱及其在裝置中的使用情況。這有助於您識別安全性差距，並加強企業的安全性態勢。瀏覽至此頁面後，您會看到一個快顯視窗，要求您確認或更新 NGFW 中的區域角色，以取得正確的安全服務建議。您可以按照此快顯視窗中的連結，將區域對應至角色。

目前，此儀表板僅支援四個安全性訂閱：進階威脅防護、進階 *URL* 篩選、*DNS* 安全性和 *Wildfire*。

1. 在 **CDSS Adoption**（**CDSS** 採用）頁面頂端，您可以檢視已知 NGFW 的總數，以及在您的執行個體中傳送遙測的 NGFW 數目。
2. 採用 CDSS 的過程需要啟動、設定和遵守最佳做法。要追蹤每個訂閱的進度，只需按一下圖表中的數字，即可檢視在此過程中需要更新的裝置清單。在這種情況下，需要檢查未設定 DNS 安全性的 NGFW。



3. 檢查已建議但未設定 DNS 安全性組態的 NGFW。**View details**（檢視詳細資料）以檢查來源角色和目的地角色。

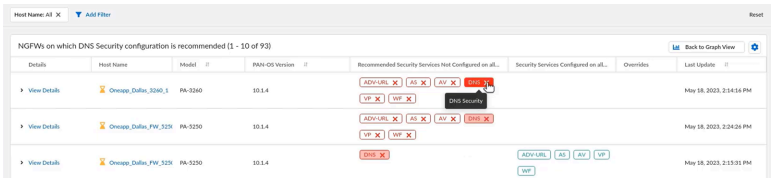


4. **View Policies**（檢視政策）以檢視規則的詳細資料，以及對應來源和目的地區域。

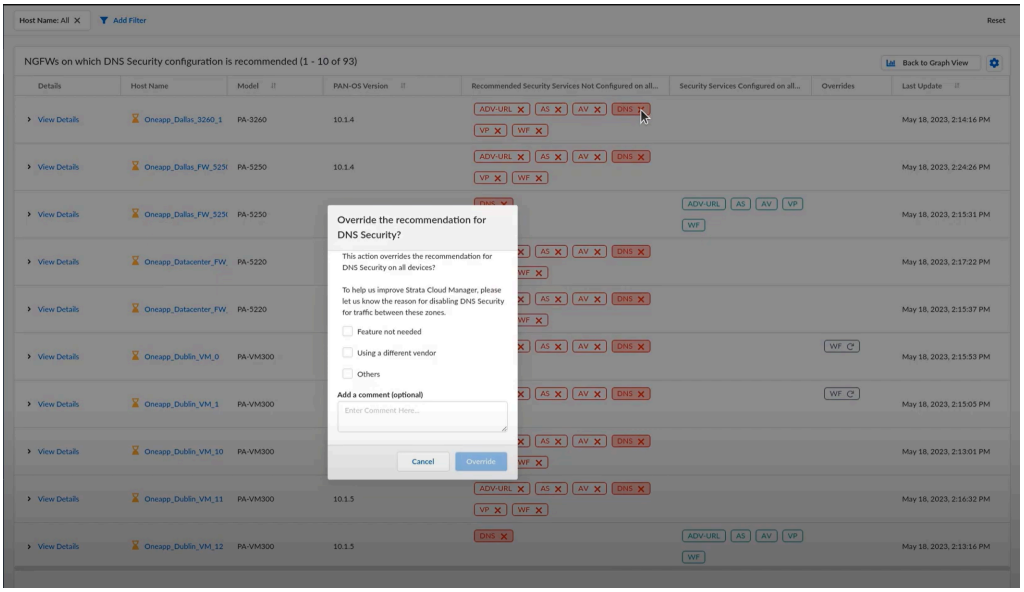
   此外，您可以按一下規則名稱以檢視其詳細資料。

5. 導覽回到漏斗圖。您也可以透過圓餅圖格式檢視相同的資訊。

6. 當您基於任何原因不需要建議的安全服務時，即可加以取代。在這種情況下，我們不需要 DNS 安全服務。按一下 **DNS** 旁邊的取消圖示。



7. 選取取代建議的其中一個原因。



8. 按一下 **Override**（取代）。

   這會總結如何檢視建議的 CDSS 訂閱及其在您的裝置中的使用情況。

如需更多詳細資訊，請參閱儀表板：CDSS 採用。

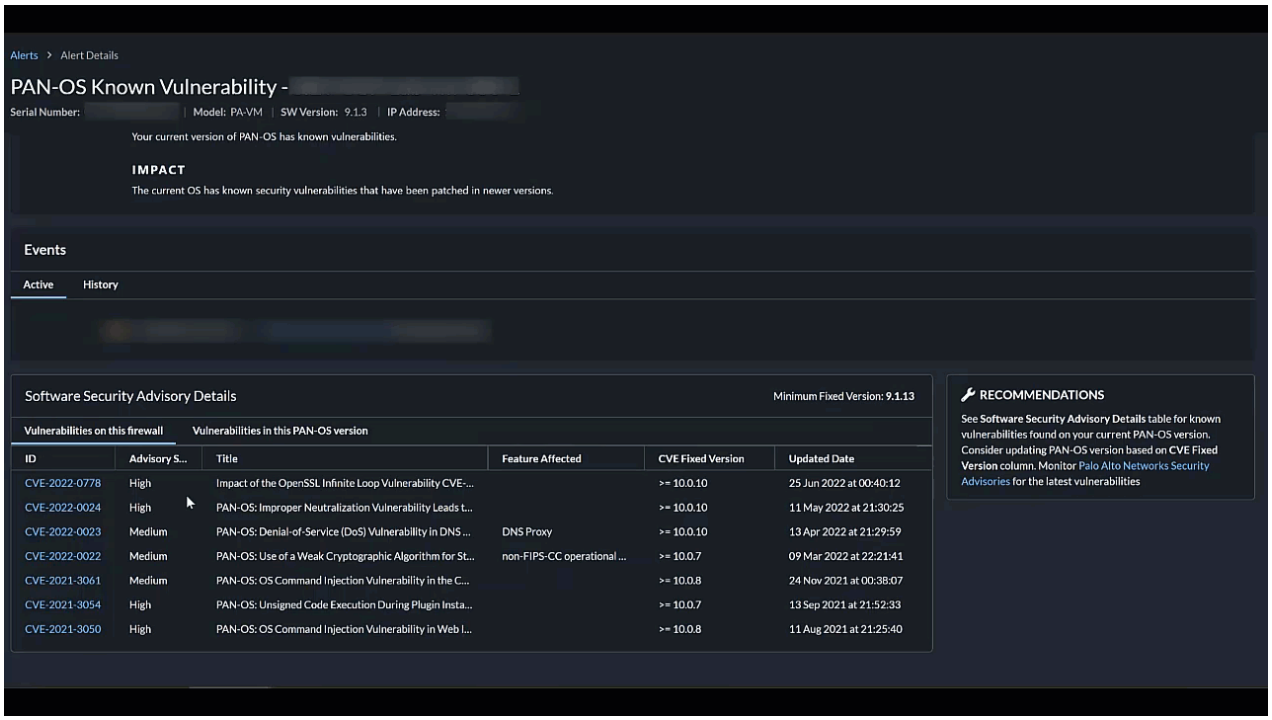
評估弱點

我可以在哪裡使用這個？	我需要哪些內容？
• ，包括由軟體 NGFW 積分資助的項目	其中一個： ❑ 或 ❑ 或

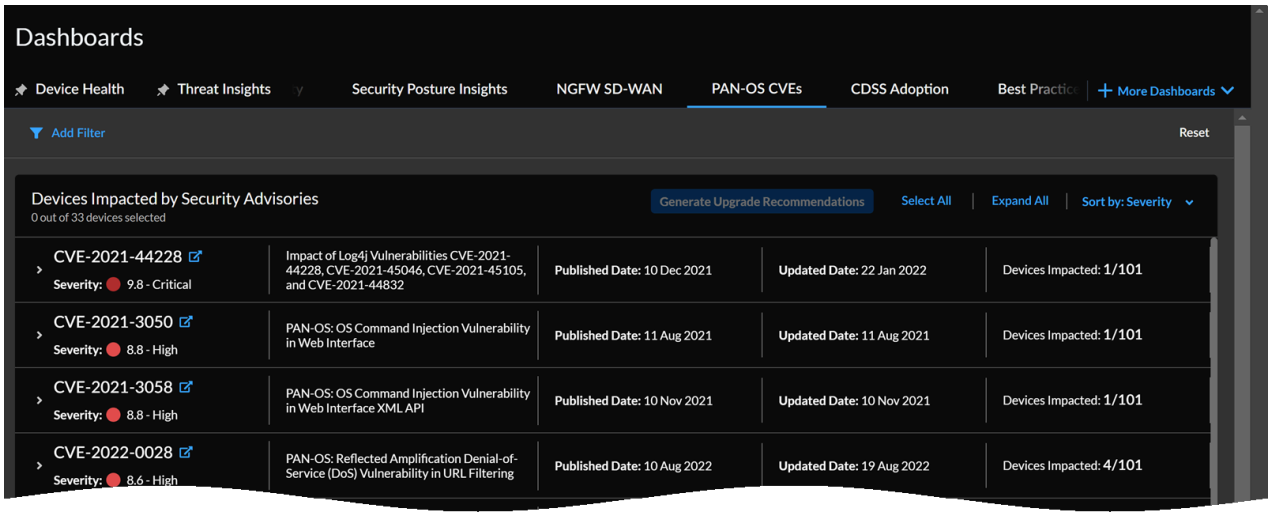
Strata Cloud Manager 會顯示哪些弱點會影響指定防火牆和 PAN-OS 版本，以協助您決定是否應該升級。瀏覽至 **Incidents & Alerts**（事件和警示）> **NGFW** > **All Alerts**（所有警示），並選取 **PAN-OS Known Vulnerability**（**PAN-OS** 已知弱點）警示，來查看產生警示且影響防火牆的最新安全諮詢。

選取 **Vulnerabilities in this PAN-OS version**（此 **PAN-OS** 版本中的弱點），以在 **Feature Affected**（受影響的功能）欄中，檢視弱點的影響功能。這可協助您根據弱點及其對啟用功能的影響，決定是否升級防火牆。如果 CVE 未與功能相關聯，則 **Feature Affected**（受影響的功能）下的值為空白。此類型的 CVE 會影響具有指定模型或版本的防火牆。

依預設，**PAN-OS Known Vulnerability**（**PAN-OS** 已知弱點）警示會顯示裝置上 PAN-OS 版本中的所有弱點。不過，如果您在防火牆上啟用「產品使用情況」遙測，您可以選擇僅根據其啟用的功能，檢視影響特定防火牆的弱點。這樣您可以進一步了解哪些弱點會影響到防火牆，並針對是否升級做出更明智的決定。



您也可以使用 **PAN-OS CVEs** 儀表板，該儀表板會根據裝置啟用的功能，顯示受特定弱點影響的裝置數目。Strata Cloud Manager 會分析已啟用的功能，以判斷受 CVE 影響的裝置。下列工作會顯示如何評估影響裝置的弱點，並產生升級建議以修正這些弱點。



此工作會顯示如何評估影響裝置的弱點，並產生升級建議以修正這些弱點。

STEP 1 | 從 Strata Cloud Manager 瀏覽至 **Dashboards**（儀表板）> **PAN-OS CVEs**。

STEP 2 | 展開 CVE 以檢視受影響的裝置。

STEP 3 | 選取您要升級的裝置以修正弱點。

STEP 4 | **Generate Upgrade Recommendations**（產生升級建議）。

STEP 5 | 按一下裝置的新產生報告。

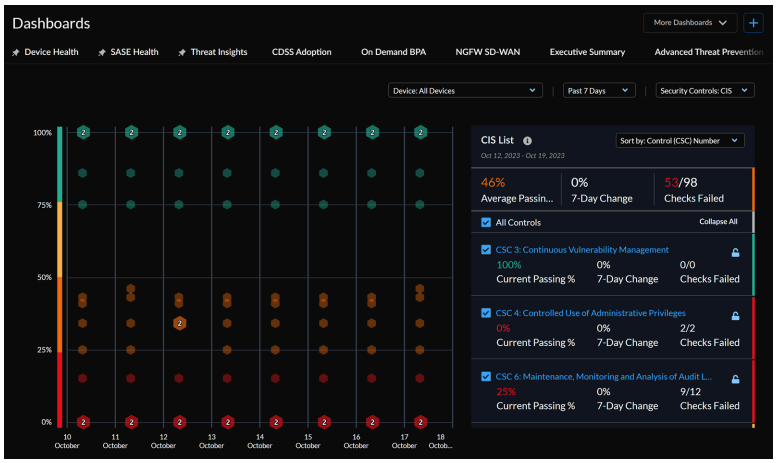
STEP 6 | 選取其中一個升級選項以檢視有關 **New Features**（新功能)、**PAN-OS Known Vulnerabilities**（**PAN-OS** 已知弱點）、**Changes of Behavior**（行為變更）和 **PAN-OS Known Issues**（**PAN-OS** 已知問題）的詳細資料

您可以在 CSV 檔案中 **Export**（匯出）詳細資料並加以下載。

監控合規性摘要

我可以在哪裡使用這個？	我需要哪些內容？
• ，包括由軟體 NGFW 積分資助的項目	❑ 或 ❑ 在儀表板中檢視受支援產品資料的授權：Prisma Access

若要存取合規摘要儀表板，請移至 **Dashboards**（儀表板），然後選取 **Compliance Summary**（合規摘要）頁籤。您可以檢視過去最多 12 個月的安全檢查變更歷史記錄，這些變更依照 Center for Internet Security (CIS) 和美國國家標準技術研究所 (NIST) 架構分組。對於每個架構，您都會看到一個控制清單，以及目前和平均合規率的百分比、最佳做法檢查的總數，以及每個控制的失敗檢查數目。與圖表和清單互動，以查看控制與其歷史統計資料之間的關係。檢視個別控制項和相關聯檢查的詳細資料，並選取最佳做法檢查，以檢視未通過檢查的防火牆設定。**CIS** 重大安全性控制架構是一組優先的建議操作和最佳做法，可協助保護組織及其資料免受已知網路攻擊媒介的侵害。



您可以檢視 11 個基本和基礎 CIS 控制（共 16 個）的檢查摘要：

- CSC 3：持續的弱點管理
- CSC 4：控制管理權限的使用
- CSC 6：稽核日誌的維護、監控和分析
- CSC 7：電子郵件和 Web 瀏覽器保護
- CSC 8：惡意軟體防禦
- CSC 9：限制和控制網路連接埠、通訊協定和服務
- CSC 11：網路裝置（如防火牆、路由器和交換機）的安全設定
- CSC 12：邊界防禦
- CSC 13：資料保護
- CSC 14：根據須知事項控制存取
- CSC 16：帳戶監控和控制

