paloalto
TECHDOCS

AI Access Security Administration

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

Découvrir les risques posés par les applications GenAI

Utilisez le tableau de bord AI Access Security Insights pour filtrer l'utilisation des applications d'IA générative (GenAI) sur votre réseau. Le tableau de bord AI Access Security Insights fournit des détails approfondis pour vous aider à comprendre quelles applis d'intelligence artificielle générative sont utilisées et leurs utilisateurs.

AI Access Security détecte les données **Allowed Users (Utilisateurs autorisés)**, les données **Blocked Users (Utilisateurs bloqués)** ou les deux en fonction des filtres suivants.

- **1 Hour (1 heure)** et **3 Heures (3 heures)**

  Les utilisateurs peuvent être comptés comme Allowed (Autorisés), Blocked (Bloqués), ou les deux.

  Par exemple, l'accès de `UtilisateurA` à `Appli-GenAI1` est bloqué en raison de `Règle de politique1`. Une heure plus tard, `UtilisateurA` se rend dans un bureau d'une filiale où `Règle de politique2` permet l'accès à `Appli-GenAI1`. Dans ce cas, `UtilisateurA` est compté à la fois dans **Allowed Users (Utilisateurs autorisés)** et **Blocked Users (Utilisateurs bloqués)**.

  Inversement, `Règle de politique1` bloque l'accès de `UtilisateurA` à `Appli-GenAI1`. Quelques minutes plus tard, votre administrateur de sécurité modifie la `Règle de politique1` pour permettre l'accès de `UtilisateurA`. Dans ce cas, `UtilisateurA` est comptabilisé dans les **Blocked Users (Utilisateurs bloqués)**. AI Access Security affiche les utilisateurs dans le nombre de **Blocked Users (Utilisateurs bloqués)** peu importe combien de fois vous avez autorisé l'accès au cours des dernières **1 Hour (1 heure)** ou **3 Hours (3 heures)** si l'utilisateur correspondait à la même règle de politique de sécurité et si son accès avait été bloqué au moins une fois.
- **24 Hours (24 heures)**, **7 Day (7 jours)**, et **30 Day (30 jours)**

  Les utilisateurs peuvent être comptés comme Allowed (Autorisés), Blocked (Bloqués), ou les deux.

  Par exemple, vous avez initialement bloqué l'accès de `UtilisateurA` à `Appli-GenAI1`. Six heures plus tard, `UtilisateurA` se rend dans un bureau d'une filiale où `Règle de politique2` permet d'accéder à `Appli-GenAI1`. Dans ce cas, `UtilisateurA` est compté à la fois dans **Allowed Users (Utilisateurs autorisés)** et **Blocked Users (Utilisateurs bloqués)**.

Découvrir les risques posés par les applications GenAI selon le cas d'utilisation

Consultez les cas d'utilisation pris en charge pour obtenir des descriptions complètes de toutes les catégories de cas d'utilisation auxquelles une application GenAI appartient.

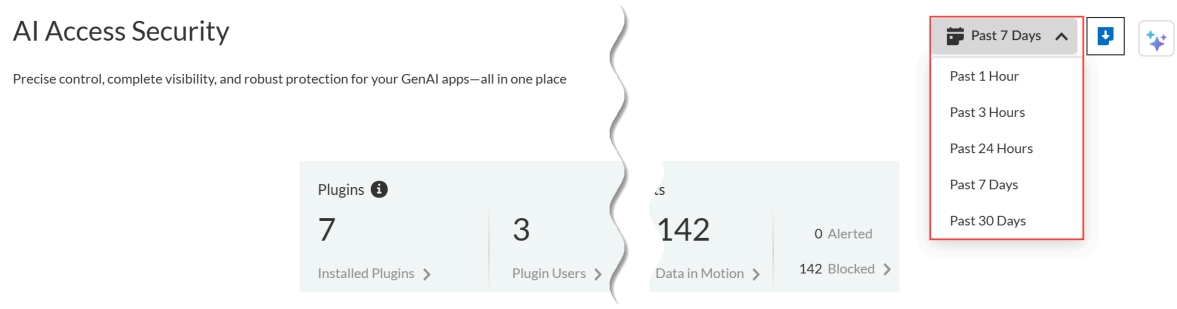
STEP 1 | Connectez-vous à Strata Cloud Manager.

STEP 2 | Sélectionnez **Insights (Informations)** > **AI Access (Accès à l'IA)** pour afficher le tableau de bord AI Access Security Insights.

Par défaut, le tableau de bord AI Access Security Insights affiche l'utilisation des applications GenAI sur votre réseau par cas d'utilisation ainsi que les informations générales suivantes sur vos principaux cas d'utilisation GenAI :

- **Filtre de temps**

  Filtrez votre répartition des cas d'utilisation GenAI pour la période que vous souhaitez examiner. Vous pouvez sélectionner **Past 1 Hour (Dernière heure)**, **Past 3 Hours (3 dernières heures)**, **Past 24 Hours (24 dernières heures)**, **Past 7 Days (7 derniers jours)** ou **Past 30 Days (30 derniers jours)**.



- **Menaces détectées**

  Les menaces sont détectées par le profil de protection contre les vulnérabilités attaché à la règle de politique de sécurité Web. Ce profil détecte des menaces telles que les URL malveillantes et de phishing, les fichiers malveillants ou les logiciels malveillants. **Threats (Detected (Menaces détectées)** résume toutes les menaces sur toutes les applications GenAI et tous les points d'application.

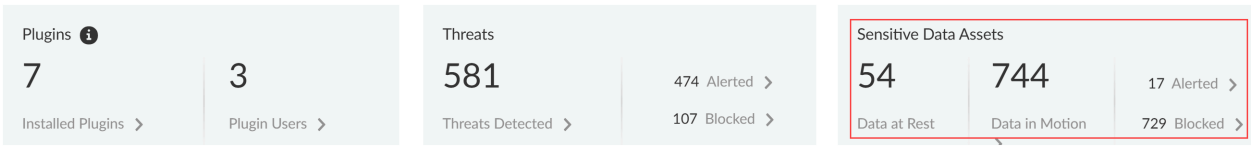
  - **Alerted (Alertes générées)** : nombre total de menaces détectées qui ont généré une alerte.

- **Blocked (Bloquées)** : nombre total de menaces détectées qui ont été bloquées par vos locataires NGFW ou Prisma Access.

- **Actifs de données sensibles**

  Les actifs de données sensibles affichent le nombre d'incidents de données sensibles détectées lorsque le trafic correspond aux critères de correspondance dans votre profil de données Enterprise Data Loss Prevention (E-DLP) pour les données au repos (Data Security) et les données en mouvement (SaaS Security Inline).

  - **Data at Rest (Données au repos)** : nombre total d'incidents DLP qui ont soit généré une alerte soit été bloqués par le canal d'application SaaS API (Data Security).
  - **Data in Motion (Données en mouvement)** : nombre total d'incidents DLP qui ont soit généré une alerte soit été bloqués par le canal d'application SaaS Security Inline.
  - **Alerted (Alertes générées)** : nombre total d'incidents DLP qui ont généré une alerte pour les données au repos et les données en mouvement.
  - **Blocked (Bloqués)** : nombre total d'incidents DLP bloqués par vos locataires NGFW ou Prisma Access pour les données au repos et les données en mouvement.



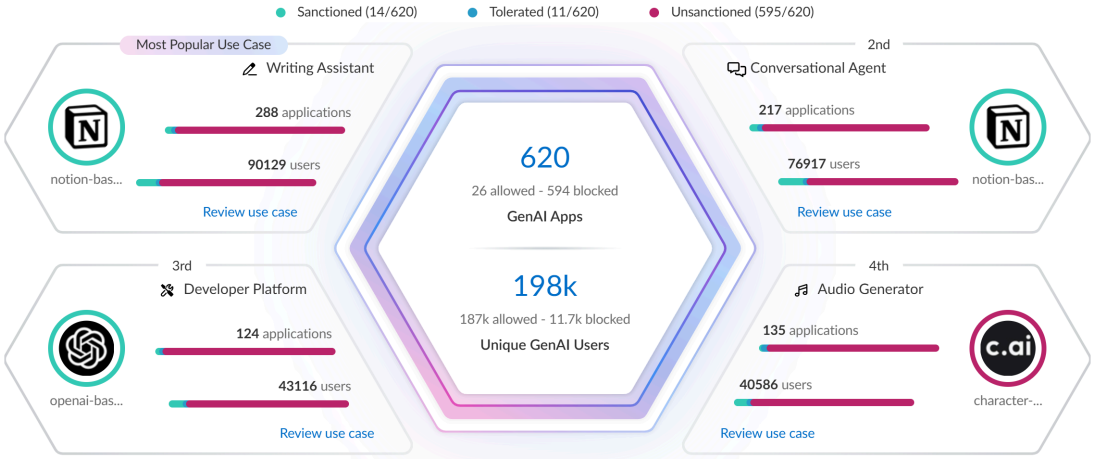
- **Principaux cas d'utilisation**

  Le tableau de bord AI Access Security Insights affiche dynamiquement les quatre principaux cas d'utilisation des applications GenAI en fonction de l'activité sur votre réseau, ainsi que le nombre total d'applications GenAI et d'utilisateurs qui ont accédé à une application GenAI pendant la période sélectionnée. Cela vous permet d'examiner rapidement les incidents de sécurité liés à vos applications GenAI les plus utilisées et de mettre en œuvre des règles de politique de contrôle d'accès.

  - **GenAI Apps (Applications GenAI)** : nombre total d'applications GenAI qui relèvent du cas d'utilisation particulier. Le nombre total d'applications GenAI est classé en trois groupes : applications GenAI approuvées, tolérées et non approuvées.
  - **Unique GenAI Users (Utilisateurs uniques de GenAI)** : nombre total d'utilisateurs ayant accédé à une application GenAI qui relève du cas d'utilisation particulier. Cliquez sur le

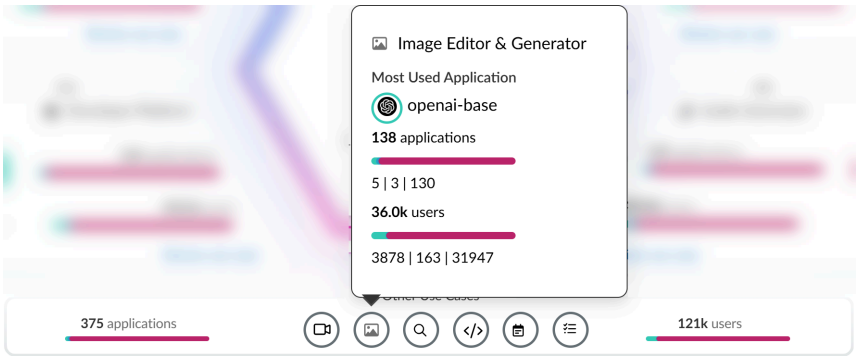
nombre **Unique GenAI Users (Utilisateurs uniques de GenAI)** pour voir la liste de chaque utilisateur unique qui a été interdit d'accéder à l'application GenAI.

*AI Access Security agrège automatiquement le total du nombre de **Unique GenAI Users (Utilisateurs uniques de GenAI)** à intervalles réguliers et génère la liste des utilisateurs immédiatement lorsque vous cliquez sur le nombre **Unique GenAI Users (Utilisateurs uniques de GenAI)**. Pour cette raison, le nombre **Unique GenAI Users (Utilisateurs uniques de GenAI)** peut différer légèrement du nombre de la liste.*



- **Tous les autres cas d'utilisation**
  - **Applications (Applications)** : nombre total d'applications GenAI qui relèvent de tout autre cas d'utilisation d'application GenAI. Le nombre total d'applications GenAI est classé en trois groupes : applications GenAI approuvées, tolérées et non approuvées.
  - **Users (Utilisateurs)** : nombre total d'utilisateurs ayant accédé à une application GenAI qui relève de tout autre cas d'utilisation d'application GenAI.

  Survolez chaque cas d'utilisation pour voir des informations résumées sur l'utilisation des applications GenAI associées au cas d'utilisation.



STEP 3 | Cliquez sur **Review use case (Examiner le cas d'utilisation)** pour voir une répartition détaillée de toutes les applications GenAI approuvées, tolérées et non approuvées dans le cas d'utilisation qui vous intéresse.

STEP 4 | Examinez la page des détails du cas d'utilisation pour comprendre l'utilisation des applications GenAI.

La page des détails du cas d'utilisation fournit des données granulaires sur l'utilisation des applications GenAI. Vous pouvez utiliser ces informations pour comprendre l'utilisation des applications GenAI afin de vous informer sur les règles de politique que vos administrateurs de sécurité doivent rédiger pour renforcer votre posture de sécurité. Cela garantit que votre organisation adopte les applications GenAI en toute sécurité et empêche l'exfiltration de données sensibles.

- **Récapitulatif du cas d'utilisation**

  Le récapitulatif du cas d'utilisation agrège toutes les informations importantes sur l'utilisation des applications GenAI pour le cas d'utilisation que vous examinez.

  - **Applications les plus utilisées** : les applications GenAI les plus utilisées pour le cas d'utilisation. Cela inclut également l'étiquette d'application (**Sanctioned [Approuvée]**, **Tolerated [Tolérée]** ou **Unsanctioned [Non approuvée]**) actuellement assignée à l'application GenAI.
  - **Application Breakdown (Répartition des applications)** : récapitulatif du nombre total d'applications GenAI associées au cas d'utilisation ainsi qu'un résumé des étiquettes d'application sur toutes les applications GenAI détectées.
  - **User Breakdown (Répartition des utilisateurs)** : récapitulatif du nombre total d'utilisateurs ayant accédé à l'une des applications GenAI associées au cas d'utilisation. Un récapitulatif du nombre d'utilisateurs ayant accédé aux applications GenAI **Sanctioned (Approuvées)**, **Tolerated (Tolérées)** ou **Unsanctioned (Non approuvées)** est également fourni.
- **Applications**

  Une liste de toutes les applications GenAI associées au cas d'utilisation et auxquelles vos utilisateurs ont accédé. Vous pouvez appliquer un filtre **Sort By (Trier par)** au cas d'utilisation des applications GenAI pour les trier par **User Count (Nombre d'utilisateurs)**, **Threats Count (Nombre de menaces)** ou **Transferred Count (Nombre de transferts)**. AI Access Security trie les applications GenAI dans l'ordre décroissant.

  La liste des applications affiche les informations suivantes sur chaque application GenAI détectée.

  - **Application Name (Nom de l'application)** : nom de l'application GenAI détectée. Cliquez sur le nom de l'application pour afficher les informations d'utilisation détaillées. Vous êtes redirigé vers la page **Applications (Applications)** des Informations sur l'activité.
  - **Tag (Étiquette)** : étiquette actuelle de l'application GenAI. Vous pouvez appliquer une nouvelle étiquette en cliquant sur celle que vous souhaitez appliquer.

