paloalto TECHDOCS

AI Access Security 管理

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

April 16, 2026

生成AIアプリケーションによるリスクを発見する

AI Access Securityインサイト ダッシュボードを使用して、ネットワーク上の生成AIアプリケーションの使用状況をフィルタリングします。AI Access Security Insightsのダッシュボードでは、どの生成AIアプリケーションが誰によって使用されているかを理解するのに役立つ詳細な情報を確認できます。

AI Access Securityは、以下のフィルタに基づいて、許可されたユーザーデータ、ブロックされたユーザーデータ、またはその両方を検出します。

- **1**時間および**3**時間

  ユーザーは、許可、ブロック、またはその両方としてカウントできます。

  たとえば、UserAは、GenAI-App1へのアクセスがポリシー ルール1によりブロックされます。1時間後、UserAは、ポリシー ルール2がGenAI-App1へのアクセスを許可する支店に移動します。この場合、UserAは、許可されたユーザーとブロックされたユーザーの両方のカウントに表示されます。

  逆に、ポリシー ルール1は、UserAがGenAI-App1にアクセスするのをブロックします。数分後、セキュリティ管理者は、ポリシー ルール1を変更してUserAのアクセスを許可します。この場合、UserAはブロックされたユーザーのカウントに表示されます。AI Access Securityは、同じセキュリティ ポリシー ルールに一致し、少なくとも1回ブロックされた場合、過去**1**時間または**3**時間の間にアクセスを許可された回数に関係なく、ブロックされたユーザーのカウントにユーザーを表示します。

- **24**時間、**7**日、および**30**日

  ユーザーは、許可、ブロック、またはその両方としてカウントできます。

  たとえば、最初にUserAがGenAI-App1にアクセスするのをブロックしました。6時間後、UserAは、ポリシー ルール2がGenAI-App1へのアクセスを許可する支店に移動します。この場合、UserAは、許可されたユーザーとブロックされたユーザーの両方のカウントに表示されます。

- ユース ケース
- リスクのあるアプリケーション
- アプリケーションユーザー
- プラグイン
- Prisma Browser

ユースケース毎に生成AIアプリケーションによって引き起こされるリスクを発見する

生成AIアプリケーションが該当するすべてのユースケースカテゴリの完全な説明については、サポートされているユースケースを確認してください。

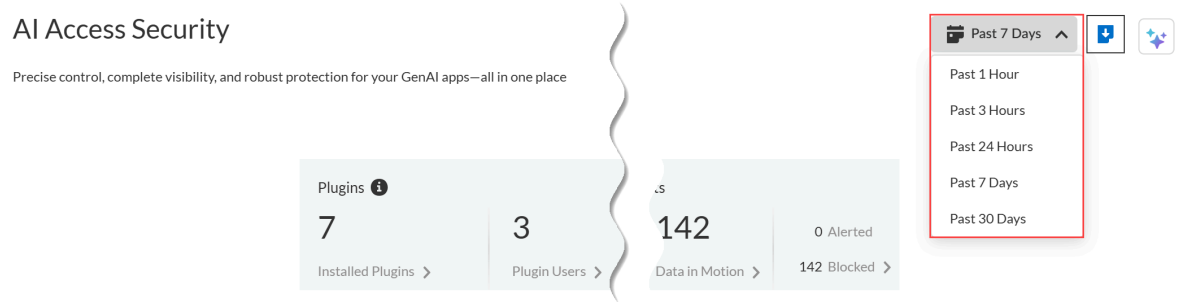
STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | [インサイト] > [AIアクセス]を選択して、[AI Access Securityインサイト]ダッシュボードを表示します。

[AI Access Securityインサイト]ダッシュボードは、デフォルトでユースケースごとのネットワーク上の生成AIアプリケーションの使用状況と、主要な生成AIユースケースに関する以下の高レベル情報を表示します:

- **Time Filter**（時間フィルタ）

  調査したい期間の生成AIユースケースの内訳をフィルタリングできます。[過去1時間]、[過去3時間]、[過去24時間]、[過去7日間]、または[過去30日間]を選択できます。



- 検出された脅威

  脅威は、Webセキュリティ ポリシー ルールに添付された脆弱性防御プロファイルによって検出されます。このプロファイルは、悪意のあるURLやフィッシングURL、悪意のある

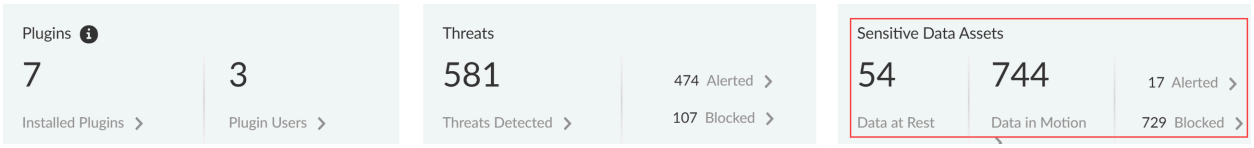
ファイル、またはマルウェアなどの脅威を検出します。検出された脅威は、すべての生成AIアプリケーションと適用ポイントにわたるすべての脅威を要約します。

- アラート済み–アラートを生成した検出された脅威の総数。
- ブロック–NGFWまたはPrisma Accessテナントによってブロックされた検出された脅威の総数。

- 機密データ アセット

  機密データアセットは、保存データ(Data Security)および移動中のデータ(SaaS Security Inline)について、トラフィックがEnterprise Data Loss Prevention (E-DLP)データプロファイルの一致条件に一致したときに検出された機密データのインシデント数を表示します。

  - 保存データ–アラートを生成したか、SaaS API(Data Security)適用チャネルを通じてブロックされたDLPインシデントの総数。
  - 移動中のデータ–アラートを生成したか、SaaS Security Inline適用チャネルを通じてブロックされたDLPインシデントの総数。
  - アラート–保存データと移動中のデータの両方に対してアラートを生成したDLPインシデントの総数。
  - ブロック–保存データと移動中のデータの両方に対してNGFWまたはPrisma AccessテナントによってブロックされたDLPインシデントの総数。



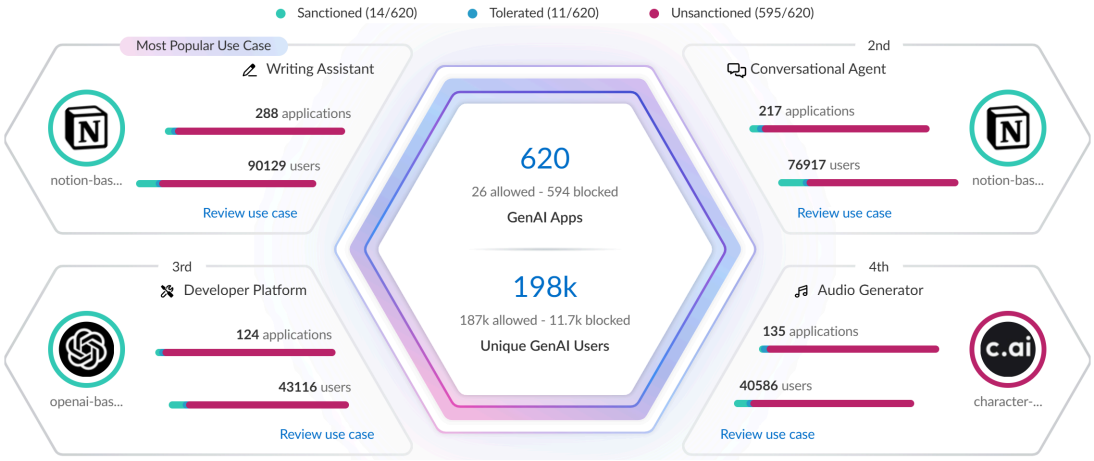
- 上位のユースケース

  AI Access Securityインサイトダッシュボードは、選択した期間にネットワーク上の活動に基づいて、上位4つの生成AIアプリケーション使用ケースを動的に表示し、アクセスした生成AIアプリケーションとユーザーの総数を表示します。これにより、最も広く使用されている生成AIアプリケーションに関連するセキュリティ インシデントを迅速に調査し、アクセス制御ポリシー ルールを実装できます。

  - 生成AIアプリケーション–特定のユースケースに該当する生成AIアプリの総数。生成AIアプリケーションの総数は、許可、許容、未許可の生成AIアプリの3つのグループに分けられます。
  - ユニーク生成AIユーザー–特定のユースケースに該当する生成AIアプリケーションにアクセスしたユーザーの総数。ユニーク生成AIユーザーのカウントをクリックすると、生

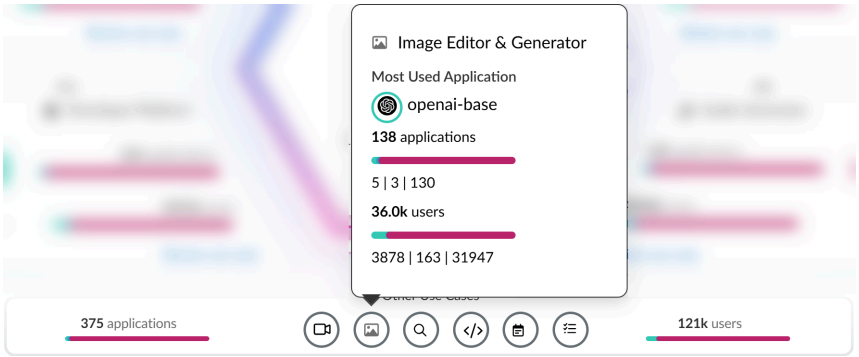
成AIアプリケーションへのアクセスがブロックされた各ユニークユーザーのリストが表示されます。

*AI Access Security*は、設定された間隔で総ユニーク生成***AI***ユーザーカウントを自動的に集計し、ユニーク生成***AI***ユーザーカウントをクリックしたときにユーザーリストを即座に生成します。これにより、ユニーク生成***AI***ユーザーカウントがリストカウントとわずかに異なる可能性があります。



- その他のすべてのユースケース
  - アプリケーション–他の生成AIアプリのユースケースに該当する生成AIアプリの総数。生成AIアプリケーションの総数は、許可、許容、未許可の生成AIアプリの3つのグループに分けられます。
  - ユーザー–他の生成AIアプリケーションのユースケースに該当する生成AIアプリにアクセスしたユーザーの総数。

  各ユースケースにマウスをホバーさせると、そのユースケースに関連する生成AIアプリケーションの使用に関する概要情報が表示されます。



STEP 3 | ユースケースをレビューして、興味のあるユースケースにおけるすべての許可済み、許容済み、未許可の生成AIアプリケーションの詳細な内訳を確認してください。

STEP 4 | ユースケースの詳細ページを確認して、生成AIアプリケーションの使用状況を理解してください。

ユースケースの詳細ページは、生成AIアプリケーションの使用状況に関する詳細なデータを提供します。この情報を使用して、生成AIアプリケーションの使用状況を理解し、セキュリティ管理者がセキュリティ態勢を強化するために必要なポリシー ルールを作成するのに役立てることができます。これにより、組織が安全に生成AIアプリケーションを採用し、機密データの流出を防ぐことが保証されます。

- ユースケースの概要

  ユースケースの概要は、調査しているユースケースに関するすべての重要な生成AIアプリケーションの使用状況を集約します。

  - 最も使用されているアプリケーション–ユースケースで最も使用されている生成AIアプリ。これには、現在生成AIアプリに割り当てられているアプリケーションタグ(許可済み、許容済み、または未承認)も含まれます。
  - アプリケーションの内訳–ユースケースに関連する生成AIアプリの総数の概要と、検出されたすべての生成AIアプリにわたるアプリタグの概要。
  - ユーザーの内訳–ユースケースに関連する生成AIアプリケーションにアクセスしたユーザーの総数の概要。許可、許容、または未許可の生成AIアプリケーションにアクセスしたユーザーの数の概要も提供されます。

- アプリケーション

  ユーザーがアクセスしたユースケースに関連するすべての生成AIアプリケーションのリスト。**[Sort By(**ソート基準)フィルタを生成AIアプリのユースケースに適用して、ユーザー数、脅威数、転送数でソートできます。AI Access Securityは生成AIアプリを多い順にソートします。

  アプリのリストには、検出された各生成AIアプリケーションに関する以下の情報が表示されます。

  - アプリケーション名–検出された生成AIアプリの名前。アプリケーション名をクリックして、詳細な使用情報を表示します。アクティビティに関するインサイトアプリケーションにリダイレクトされます。
  - タグ–現在の生成AIアプリケーションのタグ。適用したいタグをクリックすることで、新しいタグを適用できます。

