paloalto
TECHDOCS

AI Access Security Gestión

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 16, 2026

Descubra los riesgos que plantean las aplicaciones GenAI

Utilice el panel Insights de AI Access Security para filtrar el uso de aplicaciones de IA generativa (GenAI) en su red. El panel Insights de AI Access Security proporciona detalles detallados para ayudarle a comprender qué aplicaciones de GenAI se están utilizando y quién las utiliza.

AI Access Security detecta datos de **Allowed Users (Usuarios permitidos)**, datos de **Blocked Users (Usuarios bloqueados)** o ambos según los siguientes filtros.

- **1 Hour (1 hora)** y **3 Hours (3 horas)**

  Los usuarios pueden contar como Permitido, Bloqueado o ambos.

  Por ejemplo, `UserA` no puede acceder a `GenAI-App1` debido a la regla de política `Policy Rule1`. Una hora más tarde, `UserA` viaja a una sucursal donde `Policy Rule2` permite el acceso a `GenAI-App1`. En este caso, `UserA` se muestra tanto en los recuentos de **Allowed Users (Usuarios permitidos)** como **Blocked Users (Usuarios bloqueados)**.

  Por el contrario, `Policy Rule1` bloquea el acceso de `UserA` a `GenAI-App1`. Unos minutos después, su administrador de seguridad modifica la `Regla de políticas1` para permitir el acceso a `UserA`. En este caso, `UserA` se muestra en los recuentos de **Blocked Users (Usuarios bloqueados)**. AI Access Security muestra usuarios en el recuento de **Blocked Users (Usuarios bloqueados)** independientemente de cuántas veces haya permitido el acceso en las últimas **1 Hour (1 Hora)** o **3 Hours (3 horas)** si coinciden con la misma regla de la política de seguridad y se les bloqueó el acceso al menos una vez.
- **24 Hour (24 horas)**, **7 Day (7 días)** y **30 Day (30 días)**

  Los usuarios pueden contar como Permitido, Bloqueado o ambos.

  Por ejemplo, bloqueó inicialmente el acceso de `UserA` a `GenAI-App1`. Seis horas más tarde, `UserA` se desplaza a una sucursal donde `Policy Rule2` permite el acceso a `GenAI-App1`. En este caso, `UserA` se muestra tanto en los recuentos de **Allowed Users (Usuarios permitidos)** como **Blocked Users (Usuarios bloqueados)**.

Descubra los riesgos que plantean las aplicaciones GenAI según el caso de uso

Revise los Casos de uso soportados para descripciones completas de todas las categorías de casos de uso en las que se encuentra una aplicación GenAI.

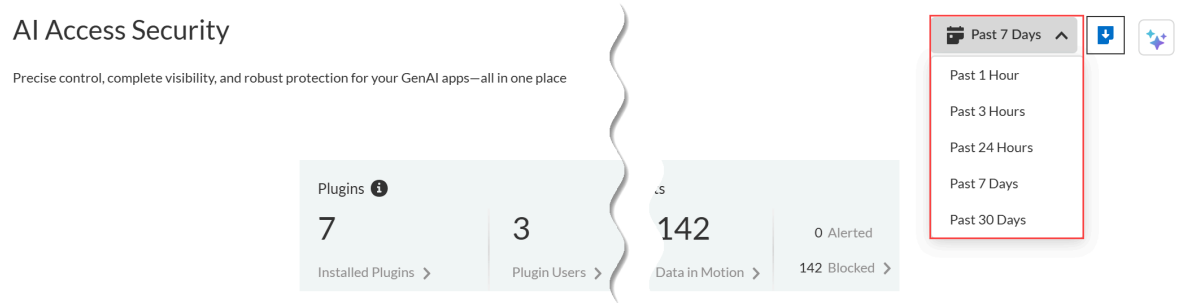
STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Insights** > **AI Access** para ver el panel de Insights de AI Access Security.

El panel Insights de AI Access Security muestra el uso de aplicaciones GenAI en su red por caso de uso de forma predeterminada, así como la siguiente información general sobre sus principales casos de uso de GenAI:

- **Time Filter (Filtro de tiempo)**

  Filtre el desglose de su caso de uso de GenAI para el período de tiempo que desea investigar. Puede seleccionar **Past 1 Hour (Última hora)**, **Past 3 Hours (Últimas 3 horas)**, **Past 24 Hours (Últimas 24 horas)**, **Past 7 Days (Últimos 7 días)** o **Past 30 Days (Últimos 30 días)**.



- **Amenazas detectadas**

  Las amenazas son detectadas por el perfil de protección frente a vulnerabilidades adjunto a la regla de política de seguridad de la Web. Este perfil detecta amenazas como URL maliciosas y de phishing, archivos maliciosos o malware. **Threats Detected (Amenazas detectadas)** resume todas las amenazas a través de todas las aplicaciones GenAI y puntos de aplicación.

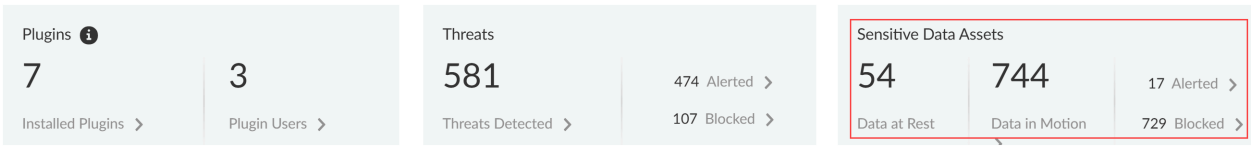
  - **Alerted (Alertado)**: número total de amenazas detectadas que generaron una alerta.

- **Blocked (Bloqueado)**: número total de amenazas detectadas que fueron bloqueadas por sus NGFW o inquilinos de Prisma Access.

- **Activos de datos sensibles**

  Los activos de datos sensibles muestran el número de incidentes de datos sensibles detectados cuando el tráfico coincide con los criterios de coincidencia en su perfil de datos de Enterprise Data Loss Prevention (E-DLP) para datos en reposo (Data Security) y datos en movimiento (SaaS Security Inline).

  - **Data at Rest (Datos en reposo)**: número total de Incidentes DLP que generaron una alerta o fueron bloqueados a través del canal de aplicación SaaS (Data Security).
  - **Data in Motion (Datos en movimiento)**: número total de Incidentes DLP que generaron una alerta o fueron bloqueados a través del canal de aplicación de SaaS Security Inline.
  - **Alerted (Alertado)**: número total de Incidentes DLP que generaron una alerta tanto para datos en reposo como para datos en movimiento.
  - **Blocked (Bloqueado)**: número total de incidentes DLP bloqueados por sus NGFW o inquilinos Prisma Access tanto para datos en reposo como para datos en movimiento.



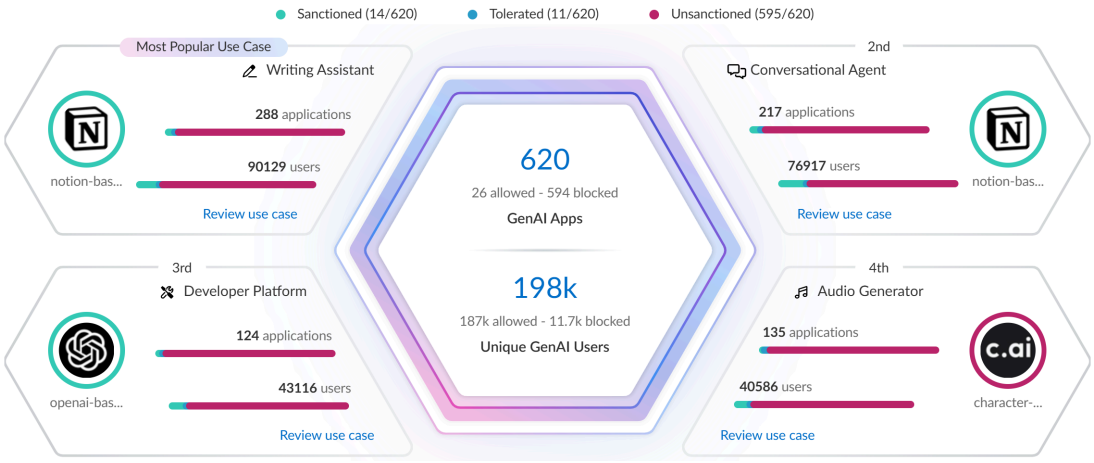
- **Principales casos de uso**

  El panel Insights de AI Access Security muestra dinámicamente los cuatro principales casos de uso de aplicaciones GenAI basados en la actividad en su red, junto con el número total de aplicaciones GenAI y usuarios que accedieron a cualquier GenAI en el período de tiempo seleccionado. Esto le permite investigar rápidamente incidentes de seguridad relacionados con sus aplicaciones GenAI más utilizadas e implementar reglas de política de control de acceso.

  - **GenAI Apps (Aplicaciones GenAI)**: número total de aplicaciones GenAI que caen en el caso de uso particular. El número total de aplicaciones GenAI se clasifica en tres grupos: aplicaciones GenAI autorizadas, toleradas y no autorizadas.
  - **Unique GenAI Users (Usuarios únicos de GenAI)**: número total de usuarios que accedieron a cualquier aplicación GenAI que cae en el caso de uso particular. Haga clic

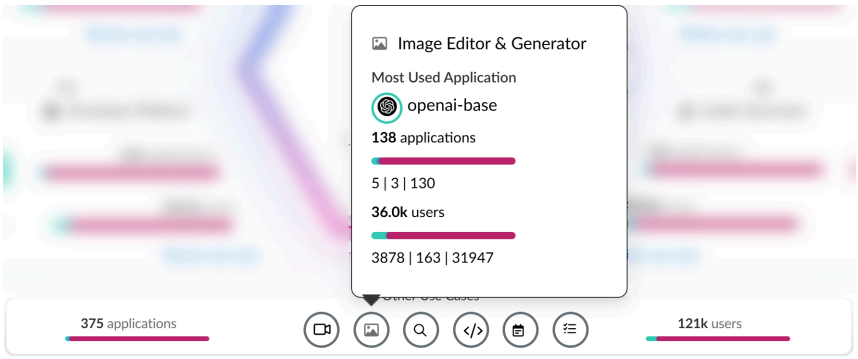
en el recuento de **Unique GenAI Users (Usuarios únicos de GenAI)** para ver una lista de cada usuario único que fue bloqueado para acceder a la aplicación GenAI.

*AI Access Security añade automáticamente el recuento total de **Unique GenAI Users (Usuarios únicos de GenAI)** en un intervalo establecido y genera la lista de usuarios inmediatamente cuando hace clic en el recuento de **Unique GenAI Users (Usuarios únicos de GenAI)**. Esto podría hacer que el conteo de **Unique GenAI Users (Usuarios únicos de GenAI)** difiera ligeramente del recuento de la lista.*



- **Todos los demás casos de uso**
  - **Applications (Aplicaciones)**: número total de aplicaciones GenAI que caen en cualquier otro caso de uso de aplicaciones GenAI. El número total de aplicaciones GenAI se clasifica en tres grupos: aplicaciones GenAI autorizadas, toleradas y no autorizadas.
  - **Users (Usuarios)**: número total de usuarios que han accedido a cualquier aplicación GenAI que cae en cualquier otro caso de uso de aplicaciones GenAI.

  Pase el ratón sobre cada uno de los casos de uso para ver información resumida sobre el uso de aplicaciones GenAI asociadas con el caso de uso.



STEP 3 | **Review use case (Revisar caso de uso)** para ver un desglose detallado de todas las aplicaciones GenAI autorizadas, toleradas y no autorizadas en el caso de uso que le interesa.

STEP 4 | Revise la página de detalles del caso de uso para entender el uso de aplicaciones GenAI.

La página de detalles del caso de uso proporciona datos granulares sobre el uso de aplicaciones GenAI. Puede usar esta información para entender el uso de aplicaciones GenAI para ayudarle a informar qué reglas de política sus administradores de seguridad necesitan escribir para fortalecer su postura de seguridad. Esto garantiza que su organización esté adoptando aplicaciones GenAI de manera segura y previene la exfiltración de datos sensibles.

- **Resumen del caso de uso**

  El resumen del caso de uso añade toda la información importante sobre el uso de aplicaciones GenAI para el caso de uso que estás investigando.

  - **Most Used Applications (Aplicaciones más utilizadas)**: la aplicación GenAI más utilizada para el caso de uso. Esto también incluye la etiqueta de la aplicación [**Sanctioned (Autorizada)**, **Tolerated (Tolerada)** o **Unsanctioned (No autorizada)**] actualmente asignada a la aplicación GenAI.
  - **Desglose de la aplicación**: resumen del número total de aplicaciones GenAI asociadas con el caso de uso, así como un resumen de las etiquetas de aplicaciones en todas las aplicaciones GenAI detectadas.
  - **User Breakdown (Desglose de usuarios)**: resumen del número total de usuarios que accedieron a cualquiera de las aplicaciones GenAI asociadas con el caso de uso. También se proporciona un resumen de cuántos usuarios accedieron a aplicaciones GenAI **Sanctioned (Autorizadas)**, **Tolerated (Toleradas)** o **Unsanctioned (No autorizadas)**.
- **Aplicaciones**

  Una lista de todas las aplicaciones GenAI asociadas con el caso de uso accedidas por sus usuarios. Puede aplicar un filtro **Sort By (Ordenar por)** al caso de uso de las aplicaciones GenAI para ordenarlas por **User Count (Recuento de usuarios)**, **Threats Count (Recuento de Amenazas)**, **Transferred Count (Recuento de transferencias)**. AI Access Security ordena las aplicaciones GenAI de mayor a menor recuento.

  La lista de aplicaciones muestra la siguiente información sobre cada aplicación GenAI detectada.

  - **Application Name (Nombre de la aplicación)**: nombre de la aplicación GenAI detectada. Haga clic en el nombre de la aplicación para ver la información de uso detallada. Será redirigido a **Applications (Aplicaciones)** de Activity Insights.
  - **Tag (Etiqueta)**: etiqueta actual de la aplicación GenAI. Puede aplicar una nueva etiqueta haciendo clic en la etiqueta que desea aplicar.

