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

发现 GenAI App 带来的风险

使用 AI Access Security Insights 仪表板过滤网络上的生成 AI (GenAI) app 使用情况。AI Access Security Insights 仪表板提供深入的详细信息，帮助您了解哪些 GenAI app 正在被使用以及由谁使用。

AI Access Security 根据以下过滤器检测 **Allowed Users**（允许的用户）数据、**Blocked Users**（被阻止用户）数据或两者。

- **1** 小时和 **3** 小时

  用户可被计为 Allowed（允许）、Blocked（被阻止）或两者。

  例如，`UserA` 因应有的策略规则 `1` 而无法访问 `GenAI-App1`。一小时后，`UserA` 将前往策略规则 `2` 允许访问 `GenAI-App1` 的分支机构。在此情况下，`UserA` 同时显示在 **Allowed Users**（允许用户） 和 **Blocked Users**（被阻止用户）的计数中。

  相反，策略规则 `1` 阻止 `UserA` 访问 `GenAI-App1`。几分钟后，您的安全管理员修改策略规则 `1` 以允许 `UserA` 访问。在这种情况下，`UserA` 会显示在 **Blocked Users**（被阻止用户）计数中。AI Access Security 会将用户显示在 **Blocked Users**（被阻止用户）计数中，无论您在过去 **1 Hour**（**1** 小时）或 **3 Hours**（**3** 小时）期间允许访问多少次，只要他们符合相同的安全策略规则并且至少被阻止访问过一次。
- **24** 小时、**7** 天和 **30** 天

  用户可被计为 Allowed（允许）、Blocked（被阻止）或两者。

  例如，您最初阻止 `UserA` 访问 `GenAI-App1`。六小时后，`UserA` 前往策略规则 `2` 允许访问 `GenAI-App1` 的分支机构。在此情况下，`UserA` 同时显示在 **Allowed Users**（允许用户） 和 **Blocked Users**（被阻止用户）的计数中。

通过用例发现 GenAI App 带来的风险

查看支持的用例，了解 GenAI app 所属的所有用例类别的完整描述。

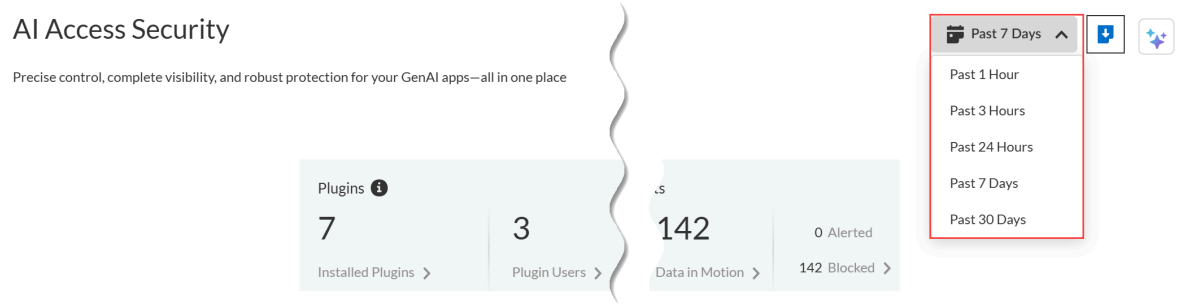
STEP 1 | 登录 Strata Cloud Manager

STEP 2 | 选择 **Insights** > **AI Access** 以查看 AI Access Security Insights 仪表板。

AI Access Security Insights 仪表板默认按用例显示 GenAI app 在您网络上的使用情况，以及以下有关 GenAI 主要用例的高层级信息：

- 时间筛选程序

  过滤 GenAI 用例细分，选择您想要调查的时间段。您可以选择 **Past 1 Hour**（过去 **1** 小时）、**Past 3 Hours**（过去 **3** 小时）、**Past 24 Hour**（过去 **24** 小时）、**Past 7 Days**（过去 **7** 天）或 **Past 30 Days**（过去 **30** 天）。



- 检测到威胁

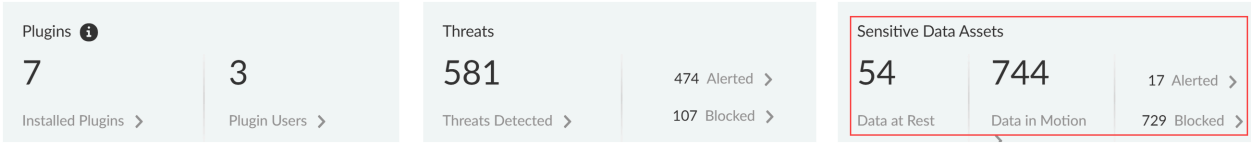
  威胁由附加到 Web 安全策略规则的 漏洞保护配置文件 检测。此配置文件可检测恶意和网络钓鱼网址、恶意文件或恶意软件等威胁。**Threats Detected**（检测到的威胁） 汇总了所有 GenAI app 和执行点中的所有威胁。

  - **Alerted**（已警报）— 检测到的发出警报的威胁总数。
  - **Blocked**（已阻止）— 检测到的威胁总数，已被您的 NGFW 或 Prisma Access 个租户拦截。

- 敏感数据资产

  敏感数据资产显示当流量符合您的 Enterprise Data Loss Prevention (E-DLP) 数据配置文件中静态数据 (Data Security) 和动态数据 (SaaS Security Inline) 的匹配条件时检测到的敏感数据事件数量。

  - **Data at Rest**（静态数据）— 通过 SaaS API (Data Security) 强制执行渠道生成警报或被阻止的 DLP 事件 总数。
  - **Data in Motion**（动态数据）— 通过SaaS Security Inline强制执行通道触发警报或被阻止的 DLP 事件总数。
  - **Alerted**（已警报）— 同时对静态数据和动态数据触发警报的 DLP 事件总数。
  - **Blocked**（已阻止） - 您的 NGFW 或 Prisma Access 租户阻止的 DLP 事件总数，包括静态数据和动态数据。