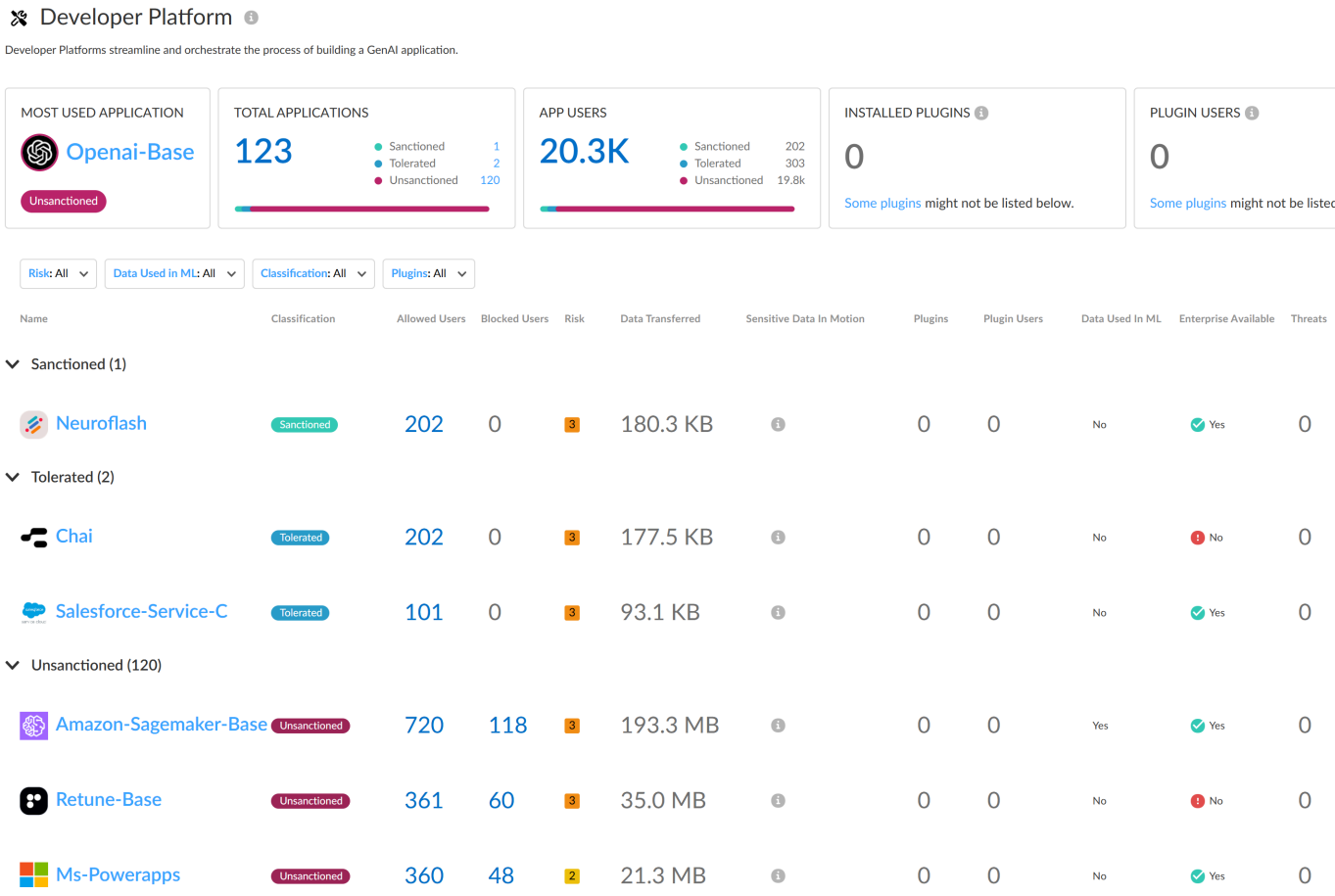
    > *Palo Alto Networks*は、コンテナ*App-ID*内のアプリケーション機能の子*App-ID*をグループ化します。ただし、*App-ID*コンテナへのタグ付けはサポートされていません。組織内で許可、未許可、または許容される特定の子*App-ID*に個別にタグ付けする必要があります。

  - 許可されたユーザー–セキュリティ ポリシー ルールで設定されたアクセス権に基づいて生成AIアプリケーションにアクセスしたユニーク ユーザーの総数。許可されたユーザーのカウントをクリックして、生成AIアプリケーションに正常にアクセスした各ユニークユーザーのリストを表示します。
  - ブロックされたユーザー–セキュリティ ポリシー ルールで設定されたアクセス権に基づいて生成AIアプリケーションへのアクセスがブロックされたユニーク ユーザーの総

数。ブロッカーユーザーのカウントをクリックして、生成AIアプリケーションへのアクセスがブロックされた各ユニーク ユーザーのリストを表示します。

- 脅威–検出された脅威アクティビティの総数。
- 転送済み–生成AIアプリケーションにアップロードまたはダウンロードされたデータの総ギガバイト数(GB)。
- 機密アセット–検出され、Enterprise DLPによってブロックされた機密データに起因するDLPインシデントの数。
- 利用可能なエンタープライズ–生成AIアプリケーションがエンタープライズプランまたはライセンススキーマを提供しているかどうかを示します。
- MLで使用するデータ–生成AIアプリケーションがユーザーがアップロードしたデータをトレーニング目的で使用しているかどうかを示します。
- リスクスコア–生成AIアプリケーションのリスクスコア。

- ユースケースのハイライト
  - アプリケーション–他の生成AIアプリのユースケースに該当する生成AIアプリの総数。生成AIアプリケーションの総数は、許可、許容、未許可の生成AIアプリの3つのグループに分けられます。
  - ユーザー–他の生成AIアプリケーションのユースケースに該当する生成AIアプリにアクセスしたユーザーの総数。



STEP 5 | 生成AIアプリケーションへのアクセスを制御するために、カスタム セキュリティ ポリシー ルールを作成します。

上記の例では、Openai-Baseがコードアシスタントとジェネレーターユースケースで最も使用されている生成AIアプリケーションです。さらに、これは未許可のアプリケーションであり、企業ネットワークでの使用が承認されていないアプリを示しています。

この場合、デフォルトの生成AIアプリケーション アクセス ポリシー ルールを変更して、組織がアクセスすべきでないアプリである場合、OpenAIへのすべてのアクセスを明示的にブロックできます。

危険なアプリによる生成AIアプリケーションがもたらすリスクの発見

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[Insights (インサイト)]** > **[Activity Insights(アクティビティに関するインサイト)]** > **[Applications(アプリケーション)]**を選択します。

STEP 3 | アプリケーション リストのフィルタを設定して、調査する生成AIアプリを絞り込みます。

1. **Time Range(期間)]**および**[Scope Selection(プッシュスコープの選択)]**を設定して、調査する特定の期間と適用ポイントをフィルタリングします。
2. **[Add Filter(フィルタの追加)]**を選択して、以下のフィルタを追加します。
   - **[Source Type - Users(ソースタイプ - ユーザー)]**–アプリケーションのリストをフィルタリングして、組織内のユーザーがアクセスした生成AIアプリケーションのみを表示します。これは必須フィルタです。
   - **[GenAI Application - TRUE(生成AIアプリケーション - TRUE)]**–アプリケーションのリストをフィルタリングして、生成AIアプリケーションのみを表示します。これは必須フィルタです。
   - **[App Risk Score(アプリケーション リスク スコア)]**–**[App Risk Score(アプリケーション リスク スコア)]**フィルタで、調査する特定のリスク スコアを選択します。1つ以上のリスクスコアを選択しない場合、すべての生成AIアプリケーションが表示されます。

     この例では、最もリスクの高いアプリケーションに起因するリスクスコアが**4**および**5**のアプリを調査しています。

STEP 4 | リストでフィルタリングされた生成AIアプリケーションを確認します。

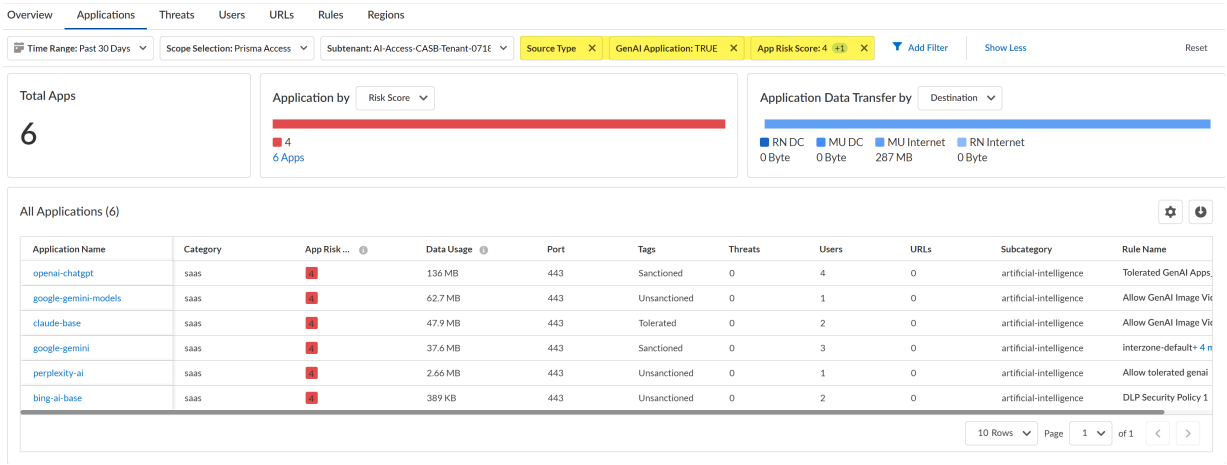
確認する重要な情報は次のとおりです。

- アプリケーション名–生成AIアプリケーションのApp-ID。
- データの使用状況–生成AIアプリケーションにアップロードまたは生成AIアプリケーションからダウンロードしたデータ量。これは、生成AIアプリケーションの使用状況を理解するのに役立ちます。生成Iアプリケーションのデータ使用量が多いということは、このアプ

リケーションが広く使用されていることを意味し、機密データや悪意のあるアクターの流出を防ぐために厳格な制御が必要になる可能性があります。

- タグ–生成AIアプリケーションの現在のアプリケーション タグ。表示されている生成AIアプリケーションの一部が使用を承認されている場合は、タグを[許容]または[許可]に変更できます。

> *Palo Alto Networks*は、コンテナ*App-ID*内のアプリケーション機能の子*App-ID*をグループ化します。ただし、*App-ID*コンテナへのタグ付けはサポートされていません。組織内で許可、未許可、または許容される特定の子*App-ID*に個別にタグ付けする必要があります。



STEP 5 | 特定のユーザーの生成AIアプリケーションへのアクセスを制御するカスタム セキュリティ ポリシー ルールを作成します。

たとえば、調査の結果、大量のデータを使用している未許可の生成AIアプリケーションが複数あることがわかりました。これは、ネットワーク上で承認されていないアプリケーションにアクセスするユーザーがおり、ダウンロードまたはアップロードされているデータを把握

できないため、セキュリティ リスクをもたらします。生成AIアプリケーションの目的と生成AIアプリケーションの使用を許可されているユーザーを理解するために適切なデュー ディリジェンスを実行できるようになるまで、生成AIアプリケーションをすべてのユーザーに対してブロックできます。

逆に、記載されている**[Unsanctioned(**未許可**)]**生成AIアプリケーションがいくつかありますが、それらは大量のデータを使用する特定のユーザーによってネットワーク上での使用が承認された生成AIアプリケーションです。この場合、タグを**[Sanctioned(**許可済み**)]**に変更し、特定のロールまたは部門のユーザーのみに対してアプリケーションの使用を**[Allow(**許可する**)]**ポリシー ルールを作成できます。ポリシー ルールでは、機密データの漏洩を防止するEnterprise Data Loss Prevention (E-DLP)データ プロファイルと、システムの欠陥を悪用する試みやシステムへの不正アクセスを阻止する脆弱性プロファイルを関連付けることができます。

生成AIアプリがアプリケーション ユーザーにもたらすリスクを発見する

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | [インサイト] > [AIアクセス]を選択して、[AI Access Securityインサイト]ダッシュボードを表示します。

これにより、リスクの高いユーザーがアクセスした上位の生成AIアプリケーションが表示され、絞り込みに役立ちます。

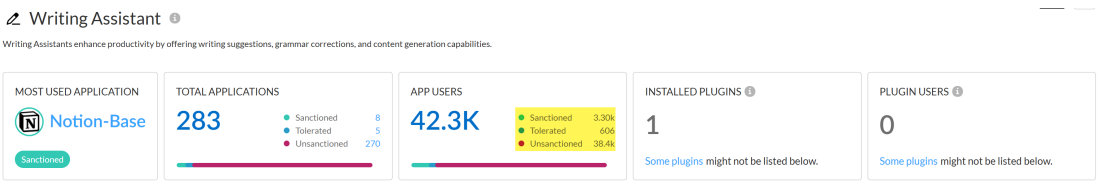
STEP 3 | リスクの高いユーザーがアクセスしている生成AIアプリケーションに関連付けられている生成AIアプリユースケースの[ユースケースの確認]をクリックします。

AI Access Security Insightsダッシュボードには、デフォルトでネットワーク上でアクセスされた生成AIアプリがユースケース別に表示され、生成AIアプリケーションのトップユーザーに関する以下の高レベルの情報が表示されます。ユーザー数をクリックすると、ユーザー名または**IP**アドレスと、ユーザーがアクセスした生成AIアプリケーションの数が表示されます。

- ユーザーの内訳

  これは、選択した生成AIユースケースに関連付けられた生成AIアプリケーションにアクセスしたユーザーの合計数を示します。AI Access Securityには、**Sanctioned(**許可済み**)**、**Tolerated(**許容済み**)**、**Unsanctioned(**未許可**)**アプリケーションにアクセスしたユーザーの数の内訳が含まれます。

  [App Users(アプリケーション ユーザー**)]**の総数をクリックすると、選択したユースケースに関連付けられた生成AIアプリケーションにアクセスした、またはアクセスをブロックされたすべてのユーザーのリストが表示されます。



- 生成**AI**ユースケース別のユーザー

  これは、選択した生成AIユースケースに関連付けられた個々の生成AIアプリケーションにアクセスしているユーザーの合計数の概要を示します。許可された生成AIアプリケーション、許容された生成AIアプリケーション、未許可生成AIアプリケーションは、個々のアプリケーションの合計ユーザー数とともに一覧表示されます。

  許可されたユーザー数とブロックされたユーザー数を確認し、生成AIアプリケーションのセキュリティ ルールとアクセス ポリシー ルールの効果を測定します。

  - 許可されたユーザー—生成AIアプリケーションへのアクセスが許可されたユーザーの合計数。この情報を使用して、許可されたユーザー数が期待値と一致することを確認して