    Palo Alto Networks regroupe les App-ID enfants pour la fonctionnalité de l'application dans un App-ID conteneur. Cependant, l'étiquetage d'un conteneur App-ID n'est pas pris en charge. Vous devez étiqueter individuellement les App-ID enfants spécifiques approuvés, non approuvés ou tolérés au sein de votre organisation.
  - **Allowed Users (Utilisateurs autorisés)** : nombre total d'utilisateurs uniques ayant accédé à l'application GenAI en fonction des privilèges d'accès configurés dans vos règles de

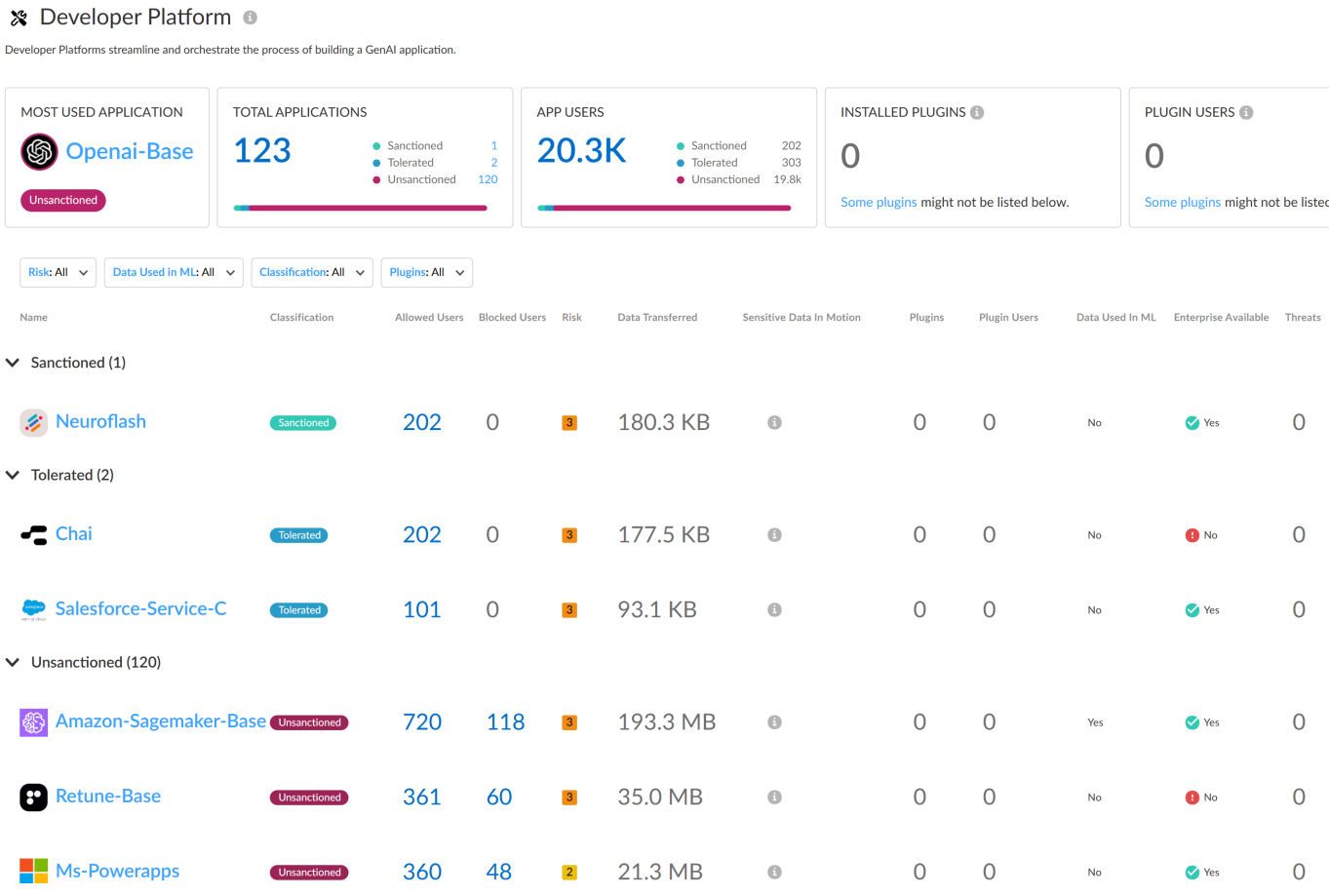
politique de sécurité. Cliquez sur le nombre **Allowed Users (Utilisateurs autorisés)** pour voir la liste de chaque utilisateur unique ayant réussi à accéder à l'application GenAI.

- **Blocked Users (Utilisateurs bloqués)** : nombre total d'utilisateurs uniques pour lesquels l'accès à l'application GenAI a été bloqué en fonction des privilèges d'accès configurés dans vos règles de politique de sécurité. Cliquez sur le nombre **Blocked Users**

(Utilisateurs bloqués) pour voir la liste de chaque utilisateur unique empêché d'accéder à l'application GenAI.

- **Threats (Menaces)** : nombre total d'activités de menaces détectées.
- **Transferred (Transferts)** : quantité totale de données en gigaoctets (Go) téléchargées ou chargées depuis l'application GenAI.
- **Sensitive Asset (Actif sensible)** : nombre d'incidents DLP générés en raison de données sensibles détectées et bloquées par Enterprise DLP.
- **Enterprise Available (Version d'entreprise disponible)** : indique si l'application GenAI propose un régime ou un modèle de licence d'entreprise.
- **Data Used in ML (Données utilisées pour le ML)** : indique si l'application GenAI utilise des données téléchargées par l'utilisateur à des fins d'entraînement.
- **Risk Score (Score de risque)** : score de risque de l'application GenAI.

- **Points forts des cas d'utilisation**
  - **Applications (Applications)** : nombre total d'applications GenAI qui relèvent de tout autre cas d'utilisation d'application GenAI. Le nombre total d'applications GenAI est classé en trois groupes : applications GenAI approuvées, tolérées et non approuvées.
  - **Users (Utilisateurs)** : nombre total d'utilisateurs ayant accédé à une application GenAI qui relève de tout autre cas d'utilisation d'application GenAI.



STEP 5 | Créez une règle de politique de sécurité personnalisée pour contrôler l'accès à une application GenAI.

Dans l'exemple ci-dessus, `Openai-Base` est l'application GenAI la plus utilisée dans le cas d'utilisation `Assistant et Générateur de Code`. De plus, il s'agit d'une application **Unsanctioned (Non approuvée)**, ce qui signifie qu'il s'agit d'une application dont l'utilisation n'a pas été approuvée sur votre réseau d'entreprise.

Dans ce cas, vous pouvez modifier la règle de politique d'accès à l'application GenAI par défaut pour bloquer explicitement tout accès à `OpenAI` s'il s'agit d'une application à laquelle votre organisation ne devrait pas accéder.

Découvrir les risques posés par les applications GenAI par des applications risquées

STEP 1 | Connectez-vous à Strata Cloud Manager.

STEP 2 | Sélectionnez **Insights (Informations)** > **Activity Insights (Informations sur l'activité)** > **Applications (Applications)**.

STEP 3 | Configurez les filtres de la liste des applications afin de réduire les applications GenAI que vous souhaitez examiner.

1. Configurez les champs **Time Range (Plage horaire)** et **Scope Selection (Sélection de l'étendue)** pour filtrer la plage horaire et le point d'application que vous souhaitez examiner.
2. Cliquez sur **Add Filter (Ajouter un filtre)** et ajoutez les filtres suivants.
   - **Source Type – Users (Type de source – Utilisateurs)** : filtre la liste des applications pour n'afficher que les applications GenAI auxquelles les utilisateurs de votre organisation ont accédé. Ce filtre est obligatoire.
   - **GenAI Application – TRUE (Application GenAI – VRAI)** : filtre la liste des applications pour n'afficher que les applications GenAI. Ce filtre est obligatoire.
   - **App Risk Score (Score de risque de l'application)** : pour le filtre **App Risk Score (Score de risque de l'application)**, sélectionnez le score de risque spécifique que vous souhaitez examiner. Si vous ne sélectionnez aucun score de risque, toutes les applications GenAI s'affichent.

     Dans cet exemple, nous enquêtons sur les applications avec un score de risque de **4** et **5**, car ce sont les scores de risque attribués aux applications les plus risquées.

STEP 4 | Examinez la liste des applications GenAI filtrées.

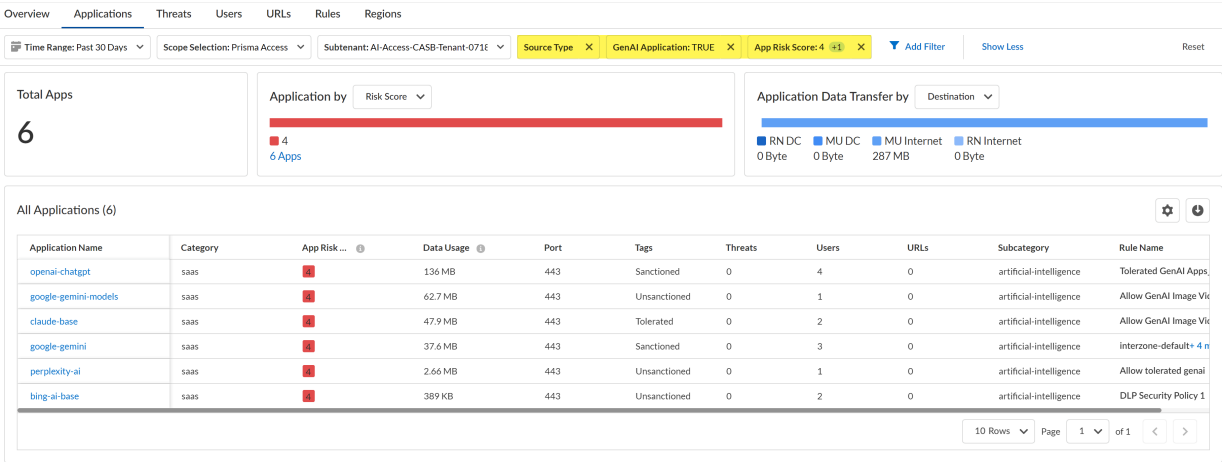
Voici quelques-unes des informations importantes à examiner.

- **Application Name (Nom de l'application)** : App-ID de l'application GenAI.
- **Data Usage (Utilisation des données)** : quantité des données téléchargées ou chargées depuis l'application GenAI. Cela peut vous aider à comprendre l'utilisation de l'application GenAI ; si une application GenAI a un volume d'utilisation des données élevé, cela peut

signifier que cette application est largement utilisée et pourrait nécessiter des contrôles stricts pour prévenir l'exfiltration de données sensibles et les acteurs malveillants.

- **Tags (Étiquettes)** : étiquette d'application actuelle de l'application GenAI. Si l'utilisation de certaines des applications GenAI répertoriées est approuvée, vous pouvez modifier l'étiquette en **Tolerated (Toléré)** ou **Sanctioned (Approuvé)**.

> *Palo Alto Networks regroupe les App-ID enfants pour la fonctionnalité de l'application dans un App-ID conteneur. Cependant, l'étiquetage d'un conteneur App-ID n'est pas pris en charge. Vous devez étiqueter individuellement les App-ID enfants spécifiques approuvés, non approuvés ou tolérés au sein de votre organisation.*



STEP 5 | Créez une règle de politique de sécurité personnalisée pour contrôler l'accès à une application GenAI pour des utilisateurs spécifiques.

Par exemple, imaginons que lors de votre enquête, vous découvrez qu'il existe plusieurs applications GenAI non approuvées avec un volume important d'utilisation de données. Cela pose un risque de sécurité, car des utilisateurs accèdent à une application non approuvée sur

le réseau et vous ne savez pas quelles données sont téléchargées ou chargées. En attendant de pouvoir effectuer une procédure de diligence raisonnable appropriée pour comprendre l'objectif de l'application GenAI et déterminer qui est autorisé à utiliser l'application GenAI, vous pouvez **Block (Bloquer)** l'application GenAI pour tous les utilisateurs.

Inversement, vous pourriez remarquer des applications GenAI **Unsanctioned (Non approuvées)** dont l'utilisation est approuvée sur votre réseau, par des utilisateurs spécifiques avec un volume important d'utilisation de données. Dans ce cas, vous pouvez changer l'étiquette en **Sanctioned (Approuvé)** et rédiger une règle de politique pour **Allow (Autoriser)** l'utilisation de l'application, mais uniquement pour les utilisateurs dans des rôles ou services précis. Dans la règle de politique, vous pouvez associer un profil de données Enterprise Data Loss Prevention (E-DLP) pour prévenir l'exfiltration de données sensibles et un profil de vulnérabilité pour arrêter les tentatives d'exploitation des failles système ou d'accès non autorisé aux systèmes.

Découvrir les risques posés par les applications GenAI par les utilisateurs d'applications

STEP 1 | Connectez-vous à Strata Cloud Manager.

STEP 2 | Sélectionnez **Insights (Informations)** > **AI Access (Accès à l'IA)** pour afficher le tableau de bord AI Access Security Insights.

Affiche les principales applications GenAI auxquelles les utilisateurs risqués ont accédé pour aider à affiner votre focus.

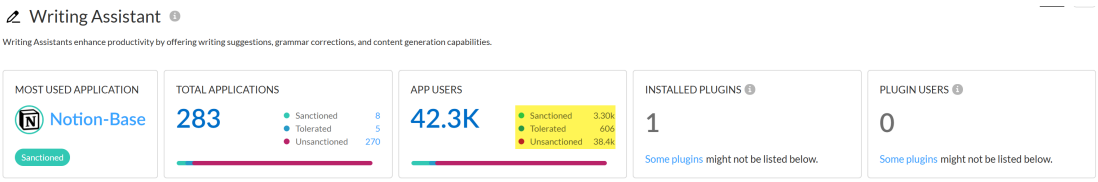
STEP 3 | Cliquez sur **Review use case (Examiner le cas d'utilisation)** pour le Cas d'utilisation de l'application GenAI à laquelle vos utilisateurs risqués accèdent.

Le tableau de bord AI Access Security Insights affiche par défaut les applications GenAI auxquelles les utilisateurs ont accédé sur votre réseau par cas d'utilisation et affiche les informations de haut niveau suivantes sur vos principaux utilisateurs d'applications GenAI. Cliquez sur le nombre d'utilisateurs pour voir le **User Name (Nom d'utilisateur)** ou l'**IP Address (Adresse IP)** et le nombre d'**Applications (Applications)** GenAI auxquelles cet utilisateur a accédé.

- **Répartition des utilisateurs**

  Fournit un résumé du nombre total d'utilisateurs accédant à toute application GenAI associée au cas d'utilisation GenAI sélectionné. AI Access Security comprend une répartition du nombre d'utilisateurs ayant accédé à des applications **Sanctioned (Approuvées)**, **Tolerated (Tolérées)**, et **Unsanctioned (Non approuvées)**.