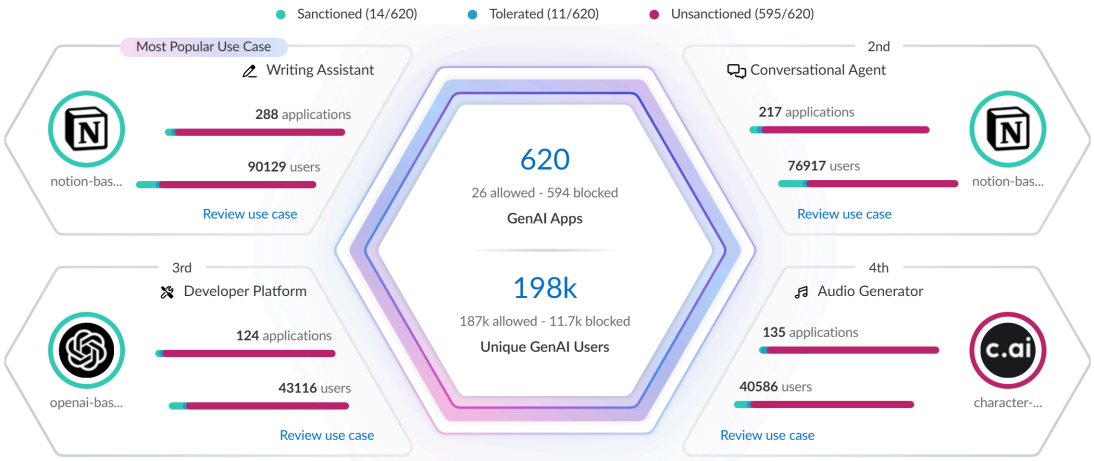


- 热门用例

  AI Access Security Insights 仪表板根据您网络上的活动动态显示前四个 GenAI app 用例，以及在选定时间段内访问过任何 GenAI 的 GenAI qpp 和用户总数。这样一来，您可以快速调查与最常用的 GenAI app 相关的安全事件，并实施访问控制策略规则。

  - **GenAI Apps** — 属于特定用例的 GenAI app 的总数。GenAI app 的总数分为三类 — 已认可、可容忍和未认可的 GenAI app。
  - **Unique GenAI Users**（唯一 **GenAI** 用户）— 访问属于特定用例的任何 GenAI app 的用户总数。单击 **Unique GenAI Users**（唯一 **GenAI** 用户）计数，查看每个被阻止访问 GenAI app 的唯一用户的列表。

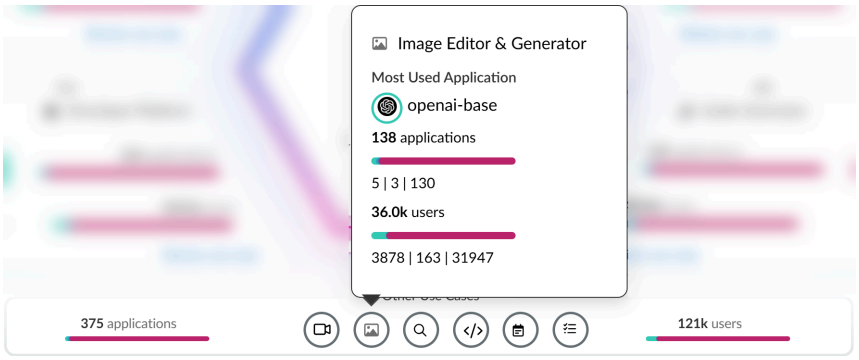
    AI Access Security 会在设定的时间间隔内自动汇总 ***Unique GenAI Users***（唯一 ***GenAI*** 用户）总数，并在您点击 ***Unique GenAI Users***（唯一 ***GenAI*** 用户）计数时立即生成用户列表。这可能会导致 ***Unique GenAI Users***（唯一 ***GenAI*** 用户）计数与列表计数略有不同。



- 所有其他用例

  - **Applications**（应用程序）— 属于任何其他 GenAI app 用例的 GenAI app 总数。GenAI app 的总数分为三类 — 已认可、可容忍和未认可的 GenAI app。
  - **Users**（用户）— 访问过任何符合其他 GenAI app 用例的 GenAI app 的用户总数。

  将鼠标悬停在每个用例上，查看与用例关联的 GenAI app 使用情况的摘要信息。



STEP 3 | **Review use case**（查看用例），以查看您感兴趣的用例中所有已认可、可容忍和未认可的 GenAI app 的详细分类。

STEP 4 | 查看用例详细信息页面，了解 GenAI app 使用情况。

用例详细信息页面提供有关 GenAI app 使用情况的粒度数据。您可以利用这些信息来了解 GenAI app 的使用情况，从而帮助您了解安全管理员需要编写哪些策略规则来加强安全态势。这样可以确保您的组织安全地采用 GenAI app，并防止敏感数据外泄。

- 用例摘要

  用例摘要汇总了您正在调查的用例的所有重要 GenAI app 使用信息。

  - 最常用应用程序— 针对该用例最常用的 GenAI app。这还包括当前分配给 GenAI app 的应用标签（**Sanctioned**（已认可）、**Tolerated**（可容忍） 或 **Unsanctioned**（未认可））。
  - **Application Breakdown**（应用程序细分）— 与用例关联的 GenAI app 总数的汇总，以及所有检测到的 GenAI app 的应用标签的汇总。
  - **User Breakdown**（用户细分）— 访问与用例相关的任何 GenAI app 的用户总数的汇总。此外，还提供了访问 **Sanctioned**（已认可）、**Tolerated**（可容忍） 或 **Unsanctioned**（未认可）GenAI app 的用户数量的汇总信息。

- 应用程序

  用户访问的与该用例相关的所有 GenAI app 列表。您可以对 GenAI app 用例应用 **Sort By**（排序依据）过滤器，按 **User Count**（用户数）、**Threats Count**（威胁

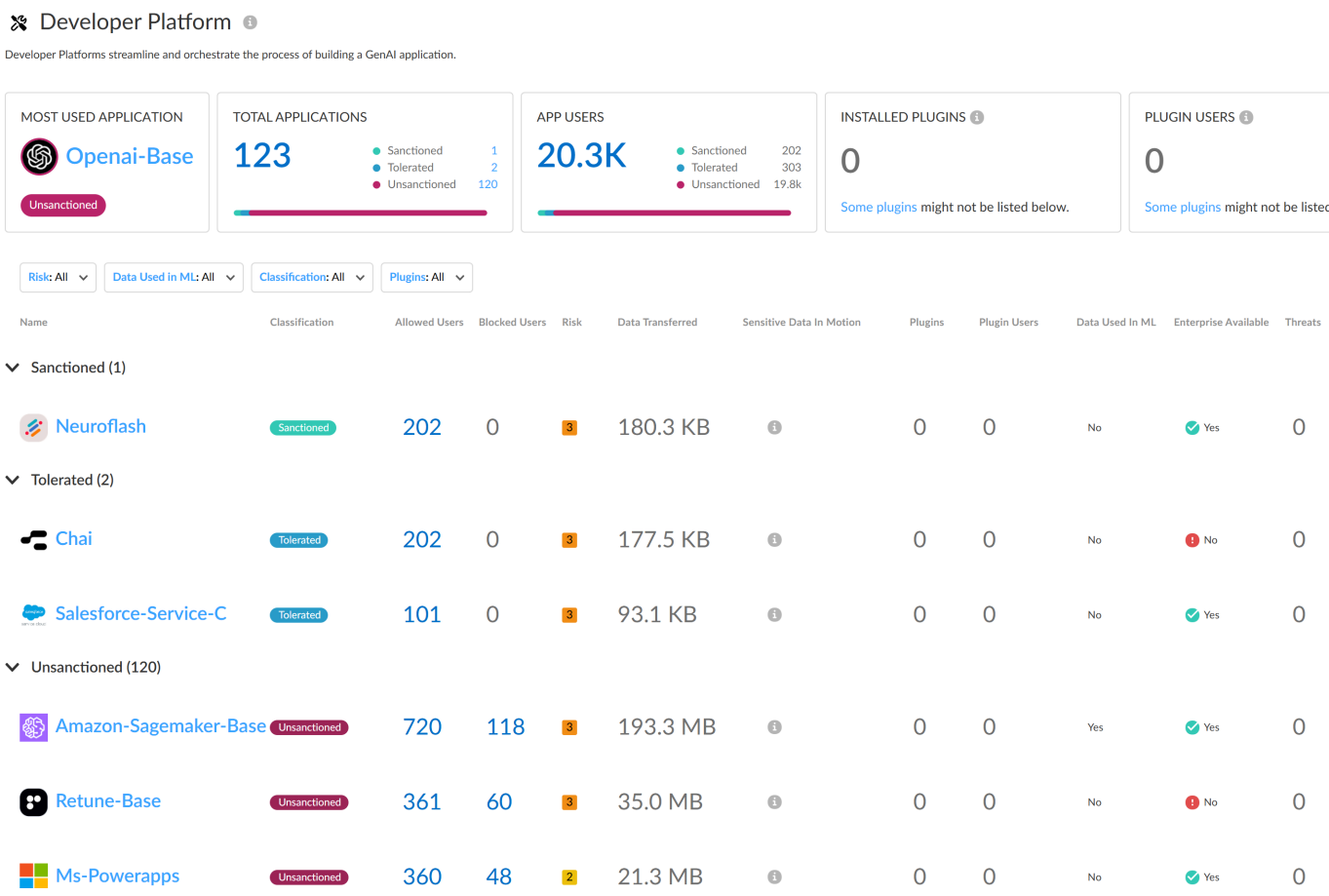
数）、**Transferred Count**（转移数） 对其进行排序。AI Access Security 将 GenAI app 按数量从高到低排序。

