paloalto TECHDOCS

AI Access Security 管理

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

April 17, 2026

探索 GenAI 應用程式所帶來的風險

使用 AI Access Security 洞察儀表板，來篩選網路上生成式 AI (GenAI) 應用程式使用情況。AI Access Security 洞察儀表板提供了深入的詳細資訊，可協助您了解哪些 GenAI 應用程式正在使用，以及由誰使用。

AI Access Security 偵測 **Allowed Users**（允許的使用者）資料、**Blocked Users**（遭封鎖的使用者）資料，或根據以下篩選器偵測兩者。

- **1 Hour**（**1** 小時）和 **3 Hours**（**3** 小時）

  使用者可以計為已允許、已封鎖或兩者。

  例如，因為 `Policy Rule1`，`UserA` 遭封鎖而無法存取 `GenAI-App1`。一小時後，`UserA` 來到分支辦公室，`Policy Rule2` 允許存取 `GenAI-App1`。在這種案例下，`UserA` 同時在 **Allowed Users**（允許的使用者）和 **Blocked Users**（遭封鎖的使用者）計數中顯示。

  相反，`Policy Rule1` 封鎖 `UserA`，使其無法存取 `GenAI-App1`。幾分鐘後，安全性管理員修改 `Policy Rule1` 以允許 `UserA` 存取。在這種情況下，`UserA` 在 **Blocked Users**（已封鎖的使用者）計數中顯示。系統會針對符合相同的安全性政策規則並至少遭封鎖而無法存取一次的使用者，AI Access Security 顯示在 **Blocked Users**（已封鎖的使用者）計數中的使用者，無論您過去 **1 Hour**（**1** 小時）或 **3 Hours**（**3** 小時）允許存取的次數如何。
- **24** 小時、**7 Day**（**7** 天）和 **30 Day**（**30** 天）

  使用者可以計為已允許、已封鎖或兩者。

  例如，您最初封鎖了 `UserA`，使其無法存取 `GenAI-App1`。六小時後，`UserA` 來到分支辦公室，`Policy Rule2` 允許存取 `GenAI-App1`。在這種案例下，`UserA` 同時在 **Allowed Users**（允許的使用者）和 **Blocked Users**（遭封鎖的使用者）計數中顯示。

依使用案例探索 GenAI 應用程式所帶來的風險

檢閱支援的使用案例，了解 GenAI 應用程式所屬的所有使用案例類別的完整說明。

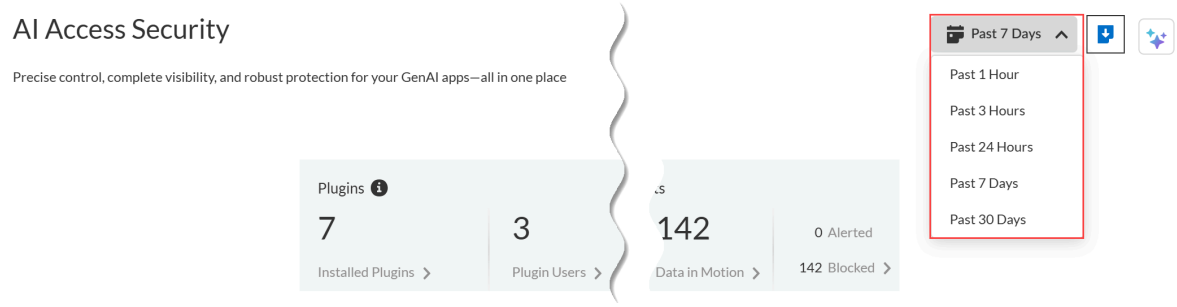
STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取 **Insights**（洞察） > **AI Access**（**AI** 存取），以檢視 AI Access Security 洞察儀表板。

AI Access Security 洞察儀表板依預設會顯示網路上 GenAI 應用程式的使用情況，以及與熱門 GenAI 使用案例有關的下列高階資訊：

- 時間篩選器

  篩選您要調查時段的 GenAI 使用案例詳細資訊。您可以選取 **Past 1 Hour**（過去 **1** 小時）、**Past 3 Hours**（過去 **3** 小時）、**Past 24 Hours**（過去 **24** 小時）、**Past 7 Days**（過去 **7** 天）或 **Past 30 Days**（過去 **30** 天）。



- 偵測到威脅

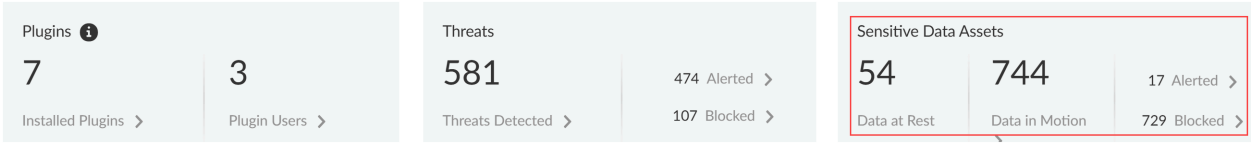
  威脅是透過附加到 Web 安全性政策規則的弱點保護設定檔偵測到的。此設定檔可偵測惡意和網路釣魚 URL、惡意檔案或惡意軟體等威脅。**Threats Detected**（偵測到的威脅）會摘要在所有 GenAI 應用程式和強制執行點間的所有威脅。

  - **Alerted**（已警示）—偵測到產生警示的威脅總數。
  - **Blocked**（已封鎖）—偵測到已遭 NGFW 或 Prisma Access 租用戶封鎖的威脅總數。

- 敏感資料資產

  敏感資料資產會針對靜態資料 (Data Security) 和動態資料 (SaaS Security Inline) 顯示流量符合 Enterprise Data Loss Prevention (E-DLP) 資料設定檔中比對規則時偵測到的敏感資料事件數。

  - **Data at Rest**（靜態資料）—產生警示或透過 SaaS API (Data Security) 強制執行通道遭到封鎖的 DLP 事件總數。
  - **Data in Motion**（動態資料）—產生警示或透過 SaaS Security Inline 強制執行通道遭到封鎖的 DLP 事件總數。
  - **Alerted**（已警示）—針對靜態資料和動態資料產生警示的 DLP 事件總數。
  - **Blocked**（已封鎖）—NGFW 或 Prisma Access 租用戶針對靜態資料和動態資料封鎖的 DLP 事件總數。

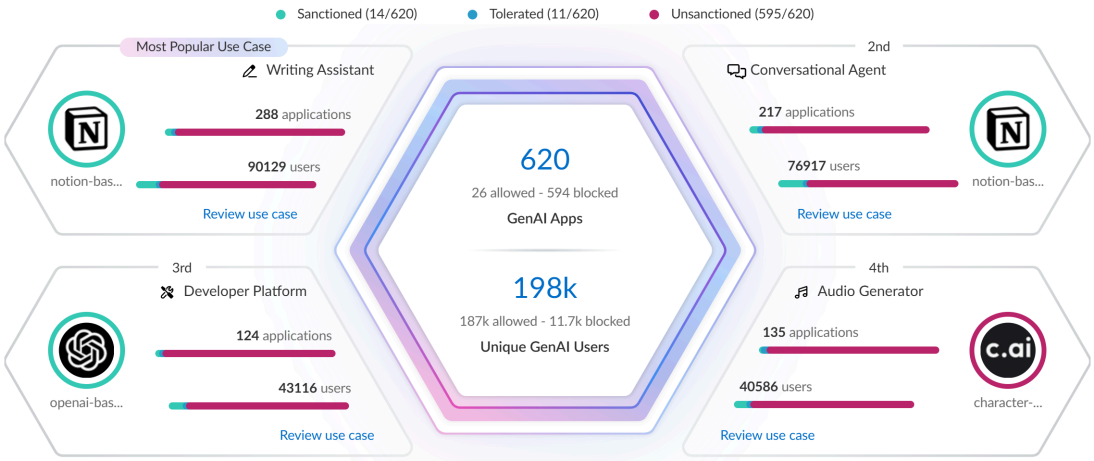


- 熱門使用案例

  AI Access Security 洞察儀表板會根據網路上的活動動態顯示前四個 GenAI 應用程式使用案例，以及 GenAI 應用程式總數以及在所選時段內存取任何 GenAI 的使用者總數。這可讓您快速調查與最常用的 GenAI 應用程式相關的安全性事件，並實作存取控制政策規則。

  - **GenAI Apps**（**GenAI** 應用程式）—屬於特定使用案例的 GenAI 應用程式總數。GenAI 應用程式的總數分為三組：已認可、已容許和未認可的 GenAI 應用程式。
  - **Unique GenAI Users**（唯一的 **GenAI** 使用者）—存取屬於特定使用案例的任何 GenAI 應用程式的使用者總數。按一下 **Unique GenAI Users**（唯一的 **GenAI** 使用者）計數，以檢視遭封鎖而無法存取 GenAI 應用程式的每個唯一使用者清單

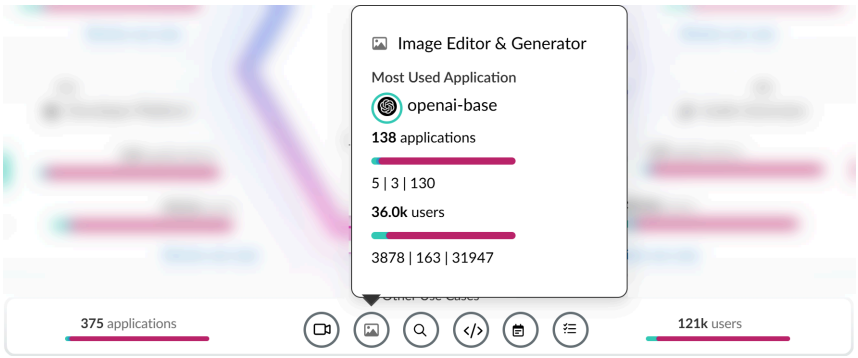
    AI Access Security 會在設定的間隔內自動彙總的 ***Unique GenAI Users***（唯一 ***GenAI*** 使用者）總數，並在您按一下 ***Unique GenAI Users***（唯一 ***GenAI*** 使用者）計數時立即產生使用者清單。這可能會導致 ***Unique GenAI Users***（唯一 ***GenAI*** 使用者）計數與清單計數略有不同。



- 所有其他使用案例

  - **Applications**（應用程式）—屬於任何其他 GenAI 應用程式使用案例的 GenAI 應用程式總數。GenAI 應用程式的總數分為三組：已認可、已容許和未認可的 GenAI 應用程式。
  - **Users**（使用者）—已存取屬於任何其他 GenAI 應用程式使用案例的任何 GenAI 應用程式的使用者總數。

  將滑鼠暫留在每個使用案例上方，以查看與使用案例相關聯的 GenAI 應用程式使用情況摘要資訊。



STEP 3 | **Review use case**（檢閱使用案例），以查看所需使用案例中所有已認可、已容許和未認可的 GenAI 應用程式詳細資訊。

STEP 4 | 檢閱使用案例詳細資訊頁面，以了解 GenAI 應用程式使用情況。

使用案例詳細資訊頁面提供 GenAI 應用程式使用情況的精細資料。您可以使用此資訊了解 GenAI 應用程式的使用情況，以協助通知您安全性管理員需要撰寫哪些政策規則來強化安全性態勢。這可確保組織安全地採用 GenAI 應用程式，並防止敏感資料外洩。

- 使用案例摘要

  使用案例摘要會針對您調查的使用案例彙總所有重要的 GenAI 應用程式使用情況資訊。

  - 最常用的應用程式授權—使用案例最常用的 GenAI 應用程式。這還包括目前指派給 GenAI 應用程式的應用程式標籤（**Sanctioned**（已認可）、**Tolerated**（已容許）或 **Unsanctioned**（未認可））。
  - **Application Breakdown**（應用程式詳細資訊）—與使用案例相關聯的 GenAI 應用程式總數摘要，以及所有偵測到的 GenAI 應用程式中的應用程式標籤摘要。
  - **User Breakdown**（使用者詳細資訊）—存取與使用案例相關聯的任何 GenAI 應用程式的使用者總數摘要。也提供了摘要，說明有多少使用者存取了 **Sanctioned**（已認可）、**Tolerated**（已容許）或 **Unsanctioned**（未認可）的 GenAI 應用程式。

- 應用程式

  與您使用者存取的使用案例相關聯的所有 GenAI 應用程式清單。您可以將 **Sort By**（排序方式）篩選器套用至使用案例 GenAI 應用程式，以依 **User Count**（使用者計數）、**Threats**