セキュリティ ポリシー ルールの有効性を測定したり、組織での使用が新たに許可された生成AIアプリケーションの導入率を測定したりできます。

- ブロックされたユーザー—生成AIアプリケーションへのアクセスをブロックされた使用済みの合計数。この情報を使用して、特定の生成AIアプリケーションのアクセスを制御するセキュリティ ポリシー ルールを正しく設定したかどうかを確認したり、組織内のユーザーが未許可の生成AIアプリにアクセスしているかどうかを把握したりできます。

たとえば、以下のGrammarly生成AIアプリケーションを考えてみてください。あなたの組織は、この生成AIアプリケーションを組織内の特定のユーザーによる使用の許可対象として分類しました。この場合、セキュリティ管理者は[許可されたユーザー]数をクリックし、生成AIアプリケーションにアクセスするすべてのユーザーが許可されることを確認しました。

逆に、セキュリティ管理者は、1,600人以上のユーザーがCharacter-Aiベースのアプリケーションにアクセスしたことがわかります。セキュリティ管理者は、この生成AIアプリケーションを未許可に分類し、組織へのすべてのアクセスを制限することを意図していました。この場合、セキュリティ管理者は、セキュリティ ポリシー ルールベースおよびCharacter-Aiベースアプリケーションへのアクセスを制御する個々のセキュリティ ポリシー ルールを見直して、セキュリティ ポリシー ルールベース内に正しく配置されて

いたこと、およびすべてのアクセスをブロックするように正しく設定されていることを確認する必要があります。

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 | 特定のユーザーの生成AIアプリケーションへのアクセスを制御するカスタム セキュリティ ポリシー ルールを作成します。

たとえば、調査した結果、大量のユーザーが`bing-ai-uploading`生成AIアプリケーションにアクセスしていることが判明します。これは許可された生成AIですが、組織内の特定のユーザーセットにのみ許可されます。この生成AIアプリケーションにアクセスすべきでないユーザーへのアクセスを明示的にブロックして悪用を防ぐポリシー ルールと、生成AIアプリケーションへのアクセスを承認されたユーザーへのアクセスを明示的に許可するセキュリティ ポリシー ルールを記述することができます。あるいは、すべてのユーザーにアクセスを許可するポリシー ルールを作成し、機密データの流出を防ぎ、悪意のあるURLやフィッシングURL、悪意のあるファイル、マルウェアなどの脅威を防ぐために、データ損失や脅威防御対策を実装することもできます。

生成AIアプリケーションをサードパーティ プラグインとしてインストールすることによってもたらされるリスクを発見する

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | [インサイト] > [AIアクセス]を選択して、[AI Access Securityインサイト]ダッシュボードを表示します。

ダッシュボードには、ユーザーがインストールしたサードパーティ プラグインの数と、サードパーティ プラグインをインストールしたユーザーの数が表示されます。AI Access Securityは、AI Access Securityが保存したすべてのデータからこれらの数を決定します。これらの数は、時間フィルタによって示された期間に制限されません。

STEP 3 | [インストールされたプラグイン]または[プラグイン ユーザー]をクリックして、SaaS Security Posture Management(SSPM)で詳細情報に移動します。

[インストールされたプラグイン]をクリックすると、生成AIサードパーティ プラグインの詳細を表示する[3rd Party Plugins(サードパーティ プラグイン)]ページが開きます。ここから、プラグイン情報を確認してプラグインがリスクかどうかを判断することができます。

[プラグイン ユーザー]をクリックすると、サードパーティ プラグインをインストールしたユーザーの詳細を表示する[3rd Party Plugins(サードパーティ プラグイン)]ページが開きます。各ユーザーについて、インストールしたプラグインの数と、プラグインをインストールしたマーケットプレース アプリケーションを表示できます。この情報を使用して、個々のユーザーによってもたらされるプラグイン リスクを特定します。

STEP 4 | ユースケースごとにインストールされたプラグインを表示するには、以下の手順を完了します:

1. **[インサイト] > [AIアクセス]**を選択して、[AI Access Securityインサイト]ダッシュボードを表示します。

   ダッシュボードは、ネットワーク上のアクティビティに基づいて、上位4つの生成AIアプリケーションのユースケースが目立つよう表示します。ダッシュボードには、他のユースケースのアイコンも表示されます。

2. ユースケースの詳細に移動します。上位のユースケースについては、**[ユースケースの確認]**をクリックします。他のユースケースについては、ユースケース アイコンをクリックします。

   ユースケースの詳細ページには、そのユースケースのすべての生成AIアプリケーションの表が表示されます。

   このページの概要情報には、インストールされたプラグインの数とプラグイン ユーザーの数が含まれます。これらの数値は、*AI*アクセス セキュリティが保存したすべてのデータから決定されており、時間フィルタで示された期間に限定されません。このため、これらの合計はユースケースの詳細テーブルに反映されない場合があります。

3. ユースケースの詳細テーブルでは、1つ以上のマーケットプレース アプリケーション インスタンスにプラグインとしてインストールされている生成AIアプリケーションと、そのプラグインユーザーの数を特定します。この情報は、テーブルの**[Plugins(プラグイン)]**および**[Plugin Users(プラグイン ユーザー)]**列に表示されます。

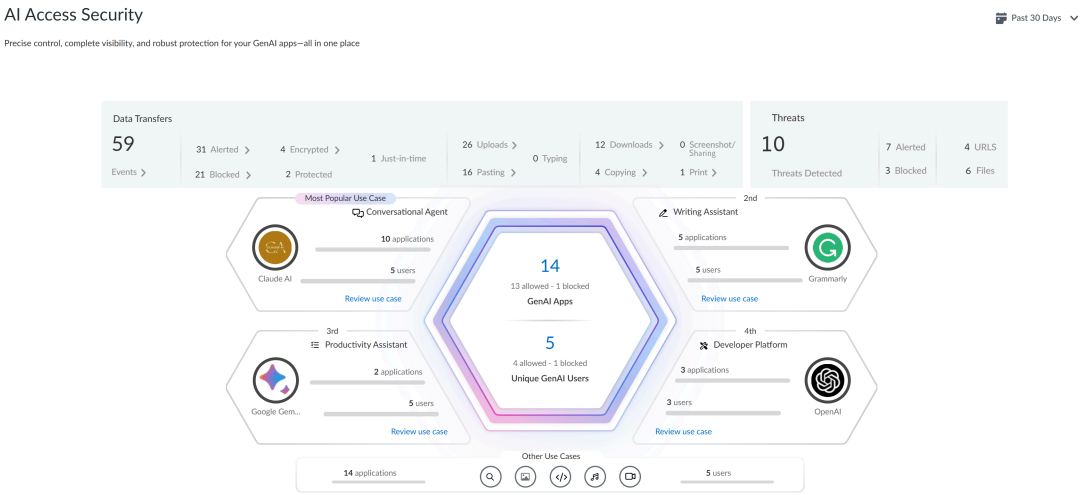
4. プラグインとしてインストールされている生成AIアプリケーションの場合、**[Plugins(プラグイン)]**または**[Plugin Users(プラグイン ユーザー)]**列の数をクリックします。

   [Plugins(プラグイン)]列の数をクリックすると、ユーザーがサードパーティ プラグインとしてインストールした生成AIアプリケーションのインスタンスを表示するSSPMのサードパーティ プラグイン ページが開きます。ここから、プラグイン情報を確認してプラグインがリスクかどうかを判断することができます。

   [Plugin Users(プラグイン ユーザー)]列の数をクリックすると、アプリケーションをサードパーティ プラグインとしてインストールしたユーザーに関する詳細を表示するサードパーティ プラグイン ページが開きます。この情報を使用して、個々のユーザーによってもたらされるプラグイン リスクを特定します。

Prisma Access Browser上の生成AIアプリケーションがもたらすリスクを発見する

Prisma Access BrowserにはAI Access Securityが組み込まれており、Prisma Access Browserスタンドアロンのお客様に包括的な生成AIアプリケーションの可視性、アクセス制御、データ、脅威防御を提供します。この統合により、データ分類やリアルタイムの脅威防御などの詳細なラストマイル制御を備えた生成AIアプリケーションの最も包括的なカタログが提供されます。Prisma Access Browserスタンドアロンのセキュリティ管理者は、[Insights(インサイト)]メニューのAI Access Securityにアクセスして、アプリケーション メトリック、ユーザー アクティビティ、検出された脅威、データ転送などの詳細な分析によるPrisma Access Browserを通じて、サードパーティのAIアプリケーションの使用状況を監視できます。

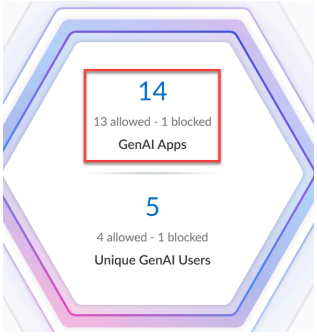


STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | [インサイト] > [AIアクセス]を選択すると、スタンドアロンPrisma Access Browserの[AI Access Securityインサイト]ダッシュボードが表示されます。

STEP 3 | [生成**AI**アプリケーション]をクリックして、**[Is GenAI:Yes(**生成**AI:**はい**)]**と[カテゴリ]の**[Application metrics(**アプリケーション メトリック**)]**を表示します。以下のメトリックを表示するために適用されたフィルタにアクセスする:

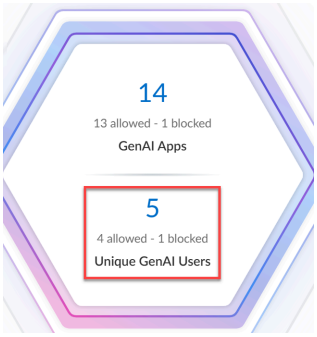
- 生成AI(GenAI)アプリケーションの総数
- 許可された生成AIアプリケーション
- ブロックされた生成AIアプリケーション

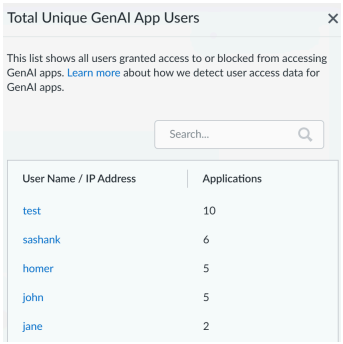


STEP 4 | **[Unique GenAI Users(**ユニーク生成**AI(GenAI)**ユーザー**)]**をクリックすると、生成AIアプリケーションへのアクセスが許可またはブロックされた生成AIアプリケーション ユーザーの合計が表示されます。ユーザーを**([Total Unique GenAI App Users(**生成**AI(GenAI)**アプリケーションのユニーク ユーザーの総数**)]**ページから)選択して、[Events(イベント)]ページに移動して**([User(**ユーザー**): <user name>**filter applied(フィルタが適用)])**、その特定のユーザーに対して許可およびブロックされた生成AIアプリケーションを確認します。使用可能なメトリックは以下のとおりです:

- 生成AIユーザーの総数
- 許可された生成AIユーザー

- ブロックされた生成AIユーザー

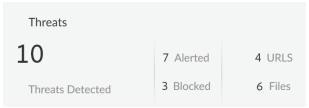




STEP 5 | [検出された脅威]ウィジェットをクリックすると、検出およびブロックされた脅威の総数が表示されます。

この情報は、[イベント]ページ(**[Is GenAI:Yes(生成AI:はい)]**、**[カテゴリ:マルウェア]**フィルタを適用)。使用可能なメトリックは以下のとおりです:

- 検出された脅威とブロックされた脅威の合計を表示する生成AI脅威の総数。
- 悪意のあるURL(適用されたフィルタ:カテゴリ:マルウェアとタイプ:悪意のあるウェブサイト)
- ファイル (適用されたフィルタ:カテゴリ:マルウェアとタイプ:特定された悪意のあるファイル)

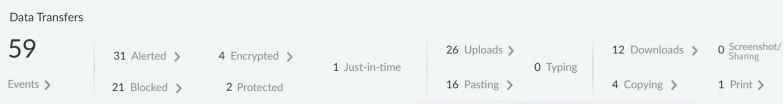


STEP 6 | **[Data Transfers(データ転送)]**ウィジェットをクリックすると、トラフィックがPrisma Access Browserのエンタープライズ データ損失防止(E-DLP)データ プロファイルの一致条件に一致する場合に検出されたデータ転送のインシデント数が表示されます。