App 列表会显示检测到的每个 GenAI app 的以下信息。

- **Application Name**（应用程序名称）— 检测到的 GenAI app 的名称。单击 app 名称查看详细使用信息。您将被重定向到 Activity Insights **Applications**（应用程序）
- **Tag**（标签）— 当前 GenAI app 标签。您可以通过点击想要添加的标签来添加新标签。

  Palo Alto Networks 将 *app* 功能的子 *App-ID* 分组到容器 *App-ID* 中。但是，不支持标记 *App-ID* 容器。您必须单独标记组织内已认可、未认可或可容忍的特定子 *App-ID*。
- **Allowed Users**（允许的用户）— 根据安全策略规则中配置的访问权限访问 GenAI app 的唯一用户总数。单击 **Allowed Users**（允许的用户）计数，查看成功访问 GenAI app 的每个唯一用户的列表。
- **Blocked Users**（被阻止用户）— 根据安全策略规则中配置的访问权限，被阻止访问 GenAI app 的唯一用户总数。单击 **Blocked Users**（被阻止用户）计数，查看被阻止访问 GenAI app 的每个唯一用户的列表。
- **Threats**（威胁）— 检测到的威胁活动总数。
- **Transferred**（已传输）— 上传至或从 GenAI app 下载的数据总量（以千兆字节 (GB) 为单位）。
- **Sensitive Asset**（敏感资产）— 由于 Enterprise DLP 检测到并阻止敏感数据而产生的 DLP 事件的数量。
- **Enterprise Available**（企业可用）— 指示 GenAI app 是否提供企业计划或许可方案。
- **Data Used in ML**（机器学习中使用的数据）— 指示 GenAI app 是否使用用户上传的数据进行训练。
- **Risk Score**（风险评分）— GenAI app的 风险评分。

- 用例亮点
  - **Applications**（应用程序）— 属于任何其他 GenAI app 用例的 GenAI app 总数。GenAI app 的总数分为三类 — 已认可、可容忍和未认可的 GenAI app。
  - **Users**（用户）— 访问过任何符合其他 GenAI app 用例的 GenAI app 的用户总数。



STEP 5 | 创建 自定义安全策略规则 来控制对 GenAI app 的访问。

在上面的示例中，`Openai-Base` 是 代码助手和生成器 用例中最常用的 GenAI app。此外，这是一个 **Unsanctioned**（未认可） app，表示该 app 未经批准不得在您的公司网络上使用。

在这种情况下，您可以修改默认的 GenAI app 访问策略规则，以明确阻止对 `OpenAI` 的所有访问，如果这是您组织不应访问的 app。

通过高风险 App 发现 GenAI App 带来的风险

STEP 1 | 登录 Strata Cloud Manager

STEP 2 | 选择 **Insights**（见解） > **Activity Insights** > **Applications**（应用程序）。

STEP 3 | 配置 app 列表过滤器，缩小您想要调查的 GenAI app 范围。

1. 配置 **Time Range**（时间范围）和 **Scope Selection**（范围选择），以筛选要调查的特定时间范围和执行点。
2. **Add Filter**（添加过滤器）并添加以下过滤器。
   - **Source Type - Users**（源类型 - 用户）— 过滤 app 列表，仅显示您组织中用户访问的 GenAI app。这是一个必需的过滤器。
   - **GenAI Application - TRUE**（**GenAI**应用程序 - **TRUE**）— 过滤 app 列表，仅显示 GenAI app。这是一个必需的过滤器。
   - **App Risk Score**（**App** 风险评分）— 对于 **App Risk Score**（**App** 风险评分）过滤器，选择您要调查的特定风险评分。如果您未选择至少一个风险评分，则所有 GenAI app 都将显示出来。

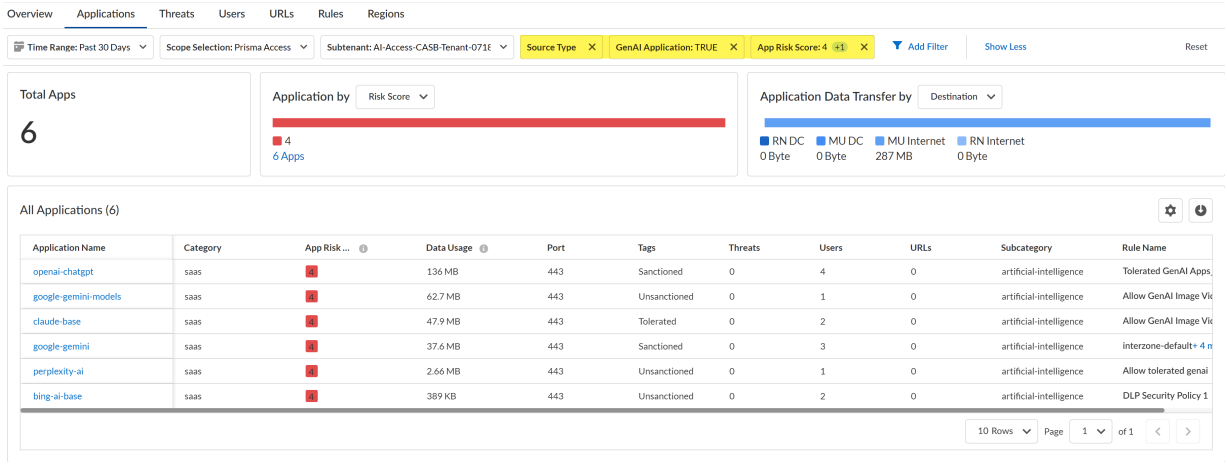
     在这个例子中，我们正在调查风险评分为 **4** 和 **5** 的 app，因为这些是风险最高的 app 风险评分。