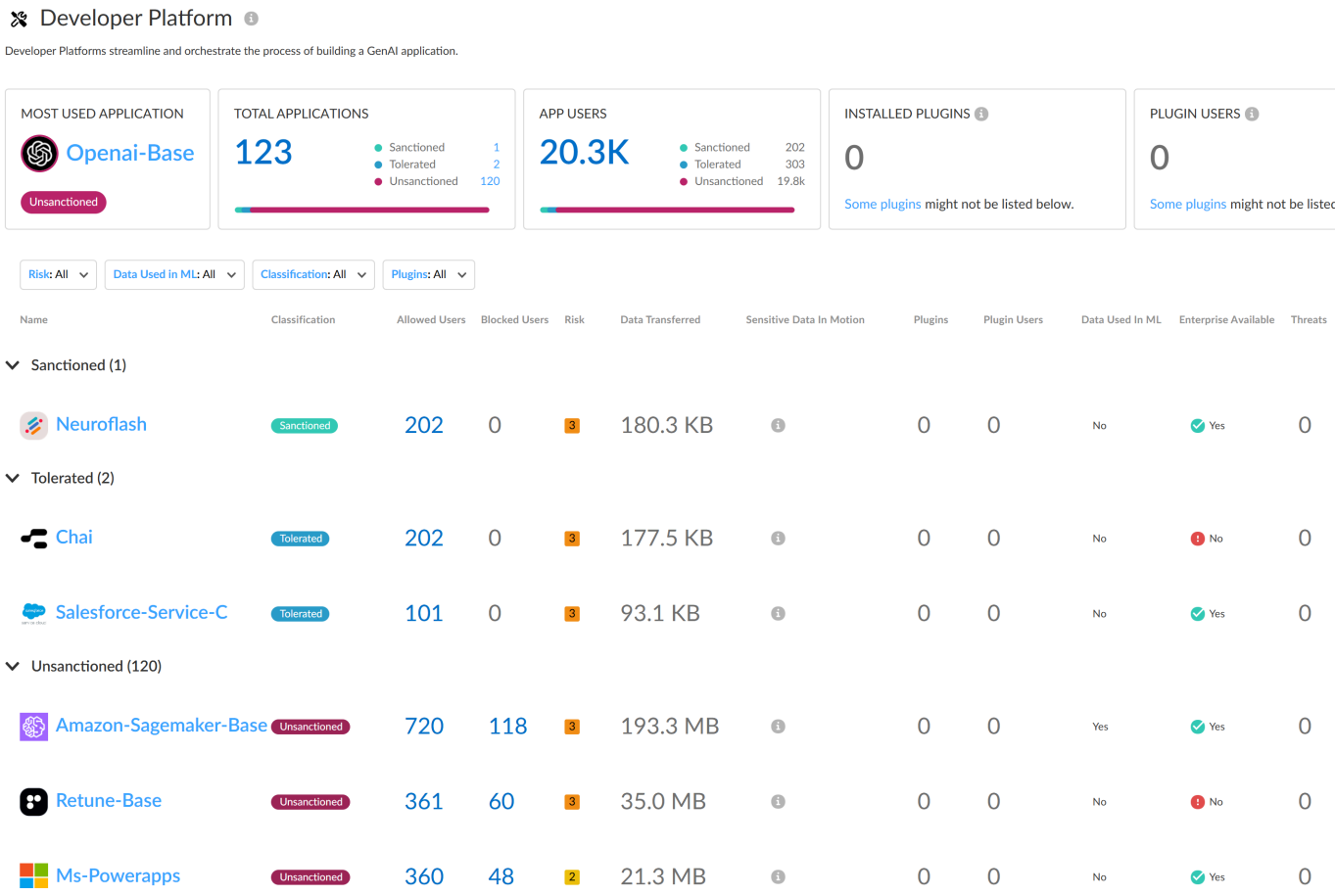
Count（威脅計數）、**Transferred Count**（傳輸計數）對其進行排序。AI Access Security 會將 GenAI 應用程式從最高到最低計數進行排序。

應用程式清單會顯示下列與每個偵測到的 GenAI 應用程式相關的資訊。

- **Application Name**（應用程式名稱）—偵測到的 GenAI 應用程式名稱。按一下應用程式名稱，以檢視詳細使用情況資訊。系統將重新導向至活動洞察 **Applications**（應用程式）
- **Tag**（標籤）—目前的 GenAI 應用程式標籤。您可以按一下要套用的標籤來套用新的標籤。

  Palo Alto Networks 會在容器 *App-ID* 中針對應用程式功能將子 *App-ID* 分組。但是，標記 *App-ID* 容器是不受支援的。您必須個別標記組織內已認可、未認可或已容許的特定子 *App-ID*。
- 允許的使用者—根據安全性政策規則中設定的存取權限存取 GenAI 應用程式的唯一使用者總數。按一下 **Allowed Users**（允許的使用者）計數，以檢視成功存取 GenAI 應用程式的每個唯一使用者清單。
- 封鎖的使用者—根據安全性政策規則中設定的存取權限，遭封鎖而無法存取 GenAI 應用程式的唯一使用者總數。按一下 **Blockers Users**（遭封鎖的使用者）計數，以檢視遭封鎖而無法存取 GenAI 應用程式的每個唯一使用者清單。
- **Threats**（威脅）—偵測到的威脅活動總數。
- **Transferred**（已傳輸）—從 GenAI 應用程式上傳或下載的資料總數（以 GB (GB) 為單位）。
- **Sensitive Asset**（敏感資產）—由於 Enterprise DLP 偵測到並封鎖敏感資料而產生的 DLP 事件數目。
- **Enterprise Available**（企業可用性）—指出 GenAI 應用程式是否提供企業方案或授權結構描述。
- **Data Used in ML**（**ML** 中使用的資料）—指出 GenAI 應用程式是否將使用者上傳的資料用於訓練目的。
- **Risk Score**（風險分數）—GenAI 應用程式的風險分數。

- 使用案例重點
  - **Applications**（應用程式）—屬於任何其他 GenAI 應用程式使用案例的 GenAI 應用程式總數。GenAI 應用程式的總數分為三組：已認可、已容許和未認可的 GenAI 應用程式。
  - **Users**（使用者）—已存取屬於任何其他 GenAI 應用程式使用案例的任何 GenAI 應用程式的使用者總數。



STEP 5 | 建立自訂安全性政策規則，以控制對 GenAI 應用程式的存取。

在上述範例中，`Openai-Base` 是程式碼助理和產生器使用案例中最常用的 GenAI 應用程式。此外，這是 **Unsanctioned**（未認可）應用程式，表示此應用程式未獲核准，無法在企業網路上使用。

在此案例中，如果這是貴組織不應存取的應用程式，您可以修改預設值 GenAI 應用程式存取政策規則，以明確封鎖對 `OpenAI` 的所有存取。

依有風險的應用程式探索 GenAI 應用程式所產生的風險

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取 **Insights**（洞察） > **Activity Insights**（活動洞察） > **Applications**（應用程式）。

STEP 3 | 設定應用程式清單的篩選器，以縮小您要調查的 GenAI 應用程式範圍。

1. 設定 **Time Range**（時間範圍）和 **Scope Selection**（範圍選擇），以篩選您要調查的特定時間範圍和強制執行點。
2. **Add Filter**（新增篩選器）並新增下列篩選器。
   - **Source Type - Users**（來源類型 - 使用者）—篩選應用程式清單，以僅顯示組織中使用者存取的 GenAI 應用程式。這是必要的篩選器。
   - **GenAI Application - TRUE**（**GenAI** 應用程式 **- TRUE**）—篩選應用程式清單以僅顯示 GenAI 應用程式。這是必要的篩選器。
   - **App Risk Score**（應用程式風險分數）—對於 **App Risk Score**（應用程式風險分數）篩選器，選取您要調查的特定風險分數。如果您未選取至少一個風險分數，則會顯示所有 GenAI 應用程式。

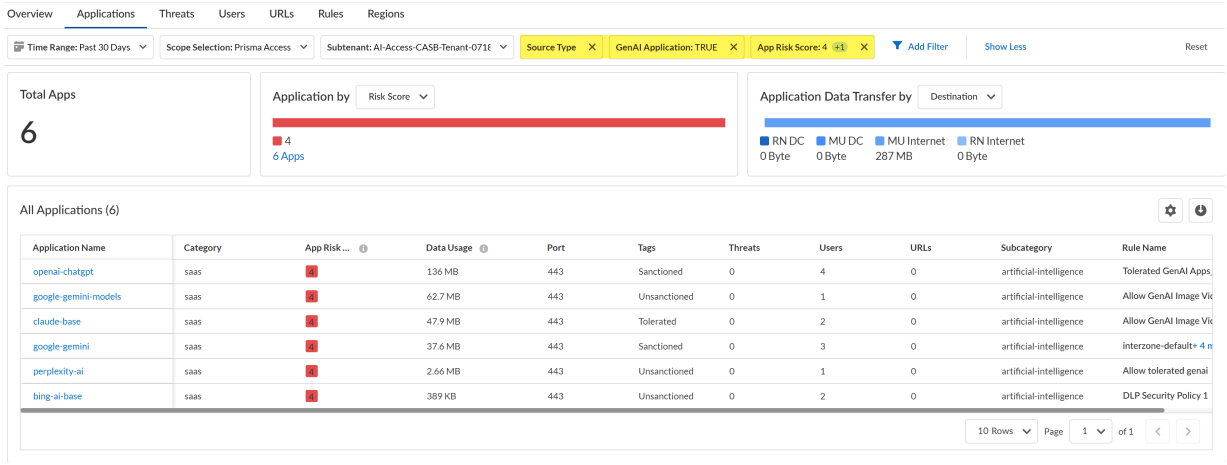
     在此範例中，我們會調查風險分數為 **4** 和 **5** 的應用程式，因為這些是風險最高應用程式所歸因的風險分數。

STEP 4 | 檢閱已篩選的 GenAI 應用程式清單。

需要檢閱的一些重要資訊包括：

- **Application Name**（應用程式名稱）—GenAI 應用程式的 App-ID。
- **Data Usage**（資料使用量）—從 GenAI 應用程式上傳或下載的資料量。這可以幫助您了解 GenAI 應用程式的使用情況；具有大量資料使用量的 GenAI 應用程式可能意味著此應用程式受到廣泛使用，並且可能需要嚴格控制，以防止敏感資料外洩和惡意行為者。
- **Tags**（標籤）—GenAI 應用程式目前的應用程式標籤。如果某些列出的 GenAI 應用程式已獲使用核准，您可以將標籤修改為 **Tolerated**（已容許）或 **Sanctioned**（已認可）。

Palo Alto Networks 會在容器 *App-ID* 中針對應用程式功能將子 *App-ID* 分組。但是，標記 *App-ID* 容器是不受支援的。您必須個別標記組織內已認可、未認可或已容許的特定子 *App-ID*。



STEP 5 | 建立自訂安全性政策規則，以控制特定使用者的 GenAI 應用程式存取。

例如，根據調查，您發現有多個未認可的 GenAI 應用程式，這些應用程式都有大量資料使用量。這會帶來安全性風險，因為網路上有使用者存取未經核准的應用程式，而且您不知道正在下載或上傳的資料有哪些。在您可以執行適當的盡職調查，以了解 GenAI 應用程式的用途以及允許誰使用 GenAI 應用程式之前，您可以為所有使用者 **Block**（封鎖）GenAI 應用程式。

相反地，您注意到列出的一些**Unsanctioned**（未認可）GenAI 應用程式，但這些應用程式是獲特定使用者核准在網路上使用且有大量資料使用量的 GenAI 應用程式。在此情況下，您可以將標籤變更為 **Sanctioned**（已認可），並撰寫政策規則，以 **Allow**（允許）應用程式的使用，但僅適用於特定角色或部門中的使用者。在政策規則中，您可以為 Enterprise Data Loss Prevention (E-DLP) 資料設定檔建立關聯，以防止敏感資料外洩，以及為弱點設定檔建立關聯，以阻止入侵系統缺陷或系統未經授權存取的嘗試。

探索應用程式使用者所帶來的 GenAI 應用程式風險

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取 **Insights**（洞察） > **AI Access**（**AI** 存取），以檢視 AI Access Security 洞察儀表板。

這顯示了有風險使用者存取的熱門 GenAI 應用程式，以幫助限縮焦點。

STEP 3 | 按一下 **Review use case**（檢閱使用案例），以查看與有風險使用者存取的 GenAI 應用程式使用案例相關的 GenAI 應用程式。

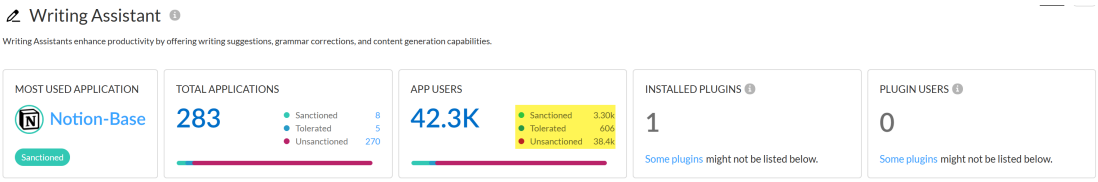
AI Access Security 洞察儀表板顯示了按使用案例存取網路上 GenAI 應用程式的預設情況，並顯示與熱門 GenAI 應用程式使用者有關的以下高階資訊。按一下使用者計數，以檢視 **User**