  Cliquez sur le nombre total des **App Users (Utilisateurs d'applications)** pour voir une liste de tous les utilisateurs qui ont accédé à une application GenAI associée au cas d'utilisation sélectionné ou dont un tel accès a été bloqué.



- **Utilisateurs par cas d'utilisation d'application GenAI**

  Fournit un résumé du nombre total d'utilisateurs accédant à chaque application GenAI associée au cas d'utilisation GenAI sélectionné. Les applications GenAI **Sanctioned (Approuvées)**, **Tolerated (Tolérées)** et **Unsanctioned (Non autorisées)** sont répertoriées avec le nombre total d'utilisateurs pour chaque application.

  Examinez les nombres **Allowed Users (Utilisateurs autorisés)** et **Blocked Users (Utilisateurs bloqués)** pour mesurer l'efficacité de vos règles de sécurité et de politique d'accès à l'application GenAI.

  - **Allowed Users (Utilisateurs autorisés)** : nombre total d'utilisateurs autorisés à accéder à l'application GenAI. Utilisez ces informations pour mesurer l'efficacité de votre règle de politique de sécurité en vérifiant que le nombre d'utilisateurs autorisés correspond à

vos attentes, ou pour évaluer le taux d'adoption d'une application GenAI nouvellement autorisée pour une utilisation par votre organisation.

- **Blocked Users (Utilisateurs bloqués)** : nombre total d'utilisateurs bloqués d'accéder à l'application GenAI. Utilisez ces informations pour vérifier si vous avez configuré correctement les règles de politique de sécurité contrôlant l'accès à une application GenAI spécifique, ou pour comprendre si les utilisateurs de votre organisation accèdent à des applications GenAI non autorisées.

Par exemple, considérez l'application GenAI `Grammarly` ci-dessous. Votre organisation a classé cette application GenAI comme `Approuvée` pour être utilisée par certains utilisateurs spécifiques au sein de votre organisation. Dans ce cas, votre administrateur de sécurité a cliqué sur le compte **Allowed Users (Utilisateurs autorisés)** et a vérifié que tous les utilisateurs accédant à l'application GenAI sont autorisés à le faire.

Inversement, votre administrateur de sécurité constate que plus de 1 600 utilisateurs ont accédé à l'application `Character-Ai-base`. Votre administrateur de sécurité a classé cette application GenAI comme `Non approuvées` et a l'intention de restreindre tout accès au sein de votre organisation. Dans ce cas, votre administrateur de sécurité doit examiner votre base de règles de politique de sécurité et les règles de politique de sécurité individuelles contrôlant l'accès à l'application `Character-Ai-base` pour confirmer qu'elle

est correctement positionnée dans votre base de règles de politique de sécurité et qu'elle est configurée correctement pour bloquer tout accès.

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 | Créez une règle de politique de sécurité personnalisée pour contrôler l'accès à une application GenAI pour des utilisateurs spécifiques.

Par exemple, après examen, vous découvrez qu'un grand nombre d'utilisateurs accèdent à l'application GenAI `bing-ai-uploading`. Bien que ce soit une application GenAI **Sanctioned (Approuvée)**, elle n'est approuvée que pour un ensemble spécifique d'utilisateurs au sein de votre organisation. Vous pouvez décider d'écrire une règle de politique pour bloquer explicitement l'accès aux utilisateurs qui ne devraient pas avoir accès à cette application GenAI afin de prévenir les abus et une règle de politique de sécurité pour autoriser explicitement l'accès aux utilisateurs qui sont approuvés pour accéder à l'application GenAI. Alternativement, vous pouvez écrire une règle de politique pour autoriser l'accès à tous les utilisateurs, mais mettre en œuvre des mesures de prévention de la perte de données et de menaces pour empêcher l'exfiltration de données sensibles et prévenir des menaces telles que des URL malveillantes et de phishing, des fichiers malveillants ou des logiciels malveillants.

Découvrir les risques posés par les applications GenAI installées en tant que plug-ins tiers

STEP 1 | Connectez-vous à Strata Cloud Manager.

STEP 2 | Sélectionnez **Insights (Informations)** > **AI Access (Accès à l'IA)** pour afficher le tableau de bord AI Access Security Insights.

Le tableau de bord affiche le nombre de plug-ins tiers que les utilisateurs ont installés et le nombre d'utilisateurs qui ont installé des plug-ins tiers. AI Access Security détermine ces nombres à partir de toutes les données que AI Access Security a stockées. Ces nombres ne sont pas limités à la période indiquée par le filtre de temps.

STEP 3 | Cliquez sur **Installed Plugins (Plug-ins installés)** ou **Plugin Users (Utilisateurs de plug-ins)** pour accéder à des informations détaillées dans SaaS Security Posture Management (SSPM).

Cliquez sur **Installed Plugins (Plug-ins installés)** pour ouvrir la page 3rd Party Plugins (Plugins tiers), qui contient des détails sur les plug-ins GenAI tiers. De là, vous pouvez examiner les informations sur le plug-in pour déterminer si les plug-ins représentent un risque.

Cliquez sur **Plugin Users (Utilisateurs des plug-ins)** pour ouvrir la page 3rd Party Plugins (Plugins tiers), qui contient des détails sur les utilisateurs qui ont installé des plug-ins tiers. Pour chaque utilisateur, vous pouvez voir combien de plug-ins il a installés, et les applications du marché dans lesquelles il a installé des plug-ins. Utilisez ces informations pour identifier les risques de plug-ins posés par des utilisateurs individuels.

STEP 4 | Pour afficher les plug-ins installés par cas d'utilisation, suivez les étapes ci-dessous :

1. Sélectionnez **Insights (Informations)** > **AI Access (Accès à l'IA)** pour afficher le tableau de bord AI Access Security Insights.

   Le tableau de bord affiche en évidence les quatre principaux cas d'utilisation des applications GenAI, basés sur l'activité sur votre réseau. Le tableau de bord affiche également des icônes pour les autres cas d'utilisation.

2. Naviguez vers les détails d'un cas d'utilisation. Pour un cas d'utilisation principal, cliquez sur **Review use case (Examiner le cas d'utilisation)**. Pour d'autres cas d'utilisation, cliquez sur l'icône du cas d'utilisation.

   La page des détails du cas d'utilisation affiche un tableau de toutes les applications GenAI pour le cas d'utilisation.

   *Les informations résumées sur cette page incluent le nombre de **INSTALLED PLUGINS (PLUG-INS INSTALLÉS)** et le nombre de **PLUGIN USERS (UTILISATEURS DE PLUG-INS)**. Ces nombres sont déterminés à partir de toutes les données qu'AI Access Security a stockées et ne sont pas limités à la période indiquée par le filtre de temps. Pour cette raison, il est possible que ces totaux ne soient pas reflétés dans le tableau des détails des cas d'utilisation.*

3. Dans le tableau des détails des cas d'utilisation, identifiez les applications GenAI qui sont installées en tant que plug-ins dans une ou plusieurs instances d'applications du marché,

ainsi que le nombre d'utilisateurs de plug-ins. Cette information est affichée dans les colonnes **Plugins (Plug-ins)** et **Plugin Users (Utilisateurs de plug-ins)** du tableau.

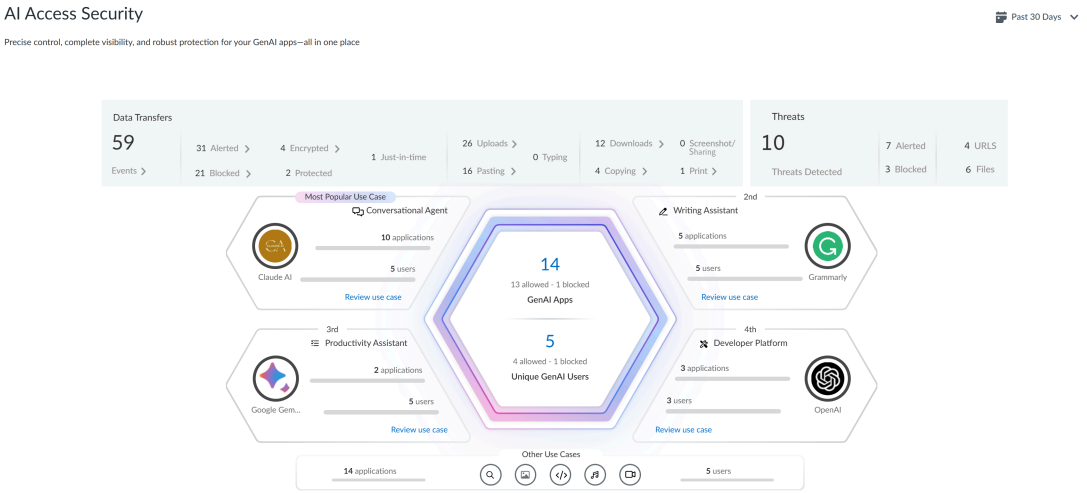
4. Pour une application GenAI installée en tant que plug-in, cliquez sur le nombre dans les colonnes **Plugins (Plug-ins)** ou **Plugin Users (Utilisateurs de plug-ins)**.

   Cliquez sur le nombre dans la colonne **Plugins (Plug-ins)** pour ouvrir la page 3rd Party Plugins (Plug-ins tiers) dans SSPM, qui affiche les instances de l'application GenAI que les utilisateurs ont installées en tant que plug-ins tiers. De là, vous pouvez examiner les informations sur le plug-in pour déterminer si les plug-ins représentent un risque.

   Cliquez sur le nombre dans la colonne **Plugin Users (Utilisateurs de plug-ins)** pour ouvrir la page 3rd Party Plugins (Plug-ins tiers), qui affiche des détails sur les utilisateurs qui ont installé l'application en tant que plug-in tiers. Utilisez ces informations pour identifier les risques de plug-ins posés par des utilisateurs individuels.

Découvrir les risques posés par les applications GenAI sur Prisma Access Browser

Prisma Access Browser est intégré à AI Access Security pour fournir une visibilité complète des applications GenAI, un contrôle d'accès, des données et une protection contre les menaces pour les clients de Prisma Access Browser autonome. Cette intégration offre le catalogue d'application GenAI le plus complet avec des contrôles approfondis de dernière minute, tels que la classification des données et la défense contre les menaces en temps réel. En tant qu'administrateur de sécurité de Prisma Access Browser autonome, vous pouvez accéder à AI Access Security dans le menu Insights (Informations) pour surveiller l'utilisation des applications d'IA tierces sur Prisma Access Browser, avec des analyses détaillées, y compris des métriques d'application, l'activité des utilisateurs, les menaces détectées et les transferts de données.

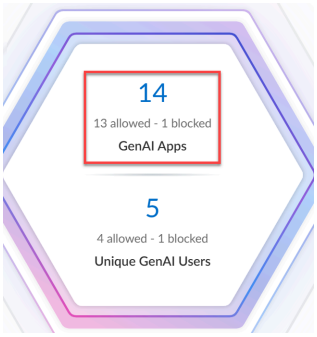


STEP 1 | Connectez-vous à Strata Cloud Manager.

STEP 2 | Sélectionnez **Insights (Informations)** > **AI Access (Accès à l'IA)** pour afficher le tableau de bord AI Access Security Insights (Informations) pour Prisma Access Browser autonome.

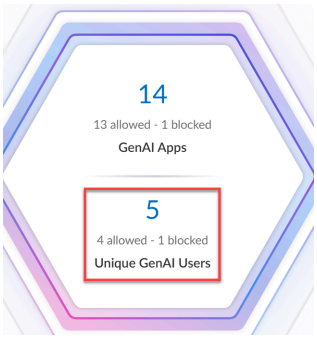
STEP 3 | Cliquez sur **GenAI Apps (Applications GenAI)** pour afficher les métriques de l'application avec **Is GenAI:Yes (Est GenAI : Oui)** et le filtre **Category: Access (Catégorie : accès)** appliqué pour afficher les métriques suivantes :

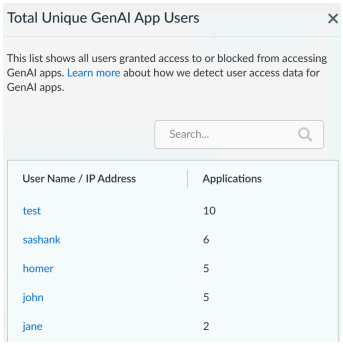
- Nombre total des applications GenAI
- Applications GenAI autorisées
- Applications GenAI bloquées



STEP 4 | Cliquez sur **Unique GenAI Users (Utilisateurs GenAI uniques**) pour afficher le nombre total d'utilisateurs pour lesquels l'accès aux applications GenAI est autorisé ou bloqué. Sélectionnez l'utilisateur (à partir de la page **Total Unique GenAI App Users (Total des utilisateurs uniques de l'application GenAI)**) pour accéder à la page Events (Événements) (avec le filtre **User: [Utilisateur :]<user name>** appliqué) pour connaître les applications GenAI autorisées et bloquées pour cet utilisateur particulier. Les métriques disponibles sont :

- Nombre total d'utilisateurs GenAI
- Utilisateurs GenAI autorisés
- Utilisateurs GenAI bloqués

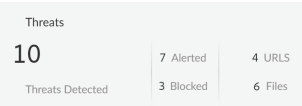




STEP 5 | Cliquez sur le widget **Threats Detected (Menaces détectées)** pour afficher le nombre total de menaces détectées et bloquées.

Ces informations sont disponibles sur la page Events (Événements) (avec **Is GenAI:Yes [Est GenAI : Oui]** et le filtre **Category: Malware [Catégorie : Logiciel malveillant]** appliqué). Les métriques disponibles sont :

- Nombre total de menaces GenAI, qui affichent le nombre total de menaces détectées et bloquées.
- URL malveillantes (filtre appliqué : **Category: Malware [Catégorie : Logiciel malveillant]** et **Type: Malicious website [Type: Site Web malveillant]**)
- Fichiers (filtre appliqué : **Category: Malware [Catégorie : Logiciel malveillant]** et **Type: Malicious file identified [Type : Fichier malveillant identifié]**)



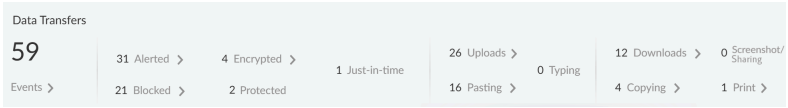
STEP 6 | Cliquez sur le widget **Data Transfers (Transferts de données**) pour afficher le nombre d'incidents de transferts de données détectés lorsque le trafic correspond aux critères de correspondance de votre profil de données Enterprise Data Loss Prevention (E-DLP) pour votre Prisma Access Browser.

Ces informations sont disponibles sur la page Events (Événements) (avec **Is GenAI:Yes [Est GenAI : Oui]** et le filtre **Category: DLP [Catégorie : DLP]** appliqué).