STEP 4 | 查看已筛选的 GenAI app 列表。

需要了解的一些重要信息包括：

- **Application Name**（应用程序名称）— GenAI app 的 App-ID。
- **Data Usage**（数据使用量）— 上传到或从GenAI app 下载的数据量。这可以帮助您了解 GenAI app 的使用情况；数据使用量大的 GenAI app 可能意味着该 app 被广泛使用，需要严格的控制措施来防止敏感数据泄露和恶意行为者入侵。
- **Tags**（标签）— GenAI app 的当前 app 标签。如果列出的 GenAI app 中的某些 app 获得批准使用，您可以将标签修改为 **Tolerated**（可容忍） 或 **Sanctioned**（已认可）。

Palo Alto Networks 将 *app* 功能的子 *App-ID* 分组到容器 *App-ID* 中。然而，不支持对 *App-ID* 容器进行标记。您必须单独标记组织内已认可、未认可或可容忍的特定子 *App-ID*。



STEP 5 | 创建 自定义安全策略规则，以控制特定用户对 GenAI app 的访问权限。

例如，根据您的调查发现，存在多个未认可的 GenAI app，且其数据使用量巨大。这会带来安全风险，因为有用户正在网络上访问未经批准的 app，而您不知道正在下载或上传什么数据。在您能够进行适当的尽职调查以了解 GenAI app 的目的以及谁被允许使用 GenAI app 之前，您可以 **Block**（阻止）所有用户访问 GenAI app。

相反，您会注意到列出了一些 **Unsanctioned**（未认可）GenAI app，但它们是 GenAI 批准供特定用户在您的网络上使用且数据使用量很大的应用。在这种情况下，您可以将标签更改为 **Sanctioned**（已认可），并编写策略规则 **Allow**（允许）使用该 app，但仅限于特定角色或部门的用户。在策略规则中，您可以关联一个 Enterprise Data Loss Prevention (E-DLP) 数据配置文件来防止敏感数据外泄，并关联一个漏洞配置文件来阻止利用系统缺陷或未经授权访问系统的尝试。

通过 App 用户发现 GenAI App 带来的风险

STEP 1 | 登录 Strata Cloud Manager

STEP 2 | 选择 **Insights** > **AI Access** 以查看 AI Access Security Insights 仪表板。

这显示了高风险用户访问最多的 GenAI app，以帮助您缩小关注范围。

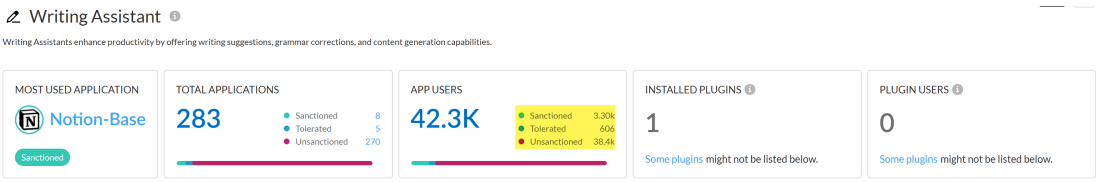
STEP 3 | 单击 **Review use case**（查看用例），查看与您的高风险用户正在访问的 GenAI app 关联的用例。

AI Access Security Insights 仪表板默认按用例显示网络上访问的 GenAI app，并显示有关 GenAI app 热门用户的以下高层级信息。点击用户计数以查看 **User Name**（用户名）或 **IP Address**（**IP** 地址）以及该用户访问的 GenAI 应用程序的数量。

- 用户细目

  此部分汇总了与所选 GenAI 用例关联的所有 GenAI app 的用户总数。AI Access Security 包括访问 **Sanctioned**（已认可）、**Tolerated**（可容忍）和 **Unsanctioned**（未认可） app 的用户数量明细。

  单击 **App Users**（**App** 用户）总数，查看所有访问或被阻止访问与所选用例关联的 GenAI app 的用户列表。



- 按 **GenAI** 用例的用户

  这提供了与所选 GenAI 用例关联的每个 GenAI app 的访问用户总数的汇总信息。列出了 **Sanctioned**（已认可）、**Tolerated**（可容忍）和 **Unsanctioned**（未认可） GenAI app，以及每个 app 的用户总数。

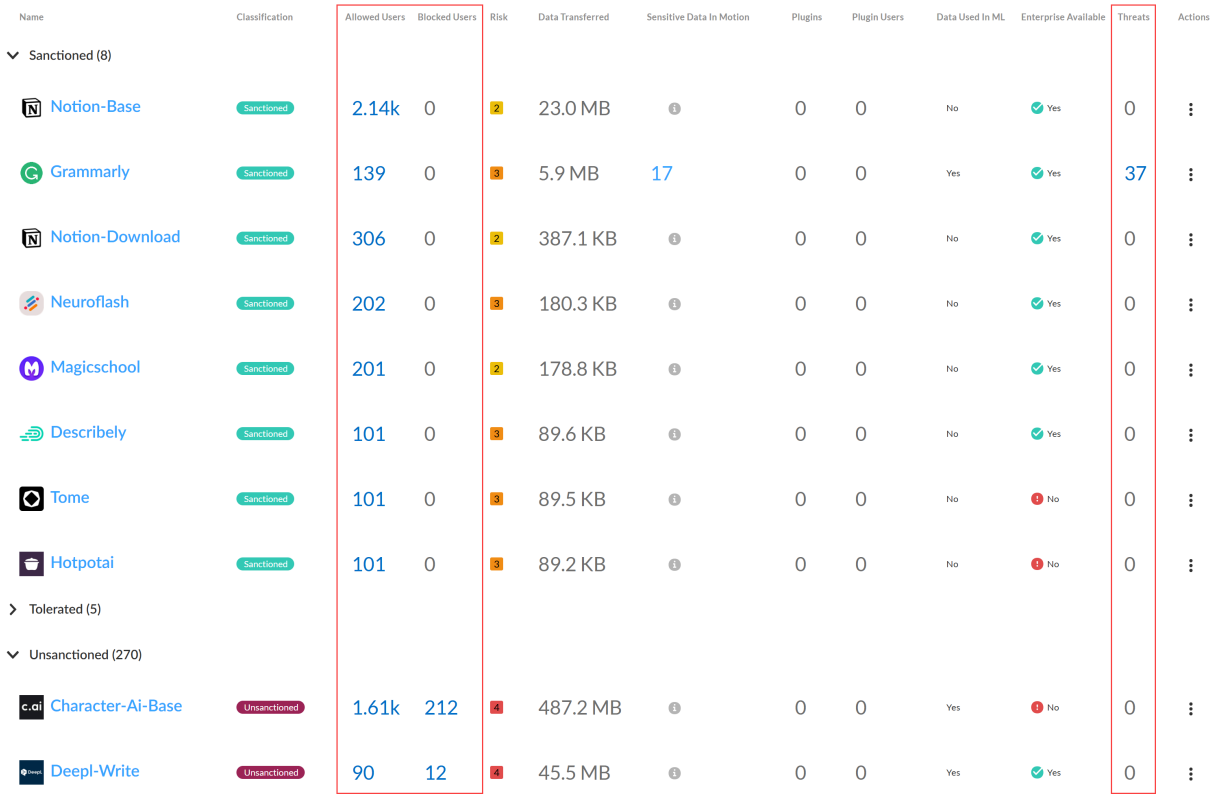
  查看 **Allowed Users**（允许的用户） 和 **Blocked Users**（已阻止用户）计数，以衡量您的 GenAI app 安全和访问策略规则的有效性。