NIST Cybersecurity Framework SP 800-53 控制架構提供了聯邦政府機構和其他組織為其資訊系統實作及維護安全與隱私控制的相關指引。您可以檢視 8 個 NIST 控制系列的檢查摘要：

- SC：存取控制
- AU：稽核和責任
- CM：設定管理
- CP：應變規劃
- IA：身份識別與驗證
- RA：風險評估
- SC：系統和通訊保護
- SI：系統和資訊完整性

如需更多詳細資訊，請參閱儀表板：合規性摘要 。

主動強制執行安全檢查

我可以在哪裡使用這個？	我需要哪些內容？
• ，包括由軟體 NGFW 積分資助的項目	❑ 或

您可以使用以下功能，為您的部署自訂安全性態勢檢查，以最佳化相關建議。

- 安全檢查

  AIOps for NGFW 用於評估設定的最佳做法檢查清單。將防火牆和 Panorama 的設定與 Palo Alto Networks 最佳做法檢查進行比較，以評估裝置的安全性態勢，並產生安全警示。您可以查看用於評估設定的最佳做法檢查清單。

  在這裡，您可以：

  1. 設定檢查的嚴重性等級以識別對您部署而言最重要的檢查。
  2. 暫時停用檢查。

     如果您選擇停用某項檢查，您可以指定將會保持停用的時間，並留下註解，解釋停用原因。
  3. 設定檢查失敗時的回應。
- 區域到角色的對應

  將 NGFW 中的區域對應到角色，以獲得自訂建議。
- 角色到安全服務的對應

  管理所有 NGFW 中，區域和角色之間的流量所需的安全服務。

Panorama CloudConnector 外掛程式可讓您透過封鎖未通過特定最佳做法檢查的提交，來針對次優設定採取主動措施。當您在 AIOps for NGFW 指出，您想要檢查 **Fail Commit**（提交失敗）時，Panorama 會自動封鎖未通過該檢查的任何設定提交。與其等待收到有關最佳做法檢查失敗的警示，不如使用外掛程式，先將設定問題排除在部署之外。

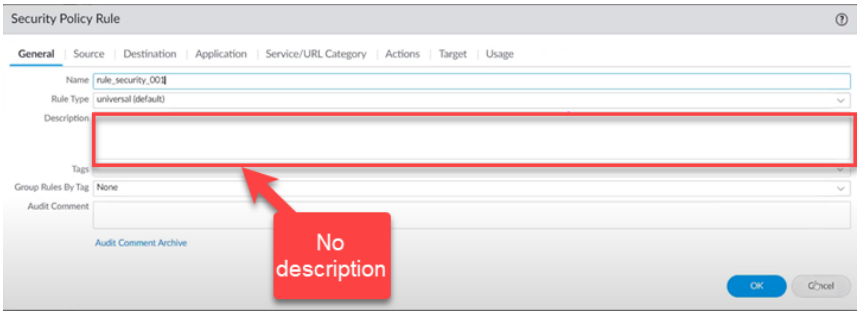
STEP 1 | 確保您滿足所有先決條件，然後安裝該外掛程式。

STEP 2 | 指定將在失敗時封鎖提交的最佳做法檢查。

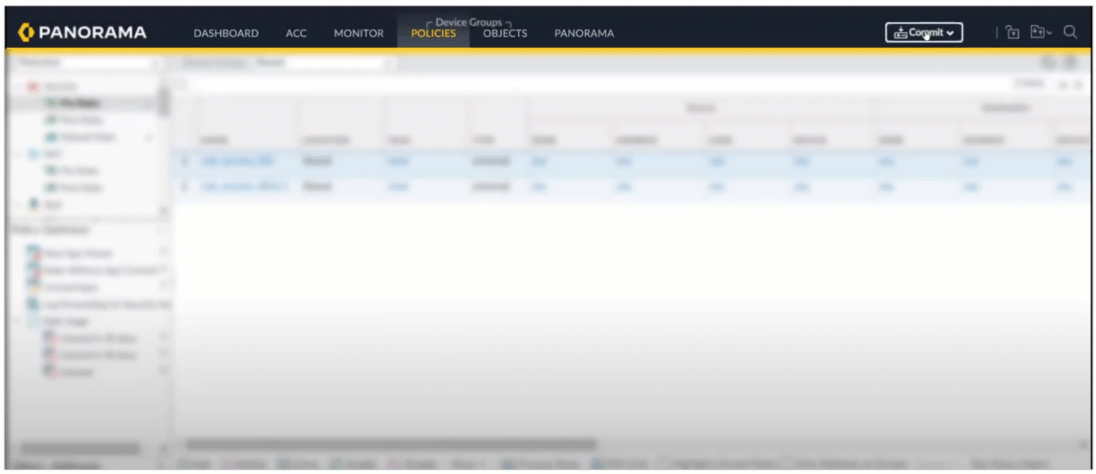
1. 選取 **Manage**（管理） > **Security Posture**（安全性態勢） > **Settings**（設定）。
2. 找到您想要封鎖提交的檢查。
3. 將 **Action on Fail**（失敗的動作）設定到 **Fail Commit**（提交失敗）。

STEP 3 | 透過嘗試提交未通過檢查的設定進行驗證。

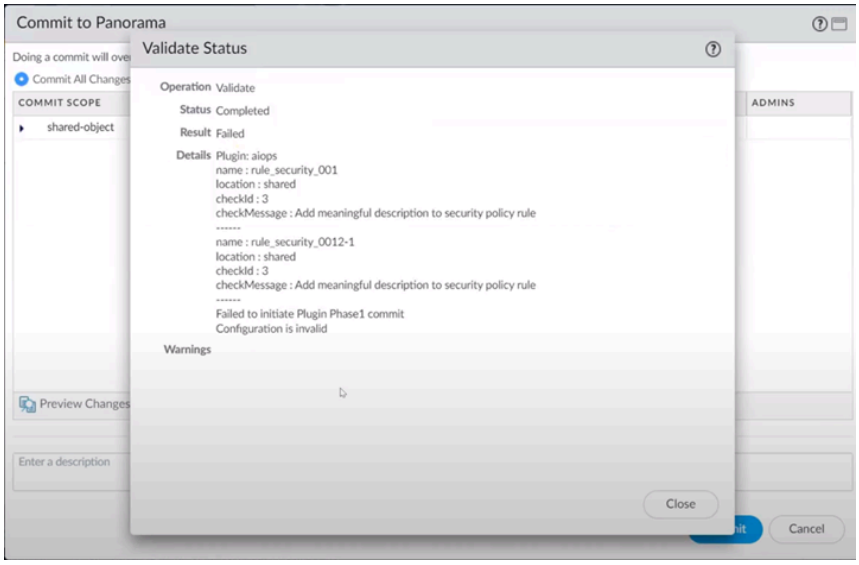
1. 登入 Panorama。
2. 違反了您指定為 **Fail Commit**（提交失敗）的最佳做法檢查。



3. 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**） > **Validate Configuration**（驗證設定）。



您應該會看到一個對話，指出驗證失敗，因為設定未通過最佳做法檢查。



將檢查設定為 ***Fail Commit***（提交失敗）會導致驗證和實際提交操作的檢查失敗。

查看 管理：安全性態勢設定，以了解更多資訊。

政策分析器

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW（Panorama 管理） • （Panorama 管理） •	❑ 或 ❑ 用於 Panorama 管理部署的Panorama CloudConnector 外掛程式

安全性政策規則的更新通常具有時效，需要您快速採取行動。但是，您需要確保對安全性政策規則庫所做的任何更新都符合您的需求，並且不會產生錯誤或設定有誤（例如導致規則重複或衝突的變更）。

Strata Cloud Manager 中的政策分析器可讓您在實施變更要求時，最佳化時間和資源。政策分析器不僅會分析並提供可能的合併或移除特定規則的建議，以滿足您的意圖，還會檢查規則庫中的異常情況，例如陰影、冗餘、一般化、相關性和合併。

使用政策分析器，來新增或最佳化您的安全性政策規則庫。

- 新增規則之前 - 請檢查是否需要新增規則。政策分析器會建議如何最好地變更現有的安全性政策規則，以滿足您的要求，且無需新增其他規則（如果可行的話）。
- 簡化和最佳化現有的規則庫 - 查看您可以在哪裡更新規則，以盡可能減少內容膨脹和消除衝突，並確保流量強制執行符合安全性政策規則庫的意圖。

在提交變更之前和之後，分析您的安全性政策規則。

- 變更前的政策分析- 使您能夠評估新規則的影響，並根據現有規則分析新規則的意圖，以建議如何最好地滿足意圖。
- 變更後的政策分析- 使您能夠透過識別隨時間累積的影子、冗餘和其他異常，來清理現有的規則庫。

- 政策分析器需要在您的 *Panorama* 設備上安裝 CloudConnector 外掛程式 *1.1.0* 或更高版本。您需要使用以下命令啟用此外掛程式：

  ```
  > 要求外掛程式 cloudconnector 啟用基本功能
  ```

- 政策分析器要求 *Panorama* 必須更新到 *PAN-OS* 版本 *10.2.3* 或更高版本。

政策分析器偵測到的異常類型

政策分析器可偵測安全性政策規則庫中以下類型的異常：

- 影子 - 由於規則庫中較高層級的規則會覆蓋相同流量，因此而未命中的規則。

  安全性政策規則會在規則庫中從上到下進行評估，因此當規則庫中較高的規則符合較低規則的相同流量，以便透過不同的動作設定相符項目和規則時，就會建立陰影。如果您按順序移除較低的規則，安全性政策不會變更。
- 冗餘 - 符合相同流量，並且透過相同動作設定的兩個以上規則。

- 一般化 - 當規則庫中較低的規則與規則庫中較高規則的流量相符（而非相反情況）時，規則將採取不同的操作。如果兩個政策規則的順序顛倒，則安全性政策會受到影響。
- 關聯 - 當一個規則與另一個規則的某些封包相符，但導致不同的操作時，與另一個規則關聯的規則。如果兩個規則的順序顛倒，安全性政策就會受到影響。
- 合併 - 您可以將這些規則合併為單一規則，因為操作相同且只有一個屬性不同。您可以透過修改其中一個規則的屬性並刪除其他規則，來將規則合併為單一規則。

變更前政策分析

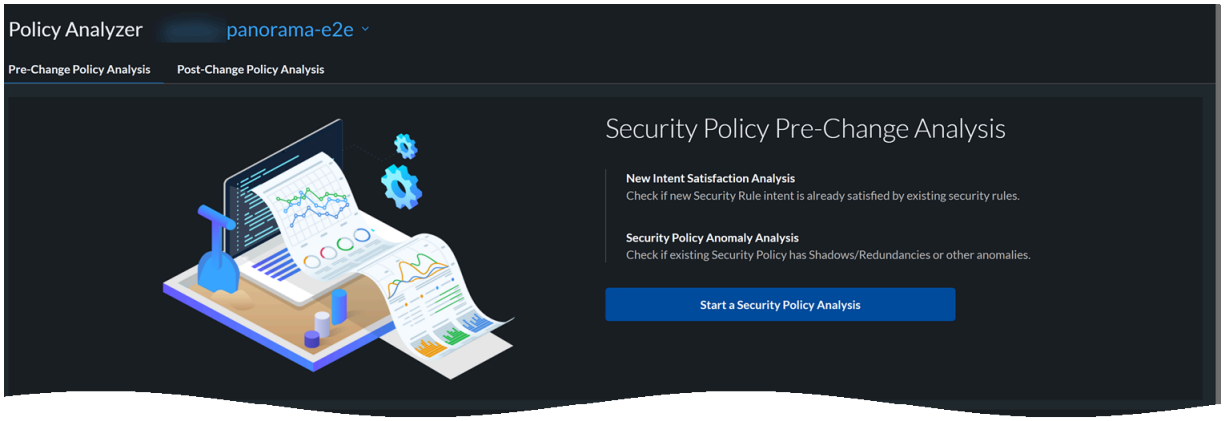
我可以在哪裡使用這個？	我需要哪些內容？
• NGFW（Panorama 管理） • （Panorama 管理） •	❑ 或 ❑ 用於 Panorama 管理部署的Panorama CloudConnector 外掛程式

安全性政策規則變更前分析會執行新的意圖滿意度分析：

- 新的意圖滿意度分析 - 檢查現有規則是否已覆蓋新的安全性政策規則意圖。

開始之前：

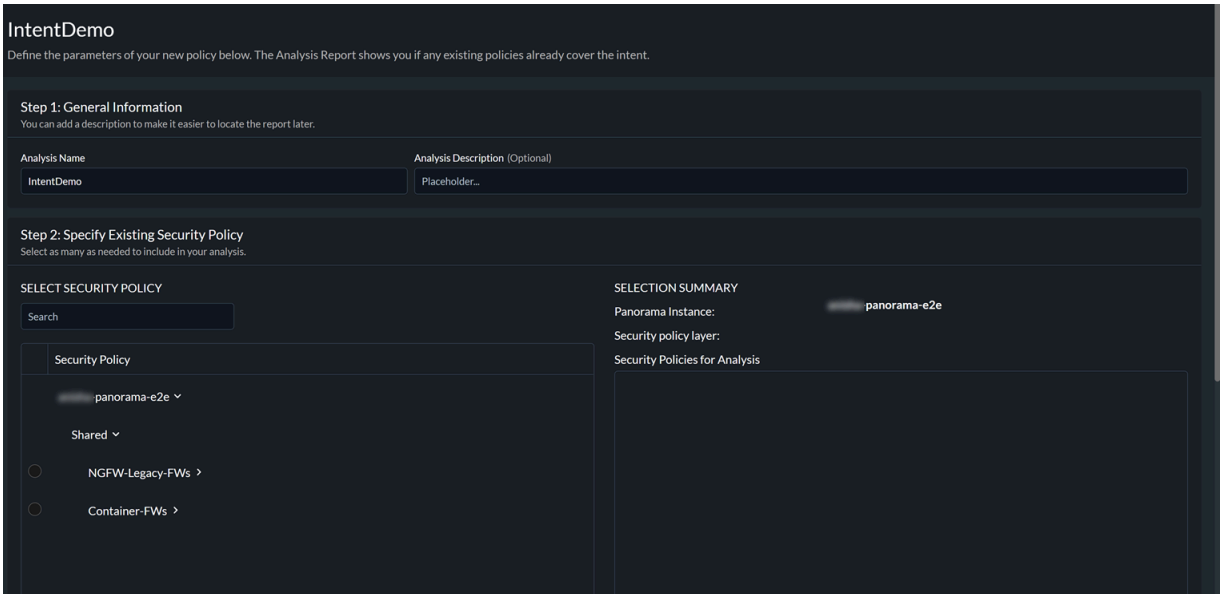
1. 前往 **Manage**（管理） > **Security Posture**（安全性態勢） > **Policy Analyzer**（政策分析器） > **Pre-change Policy Analysis**（變更前政策分析）。
2. 在 [Policy Analyzer（政策分析器）] 頁面頂部，選取包含您需要分析之政策規則的 Panorama 執行個體。