- Total des transferts de données détectés. Filtre appliqué : **Is GenAI: Yes (Est GenAI : Oui)**, **Category: DLP (Catégorie : DLP)**.
- Transferts de données ayant donné lieu à une alerte. Filtre appliqué : **Is GenAI: Yes (Est GenAI : Oui)**, **Category: DLP (Catégorie : DLP)**, **Action: Allowed (Action : Autorisé)**.
- Transferts de données bloqués. Filtre appliqué : **Is GenAI: Yes (Est GenAI : Oui)**, **Category: DLP (Catégorie : DLP)**, **Action: Blocked (Action : Bloqué)**.
- Transferts de données protégés : Action autorisée, mais qui ne peut être utilisée que par le navigateur. Par exemple, en activant le copier-coller de données entre des applications autorisées et en les bloquant pour d'autres applications dans le navigateur ou des applications de bureau locales. Filtre appliqué : **Is GenAI: Yes (Est GenAI : Oui)**, **Category: DLP (Catégorie : DLP)**, **Action: Allowed Protected (Action : autorisé, protégé)**.
- Transferts de données chiffrés : Action de cryptage pour laquelle seul le navigateur dispose de la clé de décryptage de l'utilisateur spécifique et du périphérique par lequel il a été crypté. Cela permet de télécharger des fichiers et de s'assurer qu'ils sont autorisés à être chargés (et décryptés) vers des applications spécifiques, ou ouverts dans le navigateur en mode hors ligne. Aucune autre application ne peut ouvrir le fichier, ce qui rend cette action idéale pour les fichiers que vous ne souhaitez pas voir disponibles sur le terminal, par exemple, sur des périphériques non gérés. Filtre appliqué : **Is GenAI: Yes (Est GenAI : Oui)**, **Category: DLP (Catégorie : DLP)**, **Action: Allowed Encrypted (Action : Autorisé et crypté)**.
- Contrôles « Just-in-time » des transferts de données : Actions qui incluent un avertissement de l'utilisateur avant de continuer, demandant à l'utilisateur de fournir une justification professionnelle avant de continuer ou déclencher un flux d'approbation de l'administrateur. Ces actions déclenchent un accès temporaire ou contournent les règles lors de situations d'urgence ou lorsqu'une justification et une journalisation sont nécessaires pour des raisons

de conformité. Filtre appliqué : **Is GenAI: Yes (Est GenAI : Oui)**, **Category: DLP (Catégorie : DLP)**, **Action: Permission Requested (Action : Autorisation demandée)**.

- Transferts de données chargés. Filtre appliqué : **Is GenAI: Yes (Est GenAI : Oui)**, **Category: DLP (Catégorie : DLP)**, **Type: File upload (Type : Chargement de fichiers)**.
- Transferts de données dans une activité du presse-papiers (coller). Filtre appliqué : **Is GenAI: Yes (Est GenAI : Oui)**, **Category: DLP (Catégorie : DLP)**, **Type: Clipboard Paste (Type : Coller depuis le presse-papiers)**.
- Transferts de données en train d'être saisies. Filtre appliqué : **Is GenAI: Yes (Est GenAI : Oui)**, **Category: DLP (Catégorie : DLP)**, **Type: Sanitizing Content (Type : Assainir le contenu)**).
- Transferts de données téléchargés. Filtre appliqué : **Is GenAI: Yes (Est GenAI : Oui)**, **Category: DLP (Catégorie : DLP)**, **Type: File download (Type : Téléchargement de fichiers)**.
- Transferts de données copiées. Filtre appliqué : **Is GenAI: Yes (Est GenAI : Oui)**, **Category: DLP (Catégorie : DLP)**, **Type: Clipboard Copy (Type : Copier dans le presse-papiers)**.
- Transferts de données partagées à l'aide d'une capture d'écran. Filtre appliqué : **Is GenAI: Yes (Est GenAI : Oui)**, **Category: DLP (Catégorie : DLP)**, **Type: Screen share (Type : Partage d'écran)**.
- Transferts de données imprimées. Filtre appliqué : **Is GenAI: Yes (Est GenAI : Oui)**, **Category: DLP (Catégorie : DLP)**, **Type: Print (Type : Impression)**.



Étiqueter des applications GenAI

En fonction du score de risque des applications GenAI et d'autres considérations, vous pouvez appliquer des étiquettes à chaque application pour indiquer si elle est approuvée au sein de votre organisation. Les étiquettes suivantes sont disponibles :

Étiquette	Description
Autorisées	L'application est approuvée par votre organisation et est utilisée par des membres de votre organisation.
Non autorisées	L'application n'est pas approuvée par votre organisation. Par exemple, l'utilisation d'une application peut ne pas être autorisée en raison des risques de sécurité associés à l'application. Comme les membres de votre organisation ne doivent pas utiliser l'application, vous devez prendre des mesures pour bloquer l'application. Vous pouvez utiliser une règle de politique pour bloquer l'application.
Toléré	L'application n'est pas considérée comme étant fiable au même titre qu'une application autorisée. Cependant, votre organisation permet son utilisation jusqu'à ce que votre organisation puisse identifier une application plus sécurisée. L'application est tolérée afin de ne pas inhiber la productivité de votre organisation. L'application étant autorisée malgré les risques de sécurité potentiels, il peut être souhaitable de prendre des mesures pour restreindre certaines actions. Par exemple, vous pouvez créer une règle de politique pour bloquer les opérations de téléchargement ou de téléversement pour l'application.

Palo Alto Networks regroupe les App-ID enfants pour la fonctionnalité de l'application dans un App-ID conteneur. Cependant, l'étiquetage d'un conteneur App-ID n'est pas pris en charge. Vous devez étiqueter individuellement les App-ID enfants spécifiques approuvés, non approuvés ou tolérés au sein de votre organisation.

Par exemple, considérez le conteneur App-ID `claude` qui contient les App-ID enfants suivants : `claude-base`, `claude-upload`, `claude-edit`, `claude-post` et `claude-delete`.

*Vous créez un filtre d'application pour appliquer les mêmes contrôles d'exfiltration de données pour les applications **Sanctioned (Approuvées)**. Dans ce cas, vous devez étiqueter tous les App-ID enfants du conteneur App-ID `claude` pour appliquer l'action de règle de politique pour tous les sous-processus de l'application GenAI `claude` **Sanctioned (Approuvée)**.*

*En septembre 2024, Palo Alto Networks a mis à jour la façon dont l'étiquetage des applications est mis en œuvre. Depuis septembre 2024, les étiquettes sont écrites et lues à partir d'un nouvel extrait `Application-Tagging` prédéfini. Après la publication de cette mise à jour pour votre locataire, elle prend effet la première fois que vous étiquetez une application. Les étiquettes sont écrites dans l'extrait et AI Access Security, la page Activity Insights – Applications (Informations sur l'activité – Applications) et le Strata Cloud Manager Command Center commencent à afficher les informations d'étiquetage selon l'extrait. Si vous avez étiqueté des applications avant cette mise à jour, vous ne verrez plus ces changements d'étiquettes dans AI Access Security et la page Activity Insights – Applications (Informations sur l'activité – Applications). L'extrait `Application-Tagging` garde en mémoire les applications étiquetées comme **Sanctioned (Approuvées)** ou **Tolerated (Tolérées)**. Les applications qui ne sont pas explicitement étiquetées comme **Sanctioned (Approuvées)** ou **Tolerated (Tolérées)** sont considérées comme **Unsanctioned (Non approuvées)**. Pour cette raison, seules les étiquettes que vous ajoutez après cette mise à jour seront affichées dans Strata Cloud Manager. Toutes les autres applications sont affichées comme **Unsanctioned (Non approuvées)**.*

Les étiquettes que vous avez appliquées avant cette mise à jour affectent toujours l'application des politiques basées sur les étiquettes sur le déploiement de NGFW ou Prisma Access tant que vous associez l'extrait Application-Tagging et que vous appliquez des étiquettes dans l'étendue de la configuration `Application-Tagging`.

- Configuration d'applications NGFW et Prisma Access
- Informations sur l'activité – Applications

Étiqueter les applications GenAI dans la Configuration de l'application

STEP 1 | Connectez-vous à Strata Cloud Manager.

STEP 2 | Associez l'extrait `Application-Tagging (Étiquetage d'application)` prédéfini avec l'étendue de configuration appropriée pour permettre l'application des politiques basées sur les étiquettes.

STEP 3 | Obtenez les App-ID enfants que vous souhaitez étiqueter.

Vous pouvez obtenir les App-ID enfants pour une application GenAI en utilisant l'une des méthodes suivantes.

- Utilisez le tableau de bord AI Access Security Insights pour découvrir les risques posés par les applications GenAI. AI Access Security Insights vous montre les App-ID enfants détectés utilisés dans votre organisation.
- Examinez la liste des applications GenAI prises en charge.
- Utilisez Applipedia pour rechercher les App-ID enfants des applications GenAI prises en charge fournies via une mise à jour de contenu dynamique.

  Applipedia n'affiche que les App-ID pour les applications fournies via un contenu dynamique, et n'affiche pas les applications fournies via App-ID Cloud Engine (ACE).

STEP 4 | Accédez à **Manage (Gérer)** > **Configuration (Configuration)** > **NGFW et Prisma Access** > **Objects (Objets)** > **Application (Application)** > **Applications (Applications)**.

STEP 5 | Dans **Configuration Scope (Champ de configuration)**, sélectionnez l'extrait `Application-Tagging`.

Si vous étiquetez un App-ID fourni via App-ID Cloud Engine (ACE), alors tous les locataires NGFW ou Prisma Access associés au dossier sélectionné doivent être configurés pour recevoir des mises à jour d'App-ID d'ACE.

ACE est activé par défaut pour tout locataire NGFW ou Prisma Access lorsqu'il a une licence SaaS Security Inline ou AI Access Security active. Vous pouvez également activer manuellement ACE pour votre NGFW.

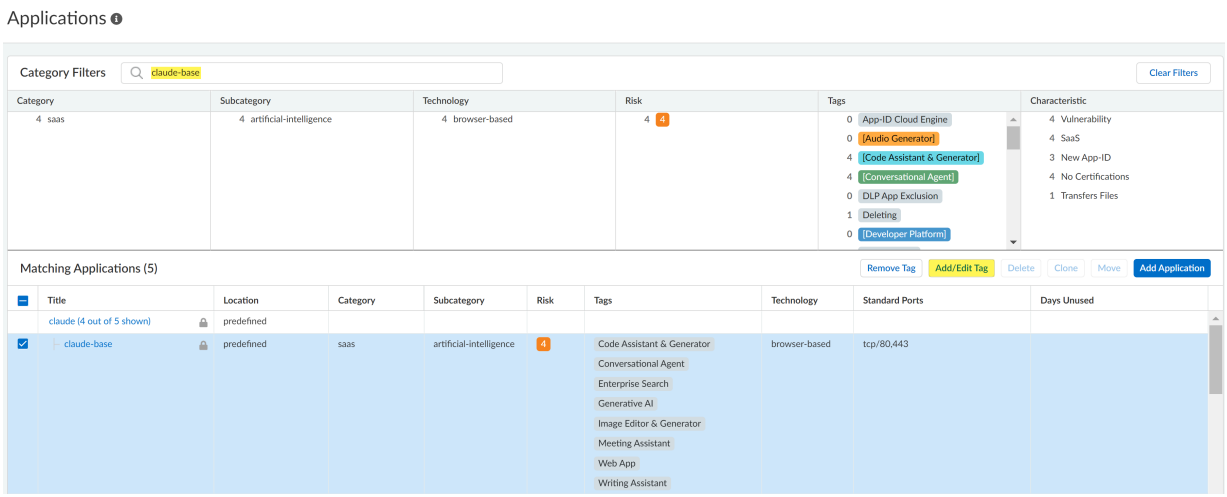
La transmission de configuration échoue si vous étiquetez un App-ID fourni par ACE et qu'au moins un locataire NGFW ou Prisma Access associé au dossier sélectionné n'est pas configuré pour recevoir des App-ID d'ACE.

Pour cette raison, Palo Alto Networks ne recommande pas de sélectionner l'étendue de configuration **Global (Globale)**.

STEP 6 | Dans le champ de recherche **Category Filters (Filtres de catégorie)**, entrez l'App-ID que vous souhaitez étiquetez et sélectionnez-le.

Vous ne pouvez étiquetez qu'un seul App-ID à la fois.

STEP 7 | Add/Edit Tag (Ajouter/modifier l'étiquette).



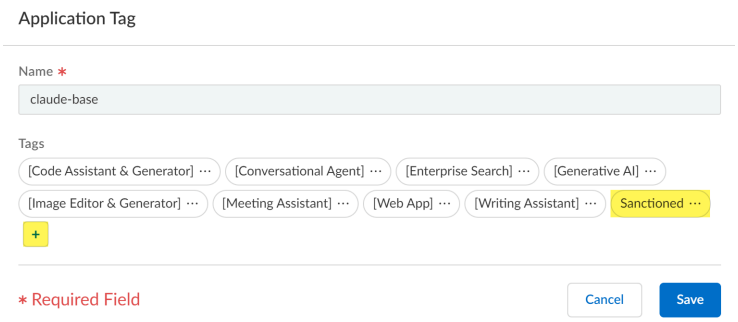
STEP 8 | Cliquez sur **+** pour appliquer une étiquette prédéfinie d'application **Sanctioned (Approuvée)** ou **Tolerated (Tolérée)**.

Dans cet exemple, l'App-ID `claude-base` est accompagné de l'étiquette **Sanctioned (Approuvée)**.

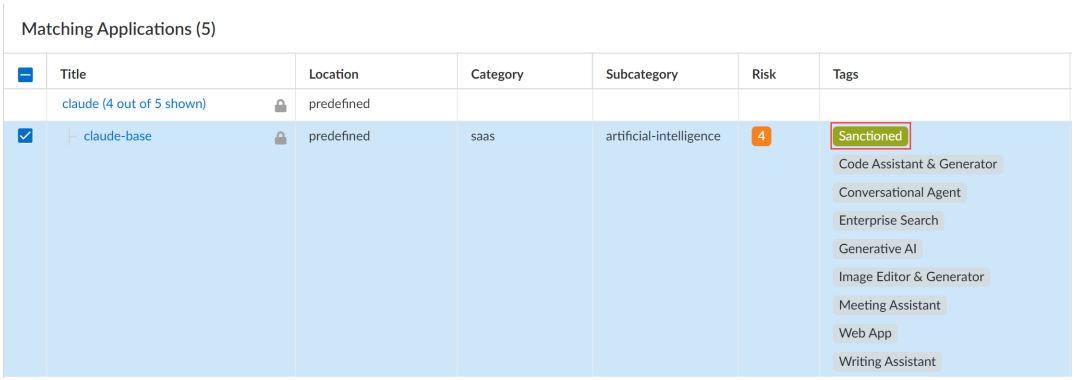
*Une application est considérée comme **Unsanctioned (Non approuvée)** en l'absence des étiquettes **Sanctioned (Approuvée)** ou **Tolerated (Tolérée)** si l'étiquette est issue de **Applications (Applications)**.*

*Si vous souhaitez changer l'étiquette de l'application de **Sanctioned (Approuvée)** ou **Tolerated (Tolérée)** à **Unsanctioned (Non approuvée)**, vous devez supprimer l'étiquette existante. Vous ne pouvez pas étiqueter manuellement une application avec l'étiquette **Unsanctioned (Non approuvée)** depuis **Applications (Applications)**.*

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



STEP 10 | Vérifiez les valeurs dans la colonne **Tag (Étiquette)** pour vérifier que vous avez appliqué avec succès l'étiquette d'application.