  - **Allowed Users**（允许的用户）— 允许访问GenAI app 的用户总数。利用这些信息来衡量安全策略规则的有效性，验证允许的用户数量是否符合预期，或者评估组织新允许使用的 GenAI app 的采用率。
  - **Blocked Users**（已阻止用户）— 被阻止访问 GenAI app 的用户总数。使用此信息来验证您是否正确配置了控制特定 GenAI app 访问权限的安全策略规则，或者了解您组织中的用户是否正在访问未认可的 GenAI app。

  例如，考虑下面的语法GenAI app。您的组织将此 GenAI app 归类为 `Sanctioned`（已认可），供您组织内的特定用户使用。在这种情况下，您的安全管理员点击了 **Allowed Users**（允许的用户）计数，并验证了所有访问 GenAI app 的用户都被允许这样做。

  相反，您的安全管理员发现有超过 1,600 名用户访问了 `Character-Ai-base` app。您的安全管理员将此 GenAI app 归类为`Unsanctioned`（未认可），并打算限制对您组织的所

有访问。在这种情况下，您的安全管理员应检查您的安全策略规则库和控制对 `Character-Ai-base` app 访问的单个安全策略规则，以确认它在安全策略规则库中的位置是否正确，并确认其配置是否正确，以阻止所有访问。



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 | 创建 自定义安全策略规则，以控制特定用户对 GenAI app 的访问权限。

例如，根据您的调查，您发现大量用户正在访问 `bing-ai-uploading` GenAI app。虽然这是 **Sanctioned**（已认可） GenAI，但它仅对组织内的特定用户集有效。您可以决定编写策略规则，明确阻止不应访问此 GenAI app 的用户进行访问，以防止滥用，并编写安全策略规则，明确允许经 app 批准的用户访问 GenAI app。或者，您可以编写策略规则，允许所有用户访问，但实施数据丢失和威胁预防措施，以防止敏感数据外泄，并防止恶意和网络钓鱼 URL、恶意文件或恶意软件等威胁。

发现作为第三方插件安装的 GenAI app 带来的风险

STEP 1 | 登录 Strata Cloud Manager

STEP 2 | 选择 **Insights** > **AI Access** 以查看 AI Access Security Insights 仪表板。

仪表盘显示用户安装的第三方插件数量以及安装第三方插件的用户数量。AI Access Security 根据 AI Access Security 存储的所有数据计算出这些数字。这些数字不限于时间过滤器所指示的时间段。

STEP 3 | 单击 **Installed Plugins**（已安装插件）或 **Plugin Users**（插件用户）以导航至 SaaS Security Posture Management (SSPM) 中的详细信息。

单击 **Installed Plugins**（已安装插件）打开第三方插件页面，显示 GenAI 第三方插件的详细信息。从这里，您可以查看插件信息，以确定插件是否存在风险。

单击 **Plugin Users**（插件用户）将打开第三方插件页面，其中显示了安装第三方插件的用户的详细信息。对于每个用户，您可以查看他们安装了多少插件，以及他们已将插件安装到哪些应用商店 app 中。利用这些信息来识别单个用户带来的插件风险。

STEP 4 | 要按用例查看已安装的插件，请完成以下步骤：

1. 选择 **Insights** > **AI Access** 以查看 AI Access Security Insights 仪表板。

   仪表盘会根据您网络上的活动情况，突出显示 GenAI app 的四个最佳用例。仪表盘板还显示其他用例的图标。

2. 导航到有关用例的详细信息。对于顶层用例，请单击 **Review use case**（查看用例）。对于其他用例，请单击用例图标。

   用例详细信息页面显示该用例的所有 GenAI 应用程序的表。本页的

   摘要信息包括 ***Installed Plugins***（已安装插件）的数量和 ***Plugin Users***（插件用户）的数量。这些数字是根据 *AI Access Security* 存储的所有数据确定的，并不限于时间过滤器指示的时间段。因此，这些总计可能不会反映在用例详细信息表中。

3. 在用例详细信息表中，标识作为插件安装在一个或多个 Market App 实例中的 GenAI app 以及插件用户数。此信息显示在表格的 **Plugins**（插件）和 **Plugin Users**（插件用户）列中。

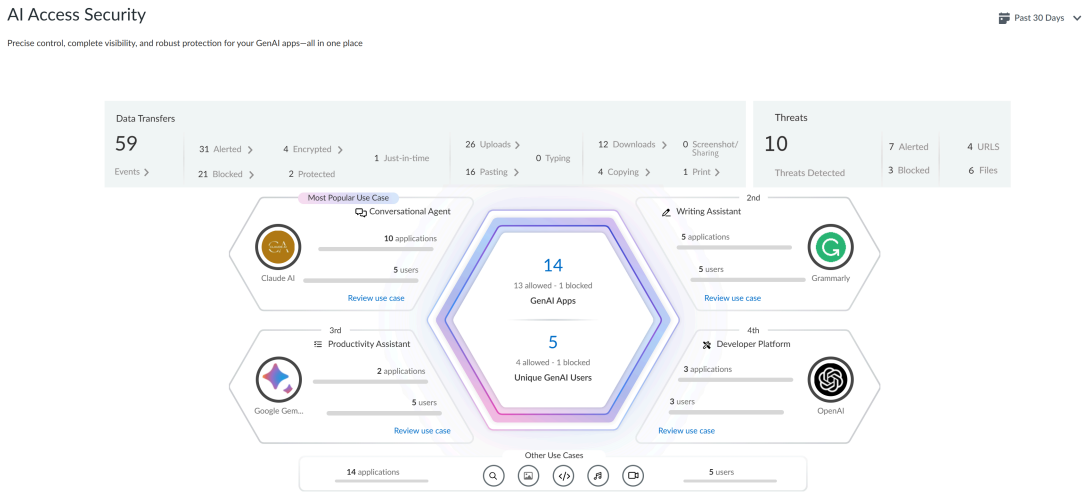
4. 对于作为插件安装的 GenAI app，请单击 **Plugins**（插件）或 **Plugin Users**（插件用户）列中的数字。