この情報は、[イベント]ページ(**[Is GenAI:Yes(生成AI:はい)]**、**[カテゴリ:適用されたDLPフィルタ)**。

- データ転送総数が検出されました。適用されたフィルタ:**[Is GenAI:Yes(生成AI:はい)]**、カテゴリ:**DLP**。
- アラート済みのデータ転送。適用されたフィルタ:**[Is GenAI:Yes(生成AI:はい)]**、カテゴリ:**DLP**、アクション:許可。
- ブロック済みのデータ転送。適用されたフィルタ:**[Is GenAI:Yes(生成AI:はい)]**、カテゴリ:**DLP**、アクション:ブロック済み。
- 保護されたデータ転送:許可されているが、ブラウザだけが使用できるアクション。たとえば、許可されたアプリケーション間でデータをコピーアンドペーストしたり、ブラウザ内の他のアプリやローカル デスクトップ アプリにブロックしたりできます。適用されたフィルタ:**[Is GenAI:Yes(生成AI:はい)]**、カテゴリ:**DLP**、アクション:許可された保護済み。
- 暗号化されたデータ転送:ブラウザのみが、特定のユーザーと暗号化対象デバイスの復号化キーを持つ暗号化アクション。これにより、ファイルをダウンロードして、特定のアプリケーションにアップロード(および復号化)したり、オフライン モードでブラウザで開いたりすることができます。他のアプリケーションはこのファイルを開くことができないため、管理対象外のデバイスなど、エンドポイントで使用したくないファイルに最適です。適用されたフィルタ:**[Is GenAI:Yes(生成AI:はい)]**、カテゴリ:**DLP**、アクション:許可済み暗号化。
- データ転送のジャスト イン タイム制御:続行する前にユーザーに警告する、続行する前にユーザーにビジネス上の正当性を示すよう求める、管理者の承認フローをトリガーするなどのアクション。これらは、緊急時に一時的なアクセスまたはルールへのバイパスをトリガーするか、コンプライアンス上の理由で正当化とロギングが必要です。適用されたフィルタ:**[Is GenAI:Yes(生成AI:はい)]**、カテゴリ:**DLP**、アクション:許可が要求されました。
- データ転送がアップロードされました。適用されたフィルタ:**[Is GenAI:Yes(生成AI:はい)]**、カテゴリ:**DLP**、タイプ:ファイルのアップロード。
- クリップボード アクティビティでのデータ転送(貼り付け)。適用されたフィルタ:**[Is GenAI:Yes(生成AI:はい)]**、カテゴリ:**DLP**、タイプ:クリップボードの貼り付け。
- その時点で入力されたデータ転送。適用されたフィルタ:**[Is GenAI:Yes(生成AI:はい)]**、カテゴリ:**DLP**、タイプ:コンテンツのサニタイズ。
- データ転送がダウンロードされました。適用されたフィルタ:**[Is GenAI:Yes(生成AI:はい)]**、カテゴリ:**DLP**、タイプ:ファイルのダウンロード。
- データ転送がコピーされました。適用されたフィルタ:**[Is GenAI:Yes(生成AI:はい)]**、カテゴリ:**DLP**、タイプ:クリップボードのコピー。
- スクリーンショットを使用して共有されるデータ転送。適用されたフィルタ:**[Is GenAI:Yes(生成AI:はい)]**、カテゴリ:**DLP**、タイプ:画面共有。

- データ転送が印刷されました。適用されたフィルタ:**[Is GenAI:Yes(**生成**AI:**はい**)]**、カテゴリ:**DLP**、タイプ:印刷。



生成AIアプリケーションのタグ付け

生成AIアプリケーションのリスク スコアやその他の考慮事項に基づいて、アプリケーションにタグを適用し、そのアプリケーションが組織内で承認されているかどうかを反映できます。以下のタグを使用できます。

タグ	詳説
許可	アプリケーションは組織によって承認され、組織のメンバーが使用しています。
未許可	アプリケーションは組織によって承認されていません。たとえば、アプリケーションに関連するセキュリティ リスクにより、アプリケーションが未許可になる可能性があります。 組織のメンバーはアプリケーションを使用すべきではないため、アプリケーションをブロックするアクションを実行する必要があります。ポリシー ルールを使用してアプリケーションをブロックできます。
寛容	アプリケーションは、許可されたアプリケーションのように信頼されません。ただし、組織は、より安全なアプリケーションを識別できるようになるまで、その使用を許可します。組織の生産性を阻害しないように、アプリケーションは許容されます。 アプリケーションは潜在的なセキュリティ リスクがあるにもかかわらず許可されているため、特定のアクションを制限する措置を取る場合があります。たとえば、アプリケーションのアップロードまたはダウンロード操作をブロックするポリシー ルールを作成できます。

*Palo Alto Networks*は、コンテナ*App-ID*内のアプリケーション機能の子*App-ID*をグループ化します。ただし、*App-ID*コンテナへのタグ付けはサポートされていません。組織内で許可、未許可、または許容される特定の子*App-ID*に個別にタグ付けする必要があります。

たとえば、`claude-base`、`claude-upload`、`claude-edit`、`claude-post`、および`claude-delete`の子*App-ID*を含む`claude`コンテナ*App-ID*があるとします。

アプリケーション フィルタを作成して、許容されたアプリケーションに対して同じデータの流出制御を適用します。この場合、許容された`claude`生成*AI*アプリケーションのすべてのサブプロセスにポリシー ルール アクションを適用するには、`claude` *App-ID*コンテナのすべての子*App-ID*にタグを付ける必要があります。

*2024*年*9*月、*Palo Alto Networks*はアプリケーションのタグ付けの実装方法を更新しました。*2024*年*9*月以降、タグは新しい事前定義済みの`[Application-Tagging(`アプリケーション タグ付け`)]`スニペットに対して読み書きされます。この更新がテナントにリリースされると、アプリケーションに初めてタグ付けしたときに有効になります。タグがスニペットと*AI Access Security*に書き込まれ、*[Activity Insights Applications(*アクティビティに関するインサイト アプリケーション*)]*ページが表示され、*Strata Cloud Manager Command Center*がスニペットからタグ情報の表示を開始します。この更新の前にアプリケーションにタグを付けた場合、それらのタグの変更は*AI Access Security*およびアクティビティに関するインサイト アプリケーションに反映されなくなります。`[Application-Tagging(`アプリケーション タグ付け`)]`スニペットは、***[Sanctioned(***許可済み***)]***または***[Tolerated(***許容済み***)]***のタグが付けられたアプリケーションを追跡します。***[Sanctioned(***許可済み***)]***または***[Tolerated(***許容済み***)]***として明示的にタグ付けされていないアプリケーションは、***[Unsanctioned(***未許可***)]***と見なされます。このため、この更新後に追加したタグのみが*Strata Cloud Manager*に表示されます。他のすべてのアプリケーションは***[Unsanctioned(***未許可***)]***として表示されます。

この更新の前に適用したタグは、[Application-Tagging(アプリケーション タグ付け)]スニペットを関連付け、`[Application-Tagging]`設定スコープ内でタグを適用している限り、*NGFW*または*Prisma Access*デプロイメントでのタグベースのポリシー適用に影響します。

- NGFWとPrisma Accessのアプリケーションの設定
- アクティビティに関するインサイト アプリケーション

アプリケーション設定で生成AIアプリをタグ付けする

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | 適切な設定スコープに事前定義済みの`[Application-Tagging(アプリケーション タグ付け)]`スニペットを関連付けることで、タグベースのポリシー適用をサポートします。

STEP 3 | タグ付けしたい子App-IDを取得します。

以下のいずれかの方法を使用して、生成AIアプリの子App-IDを取得できます。

- AI Access Securityインサイト ダッシュボードを使用して生成AIアプリケーションによってもたらされるリスクを発見します。AI Access Securityインサイトは、組織全体で使用されている検出された子App-IDを表示します。
- サポートされている生成AIアプリケーションのリストを確認します。
- Applipediaを使用して、動的コンテンツ更新を通じて配信されるサポートされている生成AIアプリの子App-IDを検索します。

  Applipediaは、動的コンテンツを通じて配信されるアプリケーションのApp-IDのみを表示し、App-ID Cloud Engine (ACE)を通じて配信されるアプリケーションは表示しません。

STEP 4 | **[Manage(管理)]** > **[Configuration(設定)]** > **[[NGFWとPrisma Access]** > **[Objects(オブジェクト)]** > **[Application(アプリケーション)]** > **[Applications(アプリケーション)]**

STEP 5 | [設定スコープ]で、`[Application-Tagging(アプリケーション タグ付け)]`スニペットを選択します。

App-ID Cloud Engine (ACE)を通じて配信されるApp-IDにタグ付けする場合、選択したフォルダに関連付けられたすべてのNGFWまたはPrisma Accessテナントは、ACEからApp-IDの更新を受け取るように設定されている必要があります。

ACEは、アクティブなSaaS Security InlineまたはAI Access Securityライセンスを持つNGFWまたはPrisma Accessテナントに対してデフォルトで有効になっています。NGFW用にACEを手動で有効にすることもできます。

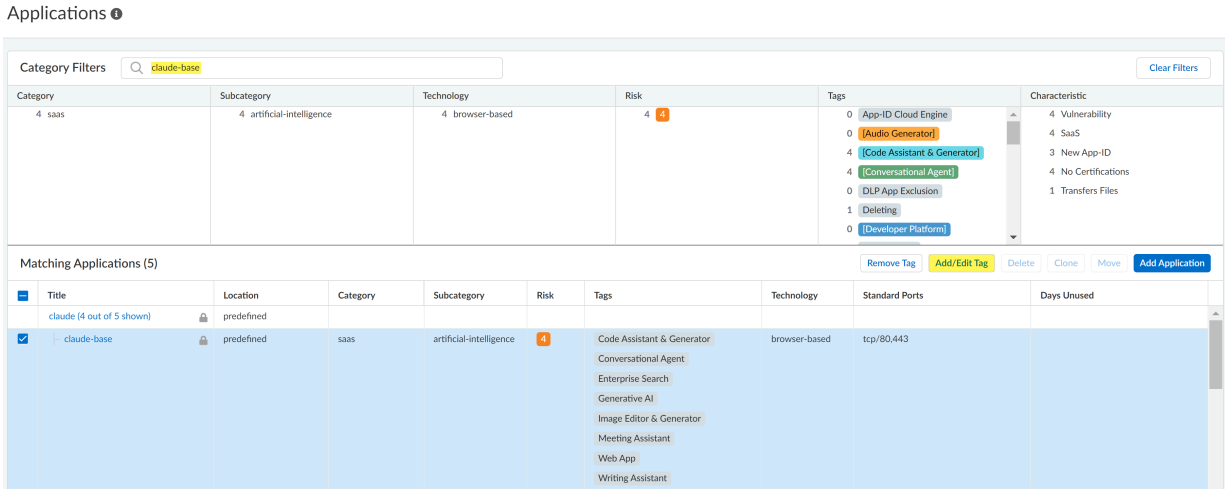
ACEから配信されたApp-IDにタグ付けし、選択したフォルダに関連付けられた少なくとも1つのNGFWまたはPrisma AccessテナントがACEからApp-IDを受け取るように設定されていない場合、設定プッシュは失敗します。

この理由から、Palo Alto Networksはグローバル設定スコープの選択を推奨しません。

STEP 6 | カテゴリ フィルタ検索フィールドに、タグ付けしたいApp-IDを入力して選択します。

一度に1つのApp-IDのみをタグ付けできます。

STEP 7 | タグを追加/編集します。



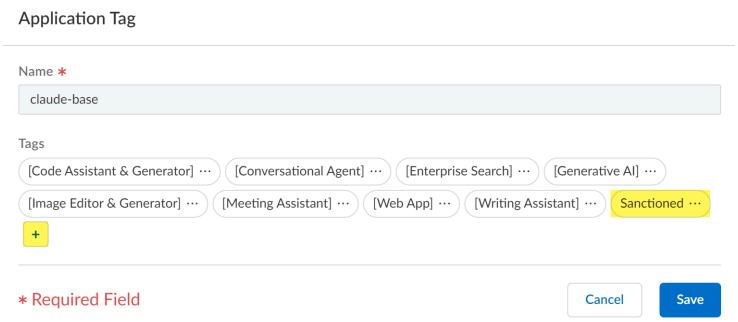
STEP 8 | **+**をクリックして、事前定義済みの許可されたまたは許容されたアプリケーションタグを適用します。

この例では、`claude-base` App-IDが許可されたタグでタグ付けされています。

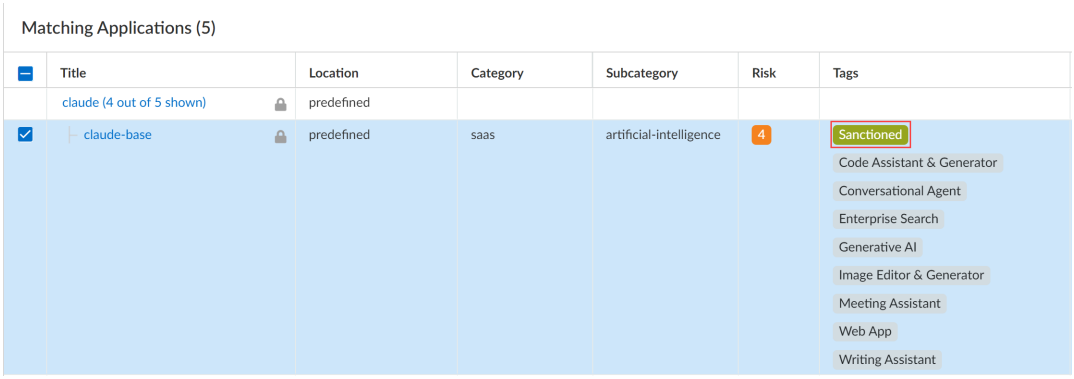
アプリは、未許可または許可された、または許容されたタグがない場合、アプリケーションからのタグ付けと見なされます。

アプリケーションのタグを許可されたまたは許容されたから未許可に変更したい場合は、既存のタグを削除する必要があります。アプリケーションから未許可としてアプリに手動でタグを付けることはできません。

STEP 9 | **Save**（保存）を選択します。



STEP 10 | タグ列の値を確認して、アプリケーション タグを正常に適用したことを確認してください。



STEP 11 | **[概要]**をクリックしてください。

STEP 12 | **[Push Config (設定をプッシュ)]**をクリックし 、設定の変更 をプッシュします 。

生成AIアプリケーションをインサイト ダッシュボードにタグ付けする

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | 適切な設定スコープに事前定義済みの`[Application-Tagging(アプリケーション タグ付け)]`スニペットを関連付けることで、タグベースのポリシー適用をサポートします。

STEP 3 | タグ付けしたい子App-IDを取得します。

以下のいずれかの方法を使用して、生成AIアプリの子App-IDを取得できます。

- AI Access Securityインサイト ダッシュボードを使用して生成AIアプリケーションによってもたらされるリスクを発見します。AI Access Securityインサイトは、組織全体で使用されている検出された子App-IDを表示します。
- サポートされている生成AIアプリケーションのリストを確認します。
- Applipediaを使用して、動的コンテンツ更新を通じて配信されるサポートされている生成AIアプリの子App-IDを検索します。