Name（使用者名稱）或 **IP Address**（**IP** 位址）以及該使用者存取的 GenAI **Applications**（應用程式）數量。

- 使用者詳細資訊

  這提供了存取與所選 GenAI 使用案例相關的任何 GenAI 應用程式的使用者總數摘要。AI Access Security 包含存取 **Sanctioned**（已認可）、**Tolerated**（已容許）和 **Unsanctioned**（未認可）應用程式的使用者數量詳細資訊。

  按一下 **App Users**（應用程式使用者）總數，以查看所有使用者清單，這些使用者曾存取或遭封鎖而無法存取與所選使用案例相關的 GenAI 應用程式。



- 按 **GenAI** 使用案例的使用者

  這提供了使用者總數的摘要，這些使用者會存取與所選 GenAI 使用案例相關的每個單獨 GenAI 應用程式。會列出 **Sanctioned**（已認可）、**Tolerated**（已容許）和 **Unsanctioned**（未認可）的 GenAI 應用程式，其中包含每個單獨應用程式的使用者總數。

  檢閱 **Allowed Users**（允許的使用者） 和 **Blocked Users**（遭封鎖使用者）的計數，以衡量 GenAI 應用程式安全性和存取政策規則的有效性。

  - **Allowed Users**（允許的使用者）—獲允許存取 GenAI 應用程式的使用者總數。使用此資訊來衡量安全性政策規則的有效性，透過驗證允許的使用者計數是否符合預期，或評估剛允許組織使用的 GenAI 應用程式採用率。
  - 遭封鎖的使用者—遭封鎖而無法存取 GenAI 應用程式的使用者總數。使用此資訊來驗證您是否正確設定了控制特定 GenAI 應用程式存取的安全性政策規則，或了解組織中的使用者是否正在存取未認可的 GenAI 應用程式。

  例如，考量下面的 `Grammarly` GenAI 應用程式。組織將此 GenAI 應用程式分類為已認可，供組織內的特定使用者使用。在這種案例下，安全管理員按一下 **Allowed Users**（允許的使用者）計數，並確認所有存取 GenAI 應用程式的使用者都獲允許這樣做。

  相反地，安全管理員看到超過 1,600 名使用者存取了 `Character-Ai-base` 應用程式。安全管理員將這個 GenAI 應用程式分類為未認可，並打算限制所有的組織存取。在這種情況下，安全管理員應檢閱安全性政策規則庫和控制對 `Character-Ai-base` 應用程式存取的

個別安全性政策規則，以確認該規則在安全性政策規則庫中正確定位，並確認其已正確設定為封鎖所有存取。

Name	Classification	Allowed Users	Blocked Users	Risk	Data Transferred	Sensitive Data In Motion	Plugins	Plugin Users	Data Used In ML	Enterprise Available	Threats	Actions
Sanctioned (8)												
Notion-Base	Sanctioned	2.14k	0	2	23.0 MB		0	0	No	Yes	0	
Grammarly	Sanctioned	139	0	3	5.9 MB	17	0	0	Yes	Yes	37	
Notion-Download	Sanctioned	306	0	2	387.1 KB		0	0	No	Yes	0	
Neuroflash	Sanctioned	202	0	3	180.3 KB		0	0	No	Yes	0	
Magicschool	Sanctioned	201	0	2	178.8 KB		0	0	No	Yes	0	
Describely	Sanctioned	101	0	3	89.6 KB		0	0	No	Yes	0	
Tome	Sanctioned	101	0	3	89.5 KB		0	0	No	No	0	
Hotpotai	Sanctioned	101	0	3	89.2 KB		0	0	No	No	0	
Tolerated (5)												
Unsanctioned (270)												
Character-Ai-Base	Unsanctioned	1.61k	212	4	487.2 MB		0	0	Yes	No	0	
Deepl-Write	Unsanctioned	90	12	4	45.5 MB		0	0	Yes	Yes	0	

STEP 4 | 建立自訂安全性政策規則，以控制特定使用者的 GenAI 應用程式存取。

例如，根據調查，您發現大量使用者正在存取 `bing-ai-uploading` GenAI 應用程式。雖然這是 **Sanctioned**（已認可）的 GenAI，但僅對組織內的特定使用者認可此應用程式。您可以決定編寫政策規則，明確封鎖不應存取此 GenAI 應用程式的使用者以防止濫用，並編寫安全性政策規則，明確允許對獲核准可存取 GenAI 應用程式之使用者的存取。或者，您可以編寫政策規則，允許所有使用者的存取，但實作資料遺失和威脅防護措施，以防止敏感資料的外洩，並防止惡意和釣魚 URL、惡意檔案或惡意軟體等威脅。

探索將 GenAI 應用程式安裝為第三方外掛程式所產生的風險

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取 **Insights**（洞察） > **AI Access**（**AI** 存取），以檢視 AI Access Security 洞察儀表板。

儀表板會顯示使用者安裝的第三方外掛程式數目，以及安裝第三方外掛程式的使用者數目。AI Access Security 會從 AI Access Security 儲存的所有資料中判斷這些數目。這些數目不限於時間篩選器指示的時段。

STEP 3 | 按一下 **Installed Plugins**（已安裝的外掛程式）或 **Plugin Users**（外掛程式使用者），以瀏覽至 SaaS Security Posture Management (SSPM) 中的詳細資訊。

按一下 **Installed Plugins**（已安裝的外掛程式）會開啟第 3 方外掛程式頁面，其中顯示 GenAI 第三方外掛程式的詳細資訊。您可以在此處檢閱外掛程式資訊，以判斷外掛程式是否存在風險。

按一下 **Plugin Users**（外掛程式使用者）會開啟第 3 方外掛程式頁面，其中顯示安裝第三方外掛程式的使用者詳細資訊。對於每個使用者，您可以檢視他們已安裝多少個外掛程式，以及他們已在其中安裝外掛程式的市集應用程式。使用此資訊來識別個別使用者所帶來的外掛程式風險。

STEP 4 | 若要依使用案例檢視已安裝的外掛程式，請完成下列步驟:

1. 選取 **Insights**（洞察） > **AI Access**（**AI** 存取），以檢視 AI Access Security 洞察儀表板。

   此儀表板會根據網路上的活動顯示前四個 GenAI 應用程式使用案例。儀表板也會顯示其他使用案例的圖示。

2. 瀏覽至與使用案例相關的詳細資訊。如需熱門使用案例，請按一下 **Review use case**（檢閱使用案例）。如需其他使用案例，請按一下使用案例圖示。

   使用案例詳細資訊頁面會顯示表格，其中列出使用案例的所有 GenAI 應用程式。此頁面上的

   摘要資訊包括 ***INSTALLED PLUGINS***（已安裝的外掛程式）數目和 ***PLUGIN USERS***（外掛程式使用者）數目。這些數字是從 *AI* 存取安全性儲存的所有資料中確定的，且不限於時間篩選器指定的時段。因此，這些總數可能不會反映在使用案例詳細資訊表格中。

3. 在使用案例詳細資訊表格中，識別在一或多個市集應用程式執行個體中安裝為外掛程式的 GenAI 應用程式，以及外掛程式使用者數目。此資訊顯示在表格的 **Plugins**（外掛程式）和 **Plugin Users**（外掛程式使用者）欄中。

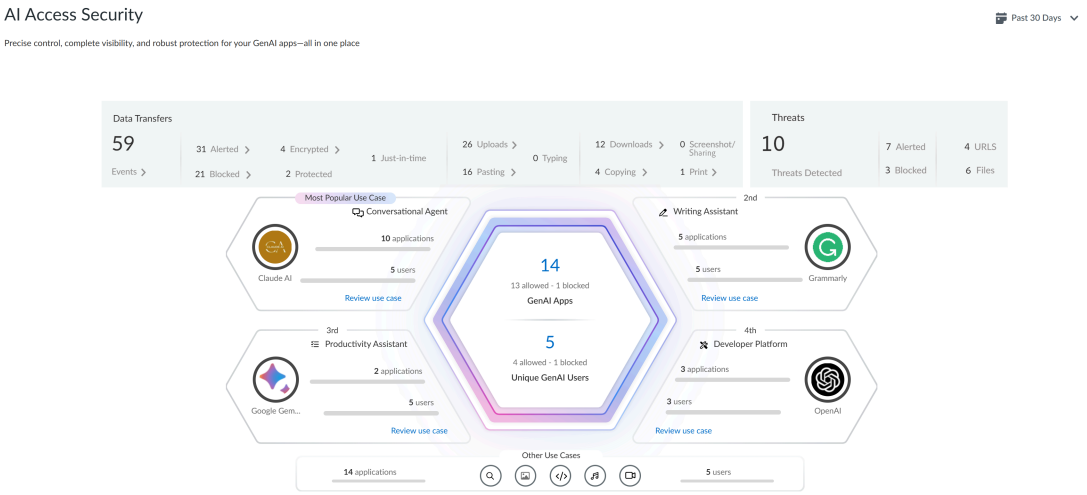
4. 針對安裝為外掛程式的 GenAI 應用程式，按一下 **Plugins**（外掛程式）或 **Plugin Users**（外掛程式使用者）欄中的數字。

   按一下 **Plugins**（外掛程式）欄中的數字，會在 SSPM 中開啟第 3 方外掛程式頁面，其中顯示使用者安裝為第三方外掛程式的 GenAI 應用程式執行個體。您可以在此處檢閱外掛程式資訊，以判斷外掛程式是否存在風險。

   按一下 **Plugin Users**（外掛程式使用者）欄中的數字會開啟第 3 方外掛程式頁面，其中顯示已將應用程式安裝為第三方外掛程式的使用者詳細資訊。使用此資訊來識別個別使用者所帶來的外掛程式風險。

探索 Prisma Access Browser 上 GenAI 應用程式所帶來的風險

Prisma Access Browser 內嵌於 AI Access Security，為 Prisma Access Browser 獨立客戶提供全面的 GenAI 應用程式可視性、存取控制、資料和威脅防護。此整合提供最全面的 GenAI 應用程式目錄，內含資料分類和即時威脅防禦等深度最後一哩路控制功能。身為 Prisma Access Browser 獨立安全性管理員，您可以在 [Insights（洞察）] 功能表下存取 AI Access Security，以透過 Prisma Access Browser 監控第三方 AI 應用程式使用情況，並掌握詳細分析，包括應用程式指標、使用者活動、偵測到的威脅和資料傳輸。

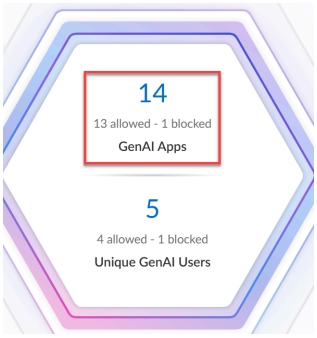


STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取 **Insights**（洞察） > **AI Access**（**AI** 存取），以檢視獨立 Prisma Access Browser 的 AI Access Security 洞察儀表板。

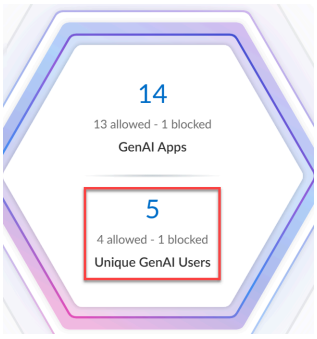
STEP 3 | 按一下 **GenAI** 應用程式，以檢視應用程式指標，內含 **Is GenAI:Yes**（是 **GenAI**：是）和 **Category:Access**（類別：存取）篩選器以檢視下列指標：

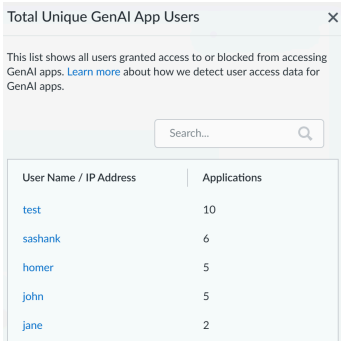
- GenAI 應用程式總數
- 允許的 GenAI 應用程式
- 已封鎖的 GenAI 應用程式



STEP 4 | 按一下 **Unique GenAI Users**（唯一的 **GenAI** 使用者），以檢視已獲授予存取或遭封鎖而無法存取 GenAI 應用程式的 GenAI 應用程式使用者總數。選取使用者（從 **Total Unique GenAI App Users**（唯一 **GenAI** 應用程式使用者總數）頁面，以瀏覽至事件頁面（已套用 **User:**（使用者：）**<user name>**篩選器），以了解針對該特定使用者允許和封鎖的 GenAI 應用程式。可用的指標包括：

- GenAI 使用者總數
- 允許的 GenAI 使用者
- 已封鎖的 GenAI 使用者

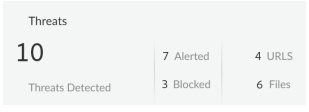




STEP 5 | 按一下 **Threats Detected**（偵測到威脅） Widget，以檢視偵測到和封鎖的威脅總數。

此資訊可在事件頁面取得（已套用 **Is GenAI:Yes**（是 **GenAI**：是），**Category:Malware**（目錄：惡意軟體）篩選器）。可用的指標包括：