   点击 **Plugins**（插件）列中的数字，即可在 SSPM 中打开第三方插件页面，显示用户安装的 GenAI app 的第三方插件实例。从这里，您可以查看插件信息，以确定插件是否存在风险。

   点击 **Plugin Users**（插件用户）列中的数字，即可打开第三方插件页面，显示有关将该 app 安装为第三方插件的用户的详细信息。利用这些信息来识别单个用户带来的插件风险。

发现 GenAI App 在 Prisma Access Browser 上带来的风险

Prisma Access Browser 与 AI Access Security 集成，为 Prisma Access Browser 独立版客户提供全面的 GenAI app 可见性、访问控制、数据和威胁保护。这种集成提供了最全面的 GenAI app 目录，并具备数据分类和实时威胁防御等深度最后一公里控制功能。作为 Prisma Access Browser 独立版安全管理员，您可以通过 Insights 菜单访问 AI Access Security，并通过 Prisma Access Browser 监控第三方 AI 应用程序的使用情况，获取包括应用程序指标、用户活动、检测到的威胁和数据传输在内的详细分析。

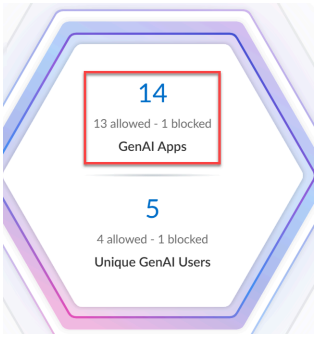


STEP 1 | 登录 Strata Cloud Manager

STEP 2 | 选择 **Insights**（见解） > **AI Access**（**AI** 访问）以查看 独立版 Prisma Access Browser 的 AI Access Security Insights 仪表板。

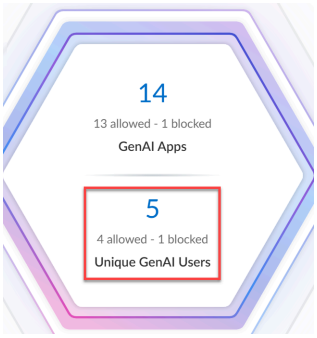
STEP 3 | 单击 **GenAI Apps** 以查看具有 **Is GenAI:Yes** 和 **Category:**（类别：）的应用程序指标。已应用 **Access** 过滤器以查看以下指标：

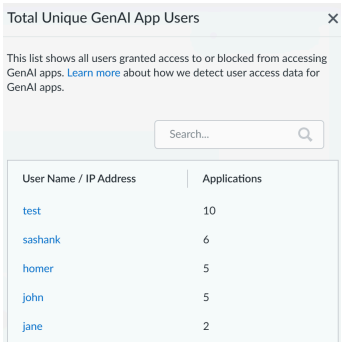
- GenAI 应用程序程序总数
- 允许的 GenAI App
- 阻止的 GenAI App



STEP 4 | 单击 **Unique GenAI Users**（唯一 **GenAI** 用户）以查看被授予访问或阻止访问 GenAI app 的 GenAI app 用户总数。选择用户（从 **Total Unique GenAI App Users**（唯一 **GenAI App** 用户总数） 页面）以导航到 Events（事件）页面（应用 **User:**（用户：）**<user name>**过滤器），从而了解允许和阻止该特定用户的 GenAI app。可用的指标包括：

- GenAI 用户总数
- 允许的 GenAI 用户
- 阻止的 GenAI 用户

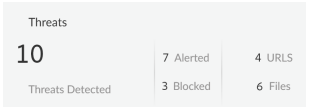




STEP 5 | 单击 **Threats Detected**（检测到的威胁）小部件以查看检测到和阻止的威胁总数。

此信息可在活动页面中找到（包含 **Is GenAI:Yes**，类别：已应用恶意软件 过滤器）。可用的指标包括：

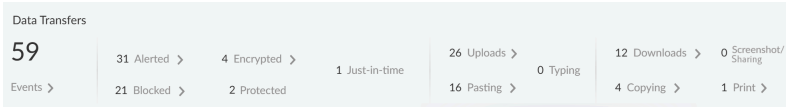
- Total GenAI Threats（GenAI 威胁总数），显示检测到和阻止的威胁总数。
- 恶意 URL（已应用过滤器：类别：恶意软件 和 类型：恶意网站）
- 文件（应用的过滤器：类别：恶意软件 和 类型：已识别恶意文件）



STEP 6 | 单击 **Data Transfers**（数据传输）小部件，查看当流量符合您的企业数据丢失防护 (E-DLP) 数据配置文件 中的匹配条件时检测到的数据传输事件数量，以用于您的 Prisma Access Browser。

此信息可在活动页面中找到（包含 **Is GenAI:Yes**，类别：已应用 **DLP** 过滤器器）。

- 检测到的总数据传输量。应用的筛选器：**Is GenAI:Yes**，类别：**DLP**。
- 数据传输已发出警报。应用的筛选器：**Is GenAI:Yes**，类别：**DLP**，操作：允许的。
- 数据传输已阻止。应用的筛选器：**Is GenAI:Yes**，类别：**DLP**，操作：阻止的。
- 受保护的数据传输：允许但只能由浏览器执行的操作。例如，允许在已许可 app 之间复制和粘贴数据，并阻止在浏览器或本地桌面应用程序中对其他 app 进行复制和粘贴。应用的筛选器：**Is GenAI:Yes**，类别：**DLP**，操作：允许受保护。
- 数据传输已加密：一种加密操作，只有浏览器拥有针对特定用户和加密设备的解密密钥。这样就可以下载文件，并确保允许将文件上传（和解密）到特定 app，或在离线模式下在浏览器中打开。没有其他 app 可以打开该文件，因此它非常适合您不想在终端上访问的文件，例如在非托管设备上的文件。应用的筛选器：**Is GenAI:Yes**，类别：**DLP**，操作：允许加密。
- 数据传输的实时控制：操作包括：在继续操作之前警告用户、要求用户在继续操作之前提供业务理由，或触发管理员审批流程。这些操作会在紧急情况下触发临时访问权限或绕过规则，或者出于合规性原因需要进行理由说明和记录。应用的筛选器：**Is GenAI:Yes**，类别：**DLP**，操作：请求权限。
- 数据传输已上传。应用的筛选器：**Is GenAI:Yes**，类别：**DLP**，类型：文件上传。
- 剪贴板活动中的数据传输（粘贴）。应用的筛选器：**Is GenAI:Yes**，类别：**DLP**，类型：剪贴板粘贴。
- 当前键入的数据传输。应用的筛选器：**Is GenAI:Yes**，类别：**DLP**，类型：清理内容。
- 数据传输已下载。应用的筛选器：**Is GenAI:Yes**，类别：**DLP**，类型：文件下载。
- 数据传输已复制。应用的筛选器：**Is GenAI:Yes**，类别：**DLP**，类型：剪贴板复制。
- 使用屏幕截图共享数据传输。应用的筛选器：**Is GenAI:Yes**，类别：**DLP**，类型：屏幕共享。
- 数据传输已打印。应用的筛选器：**Is GenAI:Yes**，类别：**DLP**，类型：打印。