  Applipediaは、動的コンテンツを通じて配信されるアプリケーションのApp-IDのみを表示し、App-ID Cloud Engine (ACE)を通じて配信されるアプリケーションは表示しません。

STEP 4 | **[Insights (インサイト)]** > **[Activity Insights(アクティビティに関するインサイト)]** > **[Applications(アプリケーション)]**を選択します。

STEP 5 | タグ付けする生成AIの子App-IDを探します。必要に応じて、生成AIアプリケーションのみを表示するようにテーブルをフィルタリングできます。

1. [フィルタの追加]を選択して、[生成**AI**アプリケーション]フィルタを追加します。
2. 生成**AI**アプリケーション フィルタを**TRUE**に設定します。

STEP 6 | 生成AI App-IDに適用されるタグを確認するには、[タグ]列の値を調べます。

STEP 7 | 子の生成AI App-IDに別のタグを適用します。

1. [アクション]列でタグ アイコンを選択し、**[Sanctioned(許可)]**、**[Tolerated(許容)]**、または**[Unsanctioned(未許可)]**タグを選択します。
2. 新しいタグを適用します。

生成AIアプリケーションに割り当てられたリスクスコアの表示

組織に最大の脅威をもたらす生成AIアプリケーションをすばやく特定できるように、AI Access Securityは各生成AIアプリケーションにリスクスコアを割り当てます。これらのリスクスコアにより、危険な生成AIアプリケーションをすばやく特定できるため、環境を保護するためのアクションを実行できます。たとえば、環境を保護するために、アプリケーションをブロックするポリシー ルールを作成できます。Unsanctioned(未許可)のタグをアプリケーションに付けることもできます。

アプリケーションのリスクスコアは1(低リスク)~5(高リスク)で、SaaSアプリ属性に基づいています。一部の属性はすべてのSaaSアプリケーションに共通ですが、属性のサブセットは生成AIアプリに固有のものです。

生成AI属性は、ユーザーがアプリケーションに入力するためのデータ タイプ、アプリが生成する出力のデータ タイプ、ユーザーが送信したデータが生成AIモデルのトレーニングにアプリで使用されるかどうかなどの属性です。生成AI属性値に基づいて、リスクスコアの計算によって生成AIリスクが決まります。

生成AI属性に加えて、リスクスコアの計算では、以下の種類の属性を使用してアプリケーションの一般的なSaaSリスクを判断します。

- コンプライアンス属性。アプリケーションがさまざまな規制要件や標準に準拠しているかどうかを識別します。
- *ID*アクセス管理属性。アプリケーションの認証およびアクセス制御機能を識別します。
- セキュリティおよびプライバシー属性。データ保護のための製品機能を特定します。このカテゴリの属性には、アプリケーションが保存データと伝送中のデータを暗号化するかどうかなどの属性が含まれます。

生成AIアプリケーションの最終リスクスコアは、一般的なSaaSリスク(SaaS属性から計算)と生成AIリスク(生成AI属性から計算)の組み合わせです。リスクスコアの計算では、最終的なリスクスコアを決定するときに生成AIリスクに重みが付けられます。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | [アクティビティに関するインサイト]ダッシュボードに移動するには、**[Insights(インサイト)]** > [アクティビティに関するインサイト] > [アプリケーション]を選択します。

STEP 3 | テーブルで生成AIアプリケーションを探します。必要に応じて、生成AIアプリケーションのみを表示するようにテーブルをフィルタリングできます。

1. [フィルタの追加]を選択して、[生成**AI**アプリケーション]フィルタを追加します。
2. 生成**AI**アプリケーション フィルタを**TRUE**に設定します。

STEP 4 | 最大の脅威をもたらす生成AIアプリケーションを特定するには、[リスク]列のリスクスコアの値を調べます。

リスクスコア	意味
4-5	High Risk(高リスク)–リスクの可能性が高いです。
3	Medium Risk(中リスク)–中程度のリスクを表します。
1-2	Low Risk(低リスク)–リスクになる可能性は低いです。

STEP 5 | 最もリスクの高いアプリケーションに対してアクションを実行します。

たとえば、これらのアプリケーションをブロックするポリシー ルールを作成したり、Unsanctioned(未許可)としてアプリケーションにタグ付けしたりできます。

生成AIアプリにアプリケーション フィルタを使う

アプリケーション フィルタは、定義したアプリケーション属性に基づいてアプリケーションを動的にグループ化します。セキュリティ ポリシー ルールで生成AIアプリやアプリケーション グループを明示的に定義するのではなく、セキュリティ ポリシー ルールでアプリケーション フィルタを使用して、アプリケーション属性に基づいて生成AIアプリへのアクセスを制御できます。

AI Access Securityには、以下の生成AIアプリケーション フィルタが事前定義されています。事前定義済みのアプリケーション フィルタは、サポートされているAI Access Securityのユース ケースに基づいています。

- オーディオ ジェネレーター
- 会話エージェント
- コードアシスタントとジェネレーター
- 開発者プラットフォーム
- エンタープライズ サーチ
- 画像エディタとジェネレータ
- ミーティング アシスタント
- 生産性アシスタント
- 動画エディター＆ジェネレーター
- ライティング アシスタント

上記のフィルタは表示タグのみです。セキュリティ ポリシー ルールでは使用できません。

- Strata Cloud Manager:
- Panorama

Strata Cloud Manager上の生成AIアプリケーション用のアプリケーション フィルタの使用

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[Manage(管理)]** > **[Configuration(設定)]** > **[Objects(オブジェクト)]** > **[Application(アプリケーション)]** > **[Application Filters(アプリケーション フィルタ)]**を選択し、**[Add Application Filter(アプリケーション フィルタの追加)]**を選択します。

STEP 3 | 分かりやすい **Name**（名前）を入力します。

STEP 4 | タグには、**Generative AI**を選択します。

NGFWまたはPrisma Accessによって検査されるすべての生成AIアプリケーションには、検査時に`genai`タグが付けられます。生成AIアプリケーション用のカスタム アプリケーション フィルタを作成する場合、Palo Alto Networksは**Generative AI**タグを選択して、アプリケーション フィルタを追加するセキュリティ ポリシー ルールが生成AIアプリケーションのトラフィックに適用されるようにすることをお勧めします。

STEP 5 | 追加のカテゴリ フィルタを設定して、影響を受ける生成AIアプリケーションの範囲を絞り込みます。生成AIアプリケーション フィルタを作成するときは、以下のタグを考慮してください。

- リスク–セキュリティ ポリシー ルールのアクションが、選択したリスクスコアを持つ生成AIアプリケーションにのみ適用されるように、リスクスコアを指定します。

  たとえば、セキュリティ ポリシー ルールを作成して、その使用に関係なく、すべての危険な生成AIアプリケーションへのアクセスをブロックします。この場合、生成AIアプリケーション**4**および**5**のアプリケーション フィルタを作成して、セキュリティ ポリシー ルールがこれらのリスクスコアを持つ生成AIアプリケーションにのみ適用されるようにすることができます。
- タグ–セキュリティ ポリシー ルールのアクションが、**[許可]**、**[許容]**、または**[不許可]**としてタグ付けされた生成AIアプリに適用されるかどうかを指定します。さらに、生成AIアプリケーションのユースケースに基づいてタグを適用できます。

  たとえば、許可されたコードアシスタントとジェネレーター生成AIアプリケーションへのアクセスを許可するセキュリティ ポリシー ルールを作成する場合です。この場合、**[Sanctioned(許可)]**タグと**[Code Asistant & Generator(コードアシスタントとジェネレーター)]**タグの両方を含むアプリケーション フィルタを作成して、セキュリティ ポリシー ルールをこのアプリケーション タグを持つ生成AIアプリケーションに適用し、そのアプリケーションがユースケース内に収まるようにすることができます。

STEP 6 | 一致するアプリケーションのリストを確認します。

STEP 7 | **Save**（保存）を選択します。

STEP 8 | **[プッシュの構成]**と**[プッシュ]**を選択します。

STEP 9 | 「生成AIアクセスを制御するカスタム セキュリティ ポリシー ルールの作成」を行います。

Panoramaで生成AIアプリ用のアプリケーション フィルタを使用する

STEP 1 | Panorama™ management serverWebインターフェースにログインします。

STEP 2 | **[Object(オブジェクト)]** > **[Application Filters(アプリケーション フィルタ)]**を選択して新規アプリケーション フィルタを**[追加]**します。

STEP 3 | 分かりやすい **Name**（名前）を入力します。

STEP 4 | タグには、**Generative AI**を選択します。

NGFWまたはPrisma Accessによって検査されるすべての生成AIアプリケーションには、検査時に`genai`タグが付けられます。生成AIアプリケーション用のカスタム アプリケーション フィルタを作成する場合、Palo Alto Networks は**Generative AI**タグを選択して、アプリケーション フィルタを追加するセキュリティ ポリシー ルールが生成AIアプリケーションのトラフィックに適用されるようにすることをお勧めします。

STEP 5 | 追加のカテゴリ フィルタを設定して、影響を受ける生成AIアプリケーションの範囲を絞り込みます。生成AIアプリケーション フィルタを作成するときは、以下のタグを考慮してください。

- リスク–セキュリティ ポリシー ルールのアクションが、選択したリスクスコアを持つ生成AIアプリケーションにのみ適用されるように、リスクスコアを指定します。

  たとえば、セキュリティ ポリシー ルールを作成して、その使用に関係なく、すべての危険な生成AIアプリケーションへのアクセスをブロックします。この場合、生成AIアプリケーション**4**および**5**のアプリケーション フィルタを作成して、セキュリティ ポリシー ルールがこれらのリスクスコアを持つ生成AIアプリケーションにのみ適用されるようにすることができます。

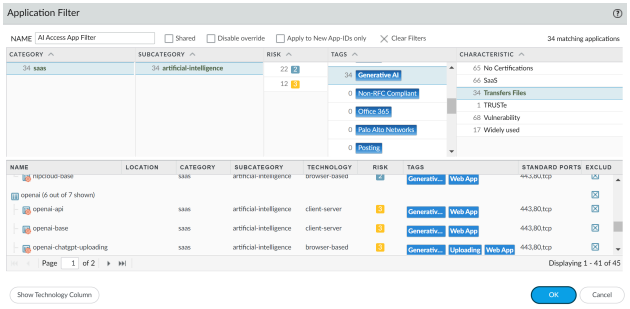
STEP 6 | 一致するアプリケーションのリストを確認します。

STEP 7 | **OK** をクリックします。

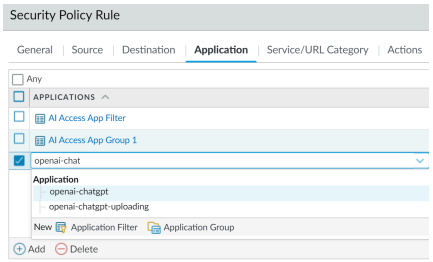
STEP 8 | **Commit (コミット)** を選択し、設定の変更を **Commit and Push (コミットおよびプッシュ)** します。

STEP 9 | 「生成AIアクセスを制御するカスタム セキュリティ ポリシー ルールの作成」を行います。

STEP 10 | 以下の例では、**AI**アクセス アプリ フィルタ アプリケーション フィルタにはカテゴリがあります:SaaS、サブカテゴリ:人工知能、タグ:生成AI、および特性:ファイルを転送します。これにより、34の一致する生成AIアプリケーションを持つフィルタが作成されます。



STEP 11 | 以下の例では、openai-chatgptがアプリケーションとして選択されています。



STEP 12 | 会話型AIに関連するCategory(カテゴリ)、Subcategory(サブカテゴリ)、Technology(テクノロジ)、Risk(リスク)、Characteristic(特性)、Tags(タグ)の各セクションから属性値を選択して、フィルタを定義します。たとえば、会話チャットに関連する値を選択すると、ダイアログの下部にある一致するアプリケーションのリストが狭まることに注意してください。フィルタの属性を調整して、安全に有効にするアプリケーションの種類と一致したら、[保存]を選択します。

デフォルトの生成AIアプリケーション アクセス ポリシー ルールを変更して生成AIアクセスを制御する

エンタープライズでの生成AIアプリケーションの使用を制御するStrata Cloud Managerに、デフォルトの生成AIアプリケーション ポリシー ルールを変更します。

- *Strata Cloud Manager*では、生成*AI*アプリケーションのセキュリティ ポリシーを使用してポリシー ルールを作成できますが、*Palo Alto Networks*は、インターネット アクセス セキュリティ ポリシー ルールを使用してポリシー ルールを効率的に作成することを推奨しています。
- *Palo Alto Networks*は、*Enterprise Data Loss Prevention (E-DLP)*ライセンスがアクティブでない場合、生成*AI*と非生成*AI*の両方のアプリケーションを同じポリシーに含めることはお勧めしません。

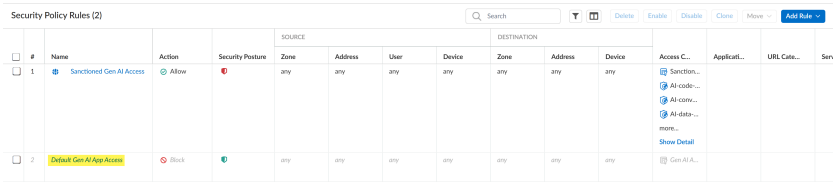
Strata Cloud Managerの場合、AI Access Securityには事前定義済みのデフォルトの生成アプリケーション アクセスが含まれており、エンタープライズで明示的に許可されていないすべての生成AIアプリケーションへのアクセスを、そのまま使用できるポリシーで制御できます。デフォルトでは、このポリシー ルールはエンタープライズ全体のすべての生成AIアプリケーションをブロックします。このポリシーを変更するには、以下の手順を実行します。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[Manage(管理)]** > **[Configuration(設定)]** > **[NGFWとPrisma Access]** > [セキュリティ サービス] > [セキュリティ ポリシー]を選択し、ターゲットの**[Configure Scope(範囲の設定)]** (生成*AI*のベストプラクティススニペット)を選択します。