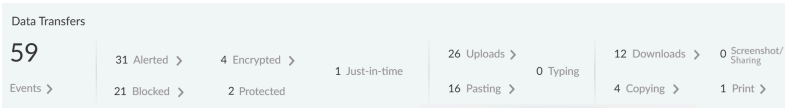
- 顯示所偵測和封鎖威脅總數的 GenAI 威脅總數。
- 惡意 URL（已套用篩選器：**Category:Malware**（目錄：惡意軟體）和 **Type:Malicious website**（類型：惡意網站））
- 檔案（已套用篩選器：**Category:Malware**（目錄：惡意軟體）和 **Type:**（類型：已識別惡意檔案））



STEP 6 | 按一下 **Data Transfers**（資料傳輸）Widget，以檢視當流量符合 Prisma Access Browser 企業資料遺失防護 (E-DLP) 資料設定檔中的比對規則時偵測到的資料傳輸事件數目。

此資訊可在事件頁面取得（已套用 **Is GenAI:Yes**（是 **GenAI**：是），**Category:DLP**（類別：**DLP**）篩選器）。

- 偵測到的資料傳輸總數。已套用的篩選器：**Is GenAI:Yes**（是 **GenAI**：是）、**Category:DLP**（類別：**DLP**）。
- 已警示資料傳輸。已套用的篩選器：**Is GenAI:Yes**（是 **GenAI**：是）、**Category:DLP**（類別：**DLP**）、**Action:Allowed**（動作：已允許）。
- 已封鎖資料傳輸。已套用的篩選器：**Is GenAI:Yes**（是 **GenAI**：是）、**Category:DLP**（類別：**DLP**）、**Action:Blocked**（動作：已封鎖）。
- 受保護的資料傳輸：允許但只能供瀏覽器使用的動作。例如，在認可的應用程式之間啟用的資料複製和貼上，並加以封鎖，使在瀏覽器或本機桌面應用程式中的其他應用程式無法使用。已套用的篩選器：**Is GenAI:Yes**（是 **GenAI**：是）、**Category:DLP**（類別：**DLP**）、**Action:Allowed Protected**（動作：允許受保護）。
- 資料傳輸已加密：加密動作，僅瀏覽器擁有針對特定使用者和其所加密裝置的解密金鑰。這允許下載檔案，並確保允許將檔案上傳（解密）至特定應用程式，或在離線模式在瀏覽器中開啟。其他應用程式無法開啟檔案，因此其是您不想在端點（例如，在未受管裝置）使用之檔案的理想選項。已套用的篩選器：**Is GenAI:Yes**（是 **GenAI**：是）、**Category:DLP**（類別：**DLP**）、**Action:Allowed Encrypted**（已允許加密）。
- 對資料傳輸進行即時控制:動作包括在繼續之前警告使用者、要求使用者在繼續之前提供業務理由，或觸發管理員核准流程。這些動作會在緊急情況下觸發暫時存取或略過規則，或出於合規性原因需要提供理由和記錄。已套用的篩選器：**Is GenAI:Yes**（是 **GenAI**：是）、**Category:DLP**（類別：**DLP**）、**Action:Permission Requested**（動作：已要求權限）。
- 資料傳輸已上傳。已套用的篩選器：**Is GenAI:Yes**（是 **GenAI**：是）、**Category:DLP**（類別：**DLP**）、**Type:File upload**（類型：檔案上傳）。
- 剪貼簿活動（貼上）中的資料傳輸。已套用的篩選器：**Is GenAI:Yes**（是 **GenAI**：是）、**Category:DLP**（類別：**DLP**）、**Type:Clipboard Paste**（類型：剪貼簿貼上）。
- 目前輸入的資料傳輸。已套用的篩選器：**Is GenAI:Yes**（是 **GenAI**：是）、**Category:DLP**（類別：**DLP**）、**Type:Sanitizing Content**（類型：清理內容）。
- 資料傳輸已下載。已套用的篩選器：**Is GenAI:Yes**（是 **GenAI**：是）、**Category:DLP**（類別：**DLP**）、**Type:File download**（類型：檔案已上傳）。
- 資料傳輸已複製。已套用的篩選器：**Is GenAI:Yes**（是 **GenAI**：是）、**Category:DLP**（類別：**DLP**）、**Type:Clipboard Copy**（類型：剪貼簿複製）。
- 使用螢幕截圖共用的資料傳輸。已套用的篩選器：**Is GenAI:Yes**（是 **GenAI**：是）、**Category:DLP**（類別：**DLP**）、**Type:Screen share**（類型：螢幕共用）。
- 資料傳輸已列印。已套用的篩選器：**Is GenAI:Yes**（是 **GenAI**：是）、**Category:DLP**（類別：**DLP**）、**Type:Print**（類型：列印）。



標記 GenAI 應用程式

根據 GenAI 應用程式的風險分數和其他考量事項，您可以將標籤套用至應用程式，以反映應用程式是否在組織內獲得核准。下列為可用的標籤:

頁籤	說明
已認可	應用程式已獲組織核准，且正由組織的成員使用。
未認可	組織未核准此應用程式。例如，由於與應用程式相關聯的安全性風險，應用程式可能未獲認可。 由於組織的成員不應使用應用程式，因此您應採取行動來封鎖應用程式。您可以使用政策規則封鎖應用程式。
已容許	應用程式不像已認可的應用程式那樣受信任。但是，組織會允許其使用，直到組織能夠識別更安全的應用程式為止。應用程式已獲容許，以免影響組織的生產力。 由於儘管存在潛在的安全性風險，但仍允許此應用程式，因此您可能會採取步驟來限制某些動作。例如，您可以建立政策規則，以封鎖應用程式的上傳或下載操作。

Palo Alto Networks 會在容器 *App-ID* 中針對應用程式功能將子 *App-ID* 分組。但是，標記 *App-ID* 容器是不受支援的。您必須個別標記組織內已認可、未認可或已容許的特定子 *App-ID*。

例如，考慮包含下列子 *App-ID* 的 `claude` 容器 *App-ID*：`claude-base`、`claude-upload`、`claude-edit`、`claude-post` 和 `claude-delete`。

您可以建立應用程式篩選器，以對已認可的應用程式強制執行相同的資料外洩控制。在此情況下，您必須標記所有 `claude` *App-ID* 容器的子 *App-ID*，以對 ***Sanctioned***（已認可）`claude` *GenAI* 應用程式的所有子程序套用政策規則動作。

2024 年 9 月，Palo Alto Networks 更新了應用程式標記的實作方式。從 2024 年 9 月開始，系統會將標籤寫入新的預先定義的 `Application-Tagging` 片段，並從中進行讀取。將此更新發佈至租用戶後，其會在您首次標記應用程式時生效。標籤會寫入至片段和 AI Access Security、活動洞察應用程式頁面，而且 Strata Cloud Manager Command Center 會開始顯示來自片段的標籤資訊。如果您在此更新之前標記了應用程式，則不會再看到在 AI Access Security 和活動洞察應用程式中反映的那些標籤變更。`Application-Tagging` 段會追蹤哪些應用程式標記為 **Sanctioned**（已認可）或 **Tolerated**（已容許）。未明確標記為 **Sanctioned**（已認可）或 **Tolerated**（已容許）的應用程式，會被視為 **Unsanctioned**（未認可）。因此，只會在 Strata Cloud Manager 中顯示您在此更新之後新增的標籤。所有其他應用程式都會顯示為 **Unsanctioned**（未認可）。

只要您在 `Application-Tagging` 設定範圍內關聯 Application-Tagging 片段並套用標籤，在此更新之前套用的標籤仍會影響在 NGFW 或 Prisma Access 部署上的以標籤為基礎政策強制執行。

- NGFW 和 Prisma Access 應用程式設定
- 活動洞察應用程式

在應用程式設定中標記 GenAI 應用程式

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 建立與預先定義的 `Application-Tagging` 片段與適當設定範圍的關聯，以支援以標籤為基礎的政策強制執行。

STEP 3 | 獲得您想要標記的子 App-ID。

您可以使用以下方法之一獲得 GenAI 應用程式的子 App-ID。

- 使用 AI Access Security 洞察儀表板來探索 GenAI 應用程式所產生的風險。AI Access Security 洞察顯示您在組織中使用的檢測到的子 App-ID。
- 檢閱支援的 GenAI 應用程式清單。
- 使用 Applipedia (應用程式百科) 搜尋透過動態內容更新傳遞的支援 GenAI 應用程式的子 App-ID。

  Applipedia (應用程式百科) 只顯示透過動態內容傳遞的應用程式 App-ID，並不顯示透過 App-ID 雲端引擎 (ACE) 傳遞的應用程式。

STEP 4 | 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（物件） > **Applications**（應用程式） > **Applications**（應用程式）。

STEP 5 | 在 **Configuration Scope**（設定範圍）中，選取 `Application-Tagging` 片段。

如果您正在標記透過 App-ID 雲端引擎 (ACE) 傳遞的 App-ID，則必須將與所選資料夾相關聯的所有 NGFW 或 Prisma Access 租用戶設定為接收來自 ACE 的 App-ID 更新。

當 NGFW 或 Prisma Access 租用戶擁有有效的 SaaS Security Inline 或 AI Access Security 授權時，ACE 預設為啟用。您也可以手動啟用 NGFW 的 ACE。

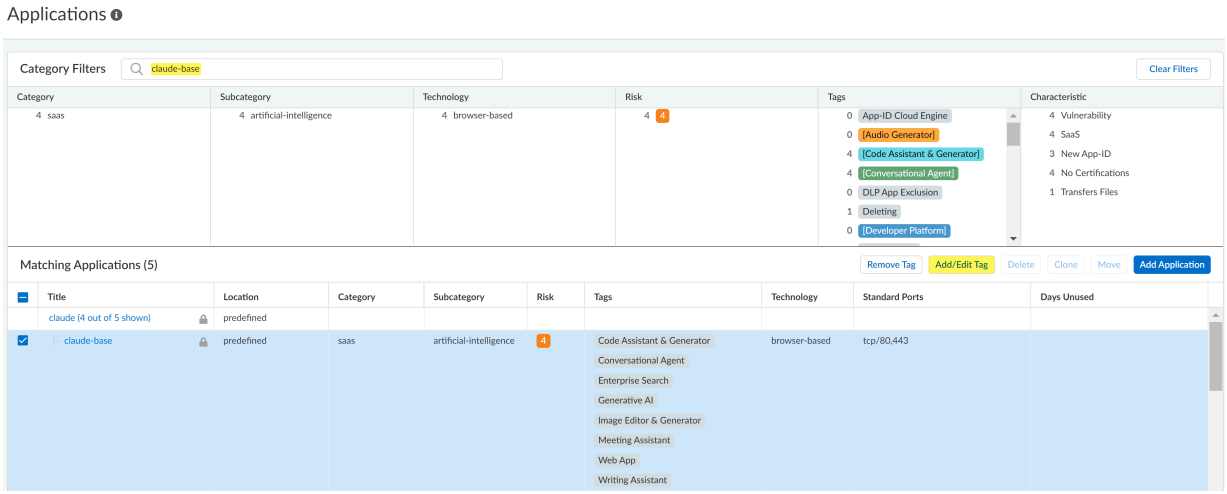
如果您標記從 ACE 傳遞的 App-ID，而且未將與所選資料夾相關聯的至少一個 NGFW 或 Prisma Access 租用戶設定為接收來自 ACE 的 App-ID 時，則設定推送會失敗。

因此，Palo Alto Networks 不建議選取 **Global**（全域）設定範圍。

STEP 6 | 在 **Category Filters**（類別篩選器）搜尋欄位中，輸入您想要標記的 App-ID 並加以選取。

您一次只能標記一個 App-ID。

STEP 7 | **Add/Edit Tag**（新增/編輯標籤）。



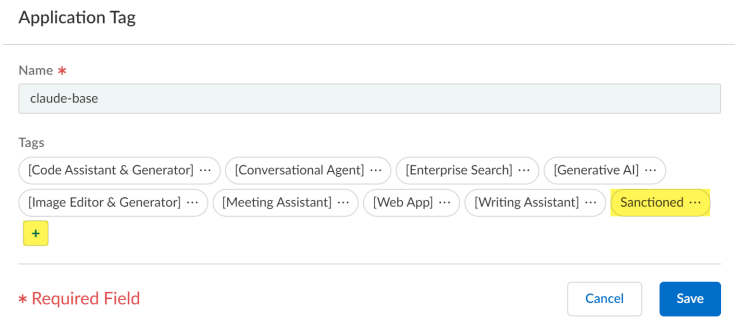
STEP 8 | 按一下 **+** 以套用預先定義的 **Sanctioned**（已認可）或 **Tolerated**（已容許）應用程式標籤。