3. 開始安全性政策分析。

執行以下步驟以開始新的分析：

STEP 1 | 進入 **Analysis Name**（分析名稱）和 **Analysis Description**（分析描述）。



在 Panorama 設備上，裝置群組是分層的。您可以建立四個層級的裝置群組，並將 NGFW 指派給階層中層級最低的裝置群組。您在更高層級建立的政策將由其下的所有裝置群組繼承。

您可以針對已直接指派 NGFW 的最多 10 個裝置群組執行分析，這樣您就可以分析推送到已直接指派 NGFW 集的所有政策規則。

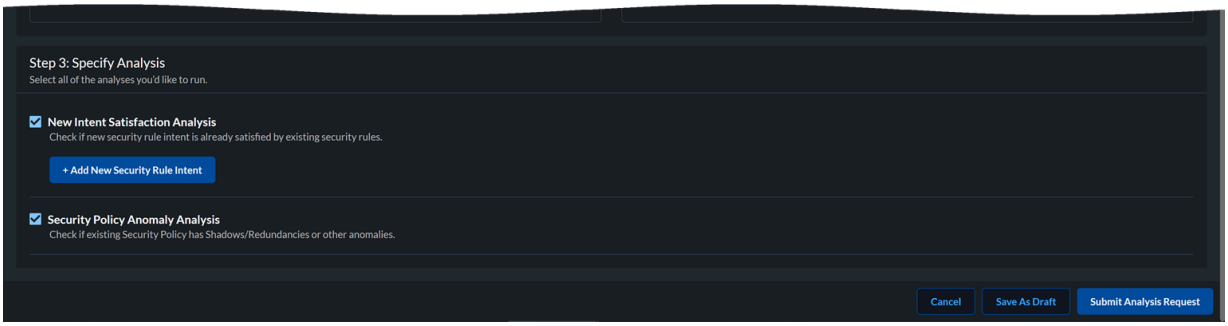
STEP 2 | 選取要分析的現有安全性政策。

每次分析最多可以選取 10 個裝置群組。

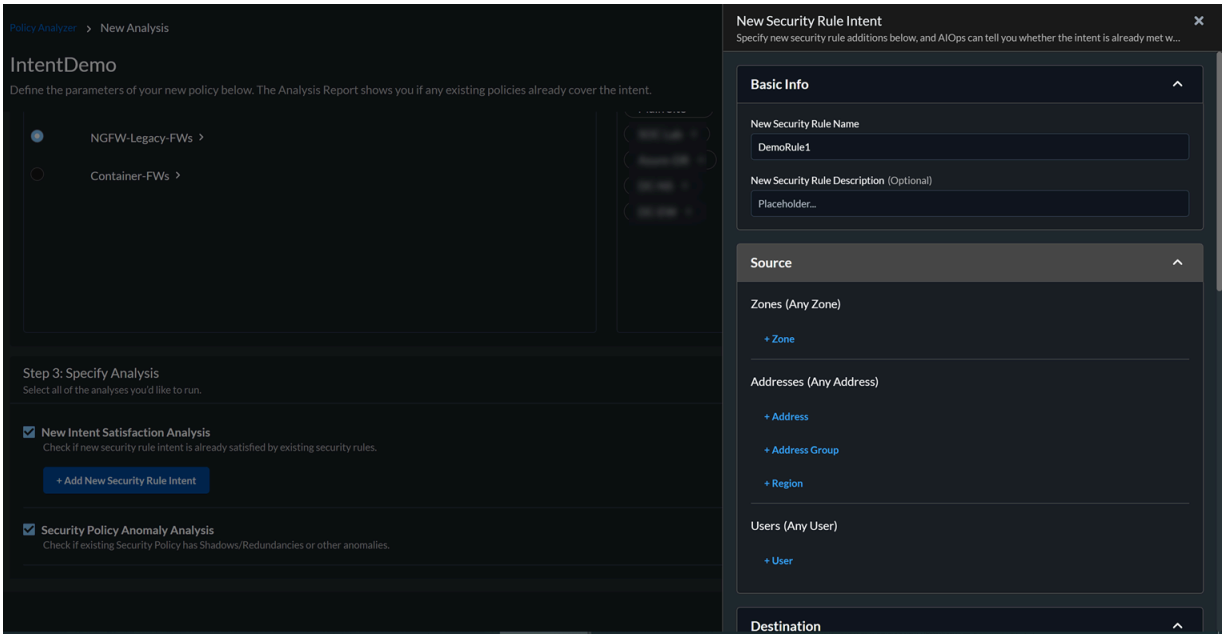
STEP 3 | 透過選取一或多個分析類型，來指定分析類型：

- 新的意圖滿意度分析

新增安全性規則意圖進行分析。



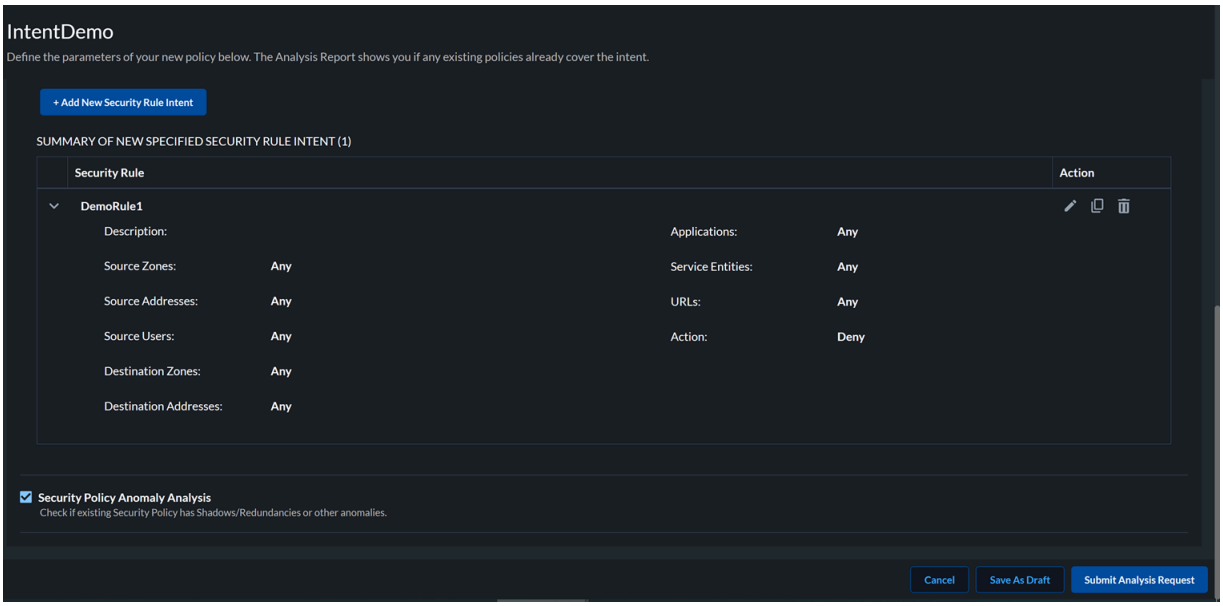
指定有關新安全規則的資訊，AIOps for NGFW 可以檢查現有規則是否涵蓋意圖。



輸入安全性政策規則的元件值。與安全規則相關的欄位預設值為「Any（任何）」。

Save（儲存）設定。

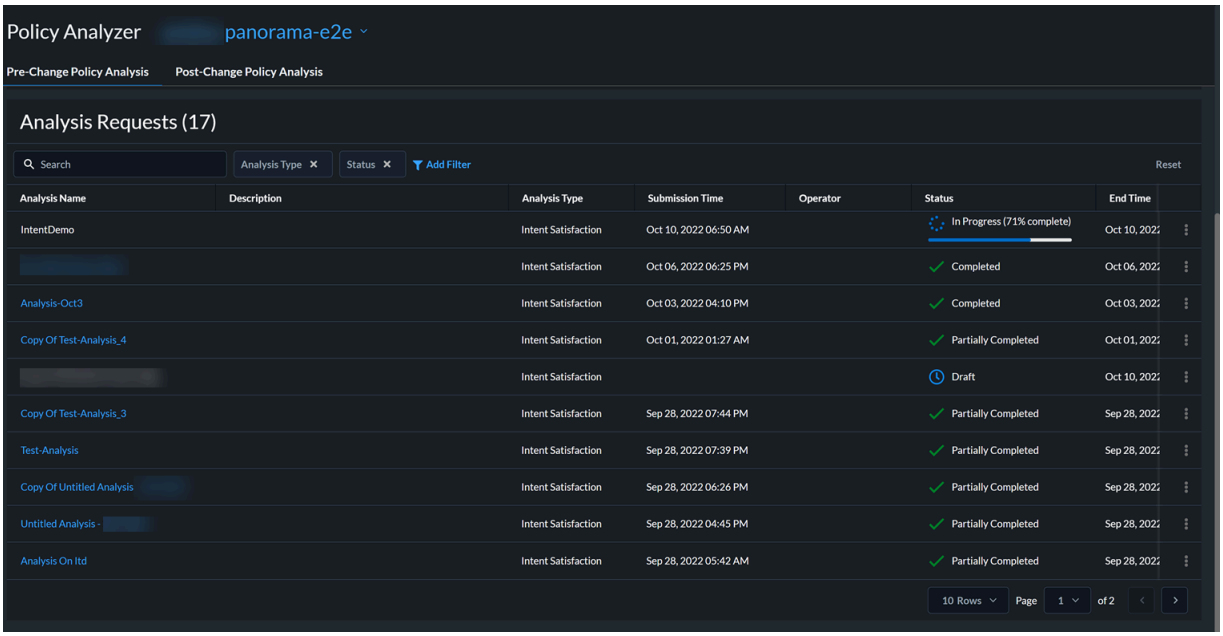
查看新安全規則意圖的摘要。



您最多可以建立 10 個新的安全規則，也可以複製規則並進行編輯。

STEP 4 | **Submit Analysis Request or Save As Draft**（提交分析要求或另存為草稿），以在稍後編輯規則。

在 [Policy Analyzer（政策分析器）] 頁面的 [Analysis Requests（分析要求）] 下檢視分析狀態。



您可以取消狀態為進行中的規則，該規則將顯示為「已取消」。

分析完成後，檢視分析報告。

變更前的政策分析報告

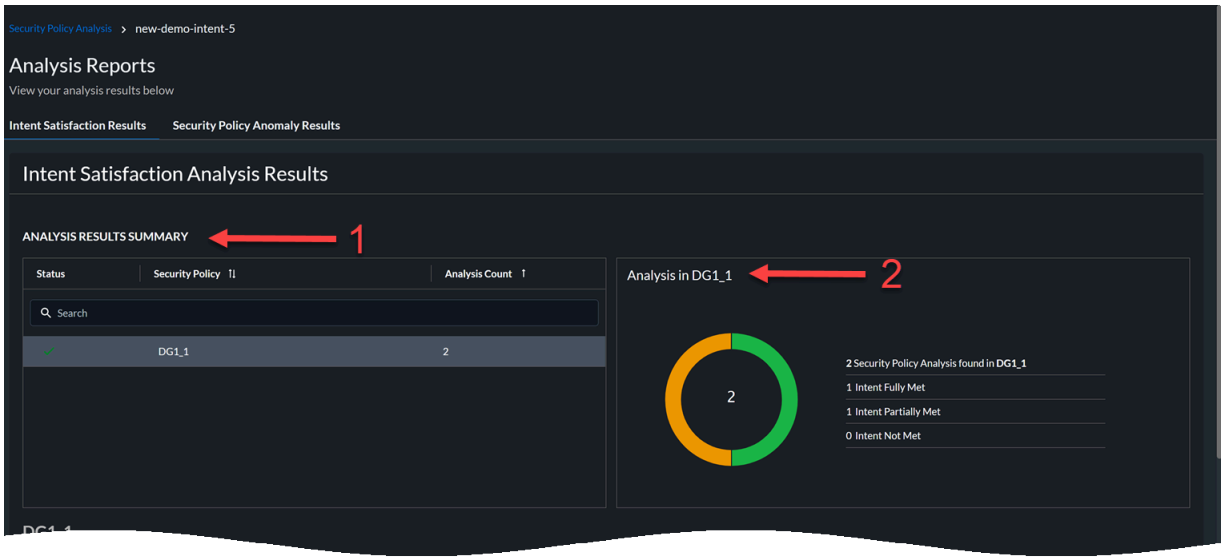
我可以在哪裡使用這個？	我需要哪些內容？
• NGFW（Panorama 管理） • （Panorama 管理） •	❑ 或 ❑ 用於 Panorama 管理部署的Panorama CloudConnector 外掛程式

選取狀態為已完成的分析報告，以檢視政策分析結果。您可以檢視分析結果。

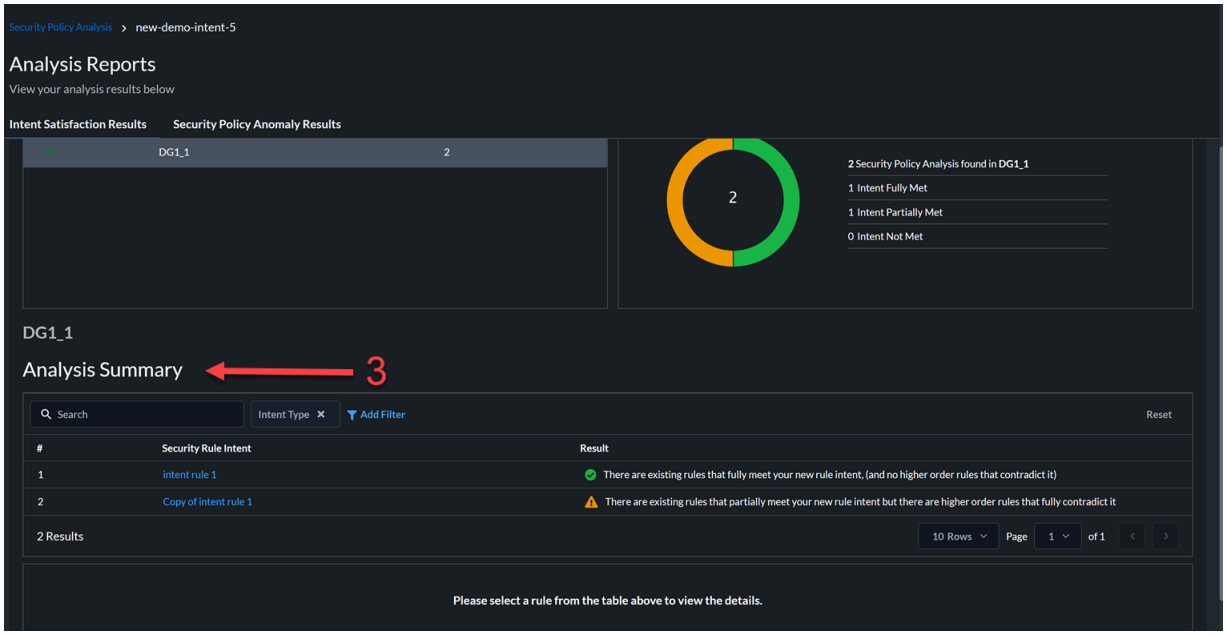
意圖滿意度結果

從 [Analysis Requests（分析要求）] 下的分析清單中，按一下分析以檢視其分析結果。這些結果包括：

1. 分析摘要，包含有關裝置群組和異常計數的詳細資料。
2. 按一下裝置群組名稱，以檢視意圖滿意度分析結果：
   - Intent Fully Met（完全滿足意圖）– 您的安全規則是裝置群組中其中一個現有規則的副本。
   - Intent Partially Met（部分滿足意圖）– 您的安全規則部分滿足裝置群組中其中一個現有規則的意圖。
   - Intent not met（未滿足意圖）- 您的安全規則是裝置群組中不存在的唯一規則。您可以將此規則新增至裝置群組。