STEP 3 | 事前定義済みのデフォルトの生成AIアプリケーション アクセス ポリシー ルールをクリックします。

このポリシー ルールは、すべての生成AIアプリケーションへのアクセスをブロックします。



STEP 4 | デフォルトの生成AIアプリケーション アクセス ポリシー ルールを有効にします。デフォルトで無効になっています。

STEP 5 | [Webアプリケーション]セクションで、必要に応じて[アプリケーション]および[URLカテゴリ]を設定します。デフォルトでは、デフォルトの生成AIアプリケーション アクセス ポリシー ルールは、すべての生成AIアプリケーションへのアクセスをブロックします。ただし、事前定義済みのポリシー ルールを変更して、個人、アプリケーション グループ、またはアプリケーション フィルタを選択することで、特定のアプリケーションをブロックできます。

- アプリケーション–1つ以上の生成AIアプリを追加します。
- アプリケーション グループ–アプリケーション グループは、作成する個々のアプリの静的なグループ化です。
- アプリケーション フィルター–アプリケーション フィルタは、定義したアプリケーション フィルタに基づいてアプリケーションを動的にグループ化します。

  たとえば、事前定義済みまたはカスタムの生成AIアプリケーション フィルタを使用して、個々の生成AIアプリを追加したり、変更が必要なたびに手動で更新する必要があるアプリケーション グループを作成するのではなく、組織内の生成AIアプリへのアクセスを動的に制御できます。

STEP 6 | **Save**（保存）を選択します。

STEP 7 | [プッシュの構成]と[プッシュ]を選択します。

生成AIアクセスを制御するカスタム セキュリティ ポリシー ルールの作成

カスタム セキュリティ ポリシー ルールを作成して、生成AIアプリケーションの使用を制御し、許可された生成AIアプリケーションへの機密データの流出を防ぐことができます。タグ、送信元(発信元に基づくトラフィック)、ユーザー グループ、およびその他の特定のパラメータを使用して、カスタム ポリシーを構築します。これにより、組織内の生成AIアプリケーション用にカスタマイズされたセキュリティ ポリシー ルールを適用できます。

(Strata Cloud Manager)事前定義済みの許可された生成AIへのアクセス カスタム インターネット アクセス ポリシー ルールを使用または変更するか、独自のカスタム インターネット アクセス ポリシー ルールを作成できます。

(Panorama™ management server)組織内での生成AIアプリケーションの使用を制御するセキュリティ ポリシー ルールを作成します。

許可された生成AIアプリケーションと許容された生成AIアプリケーションを未許可の生成AIアプリケーションから独立して制御するには、セキュリティ ポリシー ルールを作成する必要があります。たとえば、組織内の特定のユーザーのみがアクセスできる許容される生成AIアプリケーションがある場合、その特定のユーザーのみにアクセスを許可するセキュリティ ポリシー ルールを作成できます。Enterprise Data Loss Prevention (E-DLP)データ プロファイルをセキュリティ ポリシー ルールに関連付けて機密データの漏洩を防止し、脆弱性防御プロファイルに関連付けてシステムの欠陥を悪用したり、許可されたユーザーのシステムへの不正アクセスを阻止したりできます。さらに、ルールベースの階層の下位に2つ目のセキュリティ ポリシー ルールを作成し、他のすべてのユーザーへのアクセスを拒否します。

- *Strata Cloud Manager*では、生成*AI*アプリケーションのセキュリティ ポリシーを使用してカスタム ポリシー ルールを作成することもできますが、ポリシー ルールを効率的に作成するためには、インターネット アクセス ポリシー ルールを使用することをお勧めします。
- *Enterprise Data Loss Prevention (E-DLP)*ライセンスがアクティブになっていない場合、生成*AI*アプリケーションと生成*AI*以外のアプリケーションの両方を同じポリシーに含めることはお勧めできません。

- Strata Cloud Manager:
- Panorama

カスタム ポリシー ルールを作成して生成AIアプリケーションの使用を制御する(Strata Cloud Manager)

インターネット アクセス セキュリティ ポリシー ルールは、セキュリティ ポリシー ルールよりも先に評価され、適用されます。インターネット アクセス ポリシー ルールとセキュリティ ポリシー ルールの両方が同じトラフィックに適用される場合、インターネット アクセス ポリシー ルールのアクションと*Enterprise DLP*検査の設定がセキュリティ ポリシー ルールよりも優先されます。インターネット アクセス ポリシー ルールへの一致が成功すると、それ以降のポリシー ルールの評価は実行されません。

たとえば、ユーザー グループ*A*と複数の生成*AI*アプリケーションに適用されるインターネット アクセス ポリシー ルールとセキュリティ ポリシー ルールを作成します。

- インターネット アクセス ポリシー ルール*A*は、指定された生成*AI*アプリケーションへのユーザー グループ*A*のアクセスを許可し、機密データの漏洩を防ぐために、生成*AI*アプリケーションに関連付けられた*Enterprise DLP*データ プロファイル*A*を保有しています。
- セキュリティ ポリシー ルール*B*は、指定された同じ生成*AI*アプリケーションへのユーザー グループ*A*のアクセスをブロックします。

この場合、ユーザー グループ*A*のユーザーがインターネット アクセスおよびセキュリティ ポリシー ルールで指定された生成*AI*アプリケーションにアクセスすると、インターネット アクセス ポリシー ルール*A*の方がポリシー ルールベースの評価順序が高いため、これらのアプリケーションが許可され、*Enterprise DLP*検査と判定レンダリングが実行されます。

STEP 1 | AI Access Securityインサイト ダッシュボードを使用して生成AIアプリケーションによってもたらされるリスクを発見します。

AI Access Securityインサイト ダッシュボードは、組織全体の生成AIアプリケーションの使用に関する詳細で包括的な可視性を提供します。リスクのある生成AIアプリのユースケース、個々のリスクのある生成AIアプリケーション、および生成AIアプリにアクセスするリスクのあるユーザーを発見できます。

STEP 2 | スニペットで既存のポリシーを使用する場合は、初期AI Access Security設定を実行します。

Strata Cloud Managerでは、機密データの一致条件を定義するためのEnterprise Data Loss Prevention (E-DLP)データ プロファイルの作成、事前定義済みの生成AIベストプラクティスおよびアプリケーション タグ付けのスニペットの関連付け、システムの欠陥を悪用する試みやシステムへの不正アクセスを阻止するために使用される脆弱性防御プロファイルの作成が含まれます。

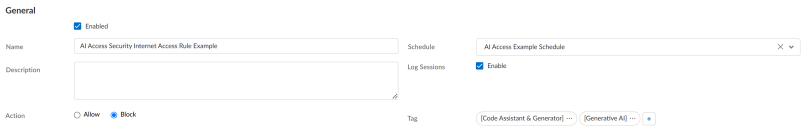
NGFWの場合、内部トラスト ゾーンとアウトバウンド アントラスト ゾーンの作成も含まれます。

STEP 3 | 独自のカスタム ポリシーを構築する場合は、Strata Cloud Managerにログインします。

STEP 4 | カスタム インターネット アクセス ポリシー ルールを作成します。

- *Strata Cloud Manager*では、生成*AI*アプリケーションのセキュリティ ポリシーを使用してカスタム ポリシー ルールを作成することもできますが、ポリシー ルールを効率的に作成するためには、インターネット アクセス ポリシー ルールを使用することをお勧めします。
- *Enterprise Data Loss Prevention (E-DLP)*ライセンスがアクティブになっていない場合、生成*AI*アプリケーションと生成*AI*以外のアプリケーションの両方を同じポリシーに含めることはお勧めできません。

1. [ルールの追加] > [インターネット アクセス ルール]を選択します。
2. インターネット アクセス ポリシー ルールを有効にします。
3. 分かりやすい **Name**（名前）を入力します。
4. (任意)インターネット アクセス ポリシー ルールの[説明]を追加し、事前定義済みのタグを追加するか、新しいタグを作成します。
5. [アクション]を設定します(ブロックまたは許可)。
6. (任意)**[Schedule(スケジュール)]**を設定して、インターネット アクセス ポリシー ルールがアクティブになる時間を指定します。



7. [一致条件]セクションで、トラフィックの[送信元](由来元)に基づいて適用するトラフィックを定義します。

   たとえば、リスク検出の調査に基づいて、ユーザー グループAに関連付けられた不正なユーザーが、ユーザー グループBによって使用が許可された生成AIアプリケーションにアクセスするかどうかを判断します。この場合、生成AIへのアクセスをブロックす

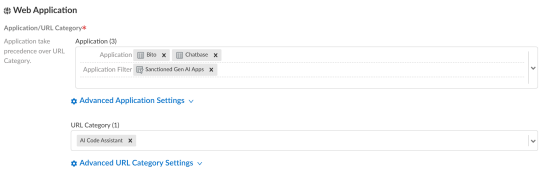
るインターネット アクセス ポリシー ルールを作成し、ユーザー　グループAをユーザー グループ[送信元]として追加できます。

8. [Webアプリケーション]セクションで、[アプリケーション]または[URLカテゴリ]を設定し、アクセスをブロックまたは許可する生成AIアプリケーションまたは生成AIアプリケーションのURLを定義します。

   (許可された生成AIアプリケーション)サポートされている生成AIアプリケーションのみを許可されたアプリケーションのリストに追加します。

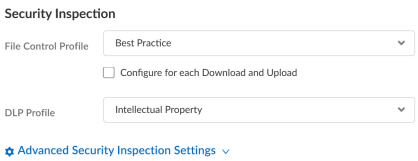
   - アプリケーション–1つ以上の生成AIアプリを追加します。
   - アプリケーション グループ–アプリケーション グループは、作成する個々のアプリの静的なグループ化です。
   - アプリケーション フィルター–アプリケーション フィルタは、定義したアプリケーション フィルタに基づいてアプリケーションを動的にグループ化します。

     たとえば、事前定義済みまたはカスタムの生成AIアプリケーション フィルタを使用して、個々の生成AIアプリを追加したり、変更が必要なたびに手動で更新する必要があるアプリケーション グループを作成するのではなく、組織内の生成AIアプリへのアクセスを動的に制御できます。



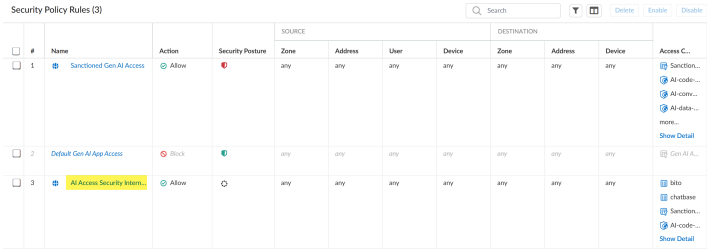
9. (許可された生成AIアプリケーション)[セキュリティ検査]セクションで、機密データの漏洩を防止するファイル ブロックおよびEnterprise DLPプロファイルを選択します。

   - ファイル制御プロファイル–ファイル ブロッキング プロファイルは、ブロックまたは監視する特定のファイル タイプを識別することができます。カスタム ファイル ブロック プロファイルを作成するか、デフォルトのベストプラクティス ファイル ブロック プロファイルを使用できます。
   - **DLP**プロファイル–Enterprise DLPデータ プロファイルを使用すると、機密データの流出を防ぐために検査およびブロックする機密データの一致条件を定義できます。生成AIアプリケーションのリスクを検出する場合は、機密アセット データを生成するデータ プロファイルを割り当てる必要があります。



10. 必要に応じて、残りのカスタム インターネット アクセス ポリシー ルールを設定します。
11. **Save**（保存）を選択します。

STEP 5 | アクセス ポリシー ルールが正常に作成されたことを確認し、必要に応じてポリシー ルール ベース内で順序を付けます。



STEP 6 | [プッシュの構成]と[プッシュ]を選択します。

カスタム ポリシー ルールを作成して生成AIアプリケーションの使用を制御する(Panorama)

STEP 1 | AI Access Securityインサイト ダッシュボードを使用して生成AIアプリケーションによってもたらされるリスクを発見します。

AI Access Securityインサイト ダッシュボードは、組織全体の生成AIアプリケーションの使用に関する詳細で包括的な可視性を提供します。リスクのある生成AIアプリのユースケース、個々のリスクのある生成AIアプリケーション、および生成AIアプリにアクセスするリスクのあるユーザーを発見できます。

STEP 2 | 初期AI Access Security設定を実行します。

これには、機密データの一致条件を定義するためのEnterprise Data Loss Prevention (E-DLP)データプロファイルの作成と、システムの欠陥を悪用したり、システムへの不正アクセスを試みたりするのを防ぐために使用される脆弱性防御プロファイルの作成が含まれます。

NGFWの場合、内部トラスト ゾーンとアウトバウンド アントラスト ゾーンの作成も含まれます。

STEP 3 | Panorama™ management serverWebインターフェースにログインします。

STEP 4 | **[Policies (ポリシー)]** > **[Security (セキュリティ)]**を選択し、[Device Group (デバイス グループ)]を指定します。

STEP 5 | セキュリティ ポリシー ルールを追加します。

STEP 6 | セキュリティ ポリシー ルール **[General(全般)**、**[Source(送信元)]**、および**[Destination(宛先)]**を設定します。