在此範例中，`claude-base` App-ID 被標記為 **Sanctioned**（已認可）標籤。

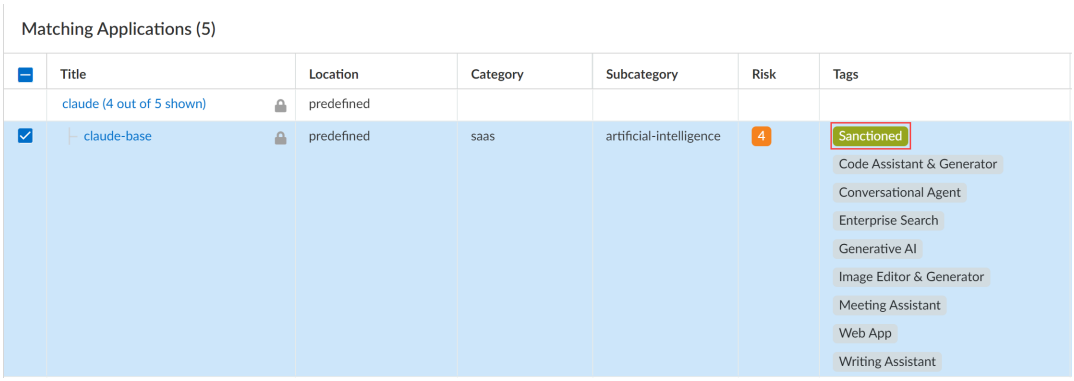
在從 ***Applications***（應用程式）進行標記時，如果沒有 ***Sanctioned***（已認可）或 ***Tolerated***（已容許）標籤，則會將應用程式視為 ***Unsanctioned***（未認可）。

如果您想將應用程式標籤從 ***Sanctioned***（已認可）或 ***Tolerated***（已容許）變更為 ***Unsanctioned***（未認可），則您需要移除現有的標籤。您不能手動從 ***Applications***（應用程式）將應用程式標記為 ***Unsanctioned***（未認可）。

STEP 9 | **Save**（儲存）。



STEP 10 | 檢閱 **Tag**（標籤）欄中的值，以驗證您是否成功套用應用程式標籤。



STEP 11 | 按一下 **Overview**（概要）。

STEP 12 | 推送設定並推送您的設定變更。

在洞察儀表板中標記 GenAI 應用程式

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 建立與預先定義的 `Application-Tagging` 片段與適當設定範圍的關聯，以支援以標籤為基礎的政策強制執行。

STEP 3 | 獲得您想要標記的子 App-ID。

您可以使用以下方法之一獲得 GenAI 應用程式的子 App-ID。

- 使用 AI Access Security 洞察儀表板來探索 GenAI 應用程式所產生的風險。AI Access Security 洞察顯示您在組織中使用的檢測到的子 App-ID。
- 檢閱支援的 GenAI 應用程式清單。
- 使用 Applipedia (應用程式百科) 搜尋透過動態內容更新傳遞的支援 GenAI 應用程式的子 App-ID。

  Applipedia (應用程式百科) 只顯示透過動態內容傳遞的應用程式 App-ID，並不顯示透過 App-ID 雲端引擎 (ACE) 傳遞的應用程式。

STEP 4 | 選取 **Insights**（洞察） > **Activity Insights**（活動洞察） > **Applications**（應用程式）。

STEP 5 | 找到您要標記的 GenAI 子 App-ID。如有必要，您可以篩選表格以僅顯示 GenAI 應用程式。

1. **Add Filter**（新增篩選器）並新增 **GenAI Application**（**GenAI** 應用程式）篩選器。
2. 將 **GenAI Application**（**GenAI** 應用程式）篩選器設為 **TRUE**。

STEP 6 | 若要檢閱在 GenAI App-ID 中套用的標籤，請檢查 **Tag**（標籤）欄中的值。

STEP 7 | 對子 GenAI App-ID 套用不同的標籤。

1. 在 **Actions**（動作）欄中，選取標籤圖示並選擇 **Sanctioned**（已認可）、**Tolerated**（已容許）或 **Unsanctioned**（未認可）標籤。
2. **Apply**（套用）新標籤。

查看指派給 GenAI 應用程式的風險分數

為了幫助您快速識別對組織構成最大威脅的 GenAI 應用程式，AI Access Security 會為每個 GenAI 應用程式指派風險分數。這些風險分數使您能夠快速識別有風險的 GenAI 應用程式，以便您採取保護環境的行動。例如，為了保護環境，您可以建立政策規則來封鎖該應用程式。您也可以選擇將該應用程式標記為未認可。

應用程式的風險分數介於 1（低風險）和 5（高風險）之間，並以 SaaS 應用程式屬性為基礎。某些屬性對所有 SaaS 應用程式是通用的，而一部分屬性則是 GenAI 應用程式特有的。

GenAI 屬性這類屬性是指使用者輸入到應用程式的資料類型、應用程式產生的輸出資料類型，以及應用程式是否使用使用者提交的資料來訓練其 GenAI 模型。根據 GenAI 屬性值，風險分數計算會判斷 GenAI 風險。

除了 GenAI 屬性外，風險分數計算還使用以下類型的屬性，來判斷應用程式的一般 SaaS 風險。

- 合規性屬性，用於識別應用程式是否遵循各種法規要求和標準。
- 識別存取管理屬性，用於識別應用程式的驗證和存取控制能力。
- 安全性和隱私權屬性，用於識別保護資料的產品功能。這類屬性包括應用程式是否對靜態資料和傳輸中的資料進行加密等屬性。

GenAI 應用程式的最終風險分數是一般 SaaS 風險（根據 SaaS 屬性計算）和 GenAI 風險（根據 GenAI 屬性計算）的組合。風險分數計算在判斷最終風險分數時，對 GenAI 風險給予額外權重。

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 要前往活動洞察儀表板，請選取 **Insights**（洞察） > **Activity Insights**（活動洞察） > **Applications**（應用程式）。

STEP 3 | 在表格中找到 GenAI 應用程式。如有必要，您可以篩選表格以僅顯示 GenAI 應用程式。

1. **Add Filter**（新增篩選器）並新增 **GenAI Application**（**GenAI** 應用程式）篩選器。
2. 將 **GenAI Application**（**GenAI** 應用程式）篩選器設為 **TRUE**。

STEP 4 | 要識別對應用程式構成最大威脅的 GenAI 應用程式，請檢查 **Risk**（風險）欄中的風險分數值。

風險分數	意義
4-5	高風險 — 很可能存在風險。
3	中風險 — 代表中等風險。
1-2	低風險 — 不太可能存在風險。

STEP 5 | 對風險最高的應用程式採取行動。

例如，您可以建立政策規則來封鎖這些應用程式或將這些應用程式標記為未認可。

使用應用程式篩選器來管理 GenAI 應用程式

應用程式篩選器根據您定義的應用程式屬性動態分組應用程式。您可以在安全性政策規則中使用應用程式篩選器，根據應用程式屬性控制對 GenAI 應用程式的存取，而不是在安全性政策規則中明確定義 GenAI 應用程式或應用程式群組。

AI Access Security 包括以下預先定義的 GenAI 應用程式篩選器。預先定義的應用程式篩選器是以支援的AI Access Security 使用案例為基礎。

- 音訊產生器
- 對話代理程式
- 程式碼助理和產生器
- 開發人員平台
- 企業搜尋
- 影像編輯器與產生器
- 會議助理
- 生產力助理
- 視訊編輯器與產生器
- 寫作助理

上述篩選器僅為顯示標籤。其不能在安全性政策規則中使用。

- Strata Cloud Manager
- Panorama

在 Strata Cloud Manager 為 GenAI 應用程式使用應用程式篩選器

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取 **Manage**（管理） > **Configuration**（設定） > **Objects**（物件） > **Application**（應用程式） > **Application Filters**（應用程式篩選器）和 **Add Applications**（新增應用程式篩選器）。

STEP 3 | 輸入描述性的 **Name**（名稱）。

STEP 4 | 對於 **Tag**（標籤），選取 **Generative AI**（生成式 **AI**）。

檢查時，會將所有由 NGFW 或 Prisma Access 檢查的 GenAI 應用程式標記為 `genai`。為 GenAI 應用程式建立自訂應用程式篩選器時，Palo Alto Networks 建議選取 **Generative AI**（生成式 **AI**）標籤，以確保將應用程式篩選器新增的安全性政策規則適用於 GenAI 應用程式流量。

STEP 5 | 設定其他類別篩選器，以縮小受影響的 GenAI 應用程式範圍。建立 GenAI 應用程式篩選器時，請考慮下列標籤。

- **Risk**（風險）—指定 **Risk**（風險）分數，以便安全性政策規則動作僅適用於具有所選風險分數的 GenAI 應用程式。

  例如，您想要撰寫安全性政策規則，以封鎖對所有有風險 GenAI 應用程式的存取，而無論其用途為何。在此情況下，您可以為 GenAI 應用程式 **4** 和 **5** 建立應用程式篩選器，以便安全性政策規則僅適用於具有這些風險分數的 GenAI 應用程式。

- **Tag**（標籤）—指定安全性政策規則動作是否適用於標記為 **Sanctioned**（已認可）、**Tolerated**（已容許）或 **Unsanctioned**（未認可）的 GenAI 應用程式。此外，您可以根據 GenAI 應用程式使用案例套用標籤。

  例如，您想要撰寫安全性政策規則，以允許對已認可程式碼助理和產生器 GenAI 應用程式的存取。在此案例中，您可以建立應用程式篩選器，其包含 **Sanctioned**（已認可）和 **Code Asistant & Generator**（程式碼助理和產生器）標籤，因此安全性政策規則僅適用於具有此應用程式標籤且屬於此使用案例的 GenAI 應用程式。

STEP 6 | 檢閱 **Matching Applications**（比對應用程式）清單。

STEP 7 | **Save**（儲存）。

STEP 8 | **Push Config**（推送設定）和 **Push**（推送）。

STEP 9 | 建立自訂安全性政策規則，以控制 GenAI 存取.

在 Panorama 使用 GenAI 應用程式的應用程式篩選器

STEP 1 | 登入 Panorama™ management server 網頁介面。

STEP 2 | 選取 **Objects**（物件） > **Application Filters**（應用程式篩選器），並 **Add**（新增）應用程式篩選器。

STEP 3 | 輸入描述性的 **Name**（名稱）。

STEP 4 | 對於 **Tag**（標籤），選取 **Generative AI**（生成式 **AI**）。

檢查時，會將所有由 NGFW 或 Prisma Access 檢查的 GenAI 應用程式標記為 `genai`。為 GenAI 應用程式建立自訂應用程式篩選器時，Palo Alto Networks 建議選取 **Generative AI**（生成式 **AI**）標籤，以確保將應用程式篩選器新增的安全性政策規則適用於 GenAI 應用程式流量。

STEP 5 | 設定其他類別篩選器，以縮小受影響的 GenAI 應用程式範圍。建立 GenAI 應用程式篩選器時，請考慮下列標籤。

- **Risk**（風險）—指定 **Risk**（風險）分數，以便安全性政策規則動作僅適用於具有所選風險分數的 GenAI 應用程式。

  例如，您想要撰寫安全性政策規則，以封鎖對所有有風險 GenAI 應用程式的存取，而無論其用途為何。在此情況下，您可以為 GenAI 應用程式 **4** 和 **5** 建立應用程式篩選器，以便安全性政策規則僅適用於具有這些風險分數的 GenAI 應用程式。

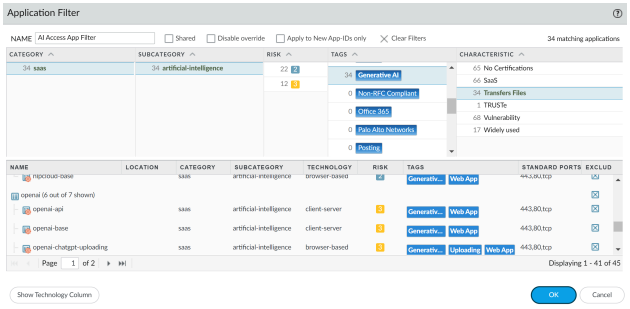
STEP 6 | 檢閱比對應用程式清單。

STEP 7 | 按一下 **OK**（確定）。

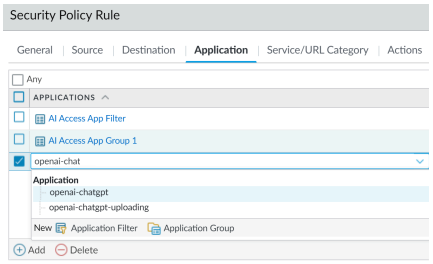
STEP 8 | 選取 **Commit**（提交）並 **Commit and Push**（提交和推送）組態變更。

STEP 9 | 建立自訂安全性政策規則，以控制 GenAI 存取.