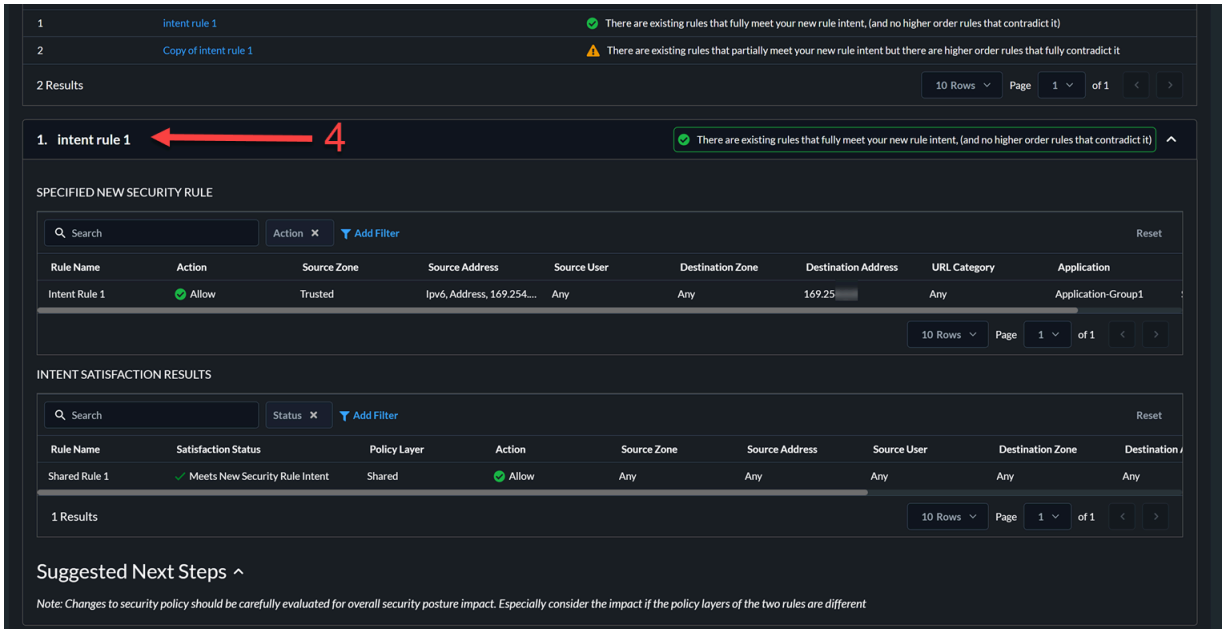


3. 檢視新安全規則意圖的分析結果。



在此範例中，有兩個規則。第一個規則的意圖與現有規則完全相符，第二個規則的意圖與現有規則部分相符。

4. 檢視新安全規則的詳細資料，並檢查意圖滿意度結果。



在此範例中，新規則意圖規則 1 的所有屬性都與現有規則「共用規則 1」的屬性相符。新規則的意圖與現有規則的意圖完全相符。因此，您無需將此新規則新增到設定中。

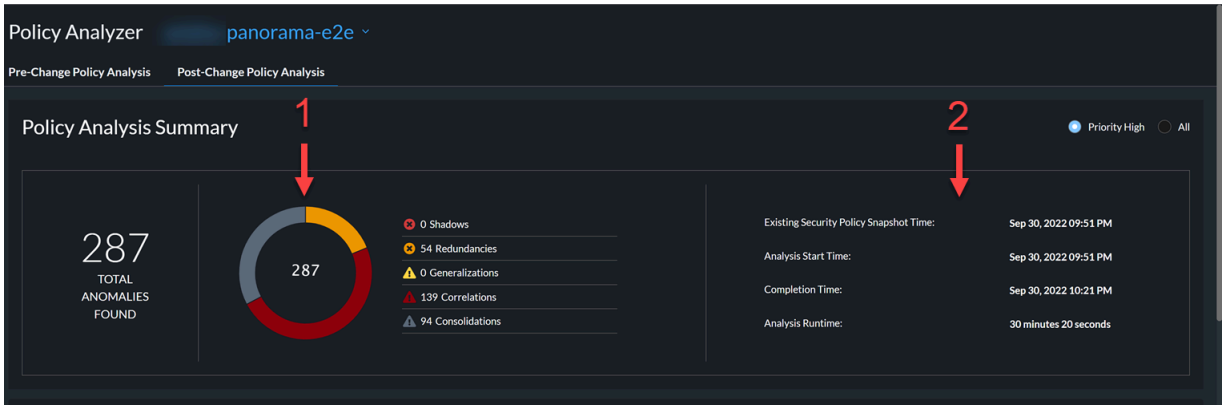
變更後政策分析

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW（Panorama 管理） • （Panorama 管理） •	❑ 或 ❑ 用於 Panorama 管理部署的Panorama CloudConnector 外掛程式

當您在 Panorama 上提交設定時，可以透過 Strata Cloud Manager 外掛程式進行分析。政策分析器會分析影子、冗餘和其他異常的這項設定，結果可在 **Manage**（管理） > **Security Posture**（安全性態勢） > **Policy Analyzer**（政策分析器） > **Post-change Policy Analysis**（變更後政策分析）中提供審閱。

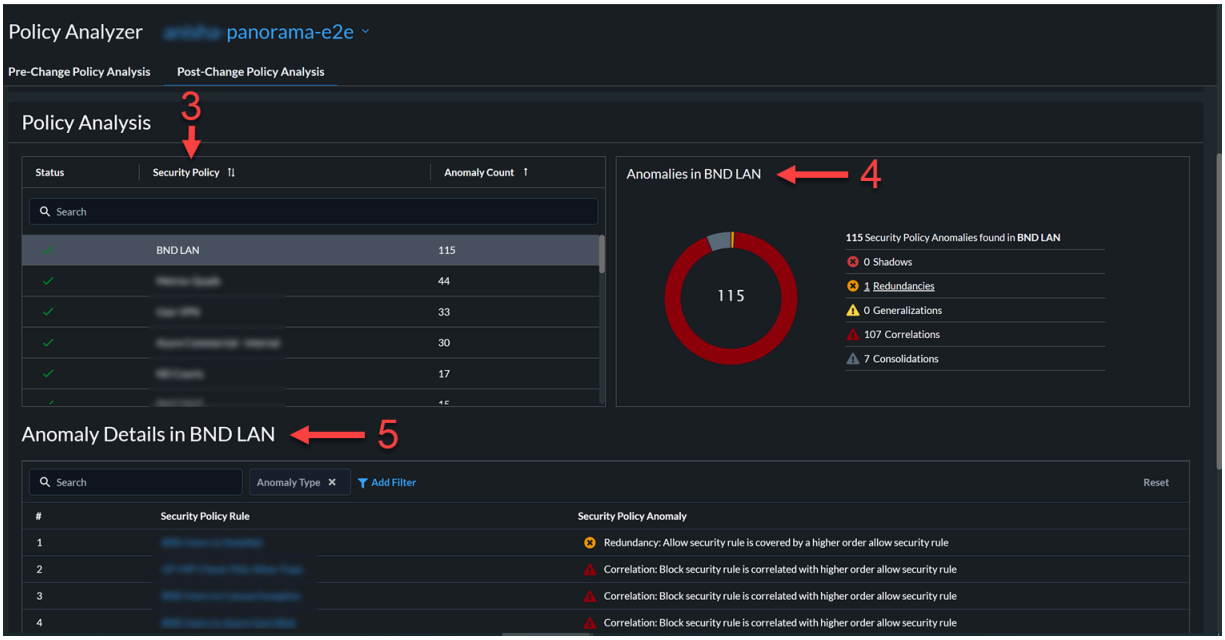
您可以檢視以下資訊：

1. 顯示所有政策集（即直接指派 NGFW 的所有裝置群組）的分析摘要。您可以檢視異常或基於高優先順序的異常情況。此報告中的值顯示在所有裝置群組中發現的唯一異常數量。圖表中的顏色表示不同類型的異常。

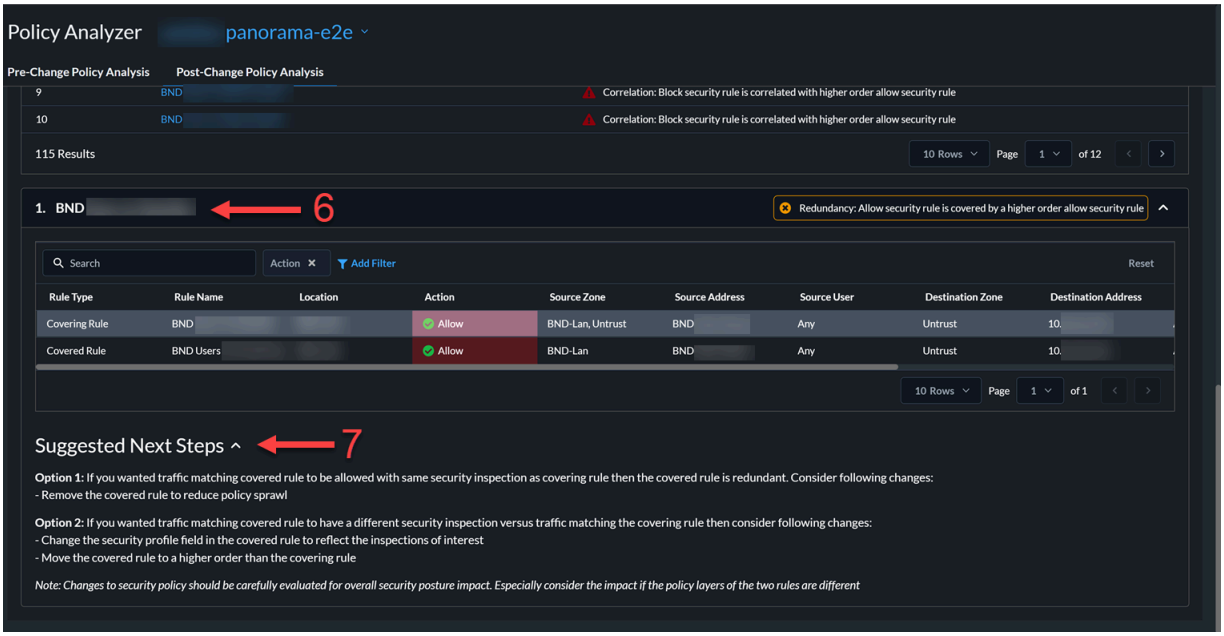


2. 用於分析的時間戳記，包括：
   - 現有安全性政策快照 - 提交後將設定標記為在 Panorama 中執行的時間戳記。
   - 時間分析開始
   - 時間分析完成
   - 完成分析所需的時間
3. 檢視安全性政策的狀態，以及每個政策的異常數量。
4. 檢視所選安全性政策的異常細項。

5. 檢視安全性政策中每個規則的異常詳細資料。



6. 檢視所選規則的屬性，以及異常的詳細資料。



此圖片顯示了冗餘異常的範例。在此範例中，BND 規則已被另一個 BND 使用者規則覆寫。因此，您可以移除 BND 規則。

7. 檢視修復異常的建議後續步驟。

NGFW 健康和軟體管理

本章介紹如何管理 NGFW 健康狀況和軟體升級。

- 檢視裝置健康情況 - 根據已載入的 NGFW 運作狀況評分，檢視部署的累積運作狀況和效能。
- 升級建議 - 建立建議以確定最適合您裝置且可升級的軟體版本。
- 分析指標容量 - 根據裝置的型號類型持續追蹤指標使用情況，藉此分析並監控裝置的資源容量。

檢視裝置健康情況

我可以在哪裡使用這個？	我需要哪些內容？
• ，包括由軟體 NGFW 積分資助的項目	其中一個： ❑ 或 ❑ 或

Device Health（裝置健康情況）儀表板會根據已載入 NGFW 的健康情況分數，顯示部署的累計健康情況狀態和效能。裝置健康情況取決於健康情況分數 (0-100) 的嚴重程度，及其對應的健康情況等級（良好、尚可、不良、嚴重）。健康情況分數會根據開放警示的優先順序、數量、類型和狀態來計算。