STEP 11 | Cliquez sur **Overview (Vue d'ensemble)**.

STEP 12 | **Push Config (Transmettre la configuration)** et **Push (Transmettre)** les modifications de votre configuration.

Étiqueter les applications GenAI dans le tableau de bord Insights (Informations)

STEP 1 | Connectez-vous à Strata Cloud Manager.

STEP 2 | Associez l'extrait `Application-Tagging (Étiquetage d'application)` prédéfini avec l'étendue de configuration appropriée pour permettre l'application des politiques basées sur les étiquettes.

STEP 3 | Obtenez les App-ID enfants que vous souhaitez étiqueter.

Vous pouvez obtenir les App-ID enfants pour une application GenAI en utilisant l'une des méthodes suivantes.

- Utilisez le tableau de bord AI Access Security Insights pour découvrir les risques posés par les applications GenAI. AI Access Security Insights vous montre les App-ID enfants détectés utilisés dans votre organisation.
- Examinez la liste des applications GenAI prises en charge.
- Utilisez Applipedia pour rechercher les App-ID enfants des applications GenAI prises en charge fournies via une mise à jour de contenu dynamique.

  Applipedia n'affiche que les App-ID pour les applications fournies via un contenu dynamique, et n'affiche pas les applications fournies via App-ID Cloud Engine (ACE).

STEP 4 | Sélectionnez **Insights (Informations)** > **Activity Insights (Informations sur l'activité)** > **Applications (Applications)**.

STEP 5 | Localisez l'App-ID enfant GenAI que vous souhaitez étiqueter. Si nécessaire, vous pouvez filtrer le tableau pour n'afficher que les applications GenAI.

1. Cliquez sur **Add Filter (Ajouter un filtre)** et ajoutez le filtre **Gen AI Application (Application GenAI)**.
2. Définissez le filtre **GenAI Application (Application GenAI)** sur **TRUE (VRAI)**.

STEP 6 | Pour examiner les tags appliqués à l'App-ID GenAI, examinez les valeurs dans la colonne **Tag (Étiquette)**.

STEP 7 | Appliquez une étiquette différente à l'App-ID GenAI enfant.

1. Dans la colonne **Actions (Actions)**, sélectionnez l'icône d'étiquette et choisissez l'étiquette **Sanctioned (Approuvée)**, **Tolerated (Tolérée)** ou **Unsanctioned (Non approuvée)**.
2. Cliquez sur **Apply (Appliquer)** pour appliquer la nouvelle étiquette.

Voir les scores de risque attribués aux applications GenAI

Pour vous aider à identifier rapidement les applications GenAI qui représentent les plus grandes menaces pour votre organisation, AI Access Security attribue à chaque application GenAI un score de risque. Ces scores de risque vous permettent d'identifier rapidement les applications GenAI à risque, afin que vous puissiez agir pour protéger votre environnement. Par exemple, pour protéger votre environnement, vous pouvez créer une règle de politique pour bloquer l'application. Vous pouvez également choisir d'étiqueter l'application comme Unsanctioned (Non approuvée).

Le score de risque d'une application est compris entre 1 (risque faible) et 5 (risque élevé) et est basé sur les attributs des applications SaaS. Certains attributs sont communs à toutes les applications SaaS, tandis qu'un sous-ensemble d'attributs est unique aux applications GenAI.

Les *attributs GenAI* sont des attributs tels que le type de données d'entrée utilisateur dans l'application, le type de données de la sortie générée par l'application, et si les données soumises par l'utilisateur sont utilisées par l'application pour entraîner ses modèles GenAI. Le calcul du score de risque détermine le risque GenAI sur la base des valeurs des attributs GenAI.

En plus des attributs GenAI, le calcul du score de risque utilise les types d'attributs suivants pour déterminer le risque général de l'application SaaS.

- Les *attributs de conformité*, qui identifient si une application respecte diverses exigences et normes réglementaires.
- Les *attributs de gestion des accès et d'identité*, qui identifient les capacités d'authentification et de contrôle d'accès d'une application.
- Les *attributs de sécurité et de confidentialité*, qui identifient les fonctionnalités du produit pour protéger les données. Cette catégorie d'attributs comprend des attributs tels que si l'application crypte les données au repos et les données en transit.

Le score de risque final d'une application GenAI est une combinaison du risque général SaaS (calculé à partir des attributs SaaS) et du risque GenAI (calculé à partir des attributs GenAI). Le calcul du score de risque accorde un poids supplémentaire au risque GenAI lors de la détermination du score de risque final.

STEP 1 | Connectez-vous à Strata Cloud Manager.

STEP 2 | Pour naviguer vers le tableau de bord Activity Insights (Informations sur l'activité), sélectionnez **Insights (Informations)** > **Activity Insights (Informations sur l'activité)** > **Applications (Applications)**.

STEP 3 | Localisez les applications GenAI dans le tableau. Si nécessaire, vous pouvez appliquer des filtres dans le tableau pour n'afficher que les applications GenAI.

1. Cliquez sur **Add Filter (Ajouter un filtre)** et ajoutez le filtre **Gen AI Application (Application GenAI)**.
2. Définissez le filtre **GenAI Application (Application GenAI)** sur **TRUE (VRAI)**.

STEP 4 | Pour identifier les applications GenAI qui posent les plus grandes menaces, examinez les valeurs de score de risque dans la colonne **Risk (Risque)**.

Score de risque	Signification
4-5	Risque élevé : il est très probable qu'il s'agisse d'un risque.
3	Risque moyen : représente un risque modéré.
1-2	Risque faible : il est peu probable qu'il s'agisse d'un risque.

STEP 5 | Agissez sur les applications les plus risquées.

Par exemple, vous pouvez créer des règles de politique pour bloquer ces applications ou étiqueter les applications comme Unsanctioned (Non approuvées)

Utiliser des filtres d’application pour les applications GenAI

Les Filtres d’application regroupent dynamiquement les applications en fonction des attributs d’application que vous définissez. Vous pouvez utiliser des filtres d’application dans vos règles de politique de sécurité pour contrôler l’accès aux applications GenAI en fonction des attributs d’application plutôt que de définir explicitement les applications GenAI ou les groupes d’application dans votre règle de politique de sécurité.

AI Access Security comprend les filtres d’application GenAI prédéfinis suivants. Les filtres d’application prédéfinis sont basés sur les AI Access Security cas d’utilisation pris en charge.

- Générateur audio
- Agent conversationnel
- Assistant et générateur de code
- Plateforme de développement
- Recherche d’entreprise
- Éditeur et générateur d’images
- Assistant de réunion
- Assistant de productivité
- Éditeur et générateur de vidéos
- Assistant de rédaction

Les filtres ci-dessus sont des étiquettes d’affichage uniquement. Ils ne peuvent pas être utilisés dans les règles de politique de sécurité.

- Strata Cloud Manager
- Panorama

Utiliser des filtres d'application pour les applications GenAI sur Strata Cloud Manager

STEP 1 | Connectez-vous à Strata Cloud Manager.

STEP 2 | Sélectionnez **Manage (Gérer)** > **Configuration (Configuration)** > **Objects (Objets)** > **Application (Application)** > **Application Filters (Filtres d'application)** et **Add Application Filter (Ajouter un filtre d'application)**.

STEP 3 | Saisissez un **Name (Nom)** descriptif.

STEP 4 | Pour le champ **Tag (Étiquette)**, sélectionnez **Generative AI (IA générative)**.

Toutes les applications GenAI inspectées par NGFW ou Prisma Access sont étiquetées avec `genai` lors de l'inspection. Lors de la création d'un filtre d'application personnalisé pour les applications GenAI, Palo Alto Networks recommande de sélectionner l'étiquette **Generative AI (IA générative)** pour s'assurer que la règle de politique de sécurité à laquelle le filtre d'application est ajouté s'applique au trafic des applications GenAI.

STEP 5 | Configurez des `Filtres de catégorie` supplémentaires pour affiner le champ d'application des applications GenAI impactées. Considérez les étiquettes suivantes lors de la création de votre filtre d'application GenAI.

- **Risk (Risque)** : spécifiez le score de **Risk (Risque)** de sorte que l'action de la règle de politique de sécurité ne s'applique qu'aux applications GenAI avec le score de risque sélectionné.

  Par exemple, vous pouvez souhaiter rédiger une règle de politique de sécurité pour bloquer l'accès à toutes les applications GenAI à risque, quel que soit leur usage. Dans ce cas, vous pouvez créer un filtre d'application pour les applications GenAI **4** et **5** afin que la règle de politique de sécurité ne s'applique qu'aux applications GenAI avec ces scores de risque.

- **Tag (Étiquette)** : précisez si l'action de la règle de politique de sécurité s'applique aux applications GenAI avec l'étiquette **Sanctioned (Approuvée)**, **Tolerated (Tolérée)** ou **Unsanctioned (Non approuvée)**. De plus, vous pouvez appliquer des étiquettes en fonction du cas d'utilisation de l'application GenAI.

  Par exemple, imaginons que vous souhaitez rédiger une règle de politique de sécurité pour autoriser l'accès aux applications GenAI approuvées Code Assistant & Generator (Assistant et générateur de code). Dans ce cas, vous pouvez créer un filtre d'application qui inclut à la fois les étiquettes **Sanctioned (Approuvée)** et **Code Assistant & Generator (Assistant et générateur de code)** afin que la règle de politique de sécurité ne s'applique qu'aux applications GenAI avec cette étiquette d'application et qui relèvent du cas d'utilisation.

STEP 6 | Examinez la liste des **Matching Applications (Applications correspondantes)**.

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

STEP 8 | **Push Config (Transmettre la configuration)** et **Push (Transmettre)**.

STEP 9 | Créer des règles de politique de sécurité personnalisées pour contrôler les applications GenAI.

Utiliser des filtres d'application pour les applications GenAI sur Panorama

STEP 1 | Connectez-vous à l'interface Web Panorama™ management server.

STEP 2 | Sélectionnez **Object (Objet)** > **Applications (Applications)**, puis **Add (Ajoutez)** un nouveau filtre d'applications.

STEP 3 | Saisissez un **Name (Nom)** descriptif.

STEP 4 | Pour le champ **Tag (Étiquette)**, sélectionnez **Generative AI (IA générative)**.

Toutes les applications GenAI inspectées par NGFW ou Prisma Access sont étiquetées avec `genai` lors de l'inspection. Lors de la création d'un filtre d'application personnalisé pour les applications GenAI, Palo Alto Networks recommande de sélectionner l'étiquette **Generative AI (IA générative)** pour s'assurer que la règle de politique de sécurité à laquelle le filtre d'application est ajouté s'applique au trafic des applications GenAI.

STEP 5 | Configurez des `Filtres de catégorie` supplémentaires pour affiner le champ d'application des applications GenAI impactées. Considérez les étiquettes suivantes lors de la création de votre filtre d'application GenAI.

- **Risk (Risque)** : spécifiez le score de **Risk (Risque)** de sorte que l'action de la règle de politique de sécurité ne s'applique qu'aux applications GenAI avec le score de risque sélectionné.

  Par exemple, vous pouvez souhaiter rédiger une règle de politique de sécurité pour bloquer l'accès à toutes les applications GenAI à risque, quel que soit leur usage. Dans ce cas, vous pouvez créer un filtre d'application pour les applications GenAI **4** et **5** afin que la règle de politique de sécurité ne s'applique qu'aux applications GenAI avec ces scores de risque.

STEP 6 | Examinez la liste des applications correspondantes.

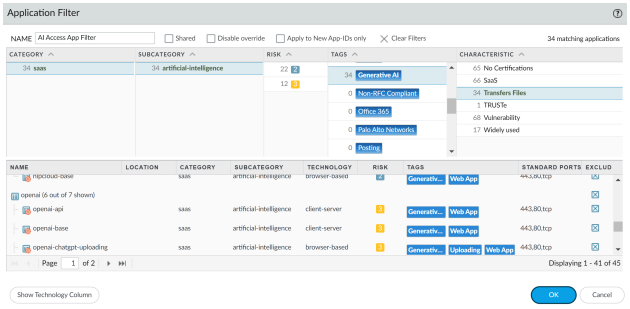
STEP 7 | Cliquez sur **OK**.

STEP 8 | Sélectionnez **Commit (Valider)** et **Commit and Push (Validez et appliquez)** les modifications de configuration.

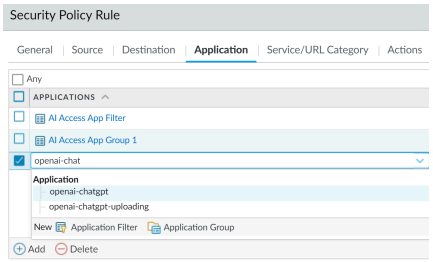
STEP 9 | Créer des règles de politique de sécurité personnalisées pour contrôler les applications GenAI.

STEP 10 | Dans l'exemple suivant, le filtre d'application **AI Access App Filter (Filtre d'application d'accès IA)** a la `catégorie : SaaS`, la `sous-catégorie : intelligence artificielle`, les `étiquettes : IA générative`, et la `caractéristique :`

`transférer des fichiers`. Cela crée un filtre avec 34 applications GenAI correspondantes.



STEP 11 | Dans l'exemple suivant, choisissez l'**Application (Application)** openai-chatgpt.



STEP 12 | Définissez le filtre en sélectionnant des valeurs d'attribut dans les sections Catégorie, Sous-catégorie, Technologie, Risques, Caractéristiques et Étiquettes. Par exemple, à mesure que vous sélectionnez des valeurs liées au chat, vous remarquerez que la liste des applications correspondantes située en bas de la boîte de dialogue se réduit. Une fois que vous aurez ajusté les attributs du filtre afin qu'ils correspondent aux types d'applications que vous souhaitez activer en toute sécurité, cliquez sur **Save (Enregistrer)**.

Modifier la règle de politique d'accès aux applications GenAI par défaut pour contrôler l'accès aux applications GenAI

Modifiez la règle de politique de l'application GenAI par défaut de Strata Cloud Manager pour contrôler l'utilisation de l'application GenAI dans votre entreprise.