    Palo Alto Networks agrupa los App-ID secundarios para funcionalidad de aplicación en un App-ID de contenedor. Sin embargo, no se admite etiquetar un contenedor de App-ID. Debe etiquetar individualmente el App-ID secundario específico que esté autorizado, no autorizado o tolerado dentro de su organización.
  - **Usuarios permitidos**: número total de usuarios únicos que accedieron a la aplicación GenAI según los privilegios de acceso configurados en las reglas de su política de

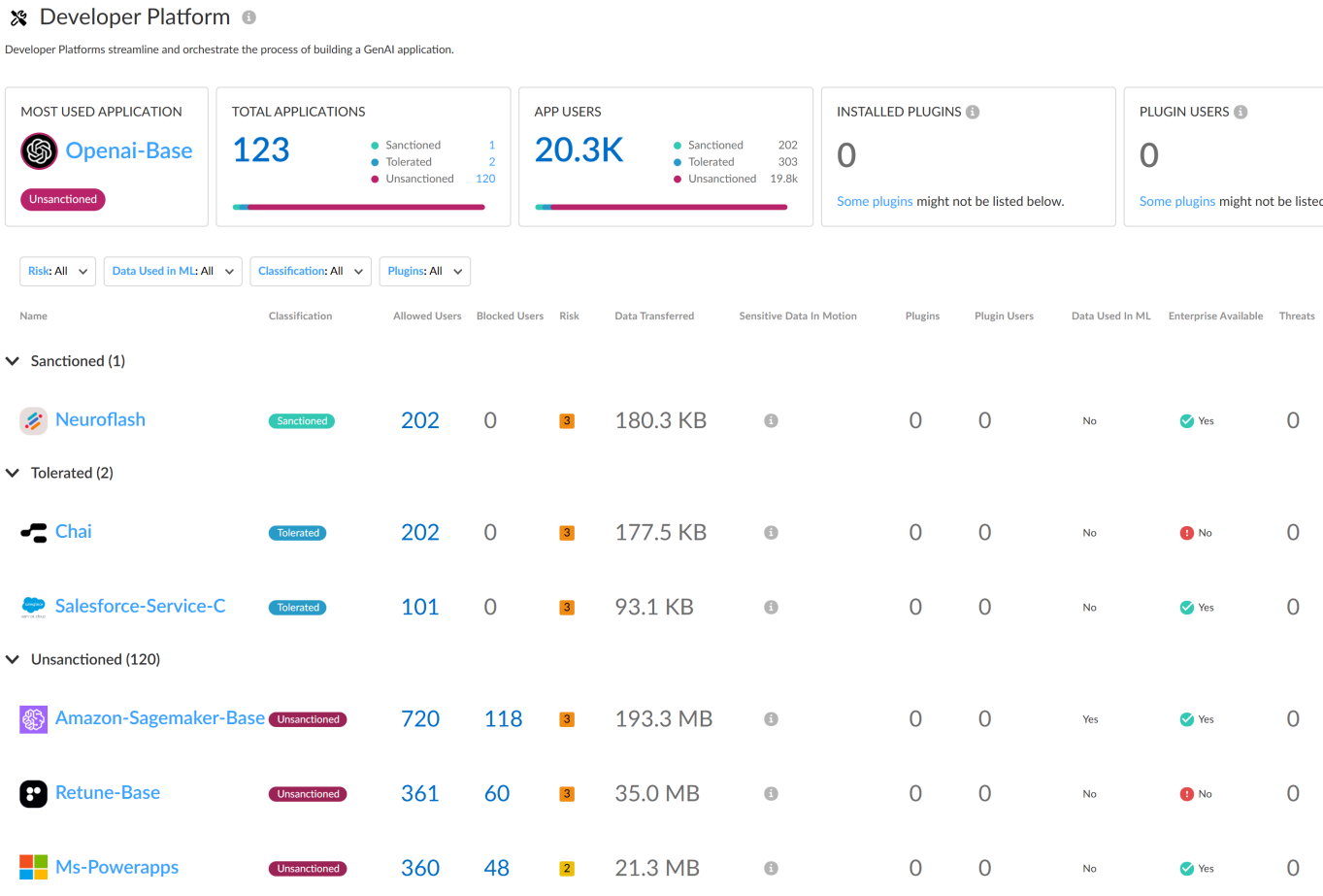
seguridad. Haga clic en el recuento de **Allowed Users (Usuarios permitidos)** para ver una lista de cada usuario único que accedió con éxito a la aplicación GenAI.

- **Usuarios Bloqueados**: número total de usuarios únicos bloqueados de acceder a la aplicación GenAI según los privilegios de acceso configurados en las reglas de su política

de seguridad. Haga clic en el recuento **Blockers Users (Usuarios bloqueadores)** para ver una lista de cada usuario único bloqueado del acceso a la aplicación GenAI.

- **Threats (Amenazas)**: número total de actividades de amenaza detectadas.
- **Transferred (Transferido)**: cantidad total de datos en gigabytes (GB) subidos o descargados de la aplicación GenAI.
- **Sensitive Asset (Activo Sensible)**: número de incidentes de DLP generados debido a datos sensibles detectados y bloqueados por Enterprise DLP.
- **Enterprise Available (Enterprise disponible)**: indica si la aplicación GenAI ofrece un plan empresarial o esquema de licencia.
- **Data Used in ML (Datos usados en ML)**: indica si la aplicación GenAI utiliza datos subidos por el usuario para fines de entrenamiento.
- **Risk Score (Puntuación de riesgo)**: Puntuación de riesgo de la aplicación GenAI.

- **Aspectos destacados del caso de uso**
  - **Applications (Aplicaciones)**: número total de aplicaciones GenAI que caen en cualquier otro caso de uso de aplicaciones GenAI. El número total de aplicaciones GenAI se clasifica en tres grupos: aplicaciones GenAI autorizadas, toleradas y no autorizadas.
  - **Users (Usuarios)**: número total de usuarios que han accedido a cualquier aplicación GenAI que cae en cualquier otro caso de uso de aplicaciones GenAI.



STEP 5 | Crea una regla de política de seguridad personalizada para controlar el acceso a una aplicación GenAI.

En el ejemplo anterior, `Openai-Base` es la aplicación GenAI más utilizada en el caso de uso `Asistente y generador de código`. Además, esta es una aplicación **Unsanctioned (No sancionada)** e indica que esta es una aplicación no aprobada para su uso en la red corporativa.

En este caso, puede modificar la regla de política de acceso predeterminado de la aplicación de GenAI para bloquear explícitamente todo acceso a `OpenAI` si esta es una aplicación a la que su organización no debería acceder.

Descubrir los riesgos que representan las aplicaciones GenAI mediante Aplicaciones peligrosas

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Insights** > **Activity Insights** > **Applications (Aplicaciones)**.

STEP 3 | Configure los filtros de la lista de aplicaciones para reducir las aplicaciones GenAI que desea investigar.

1. Configure el **Time Range (Rango de tiempo)** y la **Scope Selection (Selección de alcance)** para filtrar el rango de tiempo específico y el punto de aplicación que desea investigar.
2. **Add Filter (Añadir filtro)** y añadir los siguientes filtros.
   - **Source Type - Users (Tipo de origen - Usuarios)**: filtra la lista de aplicaciones para mostrar solo las aplicaciones GenAI a las que acceden los usuarios de su organización. Este es un filtro requerido.
   - **GenAI Application - TRUE (Aplicación GenAI - VERDADERO)**: filtra la lista de aplicaciones para mostrar solo aplicaciones GenAI. Este es un filtro requerido.
   - **App Risk Score (Puntuación de riesgo de la aplicación)**: para el filtro **App Risk Score (Puntuación de riesgo de la aplicación)**, seleccione la puntuación riesgo específica que desea investigar. Todas las aplicaciones GenAI se muestran si no selecciona al menos una puntuación de riesgo.

     En este ejemplo, estamos investigando aplicaciones con una puntuación de riesgo de **4** y **5** porque estas son las puntuaciones de riesgo atribuidas a las aplicaciones más arriesgadas.

STEP 4 | Revise la lista de aplicaciones GenAI filtradas.

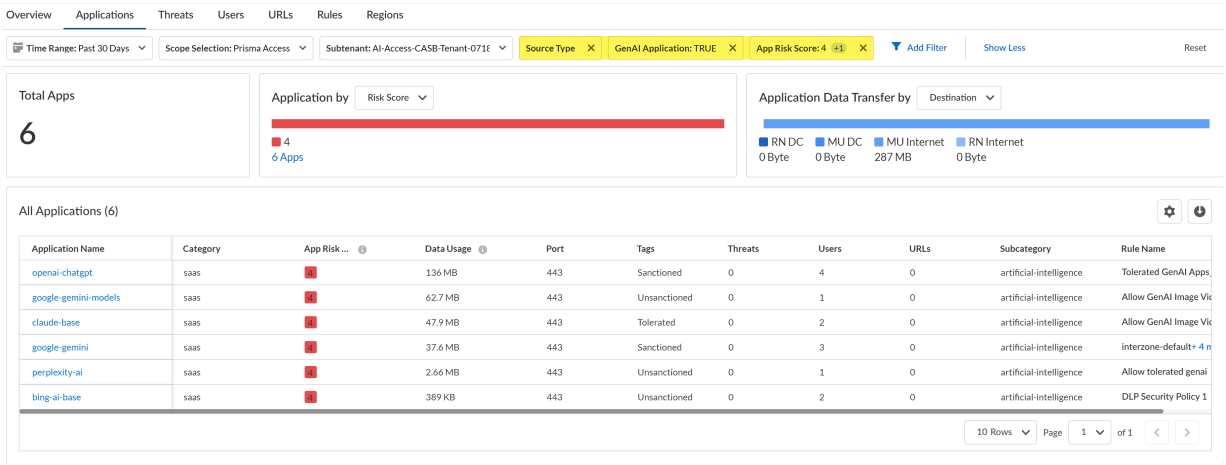
Algunas información importante a revisar es:

- **Application Name (Nombre de aplicación)**: App-ID de la aplicación GenAI.
- **Data Usage (Uso de datos)**: cantidad de datos cargados o descargados de la aplicación GenAI. Esto puede ayudarle a entender el uso de la aplicación GenAI; una aplicación GenAI con un gran volumen de uso de datos podría significar que esta aplicación es

ampliamente utilizada y podría necesitar controles estrictos para evitar la exfiltración de datos confidenciales y actores maliciosos.

- **Tags (Etiquetas)**: etiqueta de aplicación actual para la aplicación GenAI. Si algunas de las aplicaciones GenAI enumeradas están aprobadas para su uso, puede modificar la etiqueta a **Tolerated (Toleradas)** o **Sanctioned (Autorizadas)**.

Palo Alto Networks agrupa los App-ID secundarios para funcionalidad de aplicación en un App-ID de contenedor. Sin embargo, no se admite etiquetar un contenedor de App-ID. Debe etiquetar individualmente el App-ID secundario específico que esté autorizado, no autorizado o tolerado dentro de su organización.



STEP 5 | Crear una regla de política de seguridad personalizada para controlar el acceso a una aplicación GenAI para usuarios específicos.

Por ejemplo, en base a su investigación descubre que hay múltiples aplicaciones GenAI no autorizadas con un gran volumen de uso de datos. Esto supone un riesgo de seguridad porque hay usuarios que acceden a una aplicación no aprobada en la red y no sabes qué datos se están descargando o cargando. Hasta que pueda realizar la diligencia debida adecuada para

comprender el propósito de la aplicación GenAI y quién puede usar la aplicación GenAI, puede **Block (Bloquear)** la aplicación GenAI para todos los usuarios.

Por el contrario, note que hay algunas aplicaciones de GenAI **no autorizadas** en la lista, pero son aplicaciones de GenAI aprobadas para su uso en su red por usuarios específicos con un gran volumen de uso de datos. En este caso, puede cambiar la etiqueta a **Sanctioned (Sancionado)** y escribir una regla de políticas para **Allow (Permitir)** el uso de la aplicación pero solo para usuarios en roles o departamentos específicos. En la regla de políticas puede asociar un perfil de datos de Enterprise Data Loss Prevention (E-DLP) para evitar la exfiltración de datos confidenciales y un perfil de vulnerabilidad para detener los intentos de exploit de fallos del sistema u obtener acceso no autorizado a los sistemas.

Descubra los riesgos que plantean las aplicaciones GenAI para los usuarios de aplicaciones

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Insights** > **AI Access** para ver el panel de Insights de AI Access Security.

Esto muestra las principales aplicaciones GenAI a las que accedieron los usuarios peligrosos para ayudar a limitar su enfoque.

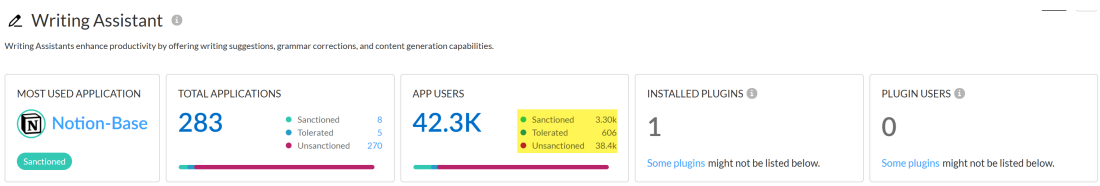
STEP 3 | Haga clic en **Review use case (Revisar caso de uso)** para el Caso de uso de la aplicación GenAI asociada a la aplicación GenAI a la que acceden sus usuarios peligrosos.

El panel Insights de AI Access Security muestra la aplicación GenAI a la que se accede en su red por caso de uso de forma predeterminada y muestra la siguiente información de alto nivel sobre los principales usuarios de la aplicación GenAI. Haga clic en el recuento de usuarios para ver el **User name (Nombre de usuario)** o la **IP Address (Dirección IP)** y el número de **Applications (Aplicaciones)** GenAI a las que accedió el usuario.

- **Desglose de usuarios**

  Esto proporciona un resumen del número total de usuarios que acceden a cualquier aplicación GenAI asociada con el caso de uso GenAI seleccionado. AI Access Security incluye un desglose del número de usuarios que accedieron a aplicaciones **Sanctioned (Autorizadas)**, **Tolerated (Toleradas)** y **Unsanctioned (No autorizadas)**.

  Haga clic en el recuento total de **App Users (Usuarios de aplicaciones)** para ver una lista de todos los usuarios que accedieron o se les bloqueó el acceso a una aplicación GenAI asociada con el caso de uso seleccionado.



- **Usuarios por caso de uso de GenAI**

  Esto proporciona un resumen del número total de usuarios que acceden a cada aplicación GenAI individual asociada con el caso de uso GenAI seleccionado. Las aplicaciones GenAI **sancionadas**, **toleradas** y **no sancionadas** se enumeran con el recuento total de usuarios para cada aplicación individual.