此儀表板可協助您：

- 查看歷史健康情況分數資料，瞭解您在一段時間內進行的部署改進。
- 減少部署時需要注意的裝置，並優先處理問題加以解決。

如需更多詳細資訊，請參閱儀表板：裝置健康情況 。

取得升級建議

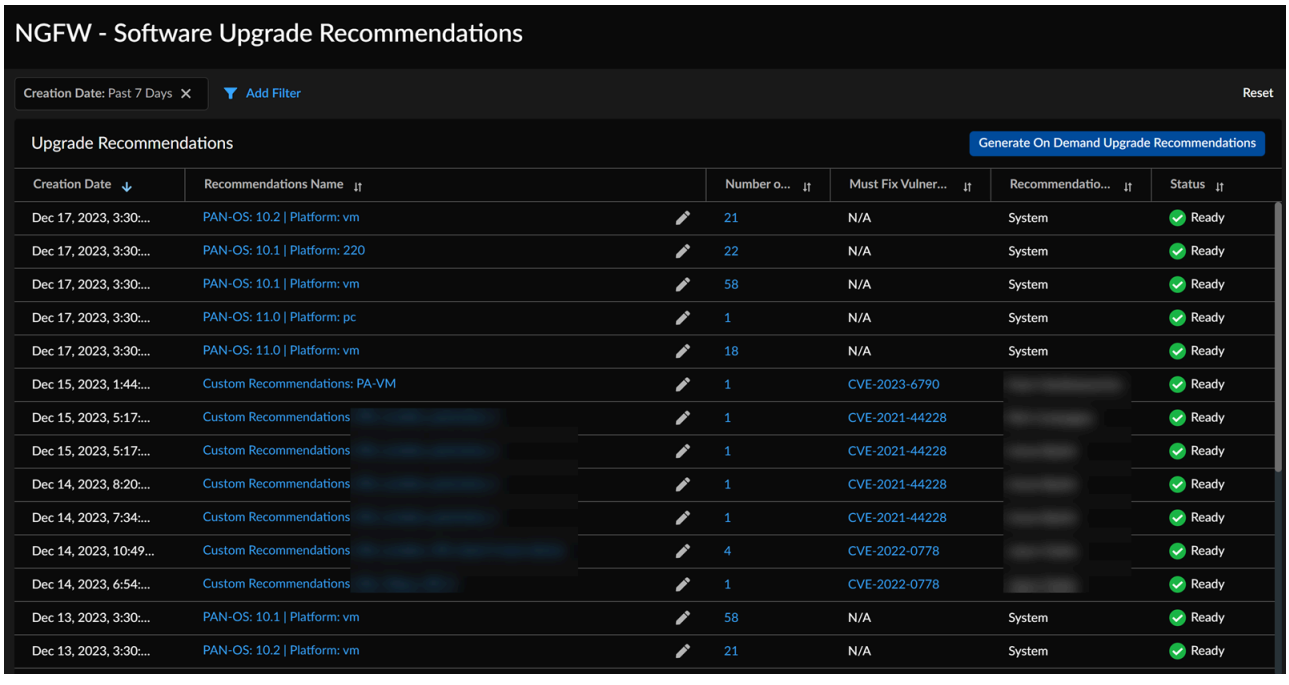
我可以在哪裡使用這個？	我需要哪些內容？
• ，包括由軟體 NGFW 積分資助的項目	❑ 或

選取 **Workflows**（工作流程） > **Software Upgrades**（軟體升級） > **Upgrade Recommendations**（升級建議），以使用 Strata Cloud Manager 來分析防火牆上啟用的功能，並建立提供網路特定資訊的自訂建議：

- 在裝置上執行的最佳軟體版本。
- 每個建議軟體版本中的新功能、行為變更、弱點和軟體問題的相關資訊。

升級建議的類型：

- 系統產生的建議，每週從裝置遙測資料產生兩次。
- 當您為特定 PAN-OS CVE 選取裝置時，所產生的使用者產生自訂建議。
- 您透過上傳防火牆技術支援檔案 (TSF) 所產生的使用者產生建議。



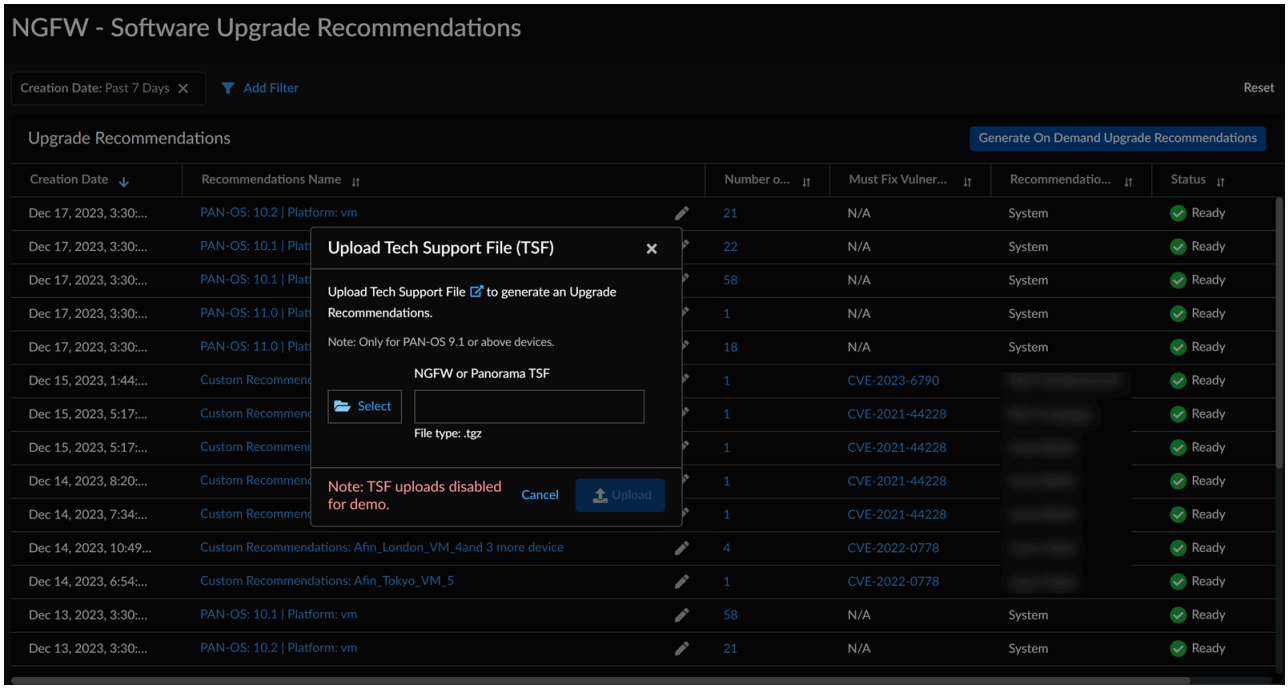
您可以針對每個建議執行下列工作。

- 檢視需要升級的裝置數目，以及您需要解決的任何弱點。
- 編輯建議名稱，以區分自訂建議。
- 依建立日期、建議名稱和產生的建議依據，來篩選建議。
- 刪除失敗或不再適用的建議。

產生隨選升級建議

1. **Generate On Demand Upgrade Recommendations**（產生隨選升級建議）。
2. **Select**（選取）技術支援檔案 (TSF)，並且 **Upload**（上傳）。

- 您一次只能上傳一部裝置的 *TSF*，且 *TSF* 必須為 *.tgz* 格式。
- 您只能從您為執行 *PAN-OS 9.1* 或更新 *PAN-OS* 版本的防火牆產生並上傳的 *TSF* 產生軟體升級建議。



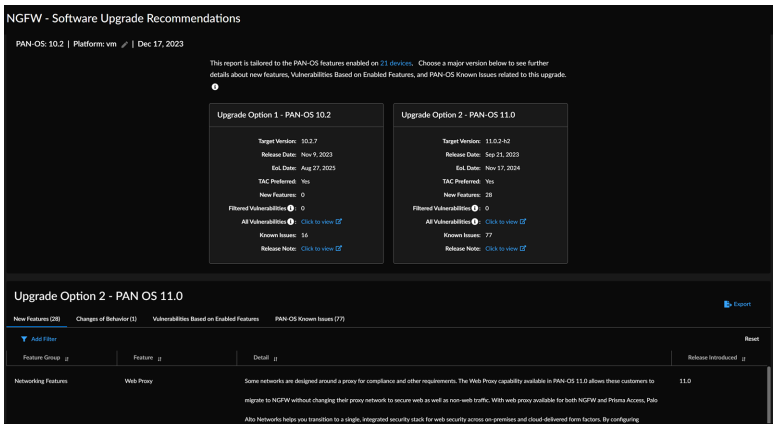
3. 在狀態為 [Ready（就緒）] 後檢視軟體升級建議。

   您也可以檢查 [Status（狀態）]，以確認是否有與 TSF 的上傳、檔案格式或處理相關的錯誤。

檢視軟體升級建議報告

按一下建議以檢視詳細報告，其中包含裝置的升級選項。選取升級選項，以檢視有關 **New Features**（新功能）、**Changes of Behavior**（行為變更）、**Vulnerabilities Based on Enabled Features**（基於啟用功能的弱點）和 **PAN-OS Known Issues**（**PAN-OS** 已知問題）的詳細資訊。您也可以透過 CSV 格式 **Export**（匯出）此報表。

- 建議報告包含您裝置上已啟用功能的特定資訊。
- 針對 ***PAN-OS Known Issues***（***PAN-OS*** 已知問題），「關聯案例計數」代表報告問題的客戶數目。



分析指標容量

我可以在哪裡使用這個？	我需要哪些內容？
•	❑ 或

從 Strata Cloud Manager 瀏覽至 **Monitor**（監控） > **Capacity Analyzer**（功能分析器），根據模型類型持續追蹤指標使用情況，藉此分析和監控裝置的資源容量。您可以使用下列方法分析指標：

- 根據指標、模型和裝置分析指標容量
- 根據裝置型號分析指標容量
- 根據指標分析指標容量

「容量分析器」已增強，可支援警示功能，協助您預測資源消耗是否接近最大容量，並提出警示。請參閱管理容量分析器警示。

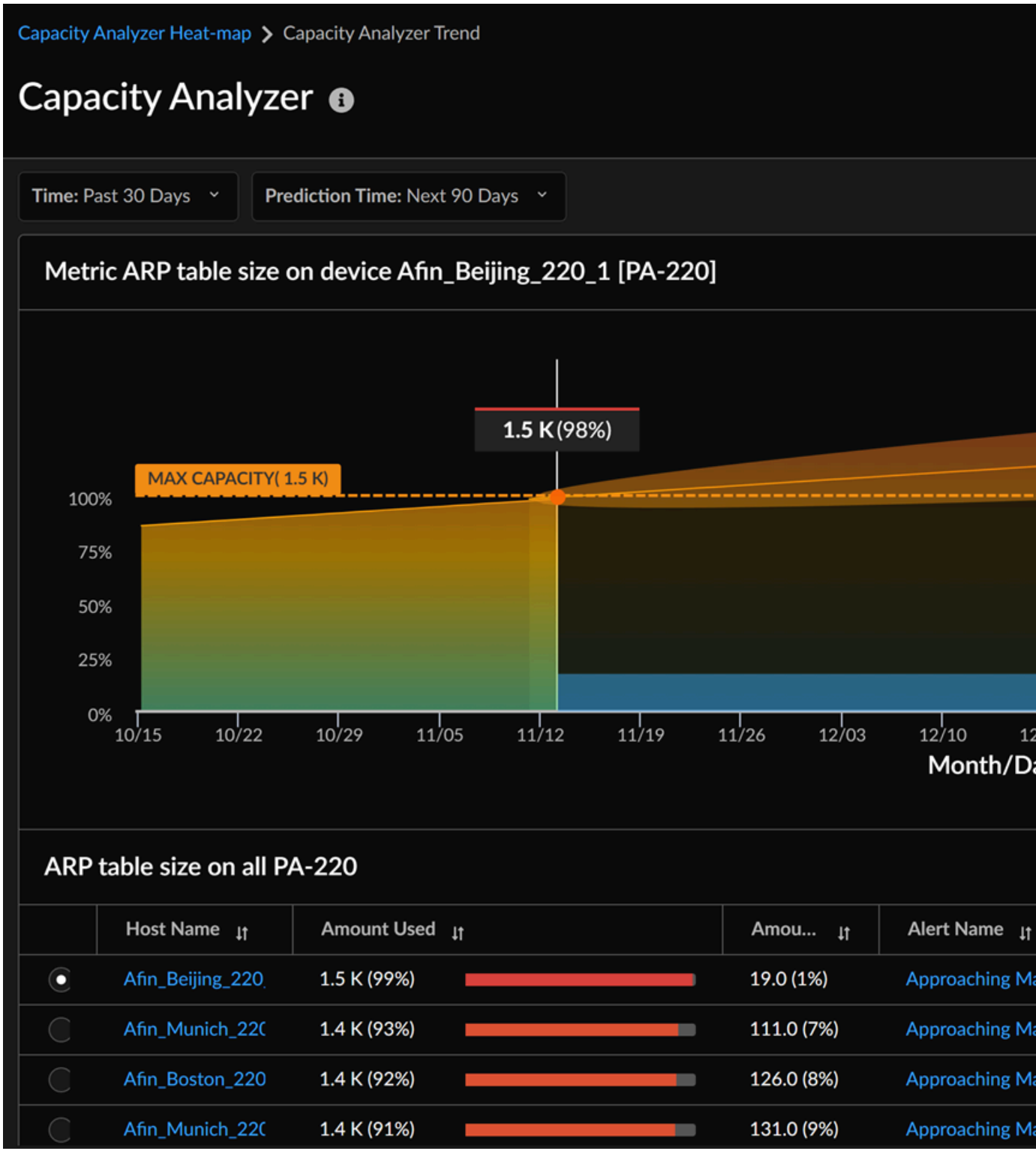
VM 系列防火牆不支援 ***Capacity Analyzer***（容量分析器）功能。