STEP 10 | 在以下範例中，**AI Access App Filter**（**AI** 存取應用程式篩選器）應用程式篩選器具有類別：SaaS、子類別：人工智慧、標籤：生成式 AI、和特性：傳輸檔案。這會建立包含 34 個相符 GenAI 應用程式的篩選器。



STEP 11 | 在以下範例中，選擇 openai-chatgpt 作為 **Application**（應用程式）。



STEP 12 | 從與對話 AI 相關的 [Category（類別）]、[Subcategory（子類別）]、[Technology（技術）]、[Risk（風險）]、[Characteristic（特性）] 和 [Tags（標籤）] 區段選取屬性值，來定義篩選器。例如，當您選取與對話聊天相關的值時，請注意對話底部的相符應用程式清單範圍會隨之縮小。當您調整篩選器屬性，以符合您要安全啟用的應用程式類型時，請選取 **Save**（儲存）。

修改預設 GenAI 應用程式存取政策規則，以控制 GenAI 存取

在 Strata Cloud Manager 中修改預設的 GenAI 應用程式政策規則，以控制企業中的 GenAI 應用程式使用情況。

- 在 *Strata Cloud Manager* 中，即使您可以透過安全性政策為 *GenAI* 應用程式建立自訂政策規則，*Palo Alto Networks* 建議您使用網際網路存取安全性政策規則來有效建立政策規則。
- 如果未啟用 *Enterprise Data Loss Prevention (E-DLP)* 授權，則 *Palo Alto Networks* 不建議在同一政策中同時擁有 *GenAI* 和非 *GenAI* 應用程式。

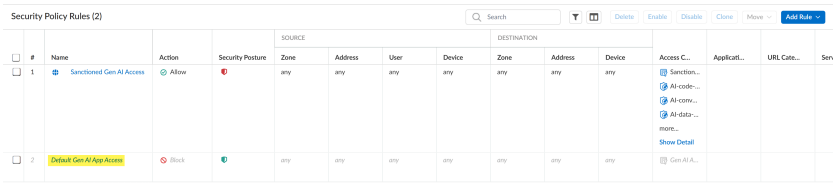
對於 Strata Cloud Manager，AI Access Security 包含預先定義的預設 GenAI 應用程式存取，以使用現成的政策，控制對企業中未明確允許的所有 GenAI 應用程式的存取。依預設，此政策規則會封鎖企業中的所有 GenAI 應用程式。若要修改此政策：

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW** 和 **Prisma Access** > **Security Services**（安全性服務） > **Security Policy**（安全性政策）並選取目標 **Configure Scope**（設定範圍）（*Gen-AI-Best-Practice* 片段）。

STEP 3 | 按一下預先定義的預設 GenAI 應用程式存取政策規則。

此政策規則會封鎖對所有 GenAI 應用程式的存取。



STEP 4 | **Enable**（啟用）預設 GenAI 應用程式存取政策規則。預設為停用。

STEP 5 | 在 [Web Application（Web 應用程式）] 區段，根據需要設定 **Application**（應用程式）和 **URL Category**（URL 類別）。依預設，預設 GenAI 應用程式存取政策規則會封鎖對所有 GenAI 應用程式的存取。但是，您可以修改預先定義的政策規則，以透過選取個別應用程式、應用程式群組或應用程式篩選器來封鎖特定應用程式。

- **Application**（應用程式）—新增一或多個 GenAI 應用程式。
- **Application Group**（應用程式群組）—應用程式群組是您建立的個別應用程式的靜態分組。
- **Application Filter**（應用程式篩選器）—應用程式篩選器會根據您定義的應用程式篩選器動態分組應用程式。

  例如，您可以使用預先定義或自訂的 GenAI 應用程式篩選器，動態控制組織中 GenAI 應用程式的存取權，而不是新增個別的 GenAI 應用程式，或建立必須在每次需要變更時手動更新的應用程式群組。

STEP 6 | **Save**（儲存）。

STEP 7 | **Push Config**（推送設定）和 **Push**（推送）。

建立自訂安全性政策規則，以控制 GenAI 存取

您可以建立自訂安全性政策規則，以控制 GenAI 應用程式的使用，並防止將敏感資料外洩到已認可的 GenAI 應用程式。使用標籤、來源（以來源來基礎的流量）、使用者群組和其他特定參數，來建置自訂政策。這有助於您在組織中，為 GenAI 應用程式強制執行自訂的安全性政策規則。

(Strata Cloud Manager) 您可以使用或修改預先定義的 **Sanctioned GenAI Access**（已認可的 **GenAI** 存取）自訂網際網路存取政策規則，或建立您自己的自訂網際網路存取政策規則。

(Panorama™ management server) 建立安全性政策規則，以控制組織中 GenAI 應用程式的使用。

您必須建立安全性政策規則，以控制獨立於未認可 GenAI 應用程式的已認可和已容許的 GenAI 應用程式。例如，如果已容許的 GenAI 應用程式只能由組織中的特定使用者存取，您可以建立安全性政策規則，只允許那些特定使用者的存取。您可以將 Enterprise Data Loss Prevention (E-DLP) 資料設定檔與安全性政策規則建立關聯，以防止敏感資料的外洩，並使用弱點保護設定檔，來阻止嘗試入侵系統缺陷或允許的使用者獲得未經授權的系統存取行為。此外，您可以在規則庫階層中建立第二個安全性政策規則，以拒絕其他所有人的存取。

- 在 *Strata Cloud Manager* 中，即使您可以透過安全性政策為 *GenAI* 應用程式建立自訂政策規則，建議您使用網際網路存取政策規則，來有效建立政策規則。
- 如果未啟用 *Enterprise Data Loss Prevention (E-DLP)* 授權，則不建議在同一政策中同時擁有 *GenAI* 和非 *GenAI* 應用程式。

- Strata Cloud Manager
- Panorama

建立自訂政策規則，以控制 GenAI 應用程式使用情況 (Strata Cloud Manager)

網際網路存取安全性政策規則的評估和執行會在安全性政策規則之前發生。如果網際網路存取和安全性政策規則都套用於相同的流量，則網際網路存取政策規則的動作和 *Enterprise DLP* 檢查設定將優先於安全性政策規則。在成功比對網際網路存取政策規則後，不會執行進一步的政策規則評估。

例如，您建立套用至使用者群組 *A* 和多個 *GenAI* 應用程式的網際網路存取政策規則和安全性政策規則。

- 網際網路存取政策規則 *A* 允許使用者群組 *A* 存取指定的 *GenAI* 應用程式，並且擁有與 *GenAI* 應用程式關聯的 *Enterprise DLP* 資料設定檔 *A*，可防止敏感資料外洩。
- 安全性政策規則 *B* 可防止使用者群組 *A* 存取相同的指定 *GenAI* 應用程式。

在這種案例下，當使用者群組 *A* 中的任何使用者存取在網際網路存取和安全性政策規則中指定的 *GenAI* 應用程式時，他們會獲允許，並且會執行 *Enterprise DLP* 檢查和裁定呈現，因為網際網路存取政策規則 *A* 在政策規則庫的評估順序中更高。

STEP 1 | 使用 AI Access Security 洞察儀表板來探索 GenAI 應用程式所產生的風險。

AI Access Security 洞察儀表板可提供整個組織 GenAI 應用程式使用情況的詳細全面檢視。您可能會發現有風險的 GenAI 應用程式使用案例、個別有風險的 GenAI 應用程式，以及存取 GenAI 應用程式的有風險使用者。

STEP 2 | 如果您想在片段中使用現有政策，請執行初始 AI Access Security 設定。

在 Strata Cloud Manager，這包括建立 Enterprise Data Loss Prevention (E-DLP) 資料設定檔以定義敏感資料比對規則、建立與預先定義的 `Gen-AI-Best-Practice` 和 `Application-Tagging` 片段的關聯，以及用於阻止試圖入侵系統缺陷或獲得未經授權系統存取的弱點保護設定檔。

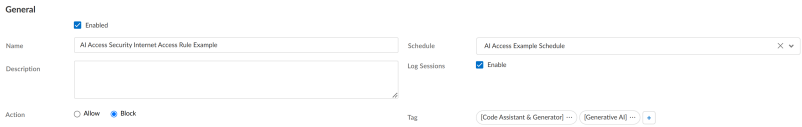
對於 NGFW，這還包括建立內部信任區域和輸出不受信任的區域。

STEP 3 | 如果您想建立自己的自訂政策，請登入 Strata Cloud Manager。

STEP 4 | 建立自訂的網際網路存取政策規則。

- 在 *Strata Cloud Manager* 中，即使您可以透過安全性政策為 *GenAI* 應用程式建立自訂政策規則，建議您使用網際網路存取政策規則，來有效建立政策規則。
- 如果未啟用 *Enterprise Data Loss Prevention (E-DLP)* 授權，則不建議在同一政策中同時擁有 *GenAI* 和非 *GenAI* 應用程式。

1. 選取 **Add Rule**（新增規則） > **Internet Access Rule**（網際網路存取規則）。
2. **Enable**（啟用）網際網路存取政策規則。
3. 輸入描述性的 **Name**（名稱）。
4. （選用）為網際網路存取政策規則新增 **Description**（描述），並新增預先定義的 **Tag**（標籤）或建立新的標籤。
5. 設定 **Action**（動作）（**Block**（封鎖）或 **Allow**（允許））。
6. （選用）設定 **Schedule**（排程），以指定網際網路存取政策規則的啟用時間。



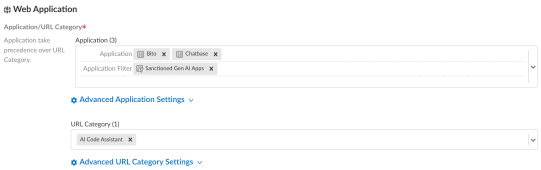
7. 在比對規則區段，定義要根據流量 **Source**（來源）（流量的來源）強制執行的流量。

   例如，根據風險探索調查，您確定與 使用者群組 A 相關的未經授權使用者存取了由 使用者群組 B 認可使用的 GenAI 應用程式。在這種案例中，您可以建立網際網路存取政策規則，以封鎖對 GenAI 的存取，並將使用者群組 A 新增為使用者群組 **Source**（來源）。
8. 在 Web 應用程式區段，設定 **Application**（應用程式）或 **URL Category**（**URL** 類別），以定義您想要封鎖或允許存取的 GenAI 應用程式或 GenAI 應用程式 URL。

   （允許的 GenAI 應用程式）只將支援的 GenAI 應用程式新增到允許的應用程式清單中。

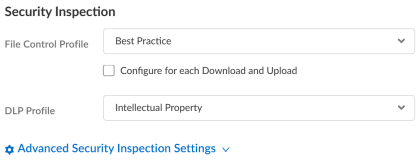
   - **Application**（應用程式）—新增一或多個 GenAI 應用程式。
   - **Application Group**（應用程式群組）—應用程式群組是您建立的個別應用程式的靜態分組。
   - **Application Filter**（應用程式篩選器）—應用程式篩選器會根據您定義的應用程式篩選器動態分組應用程式。

     例如，您可以使用預先定義或自訂的 GenAI 應用程式篩選器，動態控制組織中 GenAI 應用程式的存取權，而不是新增個別的 GenAI 應用程式，或建立必須在每次需要變更時手動更新的應用程式群組。



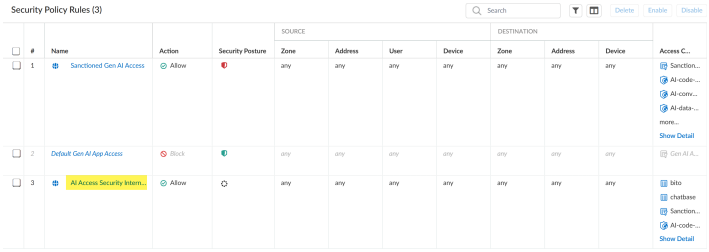
9. （允許的 GenAI 應用程式）在 [Security Inspection（安全檢查）] 區段，選取檔案封鎖和 Enterprise DLP 設定檔以防止敏感資料的外洩。

- 檔案控制設定檔—檔案封鎖設定檔可讓您識別要封鎖或監控的特定檔案類型。您可以建立自訂的檔案封鎖設定檔或使用預設的最佳做法檔案封鎖設定檔。
- **DLP** 設定檔—Enterprise DLP資料設定檔允許您定義要檢查和封鎖的敏感資料比對規則，以防止敏感資料的外洩。您必須在探索 GenAI 應用程式帶來的風險時指派資料設定檔，以產生 **Sensitive Assets**（敏感資產）資料。



10. 根據需要設定其餘的自訂網際網路存取政策規則。
11. **Save**（儲存）。

STEP 5 | 驗證存取政策規則是否成功建立，並根據需要在政策規則庫中加以排序。



STEP 6 | **Push Config**（推送設定）和 **Push**（推送）。

建立自訂政策規則，以控制 GenAI 應用程式使用情況 (Panorama)

STEP 1 | 使用 AI Access Security 洞察儀表板來探索 GenAI 應用程式所產生的風險。

AI Access Security 洞察儀表板可提供整個組織 GenAI 應用程式使用情況的詳細全面檢視。您可能會發現有風險的 GenAI 應用程式使用案例、個別有風險的 GenAI 應用程式，以及存取 GenAI 應用程式的有風險使用者。

STEP 2 | 執行初始 AI Access Security 設定。

這包括建立 Enterprise Data Loss Prevention (E-DLP) 資料設定檔，以定義敏感資料比對規則和弱點保護設定檔，用於阻止入侵系統缺陷或對系統未經授權存取的嘗試。