  Revise los recuentos de **Allowed Users (Usuarios permitidos)** y **Blocked Users (Usuarios bloqueados)** para medir la eficacia de las reglas de la política de acceso y seguridad de su aplicación GenAI.

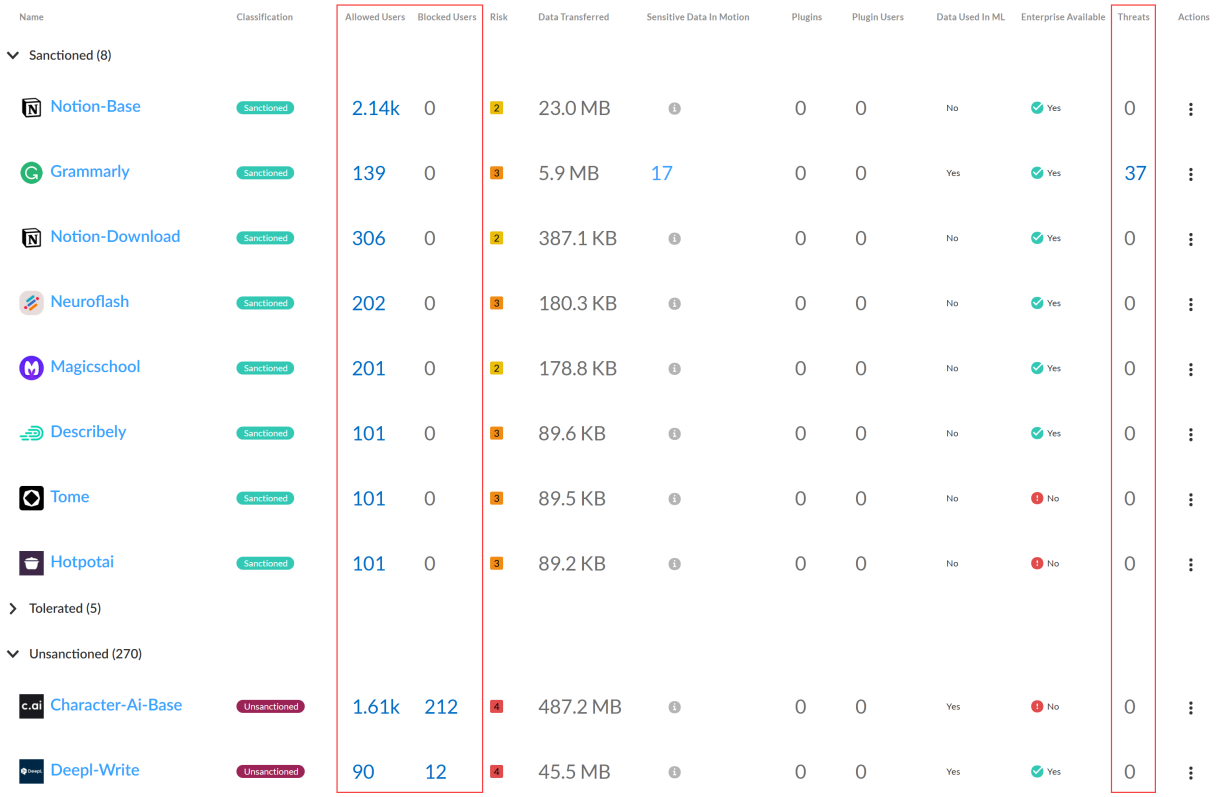
  - **Usuarios permitidos**: número total de usuarios a los que se permite acceder a la aplicación GenAI. Utilice esta información para medir la eficacia de su regla de política de seguridad verificando que el recuento de usuarios permitidos coincida con sus expectativas, o para medir la tasa de adopción de una aplicación GenAI que su organización haya permitido recientemente.

- **Blocked Users (Usuarios bloqueados)**: número total de usuarios bloqueados para acceder a la aplicación GenAI. Utilice esta información para verificar si configuró correctamente las reglas de la política de seguridad que controlan el acceso a una aplicación GenAI específica o para comprender si los usuarios de su organización acceden a aplicaciones GenAI no autorizadas.

Por ejemplo, considere la aplicación `Grammarly` de GenAI a continuación. Su organización clasificó esta aplicación GenAI como `Autorizada` para su uso por usuarios específicos dentro de su organización. En este caso, su administrador de seguridad hizo clic en el recuento de **Allowed Users (Usuarios permitidos)** y verificó que todos los usuarios que acceden a la aplicación GenAI puedan hacerlo.

Por el contrario, su administrador de seguridad ve que más de 1600 usuarios accedieron a la aplicación `Character-Ai-base`. Sus administradores de seguridad clasificaron esta aplicación GenAI como `Unsanctioned (No autorizada)` y tenían la intención de restringir todo el acceso con su organización. En este caso, el administrador de seguridad debe revisar la base de reglas de la política de seguridad y las reglas individuales de la política de seguridad que controlan el acceso a la aplicación `Character-Ai-base`

para confirmar que se colocó correctamente dentro de la base de reglas de la política de seguridad y para confirmar que se configuró correctamente para bloquear todo el acceso.



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 | Crear una regla de política de seguridad personalizada para controlar el acceso a una aplicación GenAI para usuarios específicos.

Por ejemplo, en función de su investigación, descubre que un gran número de usuarios están accediendo a la aplicación GenAI de `carga de bing-ai`. Si bien se trata de un GenAI **Sanctioned (Autorizado)**, solo está autorizado para un conjunto específico de usuarios dentro de su organización. Puede decidir escribir una regla de política para bloquear explícitamente el acceso a los usuarios que no deberían tener acceso a esta aplicación GenAI para evitar el uso indebido y una regla de política de seguridad para permitir explícitamente el acceso a los usuarios que están aprobados para acceder a la aplicación GenAI. De manera alternativa, puede escribir una regla de políticas para permitir el acceso de todos los usuarios, pero implementar medidas de prevención de amenazas y pérdida de datos para evitar la exfiltración de datos confidenciales y evitar amenazas como URL malintencionadas y de phishing, archivos malintencionados o malware.

Descubre los riesgos que representan las aplicaciones GenAI instaladas como complementos de terceros

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Insights** > **AI Access** para ver el panel de Insights de AI Access Security.

El panel muestra el número de complementos de terceros que instalaron los usuarios y el número de usuarios que instalaron complementos de terceros. AI Access Security determina estos números a partir de todos los datos que AI Access Security ha almacenado. Estos números no se limitan al período de tiempo indicado por el filtro de tiempo.

STEP 3 | Haga clic en **Installed Plugins (Complementos instalados)** o **Plugin Users (Usuarios de complementos)** para navegar a información detallada en SaaS Security Posture Management (SSPM).

Al hacer clic en **Installed Plugins (Complementos instalados)**se abre la página de complementos de terceros que muestra detalles sobre los complementos de terceros GenAI. Desde aquí, puede revisar la información del plugin para determinar si los plugins son un riesgo.

Al hacer clic en **Plugin Users (Usuarios de complementos)**, se abre la página de complementos de terceros que muestra detalles sobre los usuarios que instalaron complementos de terceros. Para cada usuario, puede ver cuántos plugins ha instalado y las aplicaciones del marketplace en las que ha instalado plugins. Utilice esta información para identificar los riesgos de plugins planteados por usuarios individuales.

STEP 4 | Para ver los plugins instalados por caso de uso, complete los siguientes pasos:

1. Seleccione **Insights** > **AI Access** para ver el panel de Insights de AI Access Security.

   El panel muestra de forma destacada los cuatro casos de uso de aplicaciones GenAI principales, según la actividad en su red. El panel también muestra iconos para los otros casos de uso.

2. Navegue para obtener detalles sobre un caso de uso. Para un caso de uso superior, haga clic en **Revisar caso de uso**. Para otros casos de uso, haga clic en el icono de caso de uso.

   La página de detalles del caso de uso muestra una tabla de todas las aplicaciones GenAI para el caso de uso.

   *La información resumida de esta página incluye el número de **INSTALLED PLUGINS (COMPLEMENTOS INSTALADOS)** y el número de **PLUGIN USERS (USUARIOS DE COMPLEMENTOS)**. Estos números se determinan a partir de todos los datos que AI Access Security ha almacenado y no se limitan al período de tiempo indicado por el filtro de tiempo. Por esta razón, es posible que esos totales no se reflejen en el cuadro de detalles del caso de uso.*

3. En la tabla de detalles del caso de uso, identifique las aplicaciones GenAI instaladas como complementos en una o más instancias de aplicaciones del mercado y el número

de usuarios de complementos. Esta información se muestra en las columnas **Plugins (Complementos)** y **Plugin Users (Usuarios de complementos)** de la tabla.

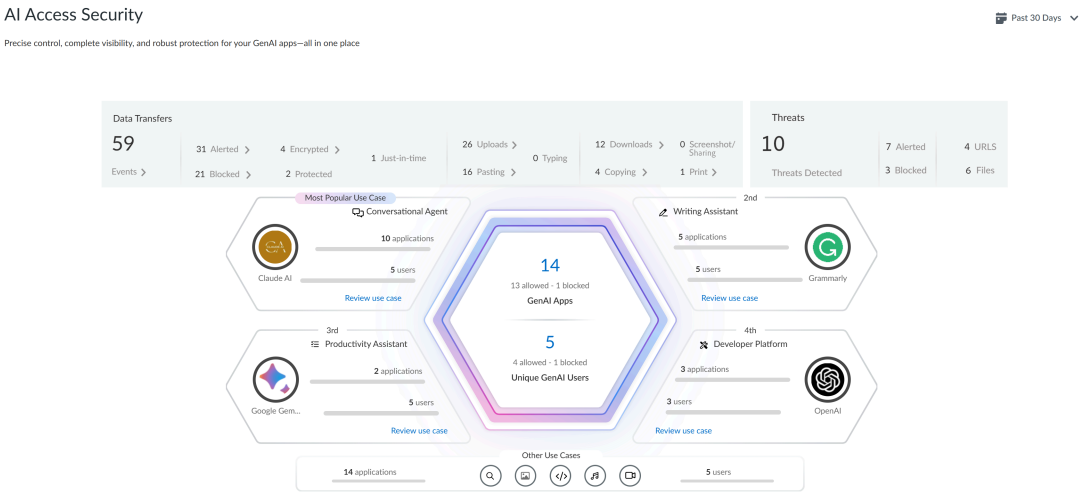
4. Para una aplicación GenAI instalada como plugin, haga clic en el número en las columnas **Plugings (Complementos)** o **Plugin Users (Usuarios de complementos)**.

   Al hacer clic en el número de la columna **Plugins (Complementos)**, se abre la página Complementos de terceros en SSPM que muestra las instancias de la aplicación GenAI que los usuarios instalaron como complementos de terceros. Desde aquí, puede revisar la información del plugin para determinar si los plugins son un riesgo.

   Al hacer clic en el número de la columna **Plugin Users (Usuarios del complemento)**, se abre la página de complementos de terceros que muestra detalles sobre los usuarios que instalaron la aplicación como complemento de terceros. Utilice esta información para identificar los riesgos de plugins planteados por usuarios individuales.

Descubra los riesgos que plantean las aplicaciones GenAI en Prisma Browser

Prisma Browser está integrado con AI Access Security para proporcionar visibilidad integral de las aplicaciones GenAI, control de acceso, protección de datos y amenazas a los clientes independientes de Prisma Browser. Esta integración ofrece el catálogo más completo de aplicaciones GenAI con profundos controles de última milla, como clasificación de datos y defensa contra amenazas en tiempo real. Como administrador de seguridad independiente de Prisma Browser, puede acceder a AI Access Security en el menú Insights para supervisar aplicaciones de IA de terceros mediante Prisma Browser con análisis detallados que incluyen métricas de aplicación, actividad usuario, amenazas detectadas y transferencias de datos.

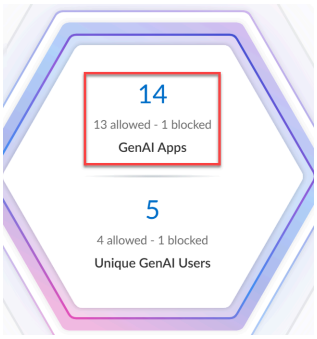


STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Insights** > **AI Access** para ver el panel de Insights de AI Access Security para Prisma Browser independiente.

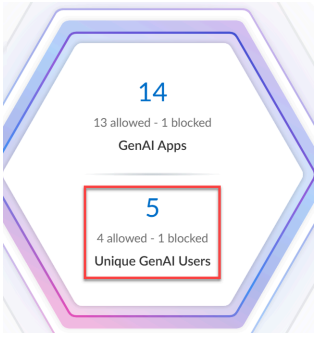
STEP 3 | Haga clic en **GenAI Apps (Aplicaciones GenAI)** para ver las Application metrics (Métricas de aplicación) con **Is GenAI:Yes (Es GenAI:Sí)** y Categoría de **: Acceso al** filtro aplicado para ver las siguientes métricas:

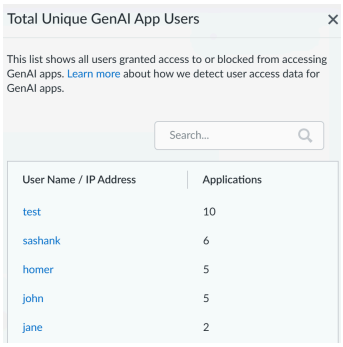
- Número total de aplicaciones de GenAI
- Aplicaciones GenAI permitidas
- Aplicaciones GenAI bloqueadas



STEP 4 | Haga clic en **Unique GenAI Users (Usuarios únicos de GenAI)** para ver el total de usuarios de aplicaciones GenAI a los que se les ha concedido acceso o se les ha bloqueado el acceso a las aplicaciones GenAI. Seleccione el usuario [de la página **Total Unique GenAI App Users (Número total de usuarios únicos de aplicaciones GenAI)**] para navegar a la Página de eventos [con el filtro **User (Usuario): <user name>** aplicado] para conocer las aplicaciones GenAI permitidas y bloqueadas para ese usuario en particular. Las métricas disponibles son:

- Número total de usuarios de GenAI
- Usuarios de GenAI permitidos
- Usuarios de GenAI bloqueados

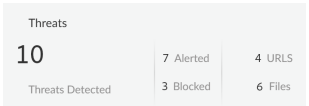




STEP 5 | Haga clic en el widget **Threats Detected (Amenazas detectadas)** para ver el total de amenazas detectadas y bloqueadas.