根據指標、模型和裝置分析指標容量

1. 在「容量分析器熱圖」上，將游標懸停在儲存格上方，以檢視屬於對應裝置型號的所有裝置指標容量使用情況。

   在此範例中，彈出式視窗會顯示屬於 **PA-220** 型號的所有裝置 **ARP table size**（**ARP** 表格大小）指標容量。

2. 按一下與裝置型號和指標相對應的儲存格，以檢查容量使用情況。在此範例中，要按一下 **PA-220** 裝置型號的 ARP 表格大小。



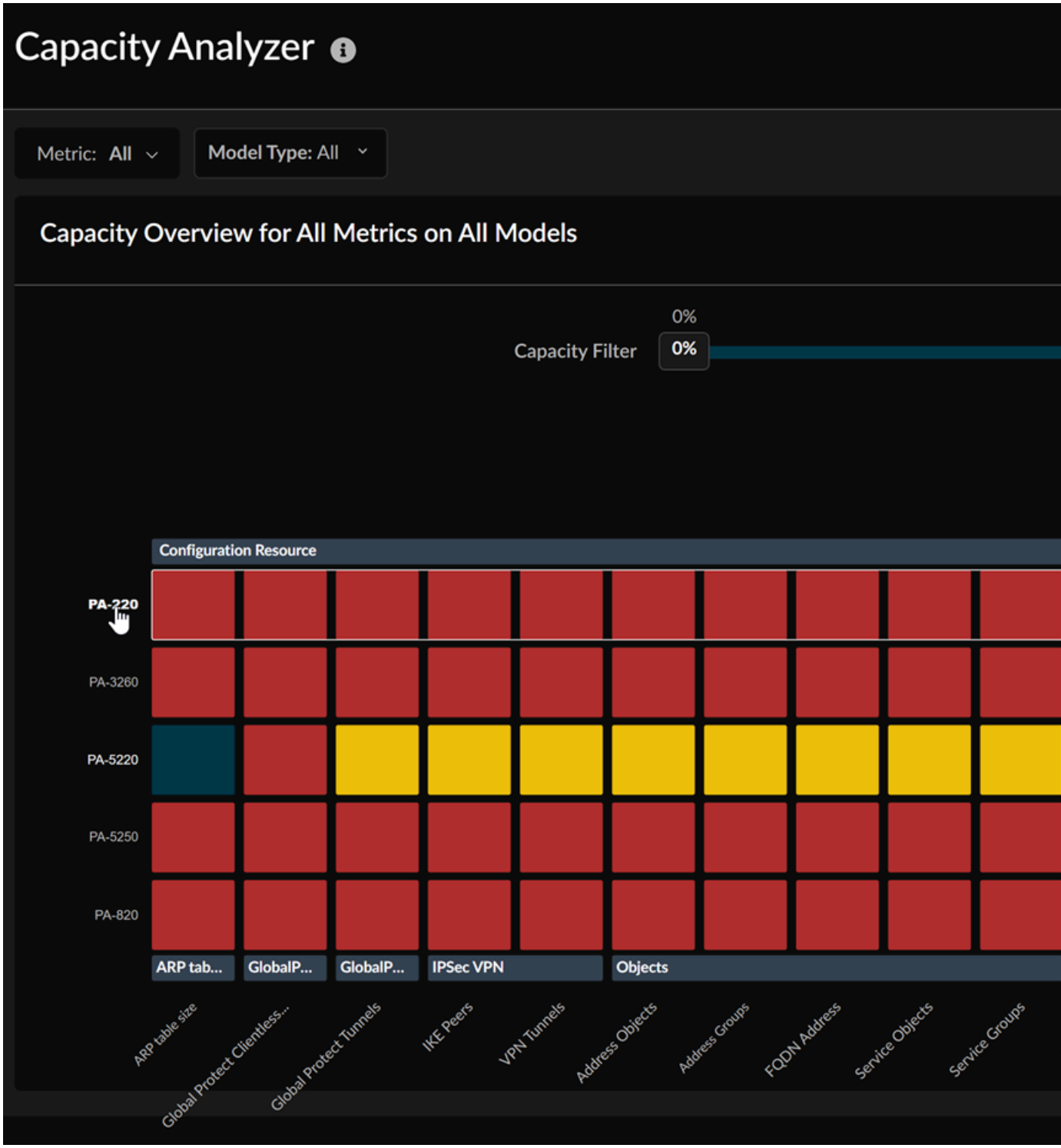
您可以檢視下列內容：

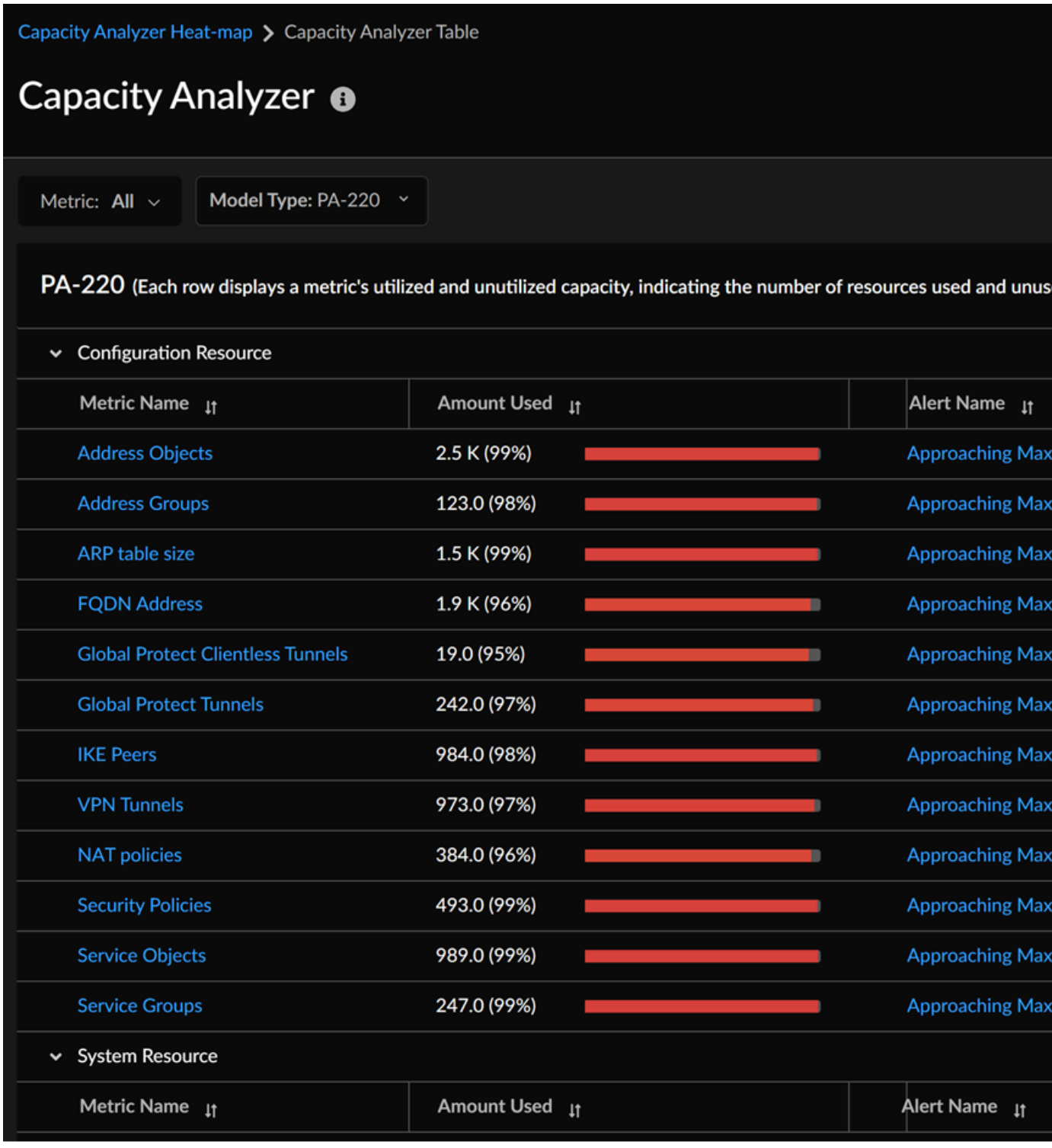
- 屬於 **PA-220** 型號的所有裝置 ARP 表格大小指標容量。

- 選取其中一個主機名稱，以檢視指標容量趨勢。
- 系統會針對指標和指標將達到最大容量的預測日期產生警示。
- 指標的預測趨勢。Strata Cloud Manager 會預測指標達到最大容量的日期。您可以將游標停留在圖表上以檢查任何特定時間點的指標容量。

根據裝置型號分析指標容量

1. 從「容量分析器」熱圖中，選取裝置型號以檢視其所有關聯的指標。





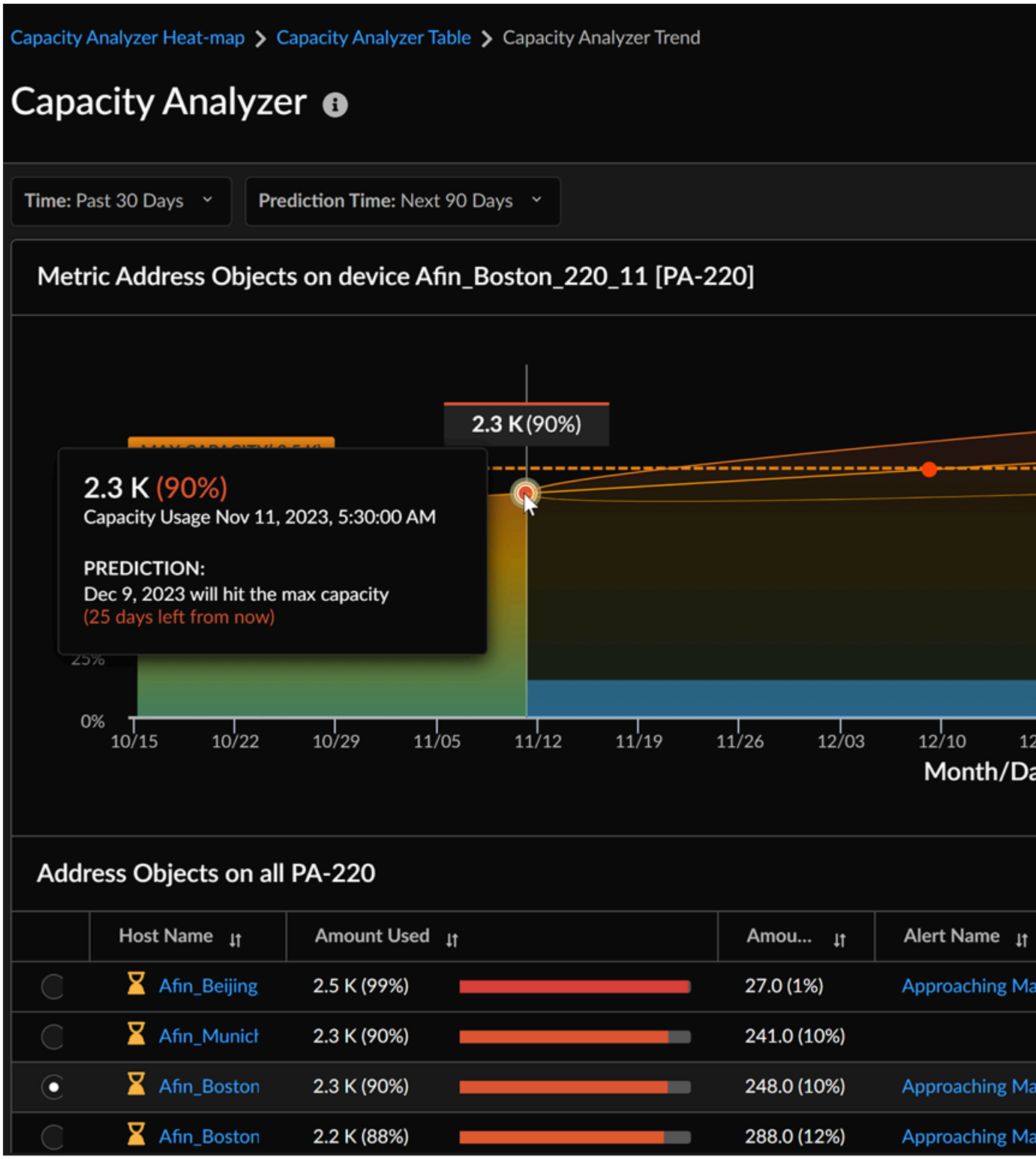
每一列都會顯示指標的使用容量，指出裝置中用於該指標的資源數目。此外，您還可以檢視針對指標以及指標將達到最大容量預測日期所產生的警示。