對於 NGFW，這還包括建立內部信任區域和輸出不受信任的區域。

STEP 3 | 登入 Panorama™ management server 網頁介面。

STEP 4 | 選取 **Policies**（原則） > **Security**（安全性），然後指定 Device Group（裝置群組）。

STEP 5 | **Add**（新增）安全性政策規則。

STEP 6 | 設定安全性政策規則 **General**（一般）、**Source**（來源）和 **Destination**（目的地）設定。

如需撰寫安全性政策規則的詳細資訊，請參閱安全性政策管理指南。

- **General**（一般）—為安全性規則指定描述性 **Name**（名稱）。您也可以選擇提供安全性政策規則的 **Description**（說明），並套用標籤來協助識別安全性政策規則的目的。
- **Source**（來源）—定義流量必須源於何處才能套用安全性政策規則。

  對於 **Source Zone**（來源區域），您可以選取內部信任區域。如果您想要將安全性政策規則套用至所有流量（而無論其來源為何），請針對所有來源設定選取 **Any**（任何）。

  例如，根據風險探索評估，您判定對 GenAI 應用程式的存取權限過度佈建，且必須限縮至特定使用者。在此情況下，您可以撰寫 **Allow**（允許）政策規則並新增所需的 **Source User**（來源使用者）。
- **Destination**（目的地）—定義要套用安全性政策規則的流量目標目的地。

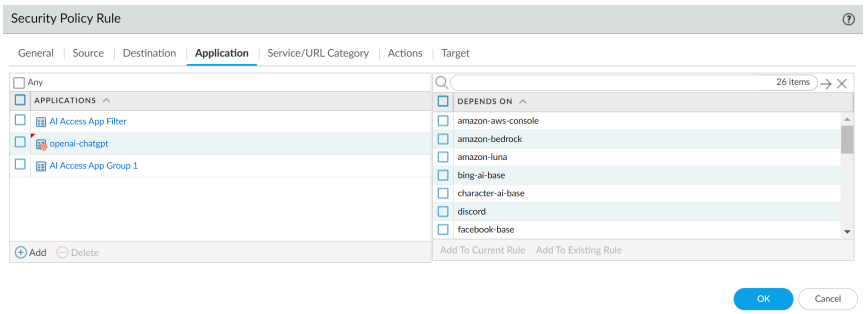
  對於 **Destination Zone**（目的地區域），您可以選取輸出不受信任的區域。如果您想要將安全性政策規則套用至所有流量（而無論流量目的地為何），請針對所有目的地設定選取 **Any**（任何）。

STEP 7 | 在 **Application**（應用程式）設定中，指定 GenAI 應用程式群組、應用程式篩選器或應用程式。

（允許的 Web 應用程式）僅將支援的 GenAI 應用程式新增至允許的應用程式清單。

- **Application**（應用程式）—新增一或多個 GenAI 應用程式。
- **Application Category**（應用程式類別）—應用程式類別（也稱為 應用程式篩選器）會根據您定義的應用程式篩選器動態分組應用程式。

  例如，您可以使用預先定義或自訂的 GenAI 應用程式篩選器，動態控制組織中 GenAI 應用程式的存取權，而不是新增個別的 GenAI 應用程式，或建立必須在每次需要變更時手動更新的應用程式群組。
- **Application Group**（應用程式群組）—應用程式群組是您建立的個別應用程式的靜態分組。



STEP 8 | 設定安全性政策規則 **Actions**（動作）。決定要對政策規則採取哪些動作。最佳做法是附加安全性設定檔，讓防火牆可以掃描所有允許的流量是否存在威脅。從 **Profile Type**（設定檔類型）下拉式清單中選取 **Profiles**（設定檔），然後選取要附加到規則的個別安全性設定檔。為 GenAI 應用程式的下列設定選擇必要動作：

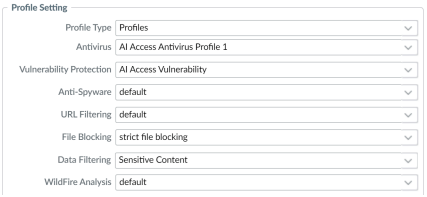
1. 對於 **Action**（動作），設定在偵測到從安全性政策規則 **Source**（來源）到 **Destination**（目的地）的流量時 NGFW 所採取的動作。

   例如，如果您想要允許存取一或多個 GenAI 應用程式，則選取 **Allow**（允許），如果您想要封鎖對一或多個 GenAI 應用程式的所有存取，則選取 **Deny**（拒絕）。
2. 針對 **Profile Type**（設定檔類型），選取 **Profiles**（設定檔）。

   您至少必須新增 **Vulnerability Protection**（弱點保護）和 **Data Filtering**（資料篩選）設定檔。發現 GenAI 應用程式所帶來的風險時，需要這些資料才能產生 **Threats**（威脅）和

Sensitive Assets（敏感資產）資料。其餘設定檔為選用設定檔，可視需要進行設定。對於下面的每種安全性設定檔，您可以選取現有設定檔或新建設定檔。

- 防毒軟體
- 漏洞保護
- 反間諜軟體
- URL 篩選
- 檔案封鎖
- 資料篩選
- WildFire 分析



在 ***Actions***（動作）頁籤中，***Profile Setting***（設定檔設定）優先於 ***Action Setting***（動作設定）。因此，最佳做法是確保這兩種設定均相符。例如，即使您將動作設定設為允許，並將其中一個設定檔設定針對 *ChatGPT* 設為封鎖，也會將其封鎖。

STEP 9 | 提交新設定並將其推送至受管理防火牆，以完成 Enterprise DLP 外掛程式安裝。

要讓 Enterprise DLP 資料篩選設定檔名稱顯示在資料篩選日誌中，必須進行此步驟。

不建議對 *Enterprise DLP* 設定變更使用 ***Commit and Push***（提交並推送）命令。使用 ***Commit and Push***（提交和推送）命令需在「推送範圍選取」中手動選取受影響的範本與受管理的防火牆，此操作會產生額外且不必要的開銷。

- 從 **Panorama** 進行完整設定推送
  1. 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**）和 **Commit**（提交）。
  2. 選取 **Commit**（提交） > **Push to Devices**（推送至裝置）並 **Edit Selections**（編輯選擇）。
  3. 選取 **Device Groups**（裝置群組），以及 **Include Device and Network Templates**（包括裝置和網路範本）。
  4. 按一下 **OK**（確定）。
  5. 透過 Enterprise DLP **Push**（推送）您的受管理防火牆設定變更。
- 從 **Panorama** 進行部分設定推送

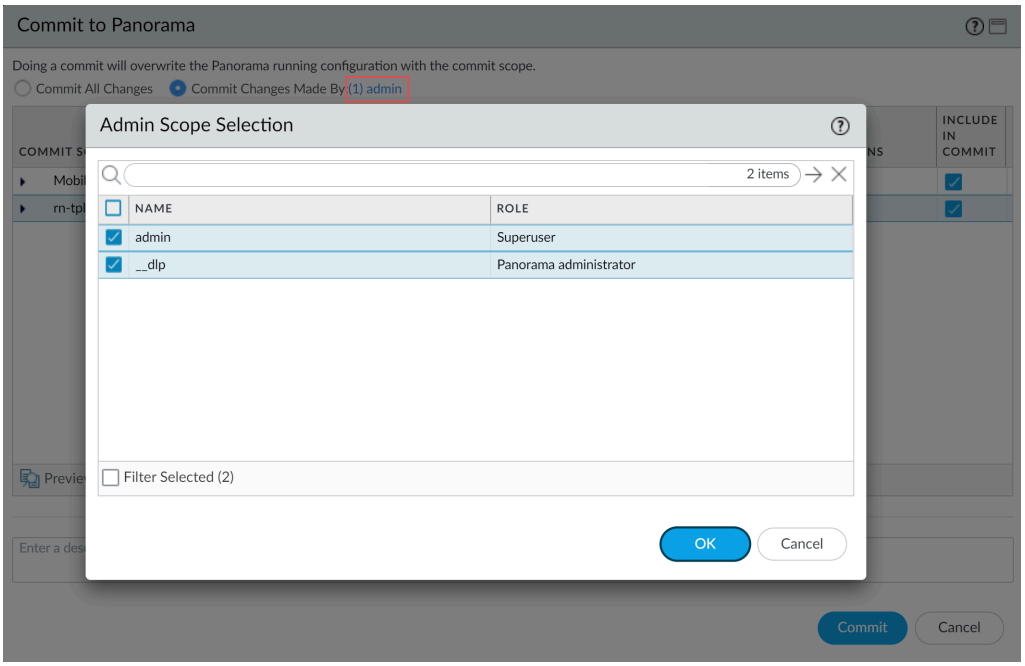
  執行部分設定推送時，請一律包含臨時 *__dlp* 管理員。這是保持 *Panorama* 和 *DLP* 雲端服務同步的必要條件。

  例如，您有允許提交和推送設定變更的管理員 *Panorama* 管理員使用者。管理員使用者對 *Enterprise DLP* 設定進行了變更，且只想提交這些變更並將其推送到受管理的防火牆。在此情況下，管理員使用者也必須在部分提交和推送操作中選取 *__dlp* 使用者。

  1. 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**）。
  2. 選取 **Commit Changes Made By**（依做成者認可變更），然後按一下目前 Panorama 管理員使用者，以選取要在部分提交中包含的其他管理員。

     在此範例中，管理員使用者目前為登入狀態並執行提交操作。管理員使用者必須按一下 **admin**（管理員），然後選取 `__dlp` 使用者。如果其他 Panorama 管理員進行了其他設定變更，也可以在此進行選取。

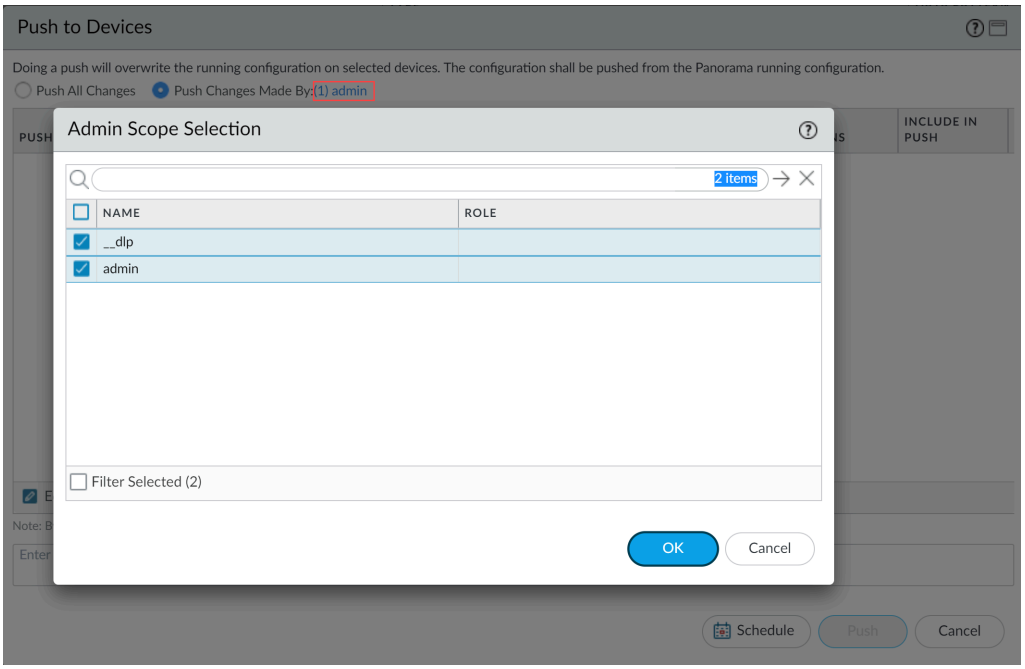
     按一下 **OK**（確定）繼續。



3. **Commit**（認可）。
4. 選取 **Commit**（提交） > **Push to Devices**（推送至裝置）。
5. 選取 **Push Changes Made By**（推送下列管理員所做的變更），然後按一下目前 Panorama 管理員使用者，以選取要在部分推送中包含的其他管理員。

   在此範例中，管理員使用者目前為登入狀態並執行推送操作。管理員使用者必須按一下 **admin**（管理員），然後選取 `__dlp` 使用者。如果其他 Panorama 管理員進行了其他設定變更，也可以在此進行選取。

   按一下 **OK**（確定）繼續。



6. 選取 **Device Groups**（裝置群組），以及 **Include Device and Network Templates**（包括裝置和網路範本）。
7. 按一下 **OK**（確定）。
8. 透過 Enterprise DLP **Push**（推送）您的受管理防火牆設定變更。

AI Access Security 建議

網路安全管理員使用 AI Access Security 儀表板和 Strata 控管中心獲得與在組織網路 GenAI 應用程式使用情況的寶貴資料。為了使網路安全管理員能夠快速解決漏洞並加強您在採用 GenAI 應用程式時的安全態勢，Palo Alto Networks 引入了 AI Access Security 建議。