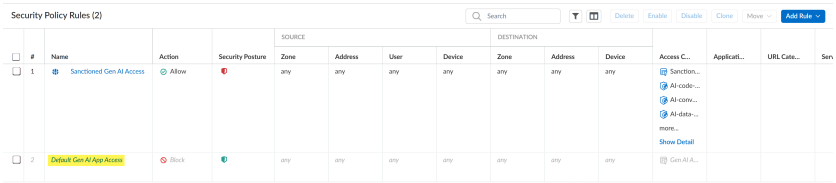
- *Dans Strata Cloud Manager, même si vous pouvez créer des règles de politique via les politiques de sécurité pour les applications GenAI, Palo Alto Networks vous recommande d'utiliser les règles de politique de sécurité de l'accès Internet pour créer des règles de politique efficacement.*
- *Palo Alto Networks ne recommande pas d'avoir des applications GenAI et non-GenAI dans la même politique si la licence Enterprise Data Loss Prevention (E-DLP) n'est pas active.*

Pour Strata Cloud Manager, AI Access Security inclut un `accès aux applications GenAI par défaut` prédéfini pour contrôler l'accès à toutes les applications GenAI non explicitement autorisées dans votre entreprise avec une politique prête à l'emploi. Par défaut, cette règle de politique bloque toutes les applications GenAI dans votre entreprise. Pour modifier cette politique :

STEP 1 | Connectez-vous à Strata Cloud Manager.

STEP 2 | Sélectionnez **Manage (Gérer)** > **Configuration (Configuration)** > **NGFW & Prisma Access (NGFW et Prisma Access** > **Security Services (Services de sécurité)** > **Security Policy (Politique de sécurité)** et sélectionnez votre cible **Configure Scope (Configurer l'étendue)** (extrait *Gen-AI-Best-Practice*).

STEP 3 | Cliquez sur la règle de politique d'`accès aux applications GenAI` prédéfinie.
Cette règle de politique bloque l'accès à toutes les applications GenAI.



STEP 4 | **Enable (Activez)** la règle de politique `d'accès aux applications GenAI par défaut`. Cette option est désactivée par défaut.

STEP 5 | Dans la section Web Application (Application Web), configurez l'**Application (Application)** et la **URL Category (Catégorie d'URL)** selon vos besoins. Par défaut, la règle de politique `d'accès aux applications GenAI` par défaut bloque l'accès à toutes les applications

GenAI. Cependant, vous pouvez modifier la règle de politique prédéfinie pour bloquer des applications spécifiques en sélectionnant des individus, des groupes d'applications ou des filtres d'application.

- **Application (Application)** : ajoutez une ou plusieurs applications GenAI.
- **Application Group (Groupe d'applications)** : un groupe d'applications est un regroupement statique d'applications individuelles que vous créez.
- **Application Filter (Filtre d'application)** : un filtre d'application regroupe dynamiquement les applications en fonction des filtres d'application que vous définissez.

  Par exemple, vous pouvez utiliser un filtre d'application GenAI prédéfini ou personnalisé pour contrôler dynamiquement l'accès aux applications GenAI dans votre organisation plutôt que d'ajouter une à une des applications GenAI ou de créer un groupe d'applications qui doit être mis à jour manuellement chaque fois qu'un changement est nécessaire.

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

STEP 7 | **Push Config (Transmettre la configuration)** et **Push (Transmettre)**.

Créer des règles de politique de sécurité personnalisées pour contrôler les applications GenAI

Vous pouvez créer des règles de politique de sécurité personnalisées pour contrôler l'utilisation des applications GenAI et empêcher l'exfiltration de données sensibles vers des applications GenAI approuvées. Utilisez les étiquettes, la source (trafic basé sur l'origine), les groupes d'utilisateurs et d'autres paramètres spécifiques pour créer votre politique personnalisée. Cela vous aide à appliquer des règles de politique de sécurité personnalisées pour les applications GenAI dans votre organisation.

(Strata Cloud Manager) Vous pouvez utiliser ou modifier la règle de politique d'accès à Internet personnalisée **Sanctioned GenAI Access (Access GenAI approuvé)** prédéfinie ou créer votre propre règle de politique d'accès à Internet personnalisée.

(Panorama™ management server) Créez des règles de politique de sécurité pour contrôler l'utilisation des applications GenAI dans votre organisation.

Vous devez créer des règles de politique de sécurité pour contrôler les applications GenAI approuvées et tolérées indépendamment des applications GenAI non approuvées. Par exemple, s'il existe des applications GenAI tolérées qui ne sont accessibles qu'à des utilisateurs spécifiques de votre organisation, vous pouvez créer une règle de politique de sécurité pour n'autoriser l'accès qu'à ces utilisateurs spécifiques. Vous pouvez associer un profil de données Enterprise Data Loss Prevention (E-DLP) à la règle de politique de sécurité pour empêcher l'exfiltration de données sensibles et un profil de protection contre les vulnérabilités pour arrêter les tentatives d'exploitation des failles du système ou d'accès non autorisé aux systèmes pour les utilisateurs autorisés. En outre, vous créez une deuxième règle de politique de sécurité plus bas dans la hiérarchie de la base de règles pour refuser l'accès à tous les autres.

- *Dans Strata Cloud Manager, même si vous pouvez créer des règles de politique personnalisées via les politiques de sécurité pour les applications GenAI, il est recommandé d'utiliser les règles de politique d'accès Internet pour créer des règles de politique efficacement.*
- *Il n'est pas recommandé d'avoir des applications GenAI et non-GenAI dans la même politique si la licence Enterprise Data Loss Prevention (E-DLP) n'est pas active.*

- Strata Cloud Manager
- Panorama

Créer des règles de politique personnalisées pour contrôler l'utilisation des applications GenAI (Strata Cloud Manager)

Vos règles de politique de sécurité d'accès à Internet sont évaluées et appliquées avant vos règles de politique de sécurité. Dans le cas où une règle de politique d'accès à Internet et une règle de politique de sécurité s'appliquent toutes deux au même trafic, l'action de la règle de politique d'accès à Internet et la configuration de l'inspection Enterprise DLP sont prioritaires sur la règle de politique de sécurité. Après une correspondance réussie avec une règle de politique d'accès à Internet, aucune autre évaluation de règle de politique n'est effectuée.

Par exemple, vous créez une règle de politique d'accès à Internet et une règle de politique de sécurité qui s'appliquent au `groupe d'utilisateurs A` et à plusieurs applications GenAI.

- *La `règle de politique d'accès à Internet A` autorise le `groupe d'utilisateurs A` à accéder aux applications GenAI spécifiées et dispose d'un `profil de données` Enterprise DLP A associé aux applications GenAI pour empêcher l'exfiltration de données sensibles.*
- *La `règle de politique de sécurité B` bloque l'accès du `groupe d'utilisateurs A` aux mêmes applications GenAI spécifiées.*

Dans ce cas, lorsqu'un utilisateur du `groupe d'utilisateurs A` accède à une application GenAI spécifiée dans les règles de politique d'accès à Internet et de sécurité, il est autorisé et l'inspection d'Enterprise DLP et le prononcé du verdict sont effectués, car la `règle de politique` d'accès Internet est plus élevée dans l'ordre d'évaluation de la base de règles de politique.

STEP 1 | Utilisez le tableau de bord AI Access Security Insights pour découvrir les risques posés par les applications GenAI.

Le tableau de bord AI Access Security Insights fournit une visibilité détaillée et complète sur l'utilisation des applications GenAI dans votre organisation. Vous pouvez découvrir des cas d'utilisation risqués d'applications GenAI, des applications GenAI individuelles risquées, ainsi que des utilisateurs risqués accédant aux applications GenAI.

STEP 2 | Si vous souhaitez utiliser les politiques existantes dans des extraits, effectuez la configuration AI Access Security initiale.

Sur Strata Cloud Manager, cela inclut la création d'un profil de données Enterprise Data Loss Prevention (E-DLP) pour définir les critères de correspondance de données sensibles, l'association des extraits prédéfinis de `Gen-AI-Best-Practice` et de `Application-Tagging`, et le profil de protection contre les vulnérabilités utilisé pour arrêter les tentatives d'exploitation des failles du système ou d'accès non autorisé aux systèmes.

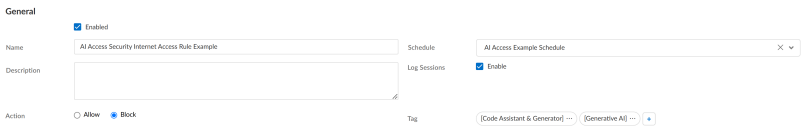
Pour NGFW, cela inclut également la création d'une zone approuvée interne et d'une zone non approuvée sortante.

STEP 3 | Si vous souhaitez créer vos propres politiques personnalisées, connectez-vous à Strata Cloud Manager.

STEP 4 | Créez une règle de politique d'accès Internet personnalisée.

- *Dans Strata Cloud Manager, même si vous pouvez créer des règles de politique personnalisées via les politiques de sécurité pour les applications GenAI, il est recommandé d'utiliser les règles de politique d'accès Internet pour créer des règles de politique efficacement.*
- *Il n'est pas recommandé d'avoir des applications GenAI et non-GenAI dans la même politique si la licence Enterprise Data Loss Prevention (E-DLP) n'est pas active.*

1. Sélectionnez **Add Rule (Ajouter une règle)** > **Internet Access Rule (Règle d'accès Internet)**.
2. Cliquez sur **Enable (Activer)** pour activer la règle de politique d'accès Internet.
3. Saisissez un **Name (Nom)** descriptif.
4. (Facultatif) Ajoutez une **Description (Description)** à la règle de politique d'accès à Internet et ajoutez une **Tag (Étiquette)** prédéfinie ou créez-en une.
5. Configurez l'**Action (Action)** (**Block (Bloquer)** ou **Allow (Autoriser)**).
6. (Facultatif) Configurez un **Schedule (Calendrier)** pour spécifier les heures auxquelles la règle de politique d'accès Internet est active.



7. Dans la section Match Criteria (Critères de correspondance), définissez le trafic à appliquer en fonction de la **Source (Source)** du trafic (d'où il provient).

   Par exemple, imaginez qu'en fonction de votre recherche des risques, vous déterminez que les utilisateurs non autorisés associés au `groupe d'utilisateurs A` accèdent à une application GenAI dont l'utilisation est approuvée pour le `groupe d'utilisateurs B`. Dans ce cas, vous pouvez créer une règle de politique

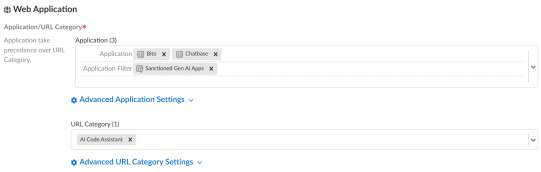
d'accès Internet pour bloquer l'accès à l'application GenAI et ajouter le `Groupe d'utilisateurs A` en tant que **Source (Source)** du groupe d'utilisateurs.

8. Dans la section Web Application (Application Web), configurez l'**Application (Application)** ou l'**URL Category (Catégorie d'URL)** pour définir les applications GenAI ou les URL d'application GenAI auxquelles vous souhaitez bloquer ou autoriser l'accès.

   (Allowed GenAI Apps [Applications GenAI autorisées]) Ajoutez uniquement les applications GenAI prises en charge à la liste des applications autorisées.

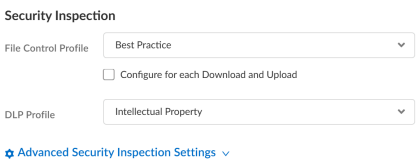
   - **Application (Application)** : ajoutez une ou plusieurs applications GenAI.
   - **Application Group (Groupe d'applications)** : un groupe d'applications est un regroupement statique d'applications individuelles que vous créez.
   - **Application Filter (Filtre d'application)** : un filtre d'application regroupe dynamiquement les applications en fonction des filtres d'application que vous définissez.

     Par exemple, vous pouvez utiliser un filtre d'application GenAI prédéfini ou personnalisé pour contrôler dynamiquement l'accès aux applications GenAI dans votre organisation plutôt que d'ajouter une à une des applications GenAI ou de créer un groupe d'applications qui doit être mis à jour manuellement chaque fois qu'un changement est nécessaire.



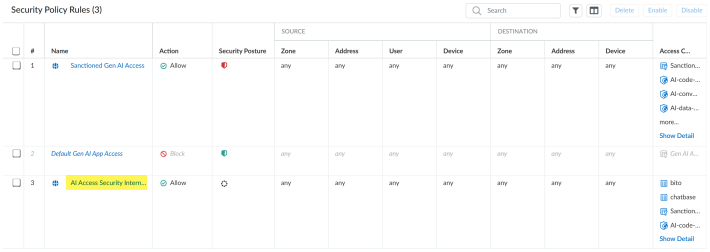
9. (Allowed GenAI Apps [Applications GenAI autorisées]) Dans la section Security Inspection (Inspection de sécurité), sélectionnez un profil Enterprise DLP et de blocage des fichiers pour empêcher l'exfiltration de données sensibles.

   - **File Control Profile (Profil de blocage des fichiers)** : un profil de blocage des fichiers vous permet d'identifier les types de fichiers spécifiques que vous souhaitez bloquer ou surveiller. Vous pouvez créer un profil de blocage des fichiers personnalisé ou utiliser le profil de blocage des fichiers par défaut recommandé par les `meilleures pratiques`.
   - **DLP Profile (Profil DLP)** : un profil de données Enterprise DLP vous permet de définir les critères de correspondance des données sensibles à rechercher pour bloquer pour empêcher l'exfiltration de données sensibles. Vous devez affecter un profil de données pour générer des données sur les **Sensitive Assets (Ressources sensibles)** lors de la découverte des risques posés par les applications GenAI.



10. Configurez le reste de la règle de politique d'accès Internet personnalisée selon vos besoins.
11. **Save (Enregistrer)**.

STEP 5 | Vérifiez que votre règle de politique d'accès a été créée avec succès et classez-la dans votre base de règles de politique si nécessaire.



STEP 6 | **Push Config (Transmettre la configuration)** et **Push (Transmettre)**.

Créer des règles de politique personnalisées pour contrôler l'utilisation des applications GenAI (Panorama)

STEP 1 | Utilisez le tableau de bord AI Access Security Insights pour découvrir les risques posés par les applications GenAI.

Le tableau de bord AI Access Security Insights fournit une visibilité détaillée et complète sur l'utilisation des applications GenAI dans votre organisation. Vous pouvez découvrir des cas d'utilisation risqués d'applications GenAI, des applications GenAI individuelles risquées, ainsi que des utilisateurs risqués accédant aux applications GenAI.

STEP 2 | Effectuez la configuration initiale de AI Access Security.