Esta información está disponible en la Página de eventos (con el **Is GenAI:Yes (Es GenAI:Sí)**, **Categoría: Malware** filtro aplicado). Las métricas disponibles son:

- Número total de amenazas GenAI que muestran el total de amenazas detectadas y bloqueadas.
- URL maliciosas (Filtro aplicado: **Categoría: Malware** y **Tipo: Sitio web malicioso**)
- Archivos (Filtro aplicado: **Categoría: Malware** y **Tipo: Archivo malicioso identificado**)

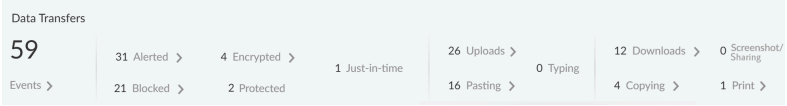


STEP 6 | Haga clic en el widget **Data Transfers (Transferencias de datos)** para ver el número de incidentes de transferencias de datos detectados cuando el tráfico coincide con los criterios

de coincidencia en su perfil de datos de Prevención de pérdida de datos empresariales (E-DLP) para su Prisma Browser.

Esta información está disponible en la Página de eventos (con el **Is GenAI:Yes (Es GenAI:Sí)**, **Categoría: Filtro DLP** aplicado).

- Total de transferencias de datos detectadas. Filtro aplicado: **Es GenAI:Sí**, **Categoría: DLP**
- Transferencias de datos alertadas. Filtro aplicado: **Es GenAI:Sí**, **Categoría: DLP**, **Acción: Permitida**.
- Transferencias de datos bloqueadas. Filtro aplicado: **Es GenAI:Sí**, **Categoría: DLP**, **Acción: Bloqueada**.
- Transferencias de datos protegidas: la acción que está permitida pero que solo se puede utilizar por el navegador. Por ejemplo, habilitar copiar y pegar datos entre aplicaciones autorizadas, y bloquearlo para otras aplicaciones en el navegador o aplicaciones de escritorio locales. Filtro aplicado: **Es GenAI:Sí**, **Categoría: DLP**, **Acción: Protegida permitida**.
- Transferencias de datos cifrados: Una acción de cifrado para la cual solo el navegador tiene la clave de descifrado para el usuario específico y el dispositivo con el que fue cifrado. Esto permite descargar archivos y asegurarse de que se permite subir (y descifrar) a aplicaciones específicas, o abrirse en el navegador en modo fuera de línea. Ninguna otra aplicación puede abrir el archivo, lo que lo hace ideal para archivos que no deseas que estén disponibles en el endpoint, por ejemplo, en dispositivos no gestionados. Filtro aplicado: **Es GenAI:Sí**, **Categoría: DLP**, **Acción: Permitida Cifrado**.
- Controles justo a tiempo en transferencias de datos: Acciones que incluyen advertir al usuario antes de continuar, pedir al usuario que proporcione justificación empresarial antes de continuar, o activar un flujo de aprobación de administración. Estos activan el acceso temporal o la omisión de reglas durante situaciones de emergencia, o bien cuando se requiere justificación y registro por motivos de cumplimiento. Filtro aplicado: **Es GenAI:Sí**, **Categoría: DLP**, **Acción: Solicitud de permiso de**
- Transferencias de datos cargadas. Filtro aplicado: **Es GenAI:Sí**, **Categoría: DLP**, **Tipo: Carga de archivo**.
- Transferencias de datos en una actividad de portapapeles (Pegado). Filtro aplicado: **Es GenAI:Sí**, **Categoría: DLP**, **Tipo: Pegado de Portapapeles**.
- Transferencias de datos escritas en el momento. Filtro aplicado: **Es GenAI:Sí**, **Categoría: DLP**, **Tipo: Depuración de contenido**.
- Transferencias de datos descargadas. Filtro aplicado: **Es GenAI:Sí**, **Categoría: DLP**, **Tipo: Descarga de archivo**.
- Transferencias de datos copiadas. Filtro aplicado: **Es GenAI:Sí**, **Categoría: DLP**, **Tipo: Copia de Portapapeles**.
- Transferencias de datos compartidas usando una captura de pantalla. Filtro aplicado: **Es GenAI:Sí**, **Categoría: DLP**, **Tipo: Uso compartido de pantalla**.
- Transferencias de datos impresas. Filtro aplicado: **Es GenAI:Sí**, **Categoría: DLP**, **Tipo: Imprimir**.



Etiquetar aplicaciones GenAI

Basado en una puntuación de riesgo de Aplicaciones GenAI y otras consideraciones, puede aplicar etiquetas a la aplicación para reflejar si la aplicación está aprobada dentro de su organización. Las siguientes etiquetas están disponibles:

Tag (Etiqueta)	Descripción
Sancionado	La aplicación es aprobada por su organización y está siendo utilizada por los miembros de su organización.
Sin autorización	La aplicación no está aprobada por su organización. Por ejemplo, la aplicación podría no estar autorizada debido a los riesgos de seguridad asociados con la aplicación. Debido a que los miembros de su organización no deben usar la aplicación, debe tomar medidas de bloqueo de la aplicación. Puede usar una regla de políticas para bloqueo la aplicación.
Tolerado	La aplicación no es fiable como una aplicación autorizada. Sin embargo, su organización permite su uso hasta que pueda identificar una aplicación más segura. La aplicación se tolera para no inhibir la productividad de su organización. Debido a que la aplicación está permitida a pesar de los posibles riesgos de seguridad, puede tomar medidas para restringir ciertas acciones. Por ejemplo, puede crear una regla de políticas de bloqueo de las operaciones de carga o descarga de la aplicación.

Palo Alto Networks agrupa los App-ID secundarios para funcionalidad de aplicación en un App-ID de contenedor. Sin embargo, no se admite etiquetar un contenedor de App-ID. Debe etiquetar individualmente el App-ID secundario específico que esté autorizado, no autorizado o tolerado dentro de su organización.

Por ejemplo, considere el App-ID del contenedor de `claude` que contiene los siguientes App-ID secundarios: `claude-base`, `claude-upload`, `claude-edit`, `claude-post` y `claude-delete`.

*Crea un filtro de aplicaciones para hacer cumplir los mismos controles de exfiltración de datos para las aplicaciones **Sanctioned (Autorizadas)**. En este caso, debe etiquetar todos los App-ID secundarios del contenedor de identificadores de aplicación de `claude` para aplicar la regla de políticas a todos los subprocesos de la aplicación GenAI de `claude` **Sanctioned (Autorizada)**.*

*En septiembre de 2024, Palo Alto Networks actualizó la forma en que se implementa el etiquetado de aplicaciones. A partir de septiembre de 2024, las etiquetas se escriben y leen en un nuevo fragmento `Application-Tagging` predefinido. Después de que se actualice para su inquilino, entrará en vigor la primera vez que etiqueta una aplicación. Las etiquetas se escriben en el fragmento y AI Access Security, la página Aplicaciones de Activity Insights y el Strata Cloud Manager Command Center comienzan a mostrar información de las etiquetas del fragmento. Si etiquetó aplicaciones antes de actualizarlas, ya no verá esos cambios de etiqueta reflejados en Aplicaciones de Activity Insights de AI Access Security. El fragmento `Application-Tagging` rastrea qué aplicaciones están etiquetadas como **Sanctioned (Autorizadas)** o **Tolerated (Toleradas)**. Las aplicaciones no etiquetadas explícitamente como **Sanctioned (Autorizadas)** o **Tolerated (Toleradas)** se consideran **Unsanctioned (No autorizadas)**. Por esta razón, solo se mostrarán en Strata Cloud Manager las etiquetas que añada después de actualizar. Todas las demás aplicaciones se muestran como **Unsanctioned (No autorizadas)**.*

Las etiquetas que aplicó antes de actualizar siguen afectando a la aplicación de políticas basadas en etiquetas en la implementación de NGFW o Prisma Access, siempre que asocie el fragmento de etiquetado de aplicaciones y aplique etiquetas mientras esté en el alcance de la configuración `Application-Tagging`.

- Configuración de la aplicación NGFW y Prisma Access
- Aplicaciones Activity Insights

Etiquetar aplicaciones GenAI en la configuración de la aplicación

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Asocie el fragmento `Application-Tagging` predefinido con el ámbito de configuración adecuado para admitir la aplicación de políticas basadas en etiquetas.

STEP 3 | Obtenga los App-ID secundarios que desea etiquetar.

Puede obtener los App-ID secundarios para una aplicación GenAI de una de las siguientes maneras.

- Utilice el panel Insights de AI Access Security para descubrir los riesgos que plantean las aplicaciones GenAI. Insights de AI Access Security le muestra los App-ID secundarios detectados que se utilizan en toda su organización.
- Revise la lista de aplicaciones GenAI compatibles.
- Utilice Applipedia para buscar los App-ID secundarios de las aplicaciones GenAI compatibles que se entregan a través de una actualización de contenido dinámico.

  Applipedia solo muestra los App-ID para aplicaciones entregadas a través de un contenido dinámico y no muestra aplicaciones entregadas a través de App-ID Cloud Engine (ACE).

STEP 4 | Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Objects (Objetos)** > **Application (Aplicación)** > **Applications (Aplicaciones)**.

STEP 5 | En el **Configuration Scope (Alcance de la configuración)**, seleccione el fragmento `Application-Tagging`.

Si está etiquetando un App-ID entregado a través de App-ID Cloud Engine (ACE), todos los inquilinos de NGFW o Prisma Access asociados con la carpeta seleccionada deben configurarse para recibir actualizaciones de App-ID de ACE.

ACE está habilitado de forma predeterminada para un inquilino de NGFW o Prisma Access cuando tienen una licencia de SaaS Security Inline o AI Access Security activa. También puede habilitar manualmente ACE para su NGFW.

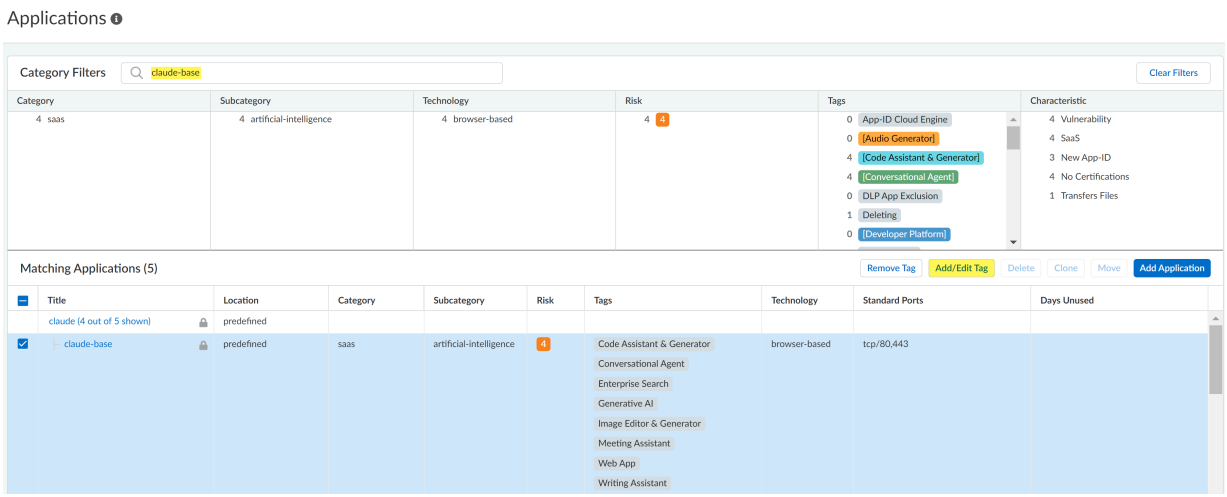
El envío de configuración falla si etiqueta un App-ID entregado desde ACE y al menos un inquilino de NGFW o Prisma Access asociado con la carpeta seleccionada no está configurado para recibir los App-ID de ACE.

Por este motivo, Palo Alto Networks no recomienda seleccionar el alcance de configuración **Global**.

STEP 6 | En el campo de búsqueda **Category Filters (Filtros de categoría)**, introduzca el App-ID que desea etiquetar y selecciónelo.

Solo puede etiquetar un App-ID a la vez.

STEP 7 | Add/Edit Tag (Añadir/Editar etiqueta)



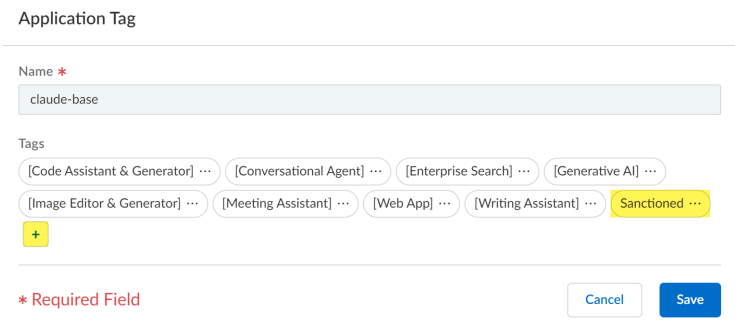
STEP 8 | Haga clic en + para aplicar una etiqueta de aplicación predefinida **Sanctioned (Autorizada)** o **Tolerated (Tolerada)**.

En este ejemplo, el App-ID `base de claude` está etiquetado con la etiqueta **Sanctioned (Autorizado)**.

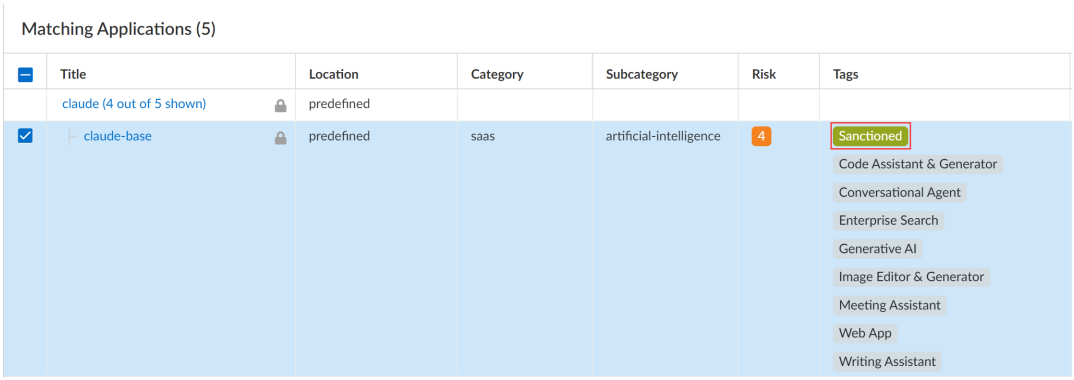
*Una aplicación se asume como **Unsanctioned (No sancionada)** en ausencia de las etiquetas **Sanctioned (Sancionada)** o **Tolerated (Tolerada)** si se etiqueta desde **Applications (Aplicaciones)**.*

*Si desea cambiar la etiqueta de la aplicación de **Sanctioned (Sancionada)** o **Tolerated (Tolerada)** a **Unsanctioned (No sancionada)**, debe eliminar la etiqueta existente. No puede etiquetar manualmente una aplicación como **Unsanctioned (No autorizada)** en **Applications (Aplicaciones)**.*

STEP 9 | **Save (Guardar).**



STEP 10 | Revise los valores de la columna **Tag (Etiqueta)** para verificar que aplicó correctamente la etiqueta de la aplicación.