セキュリティ ポリシー ルールの作成に関する詳細情報は、セキュリティ ポリシー管理ガイドを参照してください。

- **[General(一般)]**–セキュリティ ルールに分かりやすい名前を付けます。セキュリティ ポリシー ルールに対して**[Description(説明)]**を提供し、セキュリティ ポリシー ルールの目的を特定するのに役立つタグを適用するオプションもあります。
- **[Source(送信元)]**–セキュリティ ポリシー ルールが適用されるためにトラフィックがどこから発生する必要があるかを定義します。

  [Source Zone(ソースゾーン)]の場合、内部トラスト ゾーンを選択できます。トラフィックの発信元に関係なく、すべてのトラフィックにセキュリティ ポリシー ルールを適用したい場合は、すべての送信元設定に対して**[Any(任意)]**を選択します。

  たとえば、リスク発見評価に基づいて、生成AIアプリケーションへのアクセスが過剰に提供されており、特定のユーザーに絞る必要があると判断します。この場合、許可ポリシー ルールを作成し、必要な送信元ユーザーを追加できます。
- 宛先–セキュリティ ポリシー ルールが適用されるトラフィックのターゲット宛先を定義します。

  宛先ゾーンの場合、アウトバウンド アントラスト ゾーンを選択できます。トラフィックの宛先に関係なく、すべてのトラフィックにセキュリティ ポリシー ルールを適用したい場合は、すべての宛先設定に対して任意を選択します。

STEP 7 | アプリケーションの設定で、生成AIアプリケーション グループ、アプリケーション フィルタ、またはアプリケーションを指定します。

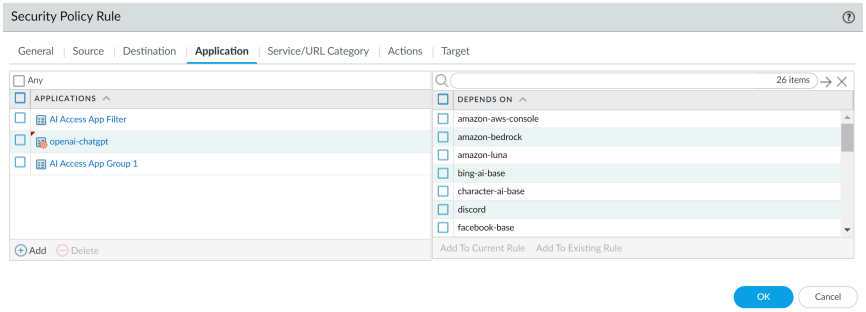
(許可されたWebアプリケーション)サポートされている生成AIアプリのみを許可されたアプリのリストに追加します。

- アプリケーション–1つ以上の生成AIアプリを追加します。
- アプリケーション カテゴリ–アプリケーション フィルタと呼ばれるアプリケーション カテゴリは、定義したアプリケーション フィルタに基づいてアプリケーションを動的にグループ化します。

  たとえば、事前定義済みまたはカスタムの生成AIアプリケーション フィルタを使用して、個々の生成AIアプリを追加したり、変更が必要なたびに手動で更新する必要があるアプリ

ケーション グループを作成するのではなく、組織内の生成AIアプリへのアクセスを動的に制御できます。

- アプリケーション グループ–アプリケーション グループは、作成する個々のアプリの静的なグループ化です。



STEP 8 | セキュリティ ポリシー ルール アクションを設定します。ポリシー ルールに対してどのアクションを実行するかを決定します。ベストプラクティスとして、セキュリティ プロファイルを付与し、その脅威に関して許可されているすべてのトラフィックをファイアウォールがスキャンできるようにします。**[Profile Type(プロファイル タイプ)]**ドロップダウンから**[Profile(プロファイル)]**を選択し、そのルールに付与する個々のセキュリティ プロファイルを選択します。生成AIアプリケーションの以下の設定に必要なアクションを選択します:

1. **[Action(アクション)]**について、**[Source(送信元)]**から**[Destination(宛先)]**へのセキュリティ ポリシー ルールNGFWが検出されたときに、[Action(アクション)]を設定します。

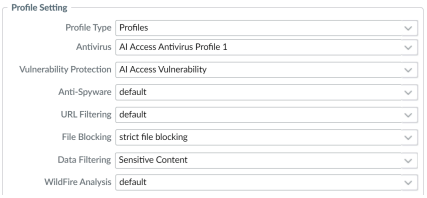
   たとえば、1つ以上の生成AIアプリケーションへのアクセスを許可したい場合は**[許可]**を選択し、1つ以上の生成AIアプリケーションへのすべてのアクセスをブロックしたい場合は**[拒否]**を選択します。

2. **[プロファイル タイプ]**で**[プロファイル]**を選択します。

   最低限、**[脆弱性防御]**と**[データ フィルタリング]**のプロファイルを追加する必要があります。これらは、生成AIアプリケーションによってもたらされるリスクを発見する際に脅威と機密アセットデータを生成するために必要です。残りのプロファイルはオプションであり、必要に応じて設定できます。以下の各セキュリティ プロファイル タイプについて、既存のプロファイルを選択するか、新しいプロファイルを作成できます。

   - Antivirus（アンチウイルス）
   - 脆弱性防御
   - アンチスパイウェア
   - URL フィルタリング
   - ファイルブロッキング
   - データのフィルタリング

- WildFire分析



*[アクション]*タブでは、*[プロファイル設定]*が*[アクション設定]*よりも優先されます。したがって、ベストプラクティスとして、両方の設定が適切に一致していることを確認してください。たとえば、アクション設定が*[許可]*で、プロファイル設定の*1*つが*ChatGPT*に対してブロックであっても、ブロックされます。

STEP 9 | 新しい設定を管理対象ファイアウォールにコミットしてプッシュし、Enterprise DLPプラグインのインストールを完了します。

この手順は、Enterprise DLPデータ フィルタリング プロファイル名をデータ フィルタリング ログに表示するために必要です。

コミットしてプッシュコマンドは、*Enterprise DLP*の設定変更には推奨されません。コミットしてプッシュコマンドを使用するには、影響を受けるテンプレートと管理対象ファイアウォールを手動で選択するという追加の不要なオーバーヘッドが必要です。

- **Panorama**からの完全な設定プッシュ
  1. **[Commit (コミット)] > [Commit to Panorama(Panorama**へのコミット**)] [Commit(**コミット**)]**を選択します。
  2. **[Commit**（コミット）**] > [Push to Devices**（デバイスへのプッシュ）**]**の順に選択し、**[Edit Selections**（選択内容の編集）**]**を行います。
  3. **Device Groups (**デバイス グループ**)** を選択して、（ **Include Device and Network Templates** ネットワークのテンプレートを含める**)** を実行します。
  4. **OK** をクリックします。
  5. Enterprise DLPを使用している管理対象ファイアウォールに設定の変更をプッシュします 。
- **Panorama**からの部分的な設定プッシュ

  部分的な設定プッシュを行う際には、常に一時的な*__dlp*管理者を含める必要があります。これは、*Panorama*と*DLP*クラウド サービスを同期させるために必要です。

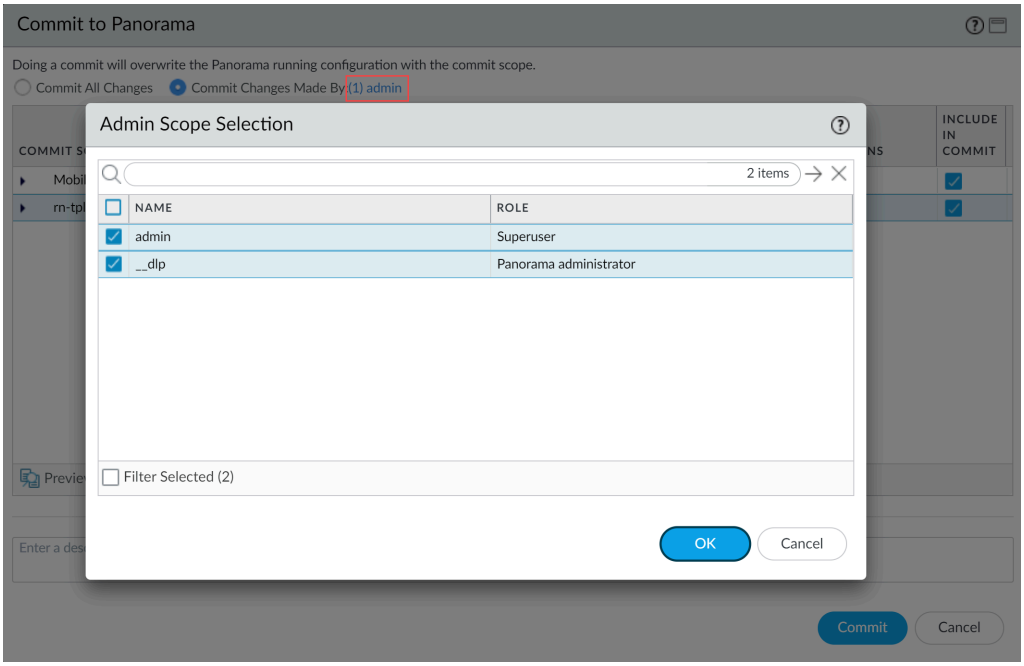
  たとえば、設定変更をコミットしてプッシュすることが許可されている*admin*Panorama管理ユーザーがいます。*admin*ユーザーは*Enterprise DLP*設定に変更を加え、これらの変更をマネージドファイアウォールにのみコミットしてプッシュしたいと考えています。この場合、*admin*ユーザーは部分的なコミットおよびプッシュ操作で*__dlp*ユーザーも選択する必要があります。

  1. **[Commit(**コミット**)] > [Commit to Panorama(Panorama**にコミット**)]**を選択します。
  2. **[**指定対象による変更のコミット**]**を選択し、次に現在のPanorama管理ユーザーをクリックして部分的なコミットに含める追加の管理者を選択します。

     この例では、adminユーザーが現在ログインしており、コミット操作を行っています。adminユーザーは**admin**をクリックし、次に__dlpユーザーを選択する必要があり

ます。他のPanorama管理者によって行われた追加の設定変更がある場合、ここでも選択できます。

[OK] クリックして続行します。

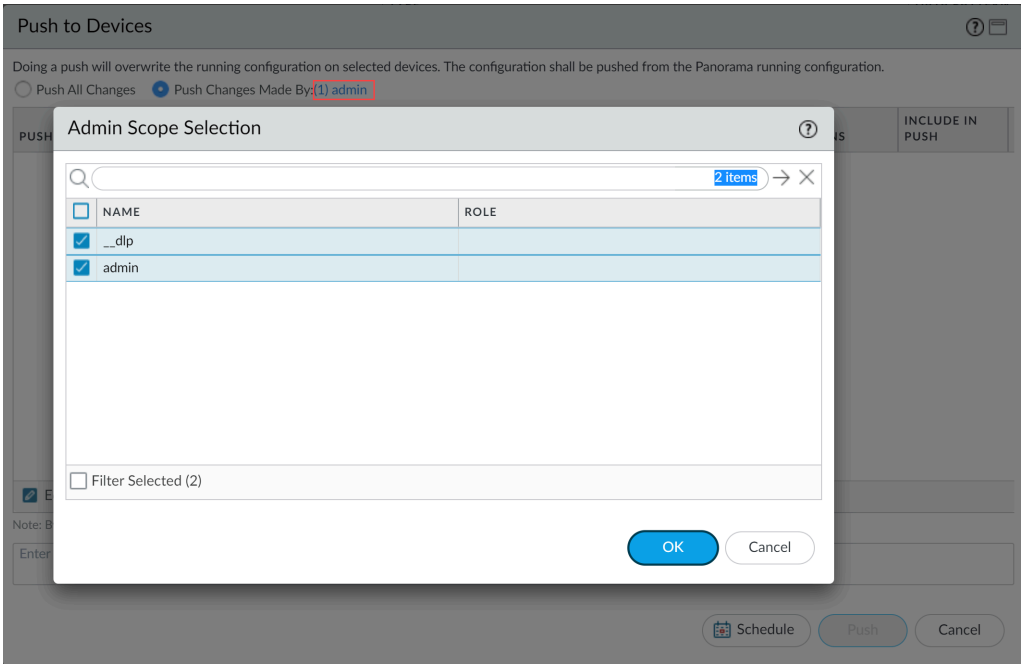


3. [コミット] します。
4. [コミット] > [デバイスにプッシュ]を選択します。
5. [変更のプッシュ作成者]を選択し、次に現在のPanorama管理ユーザーをクリックして部分的なプッシュに含める追加の管理者を選択します。

   この例では、`admin`ユーザーが現在ログインしており、プッシュ操作を行っています。`admin`ユーザーは**admin**をクリックし、次に`__dlp`ユーザーを選択する必要があり

ます。他のPanorama管理者によって行われた追加の設定変更がある場合、ここでも選択できます。

[OK] クリックして続行します。



6. **Device Groups (**デバイス グループ**)** を選択して、（ **Include Device and Network Templates** ネットワークのテンプレートを含める**)** を実行します。
7. **OK** をクリックします。
8. Enterprise DLPを使用している管理対象ファイアウォールに設定の変更をプッシュします 。

AI Access Securityの推奨事項

ネットワーク セキュリティ管理者は、AI Access Securityダッシュボードと Strataコマンド センターを使用して、組織ネットワーク上の生成AIアプリケーションの使用状況に関する貴重なデータを得ることができます。ネットワーク セキュリティ管理者が生成AIアプリケーションの採用時にギャップに迅速に対応し、セキュリティ態勢を強化できるように、Palo Alto NetworksはAI Access Securityの推奨事項を導入します。