Cela inclut la création d'un profil de données Enterprise Data Loss Prevention (E-DLP) pour définir les critères de correspondance des données sensibles et le profil de protection contre les vulnérabilités utilisé pour arrêter les tentatives d'exploitation des failles du système ou d'accès non autorisé aux systèmes.

Pour NGFW, cela inclut également la création d'une zone approuvée interne et d'une zone non approuvée sortante.

STEP 3 | Connectez-vous à l'interface Web Panorama™ management server.

STEP 4 | Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et précisez le Device Group (Groupe de périphériques).

STEP 5 | Cliquez sur **Add (Ajouter)** pour ajouter une nouvelle règle de politique de sécurité.

STEP 6 | Configurez les paramètres **General (Général)**, **Source (Source)** et **Destination (Destination)** de la règle de politique de sécurité.

Reportez-vous au Guide d'administration de la politique de sécurité pour obtenir des informations détaillées sur la rédaction d'une règle de politique de sécurité.

- **General (Général)** : donnez à la règle de sécurité un **Name (Nom)** descriptif. Vous avez également la possibilité de fournir une **Description (Description)** pour la règle de politique de sécurité et d'appliquer des étiquettes pour aider à identifier l'objectif de la règle de politique de sécurité.
- **Source (Source)** : définissez d'où le trafic doit provenir pour que la règle de politique de sécurité s'applique.

  Pour la **Source Zone (Zone source)**, vous pouvez sélectionner une zone approuvée interne. Si vous souhaitez que la règle de politique de sécurité s'applique à tout le trafic, quelle que soit son origine, sélectionnez **All (Tous)** pour tous les paramètres de source.

  Par exemple, si, en fonction de votre évaluation de recherche des risques, vous déterminez que l'accès à une application GenAI est trop provisionné et doit être limité à certains

utilisateurs. Dans ce cas, vous pouvez rédiger une règle de politique **Allow (Autoriser)** et ajouter le **Source User (Utilisateur source)** requis.

- **Destination (Destination)** : définissez la destination cible du trafic nécessaire pour que la règle de politique de sécurité s'applique.

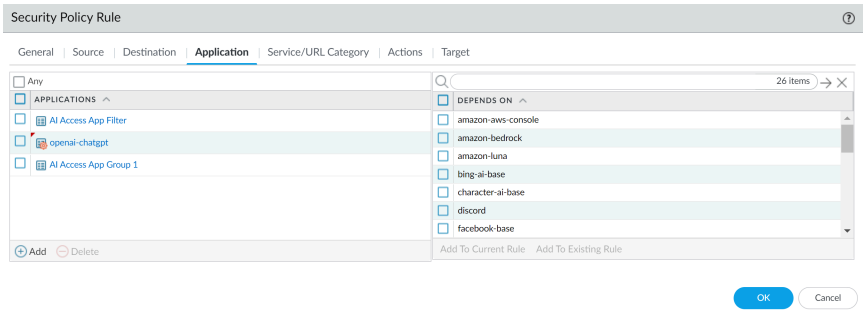
  Pour la **Destination Zone (Zone de destination)**, vous pouvez sélectionner une zone non approuvée sortante. Si vous souhaitez que la règle de politique de sécurité s'applique à tout le trafic, quelle que soit la destination du trafic, sélectionnez **All (Tous)** pour tous les paramètres de destination.

STEP 7 | Dans les paramètres **Application (Application)**, spécifiez le groupe d'applications, le filtre d'application ou les applications GenIA.

(Applications Web Autorisées) Ajoutez uniquement des applications GenAI prises en charge à la liste des applications autorisées.

- **Application (Application)** : ajoutez une ou plusieurs applications GenAI.
- **Application Category (Catégorie d'application)** : une catégorie d'application, que l'on appelle aussi filtre d'application, regroupe dynamiquement les applications en fonction des filtres d'application que vous définissez.

  Par exemple, vous pouvez utiliser un filtre d'application GenAI prédéfini ou personnalisé pour contrôler dynamiquement l'accès aux applications GenAI dans votre organisation plutôt que d'ajouter une à une des applications GenAI ou de créer un groupe d'applications qui doit être mis à jour manuellement chaque fois qu'un changement est nécessaire.
- **Application Group (Groupe d'applications)** : un groupe d'applications est un regroupement statique d'applications individuelles que vous créez.



STEP 8 | Configurez les **Actions (Actions)** de la règle de politique de sécurité. Décidez quelles actions vous souhaitez entreprendre sur votre règle de politique. Les meilleures pratiques recommandent d'associer des profils de sécurité pour permettre au pare-feu d'analyser tout le trafic autorisé afin d'y déceler des menaces. Sélectionnez **Profiles (Profils)** dans la liste déroulante **Profile Type (Type de profil)**, puis sélectionnez les profils de sécurité individuels à associer à la règle. Choisissez les actions requises pour les paramètres suivants de vos applications GenAI :

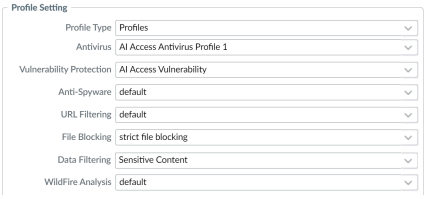
1. Dans **Action (Action)**, configurez l'action que NGFW doit effectuer lorsque le trafic de la règle de politique de sécurité **Source (Source)** vers la **Destination (Destination)** est détecté.

   Par exemple, sélectionnez **Allow (Autoriser)** si vous souhaitez autoriser l'accès à une ou plusieurs applications GenAI ou **Deny (Refuser)** si vous souhaitez bloquer tout accès à une ou plusieurs applications GenAI.

2. Dans **Profile Type (Type de profil)**, sélectionnez **Profile (Profil)**.

   Au minimum, vous devez ajouter les profils de **Vulnerability Protection (Protection contre les vulnérabilités** et de **Data Filtering (Filtrage des données)**. Cela est nécessaire pour générer des données sur les **Threats (Menaces)** et les **Sensitive Assets (Actifs sensibles)** lors de la recherche des risques posés par les applications GenAI. Les profils restants sont optionnels et peuvent être configurés selon les besoins. Pour chacun des types de profils de sécurité ci-dessous, vous pouvez sélectionner un profil existant ou en créer un nouveau.

   - Antivirus
   - Protection contre les vulnérabilités
   - Logiciel anti-espion
   - Filtrage d'URL
   - Blocage des fichiers
   - Filtrage des données
   - Analyse WildFire



*Dans l'onglet **Actions (Actions)**, le **Profile Setting (Paramètre de profil)** a la priorité sur le **Action Setting (Paramètre d'action)**. Ainsi, conformément aux meilleures pratiques, assurez-vous que les deux paramètres sont correctement assortis. Par exemple, même si vous avez le paramètre d'action comme Allow (Autoriser) et l'un des paramètres de profil comme Block (Bloquer) pour ChatGPT, il sera bloqué.*

STEP 9 | Validez et transmettez la nouvelle configuration vers vos pare-feu gérés pour compléter l'installation du plugin Enterprise DLP.

Cette étape est nécessaire afin que les noms des profils de filtrage des données de Enterprise DLP apparaissent dans les journaux de filtrage des données.

> *Il n'est pas recommandé d'utiliser la commande **Commit and Push (Valider et transmettre)** pour les changements de configuration d'Enterprise DLP. L'utilisation de la commande **Commit and Push (Valider et transférer)** entraîne des surcoûts l'étape supplémentaire de sélection manuelle des modèles impactés et des pare-feu gérés dans la sélection de l'étendue de la transmission.*

- **Transmission de configuration complète depuis Panorama**
  1. Sélectionnez **Commit (Valider)** > **Commit to Panorama** et **Commit (Valider)**.
  2. Sélectionnez **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** et cliquez sur **Edit Selections (Modifier les sélections)**.
  3. Sélectionnez **Device Groups (Groupe de périphériques)** et **Inclure les modèles de périphérique et de réseau**.
  4. Cliquez sur **OK**.
  5. Cliquez sur **Push (Transmettre)** pour appliquer les modifications de configuration à vos pare-feu gérés qui utilisent Enterprise DLP.
- **Transmission de configuration partielle depuis Panorama**

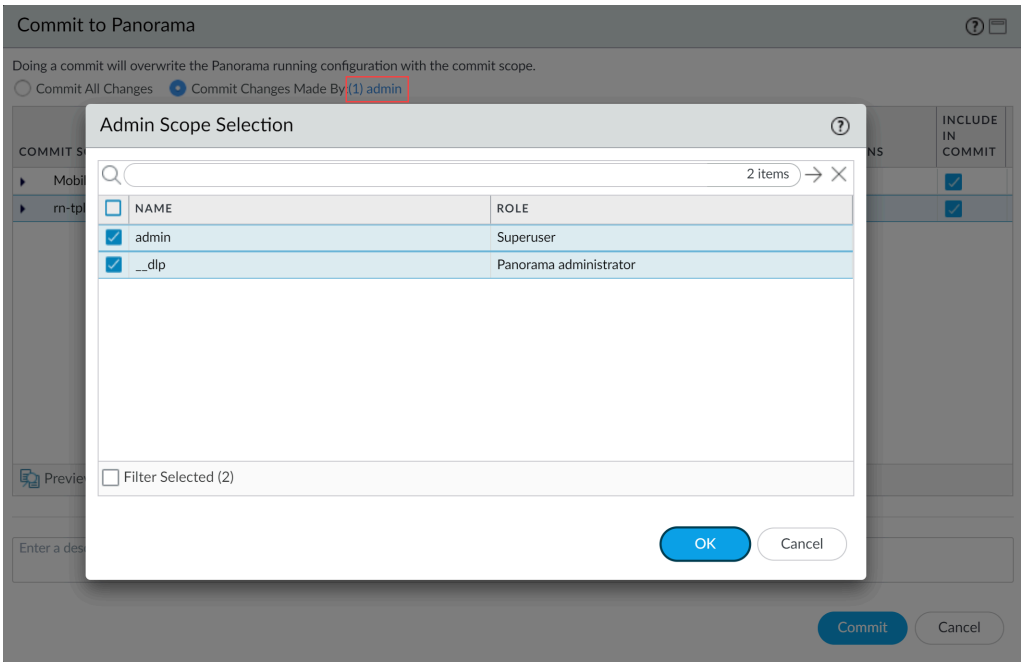
  > *Incluez toujours l'administrateur temporaire `__dlp` lors de l'exécution d'une transmission de configuration partielle. Cela est nécessaire pour conserver la synchronisation entre Panorama et le service cloud DLP.*
  >
  > *Par exemple, vous avez un utilisateur administrateur `admin` Panorama autorisé à valider et à transmettre des modifications de la configuration. L'utilisateur `admin` a apporté des modifications à la configuration Enterprise DLP et souhaite uniquement valider et transmettre ces modifications vers les pare-feu gérés. Dans ce cas, l'utilisateur `admin` doit également sélectionner l'utilisateur `__dlp` dans les opérations de validation et de transmission partielles.*

  1. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)**.
  2. Sélectionnez **Commit Changes Made By (Valider les modifications effectuées par)** puis cliquez sur l'utilisateur administrateur actuel de Panorama pour sélectionner des administrateurs supplémentaires à inclure dans la validation partielle.

     Dans cet exemple, l'utilisateur `admin` est actuellement connecté et effectue l'opération de validation. L'utilisateur `admin` doit cliquer sur **admin (admin)** puis sélectionner

l'utilisateur `__dlp`. Si d'autres modifications de configuration sont effectuées par d'autres administrateurs Panorama, il est également possible de les sélectionner ici.

Cliquez sur **OK** pour continuer.

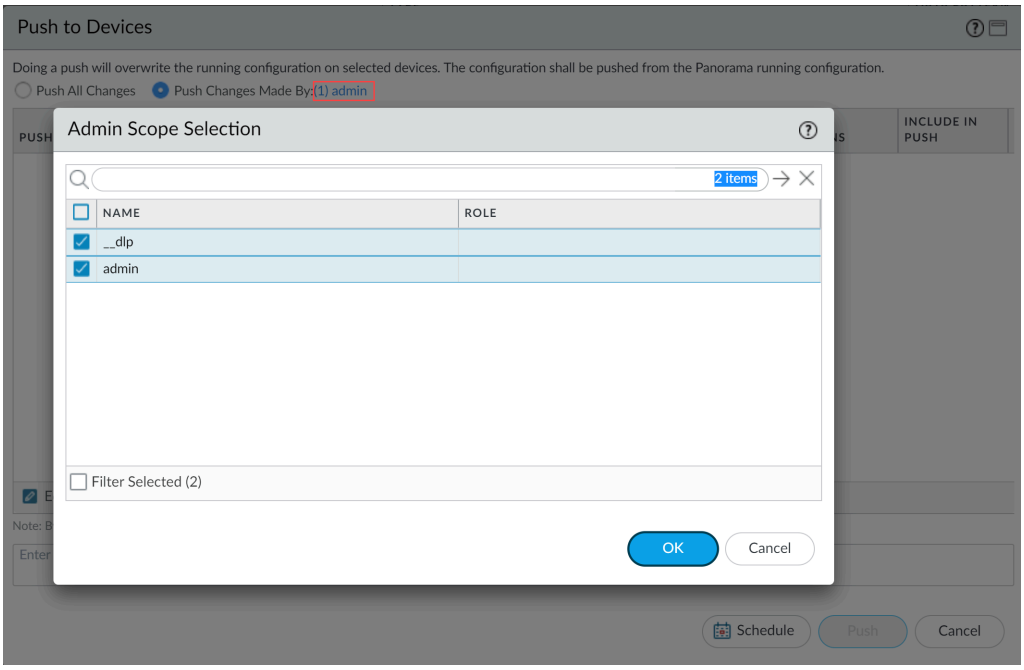


3. **Commit** (Valider).
4. Sélectionnez **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)**.
5. Sélectionnez **Push Changes Made By (Transmettre les modifications effectuées par)** puis cliquez sur l'utilisateur administrateur actuel de Panorama pour sélectionner des administrateurs supplémentaires à inclure dans la transmission partielle.

   Dans cet exemple, l'utilisateur `admin` est actuellement connecté et effectue l'opération de transmission. L'utilisateur `admin` doit cliquer sur **admin (admin)** puis sélectionner

l'utilisateur `__dlp`. Si d'autres modifications de configuration sont effectuées par d'autres administrateurs Panorama, il est également possible de les sélectionner ici.

Cliquez sur **OK** pour continuer.



6. Sélectionnez **Device Groups (Groupe de périphériques)** et **Inclure les modèles de périphérique et de réseau**.
7. Cliquez sur **OK**.
8. Cliquez sur **Push (Transmettre)** pour appliquer les modifications de configuration à vos pare-feu gérés qui utilisent Enterprise DLP.