STEP 11 | Haga clic en **Overview (Descripción general)**.

STEP 12 | **Push Config (Configuración de envío** y **Push (Enviar)** sus cambios en la configuración.

Etiquetar aplicaciones GenAI en el panel Insights

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Asocie el fragmento `Application-Tagging` predefinido con el ámbito de configuración adecuado para admitir la aplicación de políticas basadas en etiquetas.

STEP 3 | Obtenga los App-ID secundarios que desea etiquetar.

Puede obtener los App-ID secundarios para una aplicación GenAI de una de las siguientes maneras.

- Utilice el panel Insights de AI Access Security para descubrir los riesgos que plantean las aplicaciones GenAI. Insights de AI Access Security le muestra los App-ID secundarios detectados que se utilizan en toda su organización.
- Revise la lista de aplicaciones GenAI compatibles.
- Utilice Applipedia para buscar los App-ID secundarios de las aplicaciones GenAI compatibles que se entregan a través de una actualización de contenido dinámico.

  Applipedia solo muestra los App-ID para aplicaciones entregadas a través de un contenido dinámico y no muestra aplicaciones entregadas a través de App-ID Cloud Engine (ACE).

STEP 4 | Seleccione **Insights** > **Activity Insights** > **Applications (Aplicaciones)**.

STEP 5 | Localice el App-ID secundario de GenAI que desea etiquetar. Si es necesario, puede filtrar la tabla para mostrar solo las aplicaciones GenAI.

1. Seleccione **Add Filter (Añadir Filtro)** y añada el filtro **GenAI Application (Aplicación GenAI)**.
2. Establezca el filtro **GenAI Application (Aplicación GenAI)** en **TRUE (VERDADERO)**.

STEP 6 | Para revisar las etiquetas que se aplican al App-ID de GenAI, examine los valores en la columna **Tag (Etiqueta)**.

STEP 7 | Aplique una etiqueta diferente al App-ID de GenAI secundario.

1. En la columna **Actions (Acciones)**, seleccione el icono de etiqueta y seleccione la etiqueta **Sanctioned (Autorizada)**, **Tolerated (Tolerada)** o **Unsanctioned (No autorizada)**.
2. Elija **Apply (Aplicar)** para aplicar la nueva etiqueta.

Ver las puntuaciones de riesgo asignados a las aplicaciones GenAI

Para ayudarle a identificar rápidamente las aplicaciones GenAI que representan las mayores amenazas para su organización, AI Access Security asigna a cada aplicación GenAI una puntuación de riesgo. Estas puntuaciones de riesgo le permiten identificar rápidamente las aplicaciones GenAI de alto riesgo, para que pueda tomar medidas para proteger su entorno. Por ejemplo, para proteger su entorno, podría crear una regla de políticas para bloquear la aplicación. También podría optar por etiquetar la aplicación como No autorizada.

La puntuación de riesgo de una aplicación está entre 1 (bajo riesgo) y 5 (alto riesgo) y se basa en los atributos de la aplicación SaaS. Algunos atributos son comunes a todas las aplicaciones SaaS, mientras que un subconjunto de atributos son únicos para las aplicaciones GenAI.

Los *atributos de GenAI* son atributos como el tipo de datos para la entrada del usuario en la aplicación, el tipo de datos de la salida generada por la aplicación, y si los datos enviados por el usuario son utilizados por la aplicación para entrenar sus modelos GenAI. Basado en los valores de los atributos de GenAI, el cálculo de la puntuación de riesgo determina el riesgo GenAI.

Además de los atributos de GenAI, el cálculo de la puntuación de riesgo utiliza los siguientes tipos de atributos para determinar el riesgo general de la aplicación SaaS.

- *Los atributos de cumplimiento*, que identifican si una aplicación se adhiere a varios requisitos y estándares regulatorios.
- *Los atributos de gestión de acceso e identidad*, que identifican las capacidades de autenticación y control de acceso de una aplicación.
- *Los atributos de seguridad y privacidad*, que identifican las características del producto para proteger los datos. Esta categoría de atributos incluye atributos como si la aplicación cifra los datos en reposo y los datos en movimiento.

La puntuación final de riesgo de una aplicación GenAI es una combinación del riesgo general de SaaS (calculado a partir de los atributos de SaaS) y el riesgo GenAI (calculado a partir de los atributos de GenAI). El cálculo de la puntuación de riesgo otorga un peso adicional al riesgo de GenAI al determinar la puntuación de riesgo final.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Para navegar al panel Activity Insights, selecciona **Insights** > **Activity Insights** > **Applications (Aplicaciones)**.

STEP 3 | Localice las aplicaciones de GenAI en la tabla. Si es necesario, puede filtrar la tabla para mostrar solo las aplicaciones de GenAI.

1. Seleccione **Add Filter (Añadir Filtro)** y añada el filtro **GenAI Application (Aplicación GenAI)**.
2. Establezca el filtro **GenAI Application (Aplicación GenAI)** en **TRUE (VERDADERO)**.

STEP 4 | Para identificar las aplicaciones de GenAI que representan las mayores amenazas, examine los valores de la puntuación de riesgo en la columna **Risk (Riesgo)**.

Puntuación de riesgo	Significado
4-5	Alto Riesgo: muy probable que sea un riesgo.
3	Riesgo Medio: representa un riesgo moderado.
1-2	Bajo riesgo: poco probable que sea un riesgo.

STEP 5 | Tome medidas sobre las aplicaciones más peligrosas.

Por ejemplo, puede crear reglas de política para bloquear estas aplicaciones o etiquetar las aplicaciones como No aprobadas.

Usar filtros de aplicaciones para aplicaciones GenAI

Los filtros de aplicaciones agrupan dinámicamente aplicaciones según los atributos de aplicación que defina. Puede utilizar filtros de aplicación en sus Reglas de políticas de seguridad para controlar el acceso a las aplicaciones GenAI en función de los atributos de la aplicación en lugar de definir explícitamente aplicaciones GenAI o grupos de aplicaciones en su regla de la política de seguridad.

AI Access Security incluye los siguientes Filtros de aplicación GenAI predefinidos. Los Filtros de aplicación predefinidos se basan en los casos de uso de AI Access Security admitidos.

- Generador de audio
- Agente conversacional
- Asistente y generador de código
- Plataforma de desarrolladores
- Búsqueda empresarial
- Editor y generador de imágenes
- Asistente de reuniones
- Asistente de productividad
- Editor y generador de vídeo
- Asistente de escritura

Los filtros anteriores son solo etiquetas de visualización. No pueden utilizarse en las reglas de políticas de seguridad.

- Strata Cloud Manager
- Panorama

Utilice Filtros de aplicación para Aplicaciones GenAI en Strata Cloud Manager

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **Objects (Objetos)** > **Application (Aplicación)** > **Application Filters (Filtros de aplicación)** y **Add Application Filter (Añadir filtro de aplicación)**.

STEP 3 | Introduzca un **Name (Nombre)** descriptivo.

STEP 4 | Para la **Tag (Etiqueta)** seleccione **Generative AI (IA generativa)**.

Todas las aplicaciones GenAI inspeccionadas por NGFW o Prisma Access se etiquetan con `genai` cuando son inspeccionadas. Al crear un filtro de aplicación personalizado para aplicaciones GenAI, Palo Alto Networks recomienda seleccionar la etiqueta **Generative AI (IA generativa)** para asegurar que la regla de política de seguridad a la que se añade el filtro de aplicación se aplique al tráfico de aplicaciones GenAI.

STEP 5 | Configure `Filtros de categoría` adicionales para reducir el alcance de las aplicaciones GenAI afectadas. Considera las siguientes etiquetas al crear su filtro de aplicación GenAI.

- **Risk (Riesgo)**: especifique la puntuación de **Risk (Riesgo)** para que la acción de la regla de la política de seguridad solo se aplique a las aplicaciones GenAI con la puntuación de riesgo seleccionada.

  Por ejemplo, quiere escribir una regla de política de seguridad para bloquear el acceso a todas las aplicaciones GenAI de alto riesgo independientemente de su uso. En este caso, puede crear un filtro de aplicación para aplicaciones GenAI **4** y **5** para que la regla de política de seguridad solo se aplique a las aplicaciones GenAI con estas puntuaciones de riesgo.

- **Tag (Etiqueta)**: especifica si la acción de la regla de política de seguridad se aplica a las aplicaciones GenAI etiquetadas como **Sanctioned (Autorizadas)**, **Tolerated (Toleradas)**, o **Unsanctioned (No autorizadas)**. Además, puede aplicar etiquetas basadas en el caso de uso de la aplicación GenAI.

  Por ejemplo, quiere escribir una regla de política de seguridad para permitir el acceso a aplicaciones GenAI autorizadas de Asistente y generador de código. En este caso, puede crear un filtro de aplicación que incluya tanto las etiquetas **Sanctioned (Autorizadas)** como **Code Asistant & Generator (Asistente y generador de código)** para que la regla de política de seguridad solo se aplique a las aplicaciones GenAI con esta etiqueta de aplicación y que caigan dentro del caso de uso.

STEP 6 | Revise la lista de **Matching Applications (Aplicaciones coincidentes)**.

STEP 7 | **Save (Guardar)**.

STEP 8 | **Push Config (Configuración de envío)** y **Push (Envío)**.

STEP 9 | Creación de reglas de política de seguridad personalizadas para controlar el acceso a GenAI.

Utilice Filtros de aplicación para aplicaciones GenAI en Panorama

STEP 1 | Inicie sesión en la interfaz web de Panorama® management server.

STEP 2 | Seleccione **Objects (Objetos)** > **Application Filters (Filtros de aplicación)** y haga clic en **Add (Añadir)** para añadir un filtro de aplicación nuevo.

STEP 3 | Introduzca un **Name (Nombre)** descriptivo.

STEP 4 | Para la **Tag (Etiqueta)** seleccione **Generative AI (IA generativa)**.

Todas las aplicaciones GenAI inspeccionadas por NGFW o Prisma Access se etiquetan con `genai` cuando son inspeccionadas. Al crear un filtro de aplicación personalizado para aplicaciones GenAI, Palo Alto Networks recomienda seleccionar la etiqueta **Generative AI (IA generativa)** para asegurar que la regla de política de seguridad a la que se añade el filtro de aplicación se aplique al tráfico de aplicaciones GenAI.

STEP 5 | Configure `Filtros de categoría` adicionales para reducir el alcance de las aplicaciones GenAI afectadas. Considera las siguientes etiquetas al crear su filtro de aplicación GenAI.

- **Risk (Riesgo)**: especifique la puntuación de **Risk (Riesgo)** para que la acción de la regla de la política de seguridad solo se aplique a las aplicaciones GenAI con la puntuación de riesgo seleccionada.

  Por ejemplo, quiere escribir una regla de política de seguridad para bloquear el acceso a todas las aplicaciones GenAI de alto riesgo independientemente de su uso. En este caso, puede crear un filtro de aplicación para aplicaciones GenAI **4** y **5** para que la regla de política de seguridad solo se aplique a las aplicaciones GenAI con estas puntuaciones de riesgo.

STEP 6 | Revise la lista de Aplicaciones coincidentes.

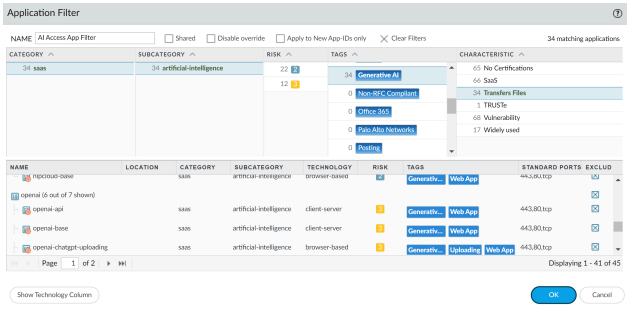
STEP 7 | Haga clic en **OK (Aceptar)**.

STEP 8 | Seleccione las opciones**Confirmar** y **Confirmar y enviar** para aplicar esos cambios en su configuración.

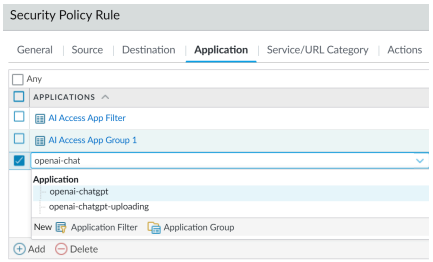
STEP 9 | Creación de reglas de política de seguridad personalizadas para controlar el acceso a GenAI.

STEP 10 | En el siguiente ejemplo, el filtro de aplicaciones **AI Access App Filter (Filtro de aplicaciones de AI Access)** tiene `Categoría: SaaS`, `Subcategoría: Inteligencia artificial`,

`Etiquetas: IA generativa` y `característica: Transferir archivos`. Esto crea un filtro con 34 aplicaciones GenAI coincidentes.



STEP 11 | En el siguiente ejemplo, openai-chatgpt se elige como la **Application (Aplicación)**.



STEP 12 | Defina el filtro seleccionando valores de atributo desde las secciones Category (Categoría), Subcategory (Subcategoría), Technology (Tecnología), Risk (Riesgo), Characteristic (Característica) y Tags (Etiquetas) relacionadas con IA conversacional. Por ejemplo, al seleccionar valores relacionados con el chat conversacional, observe que la lista de aplicaciones coincidentes en la parte inferior del cuadro de diálogo se reduce. Cuando ajuste los atributos de filtro para que coincidan con los tipos de aplicaciones que desee habilitar de forma segura, seleccione**Save (Guardar)**.