标记 GenAI App

根据 GenAI app 风险评分 和其他考虑因素，您可以为应用程序添加标签，以反映该应用程序是否在您的组织内获得批准。可用标签如下：

标记	说明
已认可	该应用程序已获得贵组织的批准，并正在由贵组织成员使用。
未认可	应用程序未获得贵组织的批准。例如，由于与应用程序相关的安全风险，该应用程序可能未受认可。 由于贵组织成员不应该使用该应用程序，因此您应该采取措施阻止该应用程序的使用。您可以使用策略规则阻止应用程序。
可容忍	该应用程序不像经过认可的应用程序那样受信任。但是，贵组织允许使用该应用程序，直到贵组织找到更安全的应用程序为止。该应用程序是可容忍的，以避免影响贵组织的效率。 尽管存在潜在的安全风险，但该应用程序仍被允许运行，因此您可以采取措施限制某些操作。例如，您可以创建一条策略规则来阻止应用程序的上传或下载操作。

Palo Alto Networks 将 *app* 功能的子 *App-ID* 分组到容器 *App-ID* 中。但是，不支持标记 *App-ID* 容器。您必须单独标记组织内已认可、未认可或可容忍的特定子 *App-ID*。

例如，考虑包含以下子 *App-ID* 的 `claude` 容器 *app-ID*：`claude-base`、`claude-upload`、`claude-edit`、`claude-post` 和 `claude-delete`。

您创建了一个 应用程序过滤器，以对 ***Sanctioned***（已认可）应用程序强制执行相同的数据泄露控制。在这种情况下，您必须标记 `claude` *App-ID* 容器的所有子 *App-ID*，以便将策略规则操作应用于 ***Sanctioned***（已认可）`claude` *GenAI app* 的所有子进程。

2024 年 9 月，Palo Alto Networks 更新了 app 标签的实现方式。从 2024 年 9 月开始，标签将写入和读取一个新的预定义 `Application-Tagging` 代码段。此更新发布到您的租户后，将在您首次标记 app 时生效。标签被写入 snippet 和 AI Access Security，即 Activity Insights页面，Strata Cloud Manager Command Center 开始显示来自代码片段的标签信息。如果您在此次更新之前标记了应用，您将不再在 AI Access Security 和 Activity Insights 应用中看到这些标记更改。`Application-Tagging` 代码片段跟踪哪些 app 序被标记为 **Sanctioned**（已认可）或 **Tolerated**（可容忍）。未明确标记为 **Sanctioned**（已认可）或 **Tolerated**（可容忍）的 app 将被视为 **Unsanctioned**（未认可）。因此，只有在此更新之后添加的标签才会显示在 Strata Cloud Manager 中。所有其他 app 均显示为 **Unsanctioned**（未认可权。

在本次更新之前应用的标签仍然会影响 NGFW 或 Prisma Access 部署上的基于标签的策略强制执行，只要您在 `Application-Tagging` 配置范围内关联 Application-Tagging 代码段并应用标签即可。

- NGFW 和 Prisma Access 应用程序配置
- Activity Insights 应用程序

在应用程序配置中标记 GenAI App

STEP 1 | 登录 Strata Cloud Manager

STEP 2 | 将预定义的 `Application-Tagging` 代码段与适当的配置范围关联起来，以支持基于标签的策略强制执行。

STEP 3 | 获取要标记的子 App-ID。

您可以使用以下方法之一获取 GenAI app 的子 App-ID。

- 使用 AI Access Security Insights 仪表板来 发现 GenAI app 带来的风险。AI Access Security Insights 向您显示在整个组织中使用的检测到的子 App-ID。
- 查看支持的 GenAI app 列表。
- 使用 Applipedia 搜索通过动态内容更新交付的受支持的 GenAI app 的子 App-ID。

  Applipedia 只显示通过动态内容提供的应用的 App-ID，而不显示通过 App-ID Cloud Engine (ACE) 提供的应用程序。

STEP 4 | 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（对象） > **Applications**（应用程序） > **Applications**（应用程序）。

STEP 5 | 在 **Configuration Scope**（配置范围）中，选择 `Application-Tagging`（应用程序标记）代码段。

如果您要标记通过 App-ID Cloud Engine (ACE) 提供的 App-ID，则与所选文件夹关联的所有 NGFW 或 Prisma Access 租户都必须配置为从 ACE 接收 App-ID 更新。

当 NGFW 或 Prisma Access 租户拥有有效的 SaaS Security Inline 或 AI Access Security 许可证时，ACE 默认启用。您还可以为 NGFW 手动启用 ACE。

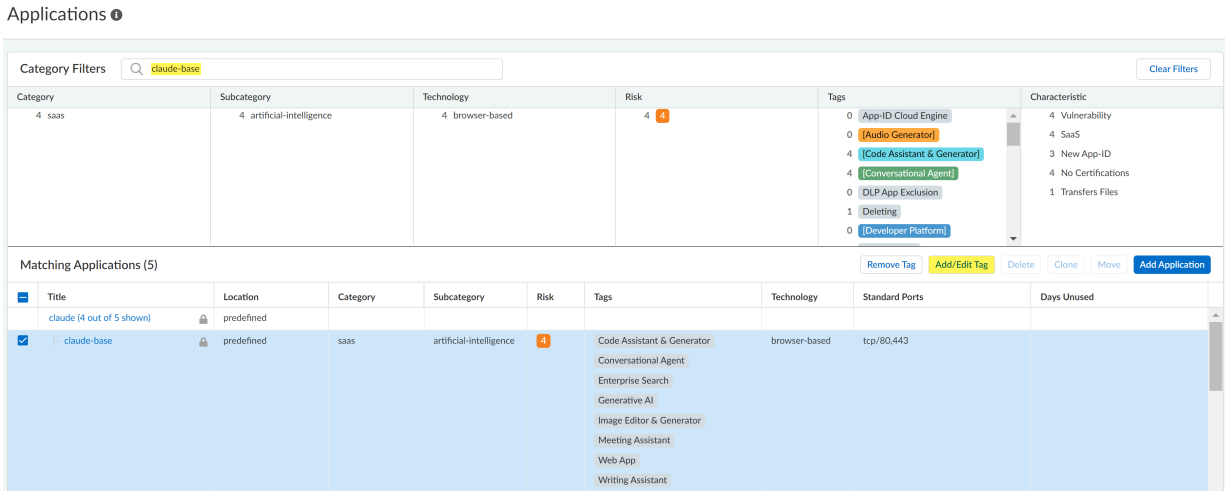
如果标记从 ACE 提供的 App-ID，并且与所选文件夹关联的至少一个 NGFW 或 Prisma Access 租户未配置为从 ACE 接收 App-ID，则配置推送将失败。