Recommandations AI Access Security

Vos administrateurs de sécurité réseau obtiennent des données précieuses sur l'utilisation des applications GenAI sur le réseau de votre organisation en utilisant le tableau de bord AI Access Security et le Centre de Commande Strata. Pour permettre à vos administrateurs de sécurité réseau de traiter rapidement les lacunes et de renforcer votre posture de sécurité lors de l'adoption des applications GenAI, Palo Alto Networks introduit les recommandations AI Access Security.

AI Access Security propose des recommandations manuelles et automatisées. Les recommandations manuelles sont celles que vous devez mettre en œuvre manuellement. AI Access Security propose des instructions étape par étape et fournit des liens vers toute la documentation pertinente pour vous aider à mettre en œuvre les changements recommandés. Le Palo Alto Networks Copilot sur Strata Cloud Manager met en œuvre les recommandations automatisées au lieu de l'administrateur. Cependant, l'administrateur qui a initié la recommandation proposée par AI Access Security doit approuver toutes les modifications.

- **Recommandations pour NGFW et Prisma Access (Géré par Strata Cloud Manager)** : les recommandations AI Access Security se mettent à jour en temps réel à mesure que vos administrateurs effectuent les changements de configuration et que AI Access Security analyse le trafic sur votre réseau. Cela vous permet de répondre rapidement à tout changement de configuration ou à tout trafic d'application GenAI risqué qui pourrait compromettre votre organisation si cela n'est pas immédiatement traité. Toute recommandation qui analyse le trafic sur votre réseau repose sur un examen des sept derniers jours.

  Si vous avez NGFW et Prisma Access (Géré par Strata Cloud Manager) ainsi que Prisma Access Browser, AI Access Security affiche des recommandations uniquement pour vos locataires NGFW et Prisma Access. Dans ce cas, AI Access Security n'affiche pas de recommandations pour Prisma Access Browser.
- **Recommandations pour NGFW et Prisma Access (Géré par Panorama)** : les recommandations AI Access Security se mettent à jour toutes les 24 heures sur Strata Cloud Manager.

  Si vous avez NGFW et Prisma Access (Géré par Panorama) ainsi que Prisma Access Browser, AI Access Security affiche des recommandations uniquement pour vos locataires NGFW et Prisma Access. Dans ce cas, AI Access Security n'affiche pas de recommandations pour Prisma Access Browser.
- **Recommandations pour Prisma Access Browser** : les recommandations AI Access Security sont statiques et persistent après la mise en œuvre. Palo Alto Networks recommande de continuer à surveiller ces recommandations après la mise en œuvre pour s'assurer que vos administrateurs de sécurité traitent toutes les lacunes dans votre stratégie d'adoption des applications GenAI.

  AI Access Security affiche des recommandations pour Prisma Access Browser uniquement lorsque vous avez une licence Prisma Access Browser autonome et que vous n'avez aucun locataire NGFW ou Prisma Access déployé.

  Si vous avez NGFW et Prisma Access (Géré par Panorama ou Strata Cloud Manager) ainsi que Prisma Access Browser, AI Access Security affiche des recommandations uniquement

pour vos locataires NGFW et Prisma Access. Dans ce cas, AI Access Security n'affiche pas de recommandations pour Prisma Access Browser.

AI Access Security fournit des recommandations pour les scénarios suivants.

- **Recommandations de classification des applications GenAI**

  Axé sur la fourniture de recommandations basées sur l'utilisation des applications GenAI sur votre réseau et leur classification d'application (Approuvée, Tolérée ou Non approuvée)

  Par exemple, si AI Access Security remarque que votre organisation permet le trafic vers des applications GenAI non approuvées. Dans ce cas, AI Access Security fournit une recommandation pour reclasser ces applications GenAI comme Sanctioned (Approuvée) ou Tolerated (Tolérée)

- **Vérifications des meilleures pratiques et recommandations de politique**

  AI Access Security utilise le service Évaluation des meilleures pratiques (BPA) pour analyser votre base de règles de politique NGFW et Prisma Access existante afin d'offrir des recommandations pour renforcer votre posture de sécurité pour adopter en toute sécurité des applications GenAI.

  Par exemple, si le service BPA découvre que vous avez une règle de politique de sécurité permettant l'accès aux applications GenAI non approuvées.

- **Recommandations de prévention des pertes de données**

  Pour prévenir l'exfiltration de données sensibles vers des applications GenAI approuvées et tolérées, AI Access Security analyse vos règles de politique de sécurité pour déterminer si vous redirigez le trafic vers Enterprise DLP pour une inspection en ligne et pour les données au repos. Cela peut également inclure des recommandations de configuration nécessaires pour rediriger le trafic vers Enterprise DLP

- **Intégration et maximisation de AI Access Security**

  Celles-ci se concentrent sur la fourniture de recommandations exploitables pour mieux tirer parti des capacités de la plate-forme. Ces recommandations portent sur la connectivité des utilisateurs à divers marchés ou sur les applications GenAI prises en charge pour les données au repos.

- **Recommandations Prisma Access Browser**

  Les recommandations pour Prisma Access Browser portent essentiellement sur des conseils ciblés pour aider les utilisateurs Prisma Access Browser autonomes à sécuriser et optimiser leur utilisation des applications GenAI. Ces recommandations peuvent inclure la configuration de l'accès aux applications GenAI, l'activation de règles de politique de sécurité prédéfinies pour sécuriser l'accès aux applications GenAI accessibles via Prisma Access Browser, et l'examen des suspicions d'incidents d'exfiltration de données sensibles vers des applications GenAI non approuvées.

Générer un rapport AI Access Security

Le rapport AI Access Security fournit un aperçu complet de l'utilisation des applications et des plug-ins GenAI et de la posture de sécurité de votre organisation. Ce rapport vous aide à comprendre et à gérer les risques associés à l'évolution rapide des applications GenAI dans votre environnement. Riche en informations exploitables et en recommandations personnalisées, ce rapport permet à vos administrateurs de sécurité de prendre des décisions éclairées sur votre stratégie d'adoption des applications GenAI et sur la sécurité.

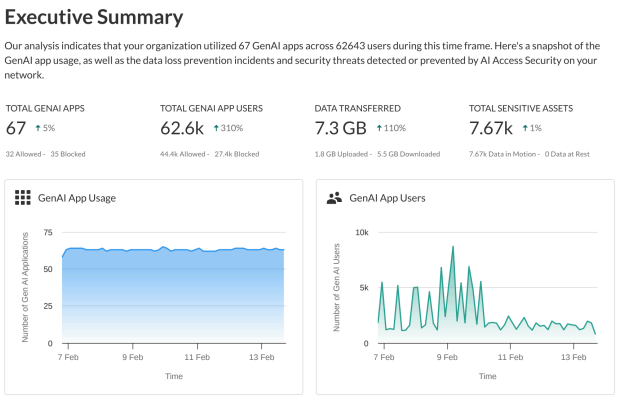
Les composants clés du rapport AI Access Security incluent :

- **Récapitulatif**

  La section Récapitulatif fournit un aperçu de haut niveau des principales métriques des applications et des plug-ins GenAI dans votre organisation. Il offre un aperçu concis de :

  - L'utilisation des applications GenAI, vous donnant une compréhension rapide de la manière dont les utilisateurs de votre organisation accèdent à ces applications.
  - Le volume de données chargées et téléchargées depuis les applications GenAI en gigaoctets (Go).
  - Le nombre d'actifs de données sensibles détectés pour les données en mouvement et au repos.

  La section Récapitulatif fournit à vos administrateurs de sécurité une vue d'ensemble rapide du paysage des applications GenAI au sein de votre organisation. Elle sert de point de départ pour accéder à des informations plus détaillées contenues dans les sections suivantes du rapport, permettant à vos administrateurs de sécurité de comprendre rapidement la posture de sécurité globale de votre organisation en matière de GenAI et d'identifier les domaines qui pourraient nécessiter une attention ou une enquête supplémentaire.

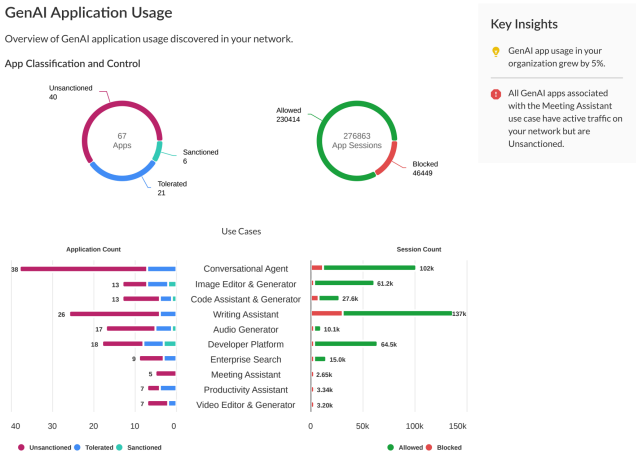


- **Utilisation de l'application GenAI**

  La section Utilisation de l'application GenAI présente une répartition complète de l'utilisation des applications GenAI au sein de votre organisation. Elle comprend :

  - Le nombre total d'applications GenAI, montrant la répartition entre les applications GenAI Autorisées et Bloquées, et les applications GenAI Approuvées, Tolérées et Non approuvées.
  - La répartition des cas d'utilisation de GenAI, classés par classification d'application (Approuvée, Tolérée ou Non approuvée) et si le trafic était Autorisé ou Bloqué.
  - Le nombre d'applications Non approuvées mais autorisées, y compris l'évolution depuis le début de la période de rapport.
  - Les données d'utilisation agrégées pour les applications GenAI non approuvées mais autorisées, y compris le nombre d'utilisateurs et la quantité totale de données transférées.
  - Les détails sur les 5 principales applications GenAI non approuvées mais autorisées, y compris le nom de l'application, le nombre d'utilisateurs, le nombre de sessions et les facteurs de risque associés.

  Cette section aide vos administrateurs de sécurité à identifier rapidement les risques de sécurité potentiels, à comprendre l'utilisation des applications GenAI à travers différents cas d'utilisation, et à prendre des décisions éclairées sur les règles de politique d'utilisation des applications et votre posture de sécurité.

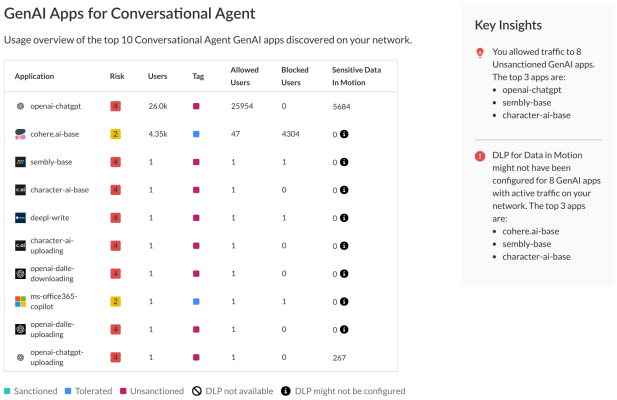


- **Applications GenAI pour les principaux cas d'utilisation**

  La section Applications GenAI pour les principaux cas d'utilisation fournit un résumé des 10 principales applications GenAI utilisées au sein de votre organisation, classées par cas d'utilisation. Elle fournit une répartition détaillée des applications GenAI les plus importantes utilisées au sein de votre organisation et inclut les éléments suivants pour chaque application GenAI :

  - Nom de l'application GenAI utilisée.
  - Score de risque associé à l'application GenAI.
  - Nombre d'utilisateurs uniques ayant utilisé l'application GenAI.
  - Classification de l'application GenAI, indiquant si l'application est approuvée, tolérée ou non approuvée.
  - Nombre de sessions uniques autorisées et bloquées pour l'application GenAI.

- Nombre d'incidents Enterprise DLP générés par des utilisateurs accédant à l'application GenAI.

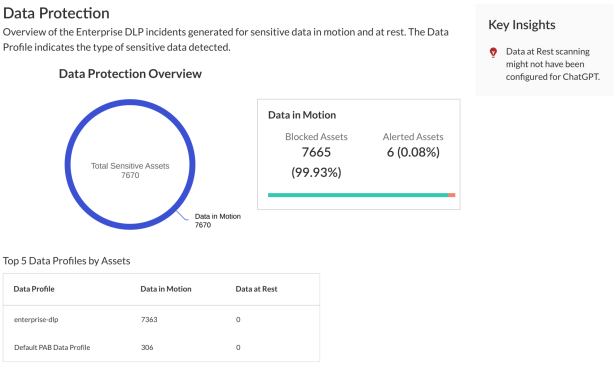


- **Protection des données**

  La section Protection des données fournit des informations cruciales sur la gestion des données sensibles au sein de l'écosystème GenAI de votre organisation. Cette section comprend :

  - Le nombre total d'actifs sensibles détectés, classés comme Autorisés ou Bloqués.
  - La répartition des actifs sensibles à travers toutes les applications GenAI, regroupés par type d'actif sensible.
  - Des informations détaillées sur les données sensibles trouvées dans les 5 principales applications GenAI.

  Ces informations aident vos administrateurs de sécurité à identifier rapidement les risques potentiels pour la sécurité des données associés à l'utilisation des applications GenAI dans votre organisation. En mettant en évidence quelles applications GenAI traitent des informations sensibles et quels types de données sensibles sont traités, vous pouvez prioriser vos efforts de protection des données et ajuster vos règles de politique de sécurité si nécessaire.



STEP 1 | Connectez-vous à Strata Cloud Manager.

STEP 2 | Sélectionnez **Insights (Informations)** > **SECURITY (SÉCURITÉ)** > **AI Access (Accès à l'IA)**.

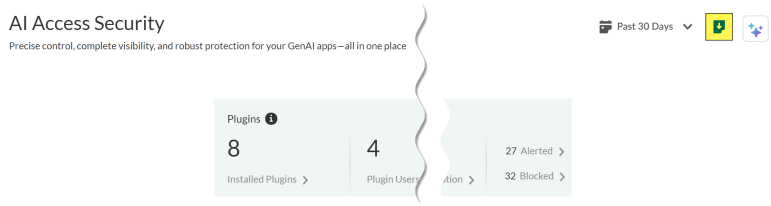
STEP 3 | Sélectionnez la période du rapport AI Access Security.

AI Access Security prend en charge la génération d'un rapport pour les **Past 24 Hours (24 dernières heures)**, **Past 7 Days (7 derniers jours)**, ou **Past 30 Days (30 derniers jours)**.

STEP 4 | Cliquez sur **Download (Télécharger)** pour enregistrer le rapport AI Access Security sur votre périphérique local au format PDF.

Le nom de fichier par défaut est `AI Access Security Report <generation-date>.pdf`.

Ne quittez pas ou ne rafraîchissez pas la page avant que le téléchargement du rapport AI Access Security soit terminé. Quitter ou rafraîchir la page avant la fin du téléchargement interrompt le téléchargement et vous devez télécharger à nouveau le rapport AI Access Security.



STEP 5 | Accédez au dossier de téléchargement que vous avez sélectionné et examinez le rapport AI Access Security.