Modificar regla de políticas predeterminadas de acceso a aplicaciones GenAI para controlar el acceso GenAI

Modifique la regla de políticas predeterminadas de aplicaciones GenAI en Strata Cloud Manager para controlar el uso de aplicaciones GenAI en su empresa.

- *En Strata Cloud Manager, aunque se pueden crear reglas de políticas mediante* Políticas de seguridad *para aplicaciones GenAI, Palo Alto Networks recomendó que se utilizaran* reglas de políticas de seguridad para crear reglas de políticas *eficientemente.*
- *Palo Alto Networks no recomienda tener aplicaciones GenAI y no GenAI en la misma política si la licencia de Enterprise Data Loss Prevention (E-DLP) no está activa.*

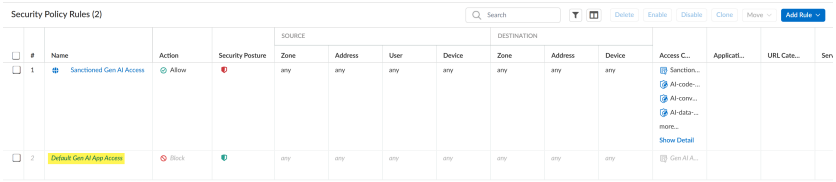
Por Strata Cloud Manager, AI Access Security incluye un `Acceso predeterminado a aplicaciones de GenAI` predefinido para controlar el acceso a todas las aplicaciones GenAI no permitidas explícitamente en su empresa con una política lista para usar. De forma predeterminada, esta regla de políticas bloquea todas las aplicaciones GenAI en toda la empresa. Para modificar esta política:

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW & Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de seguridad)** > **Security Policy (Política de seguridad)** y seleccione su objetivo **Configure Scope (Configurar alcance)** (fragmento *Gen-AI-Best-Practice*).

STEP 3 | Haga clic en la regla de políticas `Acceso predeterminado a aplicaciones de GenAI` predefinida.

Esta regla de políticas bloquea el acceso a todas las aplicaciones GenAI.



STEP 4 | **Enable (Habilitar)** la regla de políticas `Acceso predeterminado a aplicaciones de GenAI`. Esta deshabilitada de forma predeterminada.

STEP 5 | En la sección Aplicación web, configure la **Application (Aplicación)** y la **URL Category (Categoría URL)** según sea necesario. De forma predeterminada, la regla de políticas

`Acceso predeterminado a aplicaciones de GenAI` bloquea el acceso a todas las aplicaciones GenAI. Sin embargo, puede modificar la regla de políticas predefinida para bloqueo de aplicaciones específicas seleccionando individuos, grupos de aplicaciones o filtros de aplicaciones.

- **Application (Aplicación)**: añada una o más aplicaciones GenAI.
- **Application Group (Grupo de aplicaciones)**: un grupo de aplicaciones es un grupo estático de aplicaciones individuales que crea.
- **Application Filter (Filtro de aplicaciones)**: un filtro de aplicaciones agrupa dinámicamente las aplicaciones según los filtros de aplicaciones que defina.

  Por ejemplo, puede usar un filtro predefinido o personalizado para controlar dinámicamente el acceso a las aplicaciones GenAI de su organización en lugar de añadir aplicaciones GenAI individuales o crear un grupo de aplicaciones que debe actualizarse manualmente cada vez que se requiera un cambio.

STEP 6 | **Save (Guardar)**.

STEP 7 | **Push Config (Configuración de envío)** y **Push (Envío)**.

Creación de reglas de política de seguridad personalizadas para controlar el acceso a GenAI

Puede crear reglas de política de seguridad personalizadas para controlar el uso de aplicaciones GenAI y evitar la exfiltración de datos confidenciales a aplicaciones GenAI autorizadas. Utilice etiquetas, origen (tráfico basado en el origen), grupos de usuarios y otros parámetros específicos para crear su política personalizada. Esto le ayuda a hacer cumplir las reglas de política de seguridad personalizadas para las aplicaciones GenAI de su organización.

Strata Cloud Manager) Puede utilizar o modificar la regla de políticas de acceso a Internet predefinida **Sanctioned GenAI Access (Acceso GenAI autorizado)** o crear su propia regla de políticas de Acceso a Internet.

(Panorama® management server) Crear reglas de políticas de seguridad para controlar el uso de aplicaciones GenAI en su organización.

Debe crear reglas de políticas de seguridad para controlar las aplicaciones GenAI autorizadas y toleradas independientemente de las aplicaciones GenAI no autorizadas. Por ejemplo, si hay aplicaciones GenAI toleradas a las que solo pueden acceder usuarios específicos de su organización, puede crear una regla de la política de seguridad para permitir solo el acceso a esos usuarios específicos. Puede asociar un perfil de datos de Enterprise Data Loss Prevention (E-DLP) a la regla de la política de seguridad para evitar la exfiltración de datos confidenciales y un perfil de protección frente a vulnerabilidades para detener los intentos de exploit de fallos del sistema u obtener acceso no autorizado a los sistemas para los usuarios autorizados. Además, crea una segunda regla de la política de seguridad más baja en la jerarquía de la base de reglas para denegar el acceso a todos los demás.

- *En Strata Cloud Manager, aunque puede crear reglas de políticas personalizadas a través de Políticas de seguridad para aplicaciones GenAI, se recomienda que utilice reglas de políticas de acceso a Internet para crear reglas de políticas eficientemente.*
- *No se recomienda tener aplicaciones GenAI y no GenAI en la misma política si la licencia de Enterprise Data Loss Prevention (E-DLP) no está activa.*

- Strata Cloud Manager
- Panorama

Crear reglas de políticas personalizadas para controlar el uso de aplicaciones GenAI (Strata Cloud Manager)

Las reglas de políticas de seguridad de acceso a internet se evalúan y aplican por delante de sus Reglas de políticas de seguridad. En el caso de que una regla de la política de acceso a Internet y la regla de la política de seguridad se apliquen ambas al mismo tráfico, la acción Regla de políticas de acceso a internet y configuración de inspección de Enterprise DLP tienen prioridad sobre la regla de la política de seguridad. Después de una coincidencia exitosa con una regla de políticas de Acceso a Internet, no se realiza ninguna otra evaluación de reglas de políticas.

Por ejemplo, crea una regla de políticas de acceso a Internet y una regla de la política de seguridad que se aplican al `grupo de usuarios A` y a varias aplicaciones de GenAI.

- *La `regla de políticas de acceso a Internet A` permite a `grupo de usuarios A` acceder a las aplicaciones GenAI especificadas y tiene un `perfil de datos A` de Enterprise DLP asociado a las aplicaciones GenAI para evitar la exfiltración de datos sensibles.*
- *La `Regla de política de seguridad B` bloquea el acceso del `grupo de usuarios A` a las mismas aplicaciones GenAI especificadas.*

En este caso, cuando un usuario del `grupo A` accede a una aplicación GenAI especificada en las reglas de acceso a Internet y políticas de seguridad, se le permite y se inspecciona el Enterprise DLP y se emiten veredictos porque la `regla de políticas` es superior en el orden de evaluación de la base de reglas de políticas.

STEP 1 | Utilice el panel Insights de AI Access Security para descubrir los riesgos que plantean las aplicaciones GenAI.

El panel Insights de AI Access Security proporciona una visibilidad detallada y completa del uso de aplicaciones GenAI en toda su organización. Puede descubrir casos de uso de aplicaciones GenAI peligrosas, aplicaciones GenAI peligrosas individuales, así como usuarios peligrosos que acceden a aplicaciones GenAI.

STEP 2 | Si desea utilizar las políticas existentes en fragmentos, realice la configuración inicial de AI Access Security.

En Strata Cloud Manager, esto incluye la creación de un perfil Enterprise Data Loss Prevention (E-DLP) de datos para definir los criterios de coincidencia sensibles de datos, la asociación de fragmentos predefinidos de `Gen-AI-Best-Practice` y `Application-Tagging`, y el perfil

de protección frente a vulnerabilidades utilizado para detener los intentos de exploit de fallos del sistema o de acceso no autorizado a los sistemas.

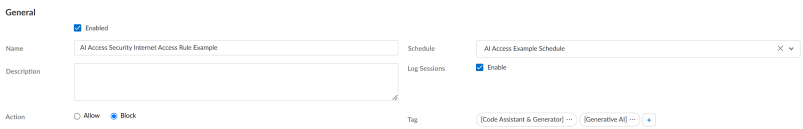
Para NGFW, esto incluye también la creación de una zona fiable interna y una zona no fiable saliente.

STEP 3 | Si desea crear sus propias políticas personalizadas, inicie sesión en Strata Cloud Manager.

STEP 4 | Crear una regla de políticas de Acceso a Internet personalizada.

- *En Strata Cloud Manager, aunque puede crear reglas de políticas personalizadas a través de Políticas de seguridad para aplicaciones GenAI, se recomienda que utilice reglas de políticas de acceso a Internet para crear reglas de políticas eficientemente.*
- *No se recomienda tener aplicaciones GenAI y no GenAI en la misma política si la licencia de Enterprise Data Loss Prevention (E-DLP) no está activa.*

1. Seleccione **Add Rule (Añadir regla)** > **Internet Access Rule (Regla de acceso a Internet)**.
2. Deberá **Active (Activar)** la regla de políticas de Acceso a Internet.
3. Introduzca un **Name (Nombre)** descriptivo.
4. (Opcional) Añada una **Description (Descripción)** para la regla de políticas Acceso a Internet y añada una **Tag (Etiqueta)** predefinida o crear una nueva.
5. Configurar la **Action (Acción)** [**Block (Bloquear)** o **Allow (Permitir)**].
6. (Opcional) Configure un **Schedule (Programa)** para especificar las veces que la regla de políticas de Acceso a Internet está activa.



7. En la sección Criterios de coincidencia, defina el tráfico que se aplicará en función del **origen** del tráfico (donde se origina).

   Por ejemplo, basándose en su investigación de detección de riesgos, usted determina que usuarios no autorizados asociados con el `grupo de usuarios A` acceden a una aplicación GenAI autorizada para su uso por el `Grupo de usuarios B`. En este caso,

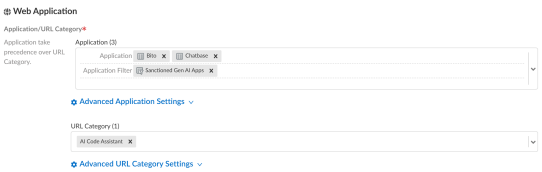
puede crear una regla de políticas de acceso a Internet para bloqueo del acceso a la GenAI y añadir el `Grupo usuario A` como **Source (Origen)** del grupo de usuarios.

8. En la sección Aplicación web, configure la **Application (Aplicación)** o **URL Category (Categoría URL)** para definir qué aplicaciones GenAI o URL GenAI desea bloquear o permitir acceso.

   (Aplicaciones GenAI permitidas) Solo añade aplicaciones GenAI compatibles a la lista de aplicaciones permitidas.

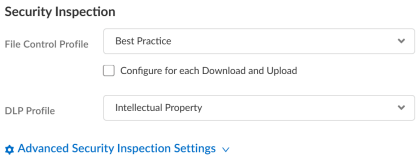
   - **Application (Aplicación)**: añada una o más aplicaciones GenAI.
   - **Application Group (Grupo de aplicaciones)**: un grupo de aplicaciones es un grupo estático de aplicaciones individuales que crea.
   - **Application Filter (Filtro de aplicaciones)**: un filtro de aplicaciones agrupa dinámicamente las aplicaciones según los filtros de aplicaciones que defina.

     Por ejemplo, puede usar un filtro predefinido o personalizado para controlar dinámicamente el acceso a las aplicaciones GenAI de su organización en lugar de añadir aplicaciones GenAI individuales o crear un grupo de aplicaciones que debe actualizarse manualmente cada vez que se requiera un cambio.



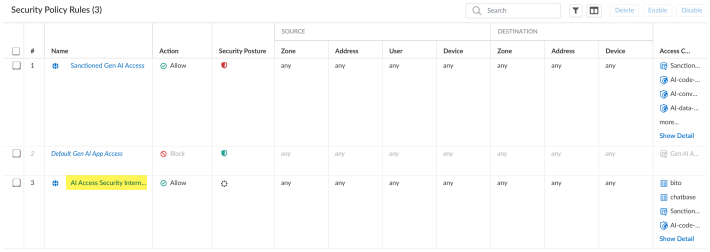
9. (Aplicaciones GenAI permitidas) En la sección Inspección de seguridad, seleccione un bloqueo de archivos y perfil de Enterprise DLP para evitar la exfiltración de datos confidenciales.

   - **Perfiles de bloqueo de archivos**: Un Perfil de bloqueo de archivos le permite identificar tipos de archivos específicos que desee bloquear o supervisar. Puede crear un perfil personalizado de bloqueo de archivos o utilizar el perfil predeterminado de bloqueo de archivos de `prácticas recomendadas`.
   - **Perfil DLP**: un perfil de datos de Enterprise DLP le permite definir los criterios de coincidencia para los datos sensibles que desea inspeccionar y bloqueo para evitar la exfiltración de datos sensibles. Debe asignar un perfil de datos para generar datos de **Sensitive Assets (Activos sensibles)** cuando descubra riesgos planteados por aplicaciones GenAI.



10. Configure el resto de la regla de políticas personalizada de Acceso a Internet según sea necesario.
11. **Save (Guardar)**.

STEP 5 | Compruebe que su regla de política de acceso se creó correctamente y ordene dentro de su base de reglas de políticas según sea necesario.



STEP 6 | **Push Config (Configuración de envío)** y **Push (Envío)**.

Crear reglas de políticas personalizadas para controlar el uso de aplicaciones GenAI (Panorama)

STEP 1 | Utilice el panel Insights de AI Access Security para descubrir los riesgos que plantean las aplicaciones GenAI.

El panel Insights de AI Access Security proporciona una visibilidad detallada y completa del uso de aplicaciones GenAI en toda su organización. Puede descubrir casos de uso de aplicaciones GenAI peligrosas, aplicaciones GenAI peligrosas individuales, así como usuarios peligrosos que acceden a aplicaciones GenAI.

STEP 2 | Realizar la configuración inicial de AI Access Security.