2. 在「容量分析器」表中，選取一個指標以檢視其在裝置上的趨勢。

3. 選取裝置以檢視其指標趨勢。

   您可以選取 **Prediction Time**（預測時間）來檢查指標的預測趨勢。Strata Cloud Manager 會預測指標達到最大容量的日期。

   您可以將游標停留在圖表上以檢查任何特定時間點的指標容量。

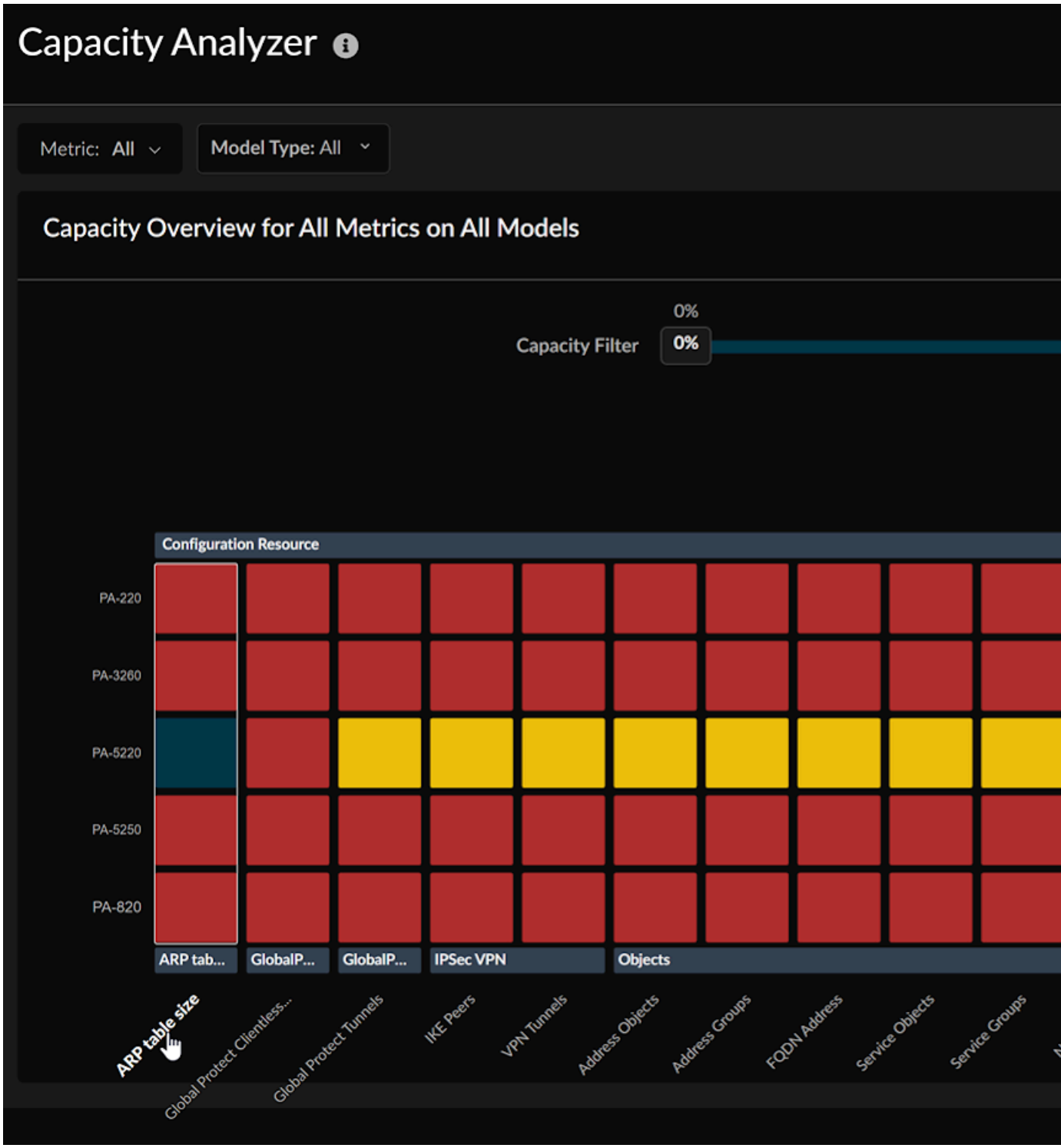


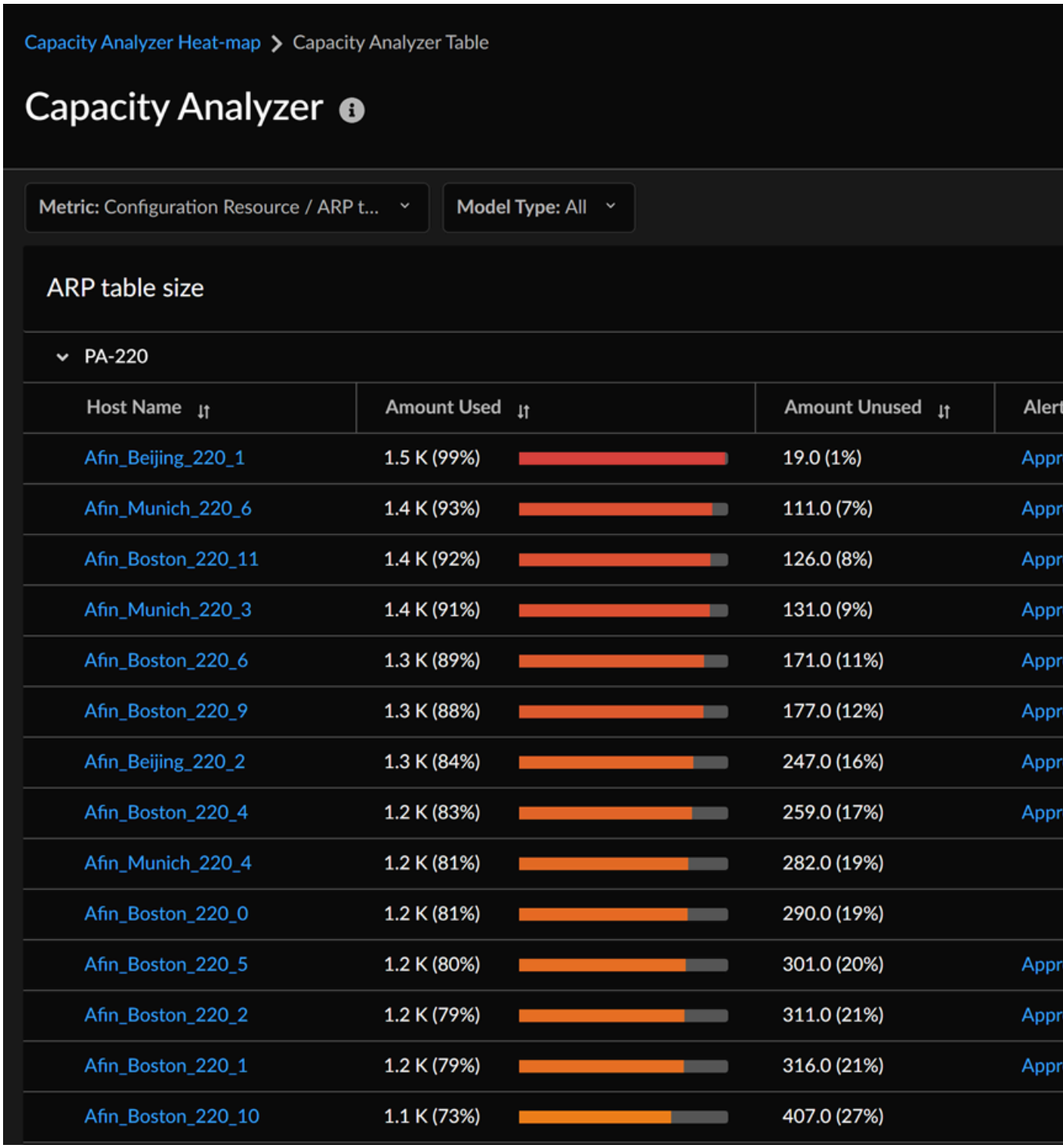
在 **Alert Name**（警示名稱）下，您可以檢視針對與主機名稱對應的位址物件指標所產生的警示。

根據指標分析指標容量

1. 從「容量分析器」熱圖中，選取一個指標，以表格格式檢視其所有裝置中的容量。在此範例中，會選取 **ARP table size**（**ARP** 表格大小）指標。

   您也可以選取指標類型並向下展開指標，以表格格式檢視其所有裝置中的容量。例如：***Configuration Resource***（設定資源）類型指標 **> *Objects***（物件）**> *Address Objects***（位址物件）。

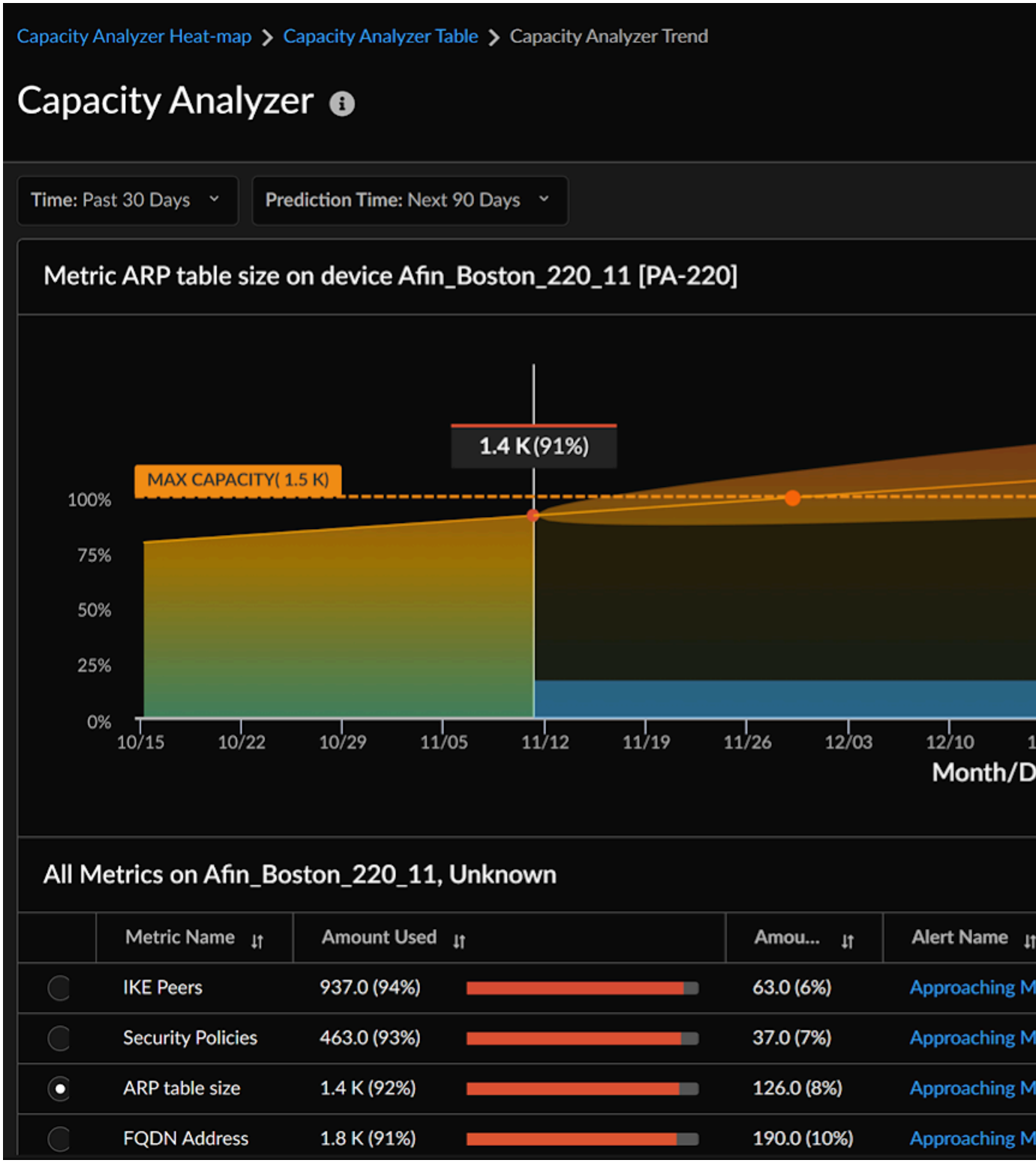




每一列都會顯示裝置模型下每個主機的 **ARP table size**（**ARP** 表格大小）指標使用和未使用的容量。此外，您還可以檢視針對每個主機的這項指標，以及指標將達到最大容量預測日期所產生的警示。

2. 選取主機名稱以檢視所選指標的圖形趨勢。

   您可以選取 **Prediction Time**（預測時間）來檢查指標的預測趨勢。Strata Cloud Manager 會預測指標達到最大容量的日期。



   您可以將游標停留在圖表上以檢查任何特定時間點的指標容量。

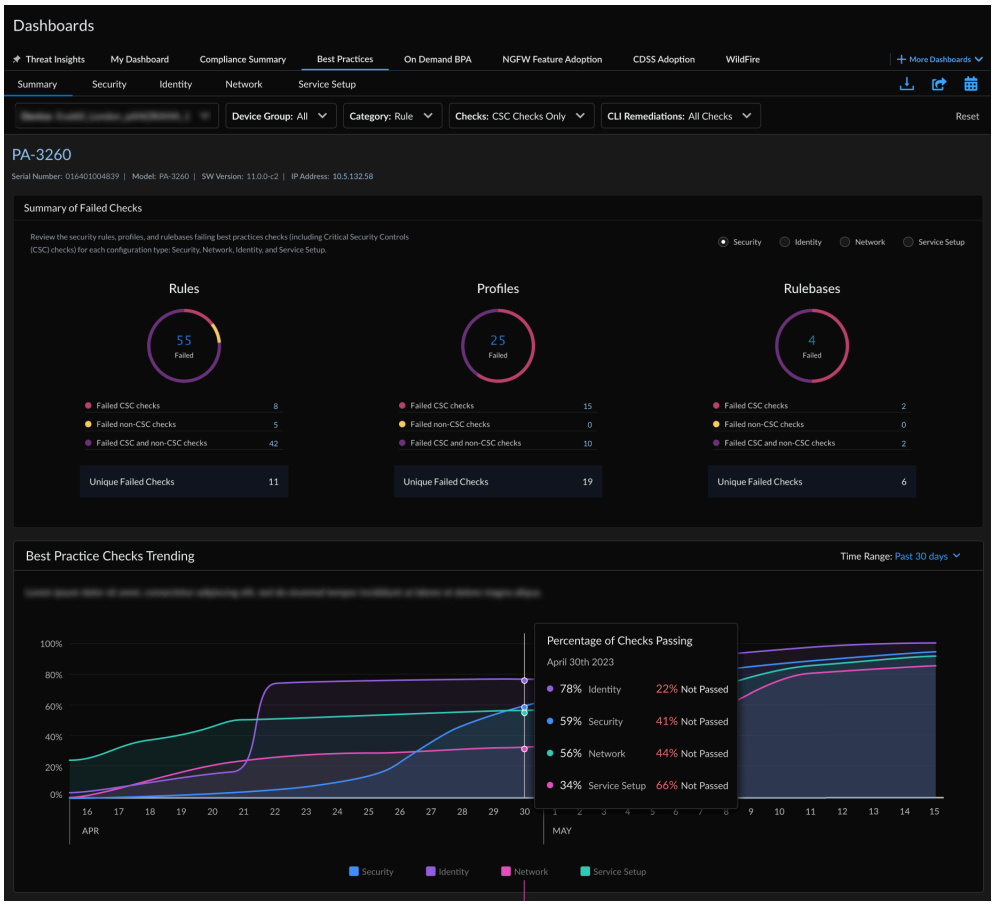
NGFW 最佳做法

我可以在哪裡使用這個？	我需要哪些內容？
• ，包括由軟體 NGFW 積分資助的項目	其中一個： ❑ 或 ❑ 或

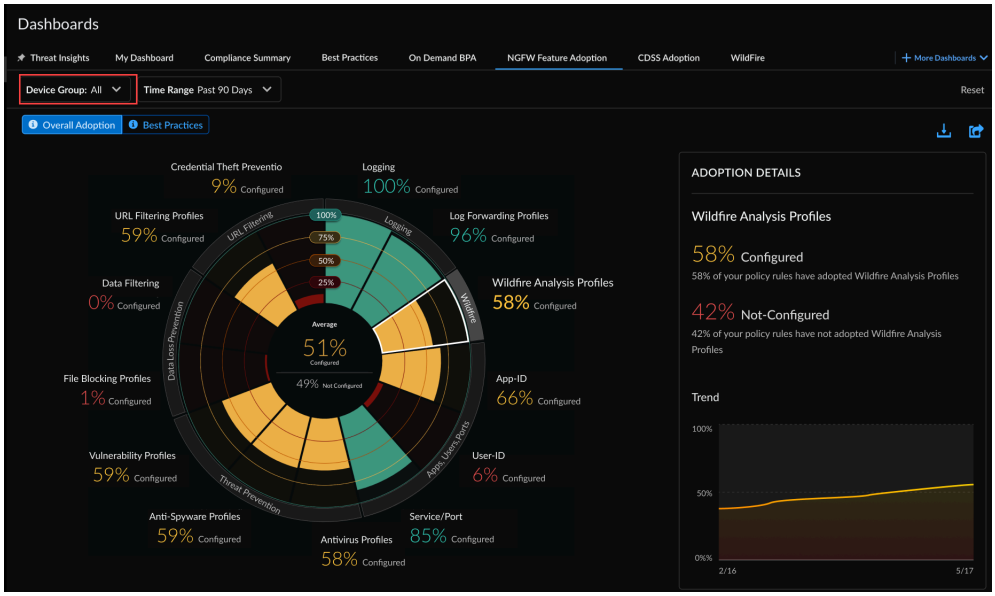
AIOps for NGFW 符合最佳做法，可協助您加強安全性態勢。您可以利用 AIOps for NGFW，根據最佳做法評估您的 Panorama、NGFW 和 Panorama 管理的 Prisma Access 安全性設定，並修復失敗的最佳做法檢查。AIOps for NGFW 簡化了檢查網路基礎架構 InfoSec 合規性的流程。

AIOps for NGFW 是免費的，無需 AIOps 高級授權即可使用以下 AIOps 最佳做法評估 (BPA) 功能。有關可用最佳做法功能的完整清單，請參閱內建最佳做法：