AI Access Security 提供手動和自動建議。手動建議是您需要手動實作的建議。AI Access Security 提供逐步說明並提供所有相關文件的連結，以幫助您成功實作建議的變更。在 Strata Cloud Manager 的 Palo Alto Networks Copilot 實作自動建議，而不是管理員。然而，發起 AI Access Security 提出之建議的管理員必須核准所有變更。

- 針對 **NGFW** 和 **Prisma Access** 的建議（由 **Strata Cloud Manager** 管理）— AI Access Security 建議會隨著管理員進行設定變更而即時更新，且 AI Access Security 會分析網路上的流量。這使您能夠快速回應任何可能危及組織的設定變更或有風險 GenAI 應用程式流量，如果不立即處理，這些問題可能會造成損害。任何分析網路上流量的建議都有七天的回顧期，該回顧期會作為建議的依據。

  如果您擁有 NGFW 和 Prisma Access（由 Strata Cloud Manager 管理）以及 Prisma Access Browser，AI Access Security 僅顯示針對 NGFW 和 Prisma Access 租用戶的建議。在這種案例下，AI Access Security 不會顯示針對 Prisma Access Browser 的建議。
- 針對 **NGFW** 和 **Prisma Access** 的建議（由 **Panorama** 管理）— AI Access Security 建議在 Strata Cloud Manager 每 24 小時進行更新。

  如果您擁有 NGFW 和 Prisma Access（由 Panorama 管理）以及 Prisma Access Browser，AI Access Security 僅顯示針對 NGFW 和 Prisma Access 租用戶的建議。在這種案例下，AI Access Security 不會顯示針對 Prisma Access Browser 的建議。
- 針對 **Prisma Access Browser** 的建議—AI Access Security 建議是靜態的，並在您實作後持續存在。Palo Alto Networks 建議在實作後繼續監控這些建議，以確保安全管理員能夠解決您在 GenAI 應用程式採用策略中的任何漏洞。

  AI Access Security 僅在您擁有獨立的 Prisma Access Browser 授權，且沒有部署任何 NGFW 或 Prisma Access 租用戶時，顯示針對 Prisma Access Browser 的建議。

  如果您擁有 NGFW 和 Prisma Access（由 Panorama 或 Strata Cloud Manager 管理）以及 Prisma Access Browser，AI Access Security 僅顯示針對 NGFW 和 Prisma Access 租用戶的建議。在這種案例下，AI Access Security 不會顯示針對 Prisma Access Browser 的建議。

AI Access Security 提供以下情況的建議。

- **GenAI** 應用程式分類建議

  專注於根據網路上 GenAI 應用程式使用情況及其應用程式分類（已認可、已容許或未認可）提供建議

  例如，如果 AI Access Security 注意到組織允許流量進入未認可的 GenAI 應用程式。在這種案例中，AI Access Security 會提供建議，將這些 GenAI 應用程式重新分類為已認可或已容許。

- 最佳做法檢查和政策建議

  AI Access Security 使用最佳做法評估 (BPA) 服務來分析您現有的 NGFW 和 Prisma Access 政策規則庫，以提供可加強安全性態勢的建議，以安全採用 GenAI 應用程式。

  例如，如果 BPA 服務發現您有一條安全性政策規則，可存取未認可的 GenAI 應用程式。

- **Data loss prevention (**資料遺失防護 **- DLP)** 建議

  為了防止將敏感資料外洩至已認可和已容許的 GenAI 應用程式，AI Access Security 會分析安全性政策規則，以判斷您是否將流量轉送到 Enterprise DLP 進行內嵌檢查和靜態資料。這也可能包括將流量轉送到 Enterprise DLP 所需的設定建議

- 裝載和最大化 **AI Access Security**

  這些專注於提供可行的建議，以更完善利用平台上的能力。這些建議專注於使用者與各種市集或支援靜態資料 GenAI 應用程式的連線能力。

- **Prisma Access Browser** 建議

  針對 Prisma Access Browser 的建議專注於提供針對性的指導，以幫助 Prisma Access Browser 獨立使用者保護和最佳化 GenAI 應用程式使用情況。這些建議可能包括 GenAI 應用程式存取的設定、啟用預先定義的安全性政策規則以保護透過 Prisma Access Browser 存取的 GenAI 應用程式，以及檢閱對未認可 GenAI 應用程式的敏感資料外洩可疑事件。

產生 AI Access Security 報告

AI Access Security 報告提供組織的 GenAI 應用程式和外掛程式使用情況和安全性態勢的全面概要。此報告可協助您了解和管理與環境中快速發展的 GenAI 應用程式相關聯的風險。此報告隨附可行的洞察和量身打造的建議，可讓安全性管理員制定與 GenAI 應用程式採用策略和安全性有關的明智決策。

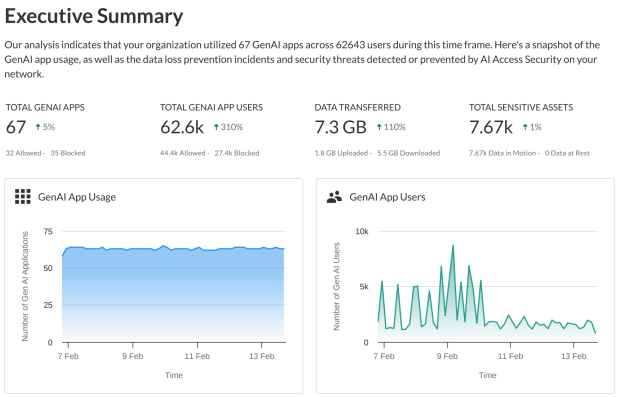
AI Access Security 報告的關鍵元件包括:

- 執行摘要

  [Executive Summary（執行摘要）] 區段提供組織中關鍵 GenAI 應用程式和外掛程式指標的高階快照。其中提供以下簡要概述:

  - GenAI 應用程式使用情況，讓您快速了解組織中使用者存取這些應用程式的普及程度。
  - 從 GenAI 應用程式上傳和下載的資料量（以 gigabyte (GB) 為單位）。
  - 偵測到動態和靜態資料的敏感資料資產數目。

  [Executive Summary（執行摘要）] 區段可讓安全性管理員快速檢視組織內的 GenAI 應用程式形態。其可作為入門點，帶您了解報告後續各節提供的更詳細資訊，讓安全性管理員能夠快速掌握組織的整體 GenAI 安全性態勢，並識別可能需要進一步關注或調查的領域。

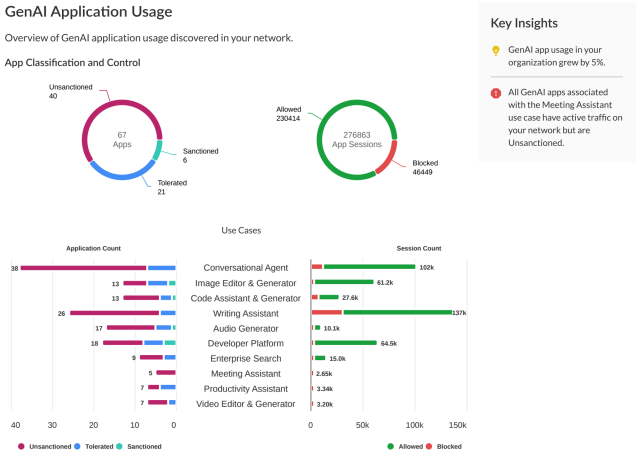


- **GenAI** 應用程式使用情況

  [GenAI App Usage（GenAI 應用程式使用情況）] 區段提供組織內 GenAI 應用程式使用情況的全面詳細資訊。其中包括:

  - GenAI 應用程式的總數，顯示允許的和已封鎖的 GenAI 應用程式，以及已認可、已容許和未認可 GenAI 應用程式之間的分佈情況。
  - GenAI 使用案例的詳細資訊，依應用程式分類（已認可、已容許或未認可），以及流量為允許還是已封鎖。
  - 未認可但允許的應用程式數目，包括報告期間開始以來的變更。
  - 彙總未認可但允許的 GenAI 應用程式的使用情況資料，包括使用者數目和傳輸的資料總量。
  - 關於前 5 個未認可但允許的 GenAI 應用程式的詳細資訊，包括應用程式名稱、使用者數目、工作階段數目和相關聯的風險因素。

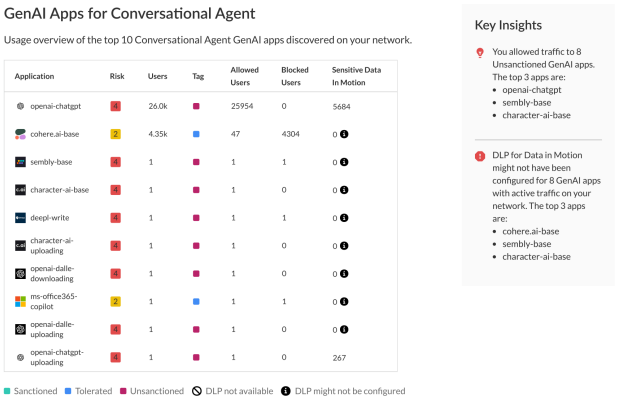
  本節可協助安全性管理員快速識別潛在的安全性風險、了解不同使用案例中的 GenAI 應用程式使用率，以及制定與應用程式使用情況政策規則和安全性態勢有關的明智決策。



- 熱門使用案例的 **GenAI** 應用程式

  最常使用的 GenAI 應用程式區段提供組織內使用的前 10 個 GenAI 應用程式摘要，這些摘要按 GenAI 應用程式使用案例分類。其提供組織內使用的最重要 GenAI 應用程式的詳細資訊，並針對每個 GenAI 應用程式包含下列資訊：

  - 使用的 GenAI 應用程式名稱。
  - 與 GenAI 應用程式相關聯的風險分數。
  - 使用 GenAI 應用程式的唯一使用者數目。
  - GenAI 應用程式分類，指示應用程式是「已認可」、「已容許」還是「未認可」。
  - GenAI 應用程式允許和封鎖的唯一工作階段數目。
  - 存取 GenAI 應用程式的使用者所產生的 Enterprise DLP 事件數目。

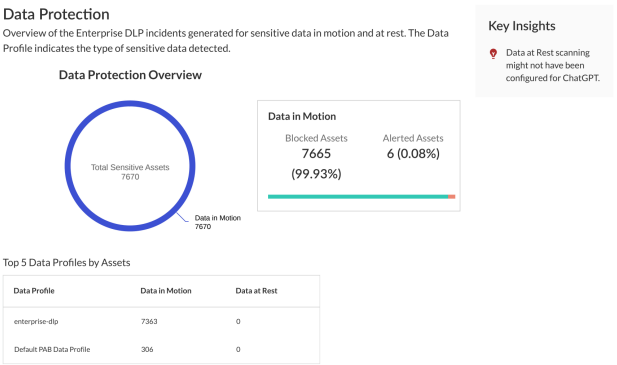


- 資料保護

  [Data Protection（資料保護）] 區段提供關鍵洞察，帶您了解如何處理組織 GenAI 生態系統內的敏感資料。本區段包括：

  - 偵測到的敏感資產總數，分類為允許或已封鎖。
  - 敏感資產在所有 GenAI 應用程式之間的分佈情況，依敏感資產類型分組。
  - 在前 5 個 GenAI 應用程式中找到的敏感資料詳細資訊。

  此資訊可協助安全性管理員快速識別與組織中 GenAI 應用程式使用情況相關聯的潛在資料安全性風險。透過反白顯示哪些 GenAI 應用程式正在處理敏感資訊以及正在處理哪些敏感資料類型，您可以排定資料保護工作的優先順序，並根據需要調整安全性政策規則。



STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取 **Insights**（洞察） > **SECURITY**（安全性） > **AI Access**（**AI** 存取）。

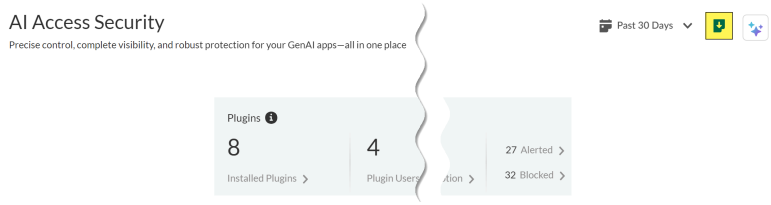
STEP 3 | 選取用於 AI Access Security 報告的時段。

AI Access Security 支援產生 **Past 24 Hours**（過去 **24** 小時）、**Past 7 Days**（過去 **7** 天）或 **Past 30 Days**（過去 **30** 天）的報告。

STEP 4 | 將 AI Access Security 報告以 PDF 格式 **Download**（下載）至本機裝置。

預設值檔案名稱為 `AI Access Security 報告 <generation-date>.pdf`。

在 *AI Access Security* 報告下載完成之前，請勿離開或重新整理頁面。在下載完成之前離開或重新整理頁面會中斷下載，而且您必須再次下載 *AI Access Security* 報告。



STEP 5 | 前往至您選取的下載資料夾，然後檢閱 AI Access Security 報告。