Esto incluye la creación de un perfil de datos de Enterprise Data Loss Prevention (E-DLP) para definir los criterios de coincidencia confidencial de datos y el perfil de protección frente a vulnerabilidades utilizado para detener los intentos de exploit de fallos del sistema u obtener acceso no autorizado a los sistemas.

Para NGFW, esto incluye también la creación de una zona fiable interna y una zona no fiable saliente.

STEP 3 | Inicie sesión en la interfaz web de Panorama® management server.

STEP 4 | Seleccione **Policies (Políticas)** > **Security (Seguridad)** y especifique el grupo de dispositivos.

STEP 5 | **Add (Añadir)** una nueva regla de política de seguridad.

STEP 6 | Configure los ajustes de la regla de la política de seguridad: **General**, **Source (Origen)** y **Destination (Destino)**.

Consulte la Guía de administración de las políticas de seguridad para obtener información detallada sobre la redacción de una regla de la política de seguridad.

- **General**: Dé a la regla un **Name (Nombre)** descriptivo. También tiene la opción de proporcionar una **Description (Descripción)** para la regla de la política de seguridad y aplicar etiquetas para ayudar a identificar el propósito de la regla de la política de seguridad.
- **Source (Origen)**: define de dónde debe proceder el tráfico para que se aplique la regla de la política de seguridad.

  Para la **Source Zone (Zona de origen)**, puede seleccionar una zona fiable interna. Si desea que la regla de la política de seguridad se aplique a todo el tráfico, independientemente de dónde se originó, seleccione **Any (Cualquiera)** para todos los ajustes de origen.

  Por ejemplo, en función de su evaluación de descubrimiento de riesgos, determina que el acceso a una aplicación GenAI está sobreaprovisionado y debe restringirse a usuarios

específicos. En este caso puede escribir una regla de políticas **Allow (Permitir)** y añadir el **Source User (Usuario de origen)** requerido.

- **Destination (Destino)**: defina el destino objetivo del tráfico para que se aplique la regla de la política de seguridad.

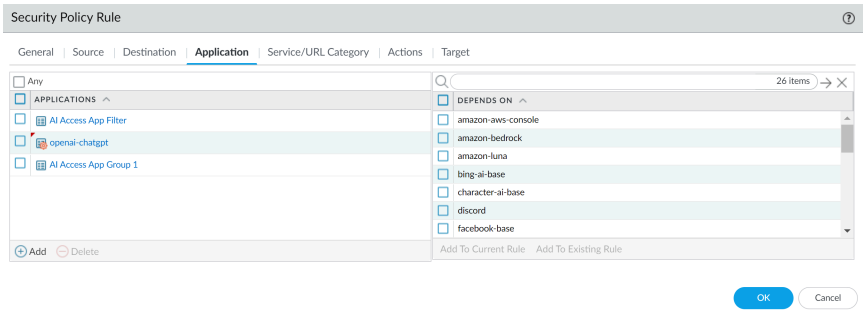
  Para la **Destination Zone (Zona de destino)**, puede seleccionar una zona no fiable saliente. Si desea que la regla de la política de seguridad se aplique a todo el tráfico independientemente de cuál sea el destino, seleccione **Any (Cualquiera)** para todos los ajustes de destino.

STEP 7 | En la configuración de **Applications (Aplicaciones)**, especifique el Grupo de aplicaciones, Filtro de aplicaciones o Aplicaciones GenAI.

(Aplicaciones web permitidas) Solo añade aplicaciones GenAI compatibles a la lista de aplicaciones permitidas.

- **Application (Aplicación)**: añada una o más aplicaciones GenAI.
- **Application Category (Categoría de aplicación)**: una categoría de aplicación, también denominada filtro de aplicaciones, agrupa dinámicamente aplicaciones según los filtros de aplicación que defina.

  Por ejemplo, puede usar un filtro predefinido o personalizado para controlar dinámicamente el acceso a las aplicaciones GenAI de su organización en lugar de añadir aplicaciones GenAI individuales o crear un grupo de aplicaciones que debe actualizarse manualmente cada vez que se requiera un cambio.
- **Application Group (Grupo de aplicaciones)**: un grupo de aplicaciones es un grupo estático de aplicaciones individuales que crea.



STEP 8 | Configure las **Actions (Acciones)** de la regla de política de seguridad. Decida qué acciones quiere tomar en su regla de políticas. Cómo práctica recomendada, adjunte perfiles de seguridad para habilitar el cortafuegos para que explore todo el tráfico permitido en busca de amenazas. Seleccione **Profiles (Perfiles)** del menú desplegable **Profile Type (Tipo de perfil)** y luego seleccione los perfiles de seguridad individuales para adjuntar a la regla. Elija las acciones necesarias para los siguientes ajustes de sus aplicaciones GenAI:

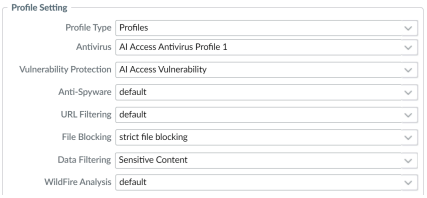
1. Para la **Action (Acción)**, configure la Action (Acción) que realiza el NGFW cuando se detecta tráfico desde el **Source (Origen)** de la regla de la política de seguridad al **Destination (Destino)**.

   Por ejemplo, seleccione **Allow (Permitir)** si desea permitir el acceso a una o más aplicaciones GenAI o **Deny (Denegar)** si desea bloquear todo el acceso a una o más aplicaciones GenAI.

2. Para el **Profile Type (Tipo de perfil)**, seleccione **Profile (Perfil)**.

   Como mínimo, debe añadir los perfiles de **Vulnerability Protection (Protección frente a vulnerabilidades)** y **Data Filtering**. Estos son necesarios para generar datos de **Threats (Amenazas)** y **Sensitive Assets (Activos sensibles)** al descubrir riesgos planteados por aplicaciones GenAI. Los perfiles restantes son opcionales y se pueden configurar según sea necesario. Para cada uno de los tipos de perfil de seguridad siguientes puede seleccionar un perfil existente o crear uno nuevo.

   - Antivirus
   - Protección contra vulnerabilidades
   - Antispyware
   - URL Filtering
   - Bloqueo de archivos
   - Data Filtering
   - Análisis de WildFire



*En la pestaña **Actions (Acciones)**, **Profile Setting (Configurar perfil)** tiene prioridad sobre **Action Setting (Ajuste de acción)**. Por lo tanto, como una práctica recomendada, asegúrese de que ambos ajustes coincidan correctamente. Por ejemplo, incluso si tiene la configuración de acción como Allow (Permitir) y una de los ajustes de perfil como Block (Bloquear) para ChatGPT, esta se bloqueará.*

STEP 9 | Confirme y envíe la nueva configuración a sus cortafuegos gestionados para completar la instalación del complemento de Enterprise DLP.

Este paso es necesario para que los nombres de perfil de filtrado de datos de Enterprise DLP aparezcan en los logs de filtrado de datos.

> *El comando **Commit and Push (Confirmar y enviar)** no se recomienda para cambios de configuración Enterprise DLP. El uso del comando **Commit and Push (Confirmar y enviar)** requiere la selección manual adicional e innecesaria de las plantillas impactadas y los cortafuegos gestionados en la Selección del ámbito de envío.*

- **Envío de configuración completa de Panorama**
  1. Seleccione **Commit (Confirmar)** > **Commit to (Confirmar en) Panorama** y **Commint (Confirmar)**.
  2. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y **Edit Selections (Editar selecciones)**.
  3. Seleccione **Device Groups (Grupos de dispositivos)** e**Include Device and Network Templates (Incluir dispositivos y plantillas de red)**.
  4. Haga clic en **OK (Aceptar)**.
  5. Seleccione **Push (Enviar)** para enviar los cambios de configuración a sus cortafuegos gestionados que utilizan Enterprise DLP.
- **Envío parcial de configuración de Panorama**

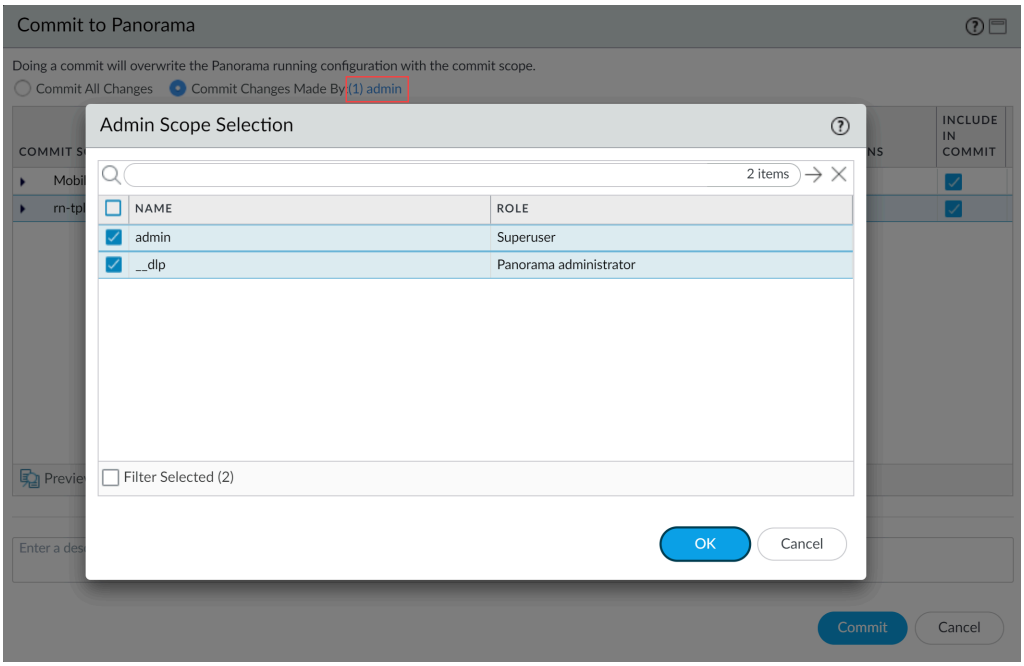
  > *Incluya siempre el administrador temporal `__DLP` cuando realice un envío parcial de configuración. Esto es necesario para sincronizar Panorama y el servicio en la nube DLP.*
  >
  > *Por ejemplo, tiene un usuario de administración `admin` Panorama que puede compilar y enviar cambios de configuración. El usuario `administrador` hizo cambios en la configuración de Enterprise DLP y solo desea confirmar y enviar estos cambios a cortafuegos gestionados. En este caso, se requiere que el usuario `administrador` también seleccione el usuario `__DLP` en las operaciones de confirmación parcial y envío.*

  1. Seleccione **Commit (Confirmar)** > **Commit (Confirmar en) Panorama**.
  2. Seleccione **Commit Changes Made By (Confirmar cambios realizados por)** y, a continuación, haga clic en el usuario administrador actual de Panorama para seleccionar administradores adicionales que se incluirán en la compilación parcial.

     En este ejemplo, el usuario `admin` ha iniciado sesión y está realizando la operación confirmar. El usuario `administrador` debe hacer clic en **admin** y luego seleccionar

el usuario __DLP. Si hay cambios de configuración adicionales realizados por otros administradores de Panorama, también se pueden seleccionar aquí.

Haga clic en **OK (Aceptar)** para continuar.

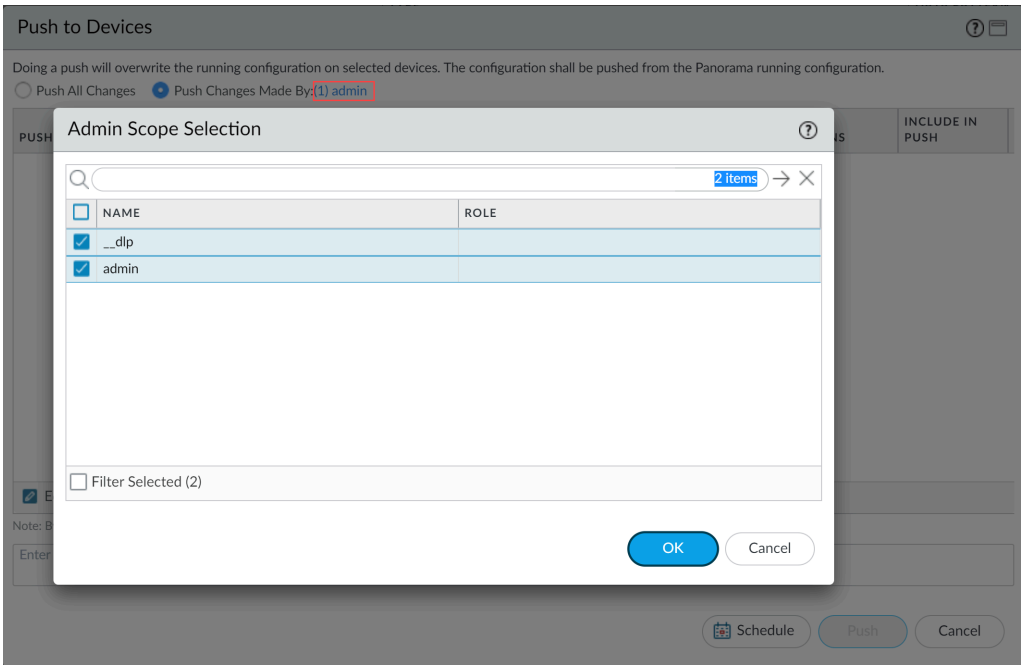


3. Seleccione **Commit (Confirmar)**.
4. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)**.
5. Seleccione **Push Changes Made By (Enviar cambios hechos por)** y, a continuación, haga clic en el usuario actual de la administración de Panorama para seleccionar administradores adicionales que se incluirán en el envío parcial.

   En este ejemplo, el usuario `admin` está actualmente conectado y realizando la operación push. El usuario `administrador` debe hacer clic en **admin** y luego seleccionar el

usuario __DLP. Si hay cambios de configuración adicionales realizados por otros administradores de Panorama, también se pueden seleccionar aquí.

Haga clic en **OK (Aceptar)** para continuar.



6. Seleccione **Device Groups (Grupos de dispositivos)** e**Include Device and Network Templates (Incluir dispositivos y plantillas de red)**.
7. Haga clic en **OK (Aceptar)**.
8. Seleccione **Push (Enviar)** para enviar los cambios de configuración a sus cortafuegos gestionados que utilizan Enterprise DLP.