- 檢查最佳做法儀表板，以獲取每日最佳做法報告，以及與 Center for Internet Security 重大安全性控制 (CSC) 檢查的對應，以協助您識別可以進行變更的領域，提升最佳做法合規性。以 PDF 格式分享最佳做法報告，並安排定期將其傳遞到您的收件匣。

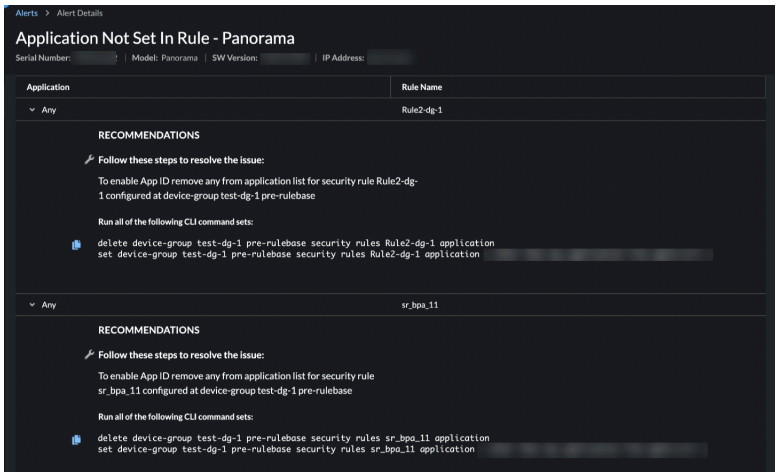


- 監控功能採用情況並隨時了解您在部署中使用的安全功能，以及覆蓋範圍中的潛在差距。



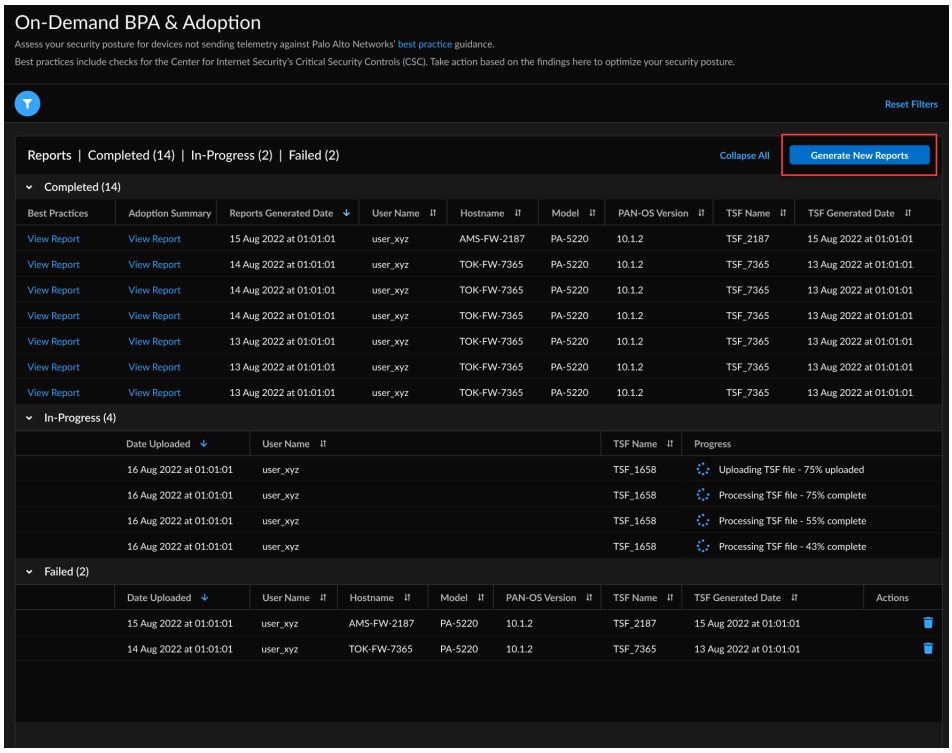
- 從 AIOps for NGFW 取得安全性態勢警示，以了解何時需要仔細檢查您的安全性設定。

  命令列介面 (CLI) 補救功能也可在 AIOps for NGFW 中的 **Alerts**（警示） > **Security**（安全性） > **Alert Details**（警示詳細資料）下找到。檢視建議，以協助您修補觸發警示的問題。



安全警示和 *CLI* 補救措施僅適用於共用遙測的裝置。此功能不支援針對執行版本 *9.1* 及更高版本的 *PAN-OS* 裝置，手動上傳技術支援檔案 *(TSF)*。

- 為執行版本 9.1 及更高版本的（非遙測）PAN-OS 裝置產生 BPA 報告（現在包括功能採用指標）。如果您一直在使用 BPA 獨立工具來產生 BPA 報告，您可能會想「我仍然可以從客戶支援入口網站產生 BPA 報告嗎？」我們也涵蓋在內了。



透過高級授權，AIOps for NGFW 還提供高級安全性態勢功能。高級功能著重於確保防火牆的充分利用和極大化安全性。查看免費和高級授權所提供的內容。

隨選 BPA 報告

我可以在哪裡使用這個？	我需要哪些內容？
• ，包括由軟體 NGFW 積分資助的項目	其中一個： ❑ 或 ❑ 或

現在您可以直接從 Strata Cloud Manager 執行最佳做法評估 (BPA) 和功能採用摘要。只需上傳技術支援檔案 (TSF) 即可。您可以為不傳送遙測資料或未載入 AIOps for NGFW 的裝置產生隨選 BPA 報告。

BPA 會根據 Palo Alto Networks 最佳做法評估您的安全性態勢，並優先進行裝置的改進。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，因此您可以知道和控制網路上的應用程式、使用者和內容。此外，最佳做法包括對 Center for Internet Security 的重大安全性控制 (CSC) 進行檢查。請參閱最佳做法指南，以加強安全性態勢並實施改善。

我仍然可以從客戶支援入口網站產生 BPA 報告嗎？

在 AIOps 出現之前，您是前往 客戶支援入口網站來存取和執行 BPA。如今，產生和下載 NGFW/Panorama 管理 Prisma Access 最佳做法評估報告的首選方式是透過 AIOps 執行。

2023 年 7 月 17 日之後，您將無法再從客戶支援入口網站存取和執行 BPA。

STEP 1 | 前往中樞並啟動 AIOps for NGFW。可以免費使用。如果您不想要載入目前已啟用遙測的裝置，可以在沒有Strata Logging Service的情況下啟動。

最佳做法儀表板、安全警示和採用摘要功能不適用於在沒有*Strata Logging Service*的情況下載入的裝置，或是未啟用遙測的裝置。

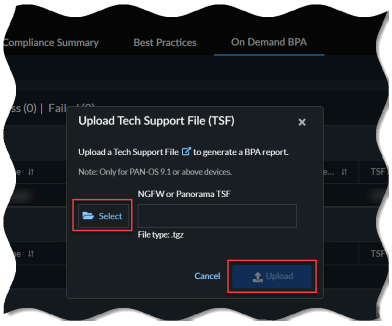
STEP 2 | 登入已啟動的執行個體 AIOps for NGFW。即使沒有 Strata Logging Service，您也會看到以下頁籤:

- 態勢
- 活動
- 設定

STEP 3 | 前往 **Dashboards**（儀表板） > **On Demand BPA**（隨選 **BPA**）。

STEP 4 | **Generate New BPA Report**（產生新的 **BPA** 報告）。

STEP 5 | **Select TSF**（選取 **TSF**）並且 **Upload TSF**（上傳 **TSF**）檔案。



上傳時間取決於 .tgz 檔案的大小和您的網路速度。對於較大的檔案，上傳檔案可能需要幾分鐘的時間。展開 **In-Progress**（進行中）以檢視 TSF 檔案的狀態。

- 隨選 *BPA* 僅支援 *.tgz* 檔案格式的技術支援檔案 *(TSF)*。
- 隨選 *BPA* 支援來自 *PAN-OS* 版本 *9.1* 或更高版本裝置的 *TSF*，用於產生報告。

STEP 6 | 處理 TSF 後，請選取 **Completed**（已完成）底下的 **View Report**（檢視報告），以檢視從裝置產生的 BPA 報告。

最佳做法

我可以在哪裡使用這個？	我需要哪些內容？
• •	❑ 或 ❑ 授權 ❑ 在裝置上啟用遙測共用

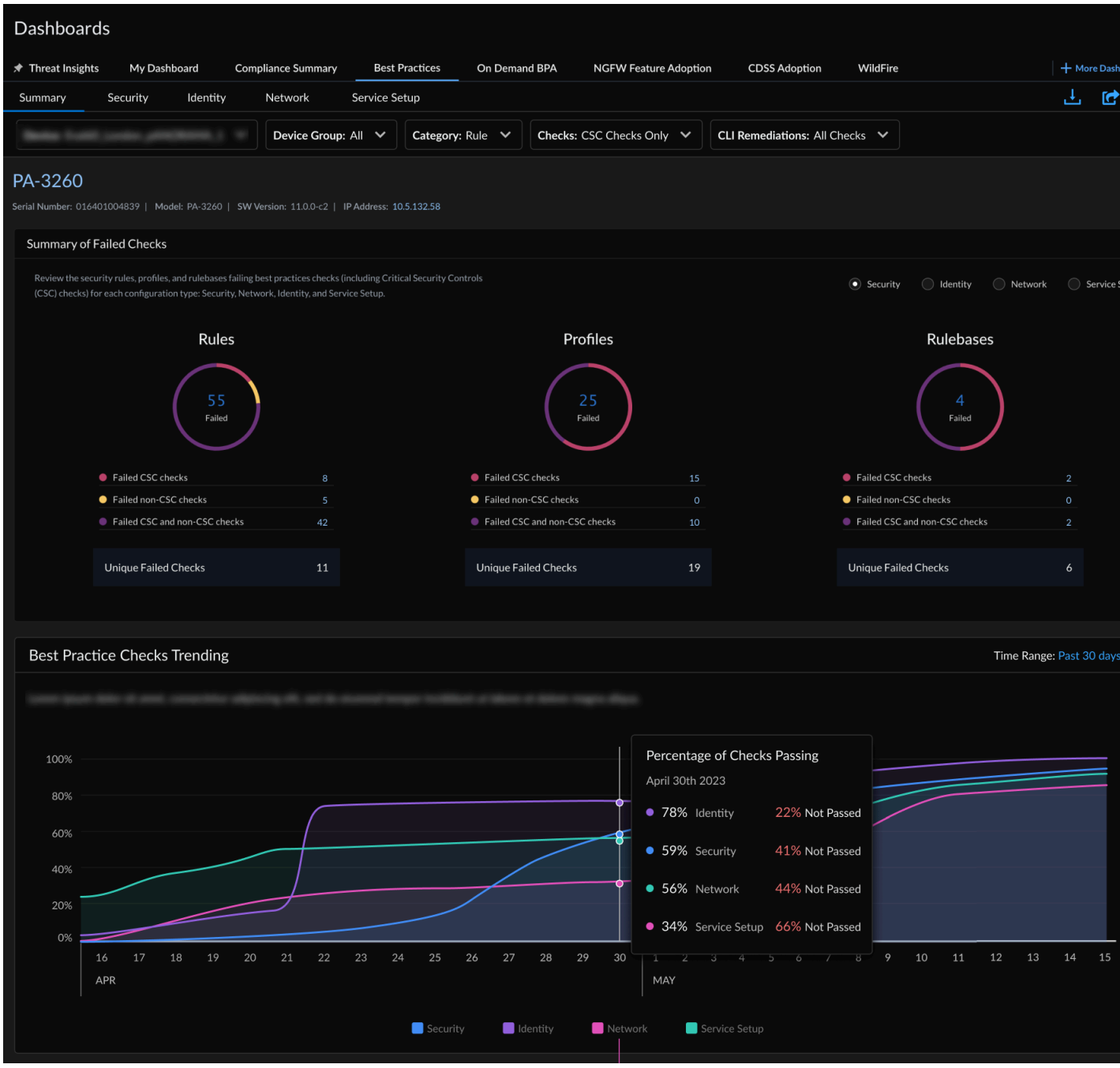
此儀表板向您展示什麼？

儀表板會根據與您租用戶相關聯的 *Prisma Access* 和 *NGFW/Panorama*，顯示彙總資料。

瀏覽至 **Strata Cloud Manager** > **Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **Best Practices**（最佳做法）儀表板，根據 Palo Alto Networks 的最佳做法指南衡量安全性態勢。重要的是，最佳做法評估包括對 Center for Internet Security 的重大安全性控制 (CSC) 進行檢查。CSC 檢查會與其他最佳做法檢查分開，因此您可以輕鬆選擇更新，並優先挑選可讓您符合 CSC 的更新。

如何使用儀表板中的資料？

雖然最佳做法指南旨在協助您加強安全性態勢，但本報告中的結果也可以協助您識別可以進行變更的領域，以便更有效地管理環境。



最佳做法儀表板分為五個部分：

- **Summary**

  讓您全面檢視不同設定類型（安全性、網路、識別和服務設定）上裝置的所有失敗檢查、以及檢視 BPA 檢查的歷史趨勢圖和評估重要功能領域的最佳做法採用率。

- **security**

  針對所選裝置和位置，顯示未通過最佳做法和 CSC 檢查的規則、規則庫或設定檔。CLI 補救功能在適用時，可讓您解決政策規則的問題。CLI 補救功能是使用您在產生 隨選 BPA 報告 時上傳的 TSF 資料所產生。

  - 規則庫

    檢視政策的組織方式，以及適用於許多規則的配置設定是否符合最佳做法（包括 CSC 檢查）。

  - 規則

    顯示未通過最佳做法和 CSC 檢查的規則。查看您可以在何處採取快速行動，來修正失敗的檢查。規則會根據工作階段計數排序，因此您可以先檢閱和更新影響最大流量的規則。

  - 設定檔

    顯示您的設定檔為何違反最佳做法（包括 CSC 檢查）。設定檔會針對與安全性或解密規則相符的流量，執行進階檢查。

- 識別

  顯示裝置的驗證強制執行設定（驗證規則、驗證設定檔和驗證入口網站）是否符合最佳做法，並且與 CSC 檢查相符。

- 網路

  檢查應用程式取代規則和網路設定是否符合最佳做法和 CSC 檢查。

- 服務設定

  了解您在裝置上啟用的訂閱如何符合最佳做法和 CSC 檢查。您可以在此處檢閱 WildFire 設定、GlobalProtect 入口網站和 GlobalProtect 閘道設定，並修正失敗的檢查。

分享、下載和排程儀表板的報表

您可以下載、分享和排程報告，涵蓋儀表板以 *PDF* 和 *.csv* 格式顯示的資料，以及 *.txt* 格式的 *CLI* 補救措施。在儀表板右上方找到這些圖示：