AI Access Securityは、手動および自動の推奨事項を提供します。手動による推奨事項は、手動で実装する必要があります。AI Access Securityでは、手順を追った説明と、推奨される変更を正常に実装するためのすべての関連ドキュメントへのリンクを提供しています。Palo Alto Networks Copilot on Strata Cloud Managerは、管理者ではなく、自動化された推奨事項を実装しています。ただし、AI Access Securityが提案した推奨事項を開始した管理者は、すべての変更を承認する必要があります。

- **NGFW**と**Prisma Access**に対する推奨事項**(Strata Cloud Manager**による管理**)**—AI Access Securityの推奨事項は、管理者が設定を変更し、AI Access Securityがネットワーク上のトラフィックを分析したときにリアルタイムで更新されます。これにより、すぐに対処しなければ組織を危険にさらす可能性のある設定変更やリスクのある生成AIアプリケーション トラフィックに迅速に対応できます。ネットワーク上のトラフィックを分析する推奨事項には、推奨事項を通知する7日間の振り返り期間があります。

  NGFWとPrisma Access(Strata Cloud Managerによる管理)およびPrisma Access Browserがある場合、AI Access SecurityはNGFWとPrisma Accessテナントに対してのみ推奨事項を表示します。この場合、AI Access SecurityはPrisma Access Browserの推奨事項を表示しません。

- **NGFW**と**Prisma Access**に対する推奨事項**(Panorama**による管理**)**—AI Access Securityの推奨事項は24時間ごとにStrata Cloud Managerで更新されます。

  NGFWとPrisma Access(Panoramaによる管理)およびPrisma Access Browserがある場合、AI Access SecurityはNGFWとPrisma Accessテナントに対してのみ推奨事項を表示します。この場合、AI Access SecurityはPrisma Access Browserの推奨事項を表示しません。

- **Prisma Access Browser**の推奨事項—AI Access Securityの推奨事項は静的であり、実装後も維持されます。Palo Alto Networksは、セキュリティ管理者が生成AIアプリケーションの採用戦略のギャップに対処できるように、実装後もこれらの推奨事項を監視し続けることをお勧めします。

  AI Access Securityは、スタンドアロンのPrisma Access Browserライセンスがあり、NGFWまたはPrisma Accessテナントがデプロイされていない場合にのみ、Prisma Access Browserの推奨事項を表示します。

  NGFWとPrisma Access(PanoramaまたはStrata Cloud Managerによる管理)およびPrisma Access Browserがある場合、AI Access SecurityにはNGFWとPrisma Accessテナントの推奨事項のみが表示されます。この場合、AI Access SecurityはPrisma Access Browserの推奨事項を表示しません。

AI Access Securityは、以下のシナリオの推奨事項を提供します。

- 生成**AI**アプリケーション分類の推奨事項

  ネットワーク上の生成AIアプリケーションの使用状況とそのアプリケーション分類(許可、許容、未許可)に基づく推奨事項の提供に焦点を当てています

  たとえば、AI Access Securityが、未許可の生成AIアプリケーションへのトラフィックを許可していることに気付いたとします。この場合、AI Access Securityはこれらの生成AIアプリケーションを許可または許容として再分類するための推奨事項を提供します。

- ベストプラクティスのチェックとポリシーの推奨事項

  AI Access Securityは、ベストプラクティス評価(BPA)サービスを使用して、既存のNGFWおよびPrisma Accessポリシー ルールベースを分析し、生成AIアプリケーションを安全に採用するためのセキュリティ態勢を強化するための推奨事項を提供します。

  たとえば、未許可の生成AIアプリケーションへのアクセスを許可するセキュリティ ポリシー ルールがあることをBPAサービスが検出した場合です。

- データ損失防止の推奨事項

  許可された生成AIアプリケーションや許容された生成AIアプリケーションへの機密データの流出を防ぐために、AI Access Securityはセキュリティ ポリシー ルールを分析して、トラフィックをEnterprise DLPに転送してインライン検査を行っているのか、それとも保存データ用に転送しているのかを判断します。これには、トラフィックをEnterprise DLPに転送するために必要な設定の推奨事項も含まれます

- **AI Access Security**のオンボーディングと最大化

  これらは、プラットフォーム全体で機能を活用するための実用的な推奨事項を提供することに重点を置いています。これらの推奨事項は、さまざまなマーケットプレースへのユーザー接続、または保存データ用にサポートされている生成AIアプリケーションに重点を置いています。

- **Prisma Access Browser**の推奨事項

  Prisma Access Browserの推奨事項は、Prisma Access Browserスタンドアロン ユーザーが生成AIアプリケーションの使用を保護および最適化できるように、ターゲットを絞ったガイダンスを提供することに重点を置いています。これらの推奨事項には、生成AIアプリケーション アクセスの設定、事前定義済みのセキュリティ ポリシー ルールのアクティブ化によるPrisma Access Browser経由でアクセスされる生成AIアプリケーションへのアクセスの保護、未許可の生成AIアプリケーションへの機密データの流出の疑わしいインシデントのレビューなどがあります。

AI Access Securityレポートを生成する

AI Access Securityレポートは、組織の生成AIアプリケーションとプラグインの使用とセキュリティ態勢に関する包括的な概要を提供します。このレポートは、お客様の環境で急速に進化する生成AIアプリケーションに関連するリスクを把握および管理するのに役立ちます。実用的なインサイトとカスタマイズされた推奨事項が詰まったこのレポートにより、セキュリティ管理者は生成AIアプリケーションの導入戦略とセキュリティについて、十分な情報に基づいた意思決定を行うことができます。

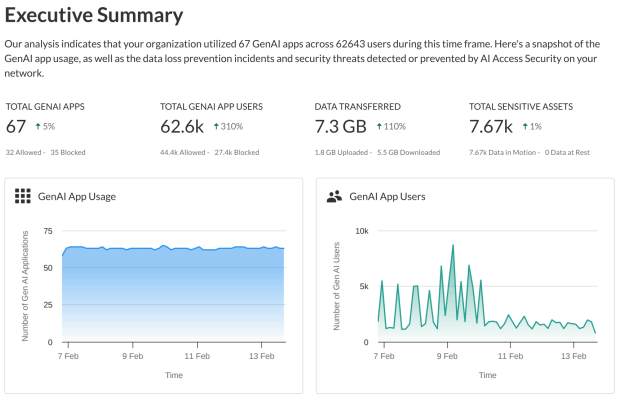
AI Access Securityレポートの主な構成要素は次のとおりです。

- エグゼクティブ概要

  エグゼクティブ概要セクションには、組織内の主要な生成AIアプリケーションとプラグインメトリックの大まかなスナップショットが表示されます。以下の概要を簡潔に説明しています:

  - 生成AIアプリケーションの使用状況。組織内のユーザーがこれらのアプリにどの程度幅広くアクセスしているかをすぐに把握できます。
  - 生成AIアプリケーションからアップロードおよびダウンロードされるデータ量(GB単位)。
  - 移動中および静止中のデータについて検出された機密データアセットの数。

  エグゼクティブ概要セクションでは、セキュリティ管理者が組織内の生成AIアプリケーションの状況を一目で把握できます。レポートの以降のセクションで提供されるより詳細な情報への入り口として機能し、セキュリティ管理者は組織の生成AIセキュリティ態勢全体をすばやく把握して、さらに注意や調査が必要な領域を特定できます。

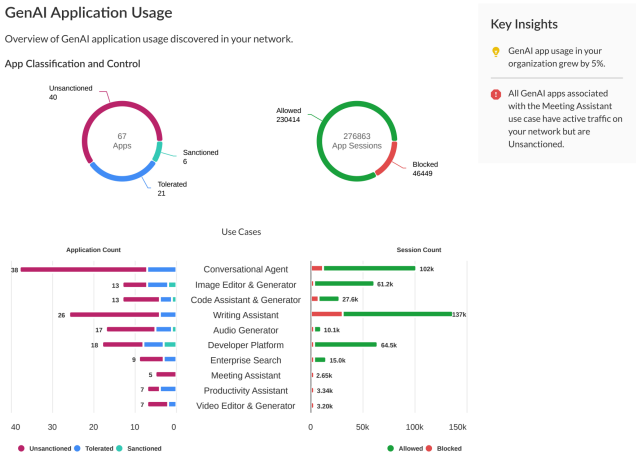


- 生成**AI(GenAI)**アプリケーションの使用状況

  生成AIアプリケーションの使用状況セクションには、組織内の生成AIアプリの使用状況の包括的な内訳が表示されます。以下が含まれます:

  - 生成AIアプリの総数。生成AIアプリケーションの許可とブロック、および許可、許容、未許可の生成AIアプリの分布を示します。
  - 生成AIのユースケースの内訳。アプリケーションの分類(許可、許容、未許可)と、トラフィックが許可またはブロックされたかどうかで分類されます。
  - 未許可(Unsanctioned)だが許可された(Allowed)アプリケーション数(報告期間開始以降の変更を含む)。
  - 未許可(Unsanctioned)だが許可されている(Allowed)生成AIアプリケーションの使用データを集計し、ユーザー数やデータ転送量の合計などを表示します。
  - アプリケーション名、ユーザー数、セッション数、関連するリスク要因など、未許可(Unsanctioned)だが許可されている(Allowed)生成AIアプリケーションの上位5件の詳細。

  このセクションは、セキュリティ管理者が潜在的なセキュリティ リスクを迅速に特定し、さまざまなユースケースにおける生成AIアプリケーションの使用率を把握し、アプリケーションの使用ポリシー ルールとセキュリティ態勢について十分な情報に基づいて意思決定を行うのに役立ちます。

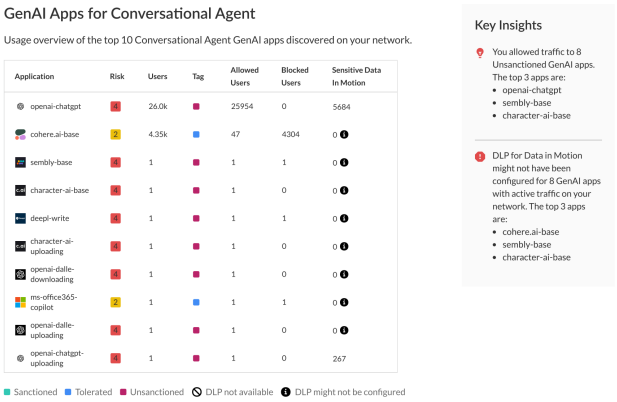


- 主なユースケース向けの生成**AI**アプリケーション

  [GenAI App for Top Uses(トップユースの生成AIアプリケーション)]セクションでは、組織内で使用している生成AIアプリケーションの上位10件を生成AIアプリケーションのユースケー

スごとにまとめています。組織内で使用されている最も著名な生成AIアプリケーションの詳細な内訳を提供しており、生成AIアプリケーションごとに以下の内容が含まれています。

- 使用する生成AIアプリケーションの名前。
- 生成AIアプリケーションに関連するリスクスコア。
- 生成AIアプリケーションを利用したユニークユーザー数。
- 生成AIアプリケーションの分類。アプリが許可済みか、許容済みか、未許可かを示します。
- 生成AIアプリケーションで許可およびブロックされた一意のセッション数。
- 生成AIアプリケーションにアクセスするユーザーが生成したEnterprise DLPインシデントの数。



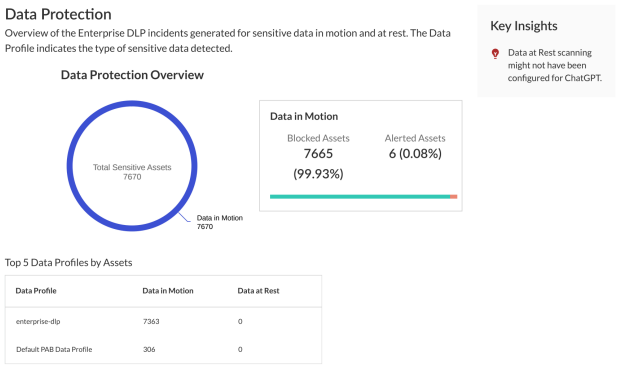
- データ保護

  データ保護セクションは、組織の生成AIエコシステム内の機密データの取り扱いに関する重要なインサイトを提供します。このセクションでは、次の内容について説明します。

  - 検出された機密アセットの総数で、許可またはブロックに分類されます。
  - 機密アセットタイプごとにグループ化したすべての生成AIアプリケーションの機密アセットの分散。
  - トップ5の生成AIアプリケーションに含まれる機密データの詳細情報。

  この情報は、セキュリティ管理者が組織内の生成AIアプリケーションの使用に関連する潜在的なデータ セキュリティ リスクを迅速に特定するのに役立ちます。どの生成AIアプリケーションが機密情報を処理し、どの種類の機密データが処理されているかを強調することで、

データ保護の取り組みに優先順位を付け、必要に応じてセキュリティ ポリシー ルールを調整できます。



STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[インサイト] > [セキュリティ] > [AIアクセス]**を選択します。

STEP 3 | AI Access Securityレポートのタイム フレームを選択します。

AI Access Securityは、過去**24**時間、過去**7**日間、または過去**30**日間のレポートの生成をサポートしています。

STEP 4 | PDF形式のAI Access Securityレポートをローカルデバイスにダウンロードします。

デフォルトのファイル名は「`AI Access Security Report<generation-date>.pdf`」です。

*AI Access Security*レポートのダウンロードが完了する前に、ページを離れたり更新したりしないでください。ダウンロードが完了する前にページを離れたり更新したりすると、ダウンロードが中断され、*AI Access Security*レポートを再度ダウンロードする必要があります。

STEP 5 | 選択したダウンロードフォルダに移動し、AI Access Securityレポートを確認します。