AI Access SecurityRecomendaciones

Los administradores de seguridad de su red obtienen datos valiosos sobre el uso de aplicaciones GenAI en la red de su organización mediante el panel de AI Access Security y el Strata Command Center. Para que los administradores de seguridad de red puedan abordar rápidamente las deficiencias y reforzar su postura de seguridad al adoptar aplicaciones GenAI, Palo Alto Networks presenta recomendaciones de AI Access Security.

AI Access Security ofrece recomendaciones manuales y automatizadas. Las recomendaciones manuales son aquellas que necesita implementar manualmente. AI Access Security ofrece instrucciones paso a paso y proporciona enlaces a toda la documentación relevante para ayudarle a implementar con éxito los cambios recomendados. El Copilot de Palo Alto Networks en Strata Cloud Manager aplica las recomendaciones automatizadas en lugar del admin. Sin embargo, la administración que inició la recomendación propuesta por AI Access Security debe aprobar todos los cambios.

- **Recomendaciones para NGFW y Prisma Access (gestionadas por Strata Cloud Manager)**: las recomendaciones de AI Access Security actualizan en tiempo real a medida que los administradores realizan cambios de configuración y AI Access Security analiza el tráfico en la red. Esto le permite responder rápidamente a cualquier cambio de configuración o tráfico de aplicaciones GenAI arriesgado que pueda comprometer su organización si no interviene de inmediato. Cualquier recomendación que analice el tráfico en su red tiene un período de siete días de revisión que informa la recomendación.

  Si tiene NGFW y Prisma Access (gestionados por Strata Cloud Manager), así como Prisma Browser, AI Access Security muestra recomendaciones solo para sus inquilinos de NGFW y Prisma Access. En este caso, AI Access Security no muestra recomendaciones para Prisma Browser.
- **Recomendaciones para NGFW y Prisma Access (gestionados por Panorama)**: las recomendaciones de AI Access Security se actualizan cada 24 horas en Strata Cloud Manager.

  Si tiene NGFW y Prisma Access (gestionados por Panorama), así como Prisma Browser, AI Access Security muestra recomendaciones solo para sus inquilinos de NGFW y Prisma Access. En este caso, AI Access Security no muestra recomendaciones para Prisma Browser.
- **Recomendaciones para Prisma Browser**: las recomendaciones de AI Access Security son estáticas y persisten después de su aplicación. Palo Alto Networks recomienda continuar la supervisión de estas recomendaciones después de la aplicación para garantizar que sus administradores de seguridad subsanen cualquier laguna en su estrategia de adopción de aplicaciones GenAI.

  AI Access Security muestra recomendaciones para Prisma Browser solo cuando tiene una licencia de Prisma Browser independiente y no tiene ningún inquilino NGFW o Prisma Access implementado.

  Si tiene NGFW y Prisma Access (gestionados por Panorama o Strata Cloud Manager), así como Prisma Browser, AI Access Security muestra recomendaciones solo para sus inquilinos de

NGFW y Prisma Access. En este caso, AI Access Security no muestra recomendaciones para Prisma Browser.

AI Access Security ofrece recomendaciones para las siguientes hipótesis.

- **Recomendaciones de clasificación de aplicaciones GenAI**

  Enfocado en proporcionar recomendaciones basadas en el uso de la aplicación GenAI en su red y su clasificación de aplicaciones (Autorizadas, Toleradas o No autorizadas).

  Por ejemplo, si AI Access Security nota que su organización permite el tráfico a aplicaciones GenAI no autorizadas. En este caso, AI Access Security recomienda reclasificar estas aplicaciones GenAI como Autorizadas o Toleradas.

- **Verificaciones de prácticas recomendadas y recomendaciones de políticas**

  AI Access Security utiliza el servicio de Evaluaciones continuas de prácticas recomendadas (BPA) para analizar su base de reglas de políticas existente de NGFW y Prisma Access, y ofrecer recomendaciones para reforzar su postura de seguridad a fin de adoptar aplicaciones GenAI de forma segura.

  Por ejemplo, si el servicio BPA descubre que tiene una regla de la política de seguridad que permite el acceso a aplicaciones GenAI no autorizadas.

- **Recomendaciones de prevención de pérdida de datos**

  Para evitar la filtración de datos confidenciales a aplicaciones GenAI autorizadas y toleradas, AI Access Security analiza las reglas de su política de seguridad para determinar si está reenviando tráfico a Enterprise DLP para inspección en línea y para datos en reposo. Esto también puede incluir recomendaciones de configuración requeridas para reenviar tráfico a Enterprise DLP

- **Incorporación y maximización de AI Access Security**

  Estos se centran en proporcionar recomendaciones prácticas para aprovechar mejor las capacidades en toda la plataforma. Estas recomendaciones se centran en la conectividad del usuario a varios mercados o para aplicaciones GenAI compatibles con datos en reposo.

- **Prisma BrowserRecomendaciones**

  Las recomendaciones de Prisma Browser se centran en proporcionar orientación específica para ayudar a los usuarios independientes de Prisma Browser a proteger y optimizar el uso de sus aplicaciones GenAI. Estas recomendaciones pueden incluir configurar el acceso a aplicaciones GenAI, activar reglas de política de seguridad predefinidas para asegurar el acceso a aplicaciones GenAI a las que se accede a través de Prisma Browser y revisar incidentes sospechosos de exfiltración de datos confidenciales a aplicaciones GenAI no autorizadas.

Generar un informe de AI Access Security

El informe de AI Access Security proporciona una descripción general completa de la aplicación GenAI de su organización, el uso del complemento y la postura de seguridad. Este informe le ayuda a comprender y gestionar los riesgos asociados con las aplicaciones GenAI en rápida evolución en su entorno. Repleto de información práctica y recomendaciones personalizadas, este informe permite a sus administradores de seguridad tomar decisiones informadas sobre la estrategia de adopción de sus aplicaciones GenAI y la seguridad.

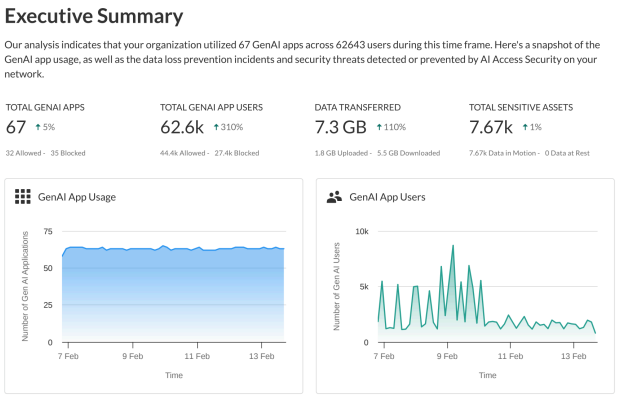
Los componentes clave del informe de AI Access Security son:

- **Resumen ejecutivo**

  La sección Resumen ejecutivo proporciona una instantánea de alto nivel de las métricas clave de la aplicación GenAI y el complemento en su organización. Ofrece una descripción general concisa de:

  - Uso de aplicaciones GenAI, lo que le brinda una comprensión rápida de la amplitud con la que los usuarios de su organización acceden a estas aplicaciones.
  - El volumen de datos cargados y descargados de las aplicaciones GenAI en gigabytes (GB).
  - Número de activos de datos sensibles detectados para datos en movimiento y en reposo.

  La sección Resumen ejecutivo ofrece a sus administradores de seguridad una vista rápida y de un vistazo del panorama de aplicaciones GenAI dentro de su organización. Sirve como punto de entrada a la información más detallada proporcionada en secciones posteriores del informe, lo que permite a sus administradores de seguridad comprender rápidamente la postura general de seguridad GenAI de su organización e identificar áreas que podrían requerir más atención o investigación.

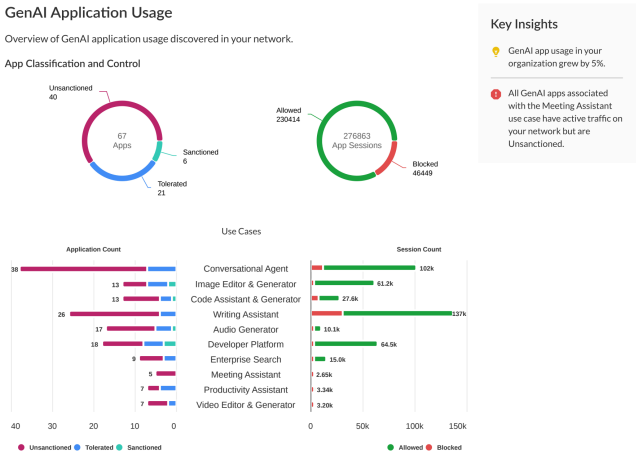


- **Uso de la aplicación de GenAI**

  La sección Uso de aplicaciones GenAI proporciona un desglose completo del uso de aplicaciones GenAI dentro de su organización. Incluye:

  - Número total de aplicaciones GenAI, que muestra la distribución entre aplicaciones GenAI permitidas y bloqueadas, y aplicaciones GenAI autorizadas, toleradas y no autorizadas.
  - Desglose de los casos de uso de GenAI, clasificados por la clasificación de la aplicación (Autorizada, Tolerada o No autorizada) y si el tráfico estaba permitido o bloqueado.
  - Número de aplicaciones no autorizadas pero permitidas, incluido el cambio desde el inicio del período del informe.
  - Datos de uso agregados de aplicaciones GenAI no autorizadas pero permitidas, incluido el número de usuarios y la cantidad total de datos transferidos.
  - Detalles sobre las 5 principales aplicaciones GenAI no autorizadas pero permitidas, incluido el nombre de la aplicación, el número de usuarios, el número de sesiones y los factores de riesgo asociados.

  Esta sección ayuda a sus administradores de seguridad a identificar rápidamente posibles riesgos de seguridad, comprender la utilización de la aplicación GenAI en diferentes casos de uso y tomar decisiones informadas sobre las reglas de la política de uso de la aplicación y su postura de seguridad.

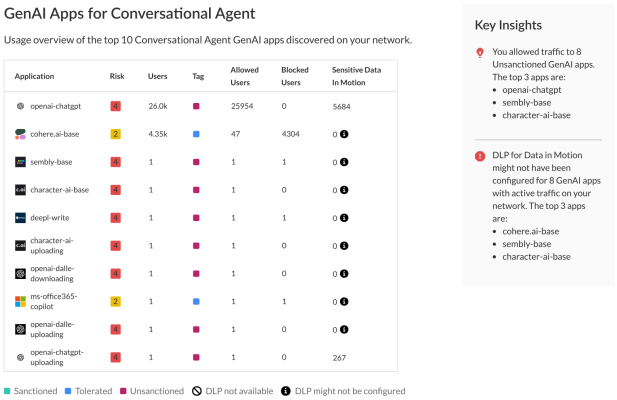


- **Aplicaciones GenAI para los principales casos de uso**

  Las secciones Aplicación GenAI para usos principales proporcionan un resumen de las 10 principales aplicaciones GenAI utilizadas dentro de su organización clasificadas por el Caso de uso de la aplicación GenAI. Proporciona un desglose detallado de las aplicaciones GenAI más destacadas utilizadas dentro de su organización e incluye lo siguiente para cada aplicación GenAI:

  - Nombre de la aplicación GenAI utilizada.
  - Puntuación de riesgo asociada con la aplicación GenAI.
  - Número de usuarios únicos que utilizaron la aplicación GenAI.
  - Clasificación de la aplicación GenAI, que indica si la aplicación está autorizada, tolerada o no.
  - Número de sesiones únicas permitidas y bloqueadas para la aplicación GenAI.

- Número de incidentes de Enterprise DLP generados por los usuarios que acceden a la aplicación GenAI.

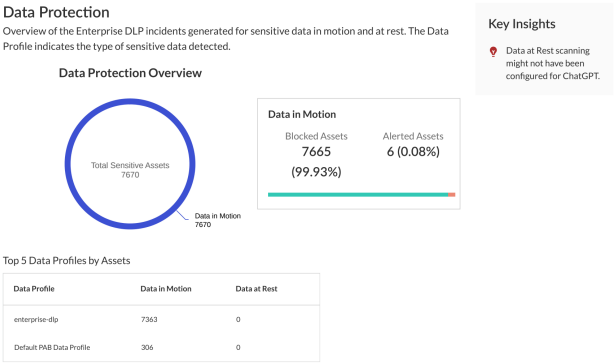


- **Protección de datos**

  La sección Protección de datos proporciona información crucial sobre la gestión de datos confidenciales dentro del ecosistema GenAI de su organización. Esta sección incluye:

  - Número total de activos sensibles detectados, clasificados como Permitidos o Bloqueados.
  - Distribución de activos sensibles entre todas las aplicaciones GenAI, agrupados por tipo de activo sensible.
  - Información detallada sobre datos confidenciales que se encuentran en las 5 aplicaciones GenAI principales.

  Esta información ayuda a sus administradores de seguridad a identificar rápidamente los posibles riesgos de seguridad de datos asociados con el uso de la aplicación GenAI en su organización. Al resaltar qué aplicaciones GenAI están gestionando información confidencial y qué tipos de datos confidenciales se están procesando, puede priorizar sus esfuerzos de protección de datos y ajustar sus reglas de política de seguridad según sea necesario.



STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Insights** > **SECURITY (SEGURIDAD)** > **AI Access**.

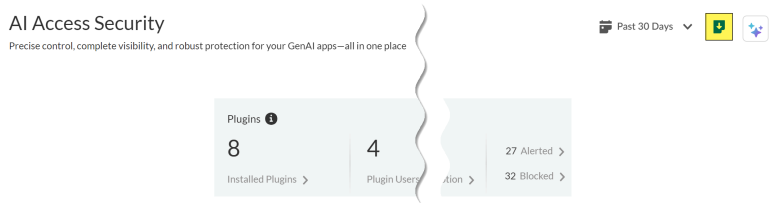
STEP 3 | Seleccione el periodo de tiempo para el informe de AI Access Security.

AI Access Security admite la generación de un informe para las **Past 24 Hours (Últimas 24 horas)**, los **Past 7 Days (Últimos 7 días)** o los **Past 30 Days (Últimos 30 días)**.

STEP 4 | **Descargue** el informe de AI Access Security en su dispositivo local en formato PDF.

El nombre de archivo predeterminado es `AI Access Security Report <generation-date>.pdf`.

No abandone ni actualice la página antes de que se complete la descarga del informe de AI Access Security. Salir o actualizar la página antes de que se complete la descarga interrumpe la descarga y debe descargar el informe de AI Access Security nuevamente.



STEP 5 | Vaya a la carpeta de descargas que seleccionó y revise el Informe de AI Access Security.