因此，Palo Alto Networks 不建议选择 **Global**（全局）配置范围。

STEP 6 | 在 **Category Filters**（类别筛选器）搜索字段中，输入要标记的 App-ID 并选择它。

一次只能标记一个 App-ID。

STEP 7 | **Add/Edit Tag**（添加/编辑标签）。



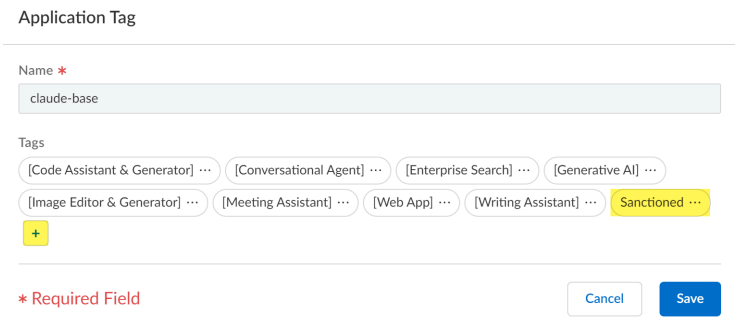
STEP 8 | 单击 **+** 应用预定义的 **Sanctioned**（已认可） 或 **Tolerated**（可容忍）应用标签。

在这个例子中，`claude-base` App-ID 被标记了 **Sanctioned**（已认可）标签。

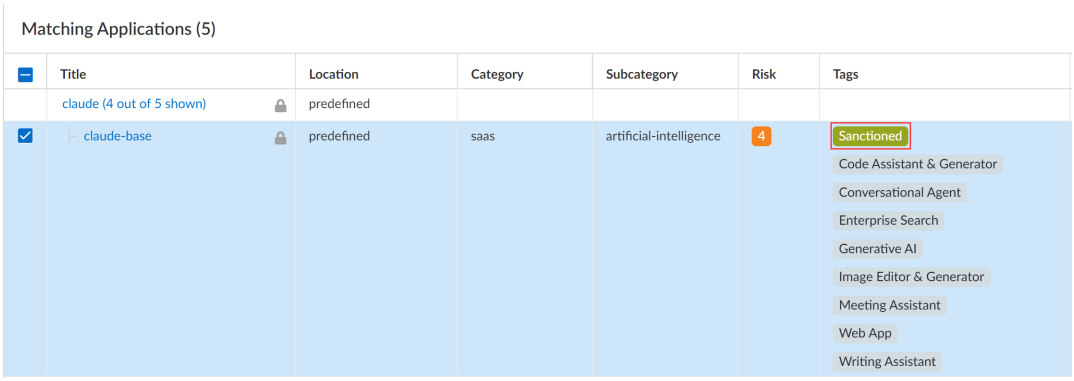
如果从 ***Applications***（应用程序）进行标记，则在没有 ***Sanctioned***（已认可） 或 ***Tolerated***（可容忍）标签的情况下，*app* 被视为 ***Unsanctioned***（未认可）。

如果要将 *app* 标签从 ***Sanctioned***已认可）或 ***Tolerated***（可容忍）更改为 ***Unsanctioned***（未认可），则需要删除现有标签。您无法从 ***Applications***（应用程序）中手动将 *app* 标记为 ***Unsanctioned***（未认可）。

STEP 9 | **Save**（保存）。



STEP 10 | 查看 **Tag**（标签）列中的值，以确认是否已成功应用应用程序标签。



STEP 11 | 单击 **Overview**（概览）。

STEP 12 | **Push Config**（推送配置）并 **Push**（推送）您的配置更改。

在 Insights 仪表板中标记 GenAI App

STEP 1 | 登录 Strata Cloud Manager

STEP 2 | 将预定义的 `Application-Tagging` 代码段与适当的配置范围关联起来，以支持基于标签的策略强制执行。

STEP 3 | 获取要标记的子 App-ID。

您可以使用以下方法之一获取 GenAI app 的子 App-ID。

- 使用 AI Access Security Insights 仪表板来 发现 GenAI app 带来的风险。AI Access Security Insights 向您显示在整个组织中使用的检测到的子 App-ID。
- 查看支持的 GenAI app 列表。
- 使用 Applipedia 搜索通过动态内容更新交付的受支持的 GenAI app 的子 App-ID。

  Applipedia 只显示通过动态内容提供的应用的 App-ID，而不显示通过 App-ID Cloud Engine (ACE) 提供的应用程序。

STEP 4 | 选择 **Insights**（见解） > **Activity Insights** > **Applications**（应用程序）。

STEP 5 | 找到您要标记的 GenAI 子 App-ID。如有必要，您可以筛选表格，仅显示 GenAI 应用程序。

1. **Add Filter**（添加过滤器）并添加 **GenAI Application**（**GenAI** 应用程序）过滤器。
2. 将 **GenAI Application**（**GenAI** 应用程序）过滤器设置为 **TRUE**。

STEP 6 | 要查看应用于 GenAI App-ID 的标签，请检查 **Tag**（标签）列中的值。

STEP 7 | 为子 GenAI App-ID 应用不同的标签。

1. 在 **Actions**（操作）列中，选择标签图标，然后选择 **Sanctioned**（已认可）、**Tolerated**（可容忍）或 **Unsanctioned**（未认可）标签。
2. **Apply**（应用）新标签。

查看分配给 GenAI App 的风险评分

为了帮助您快速识别对您的组织构成最大威胁的 GenAI app，AI Access Security 会为每个 GenAI app 分配一个风险评分。这些风险评分使您能够快速识别有风险的 GenAI app，以便您可以采取措施保护您的环境。例如，为了保护您的环境，您可以创建一个策略规则来阻止该 app。您也可以选择将该 app 标记为未许可。

App 的风险评分介于 1（低风险）和 5（高风险）之间，基于 SaaS app 属性。有些属性是所有 SaaS app 共有的，而一部分属性则是 GenAI app 独有的。

GenAI 属性是诸如用户输入到 app 的数据类型、app 生成的输出的数据类型以及 app 是否使用用户提交的数据来训练其 GenAI 模型等属性。根据 GenAI 属性值，风险评分计算确定 GenAI 风险。

除了 GenAI 属性之外，风险评分计算还使用以下类型的属性来确定 app 的一般 SaaS 风险。

- 合规性属性，用于识别 app 是否符合各种监管要求和标准。
- 身份访问管理属性，用于标识 app 的身份验证和访问控制功能。
- 安全和隐私属性，用于标识保护数据的产品功能。此类属性包括 app 是否对静态数据和传输中的数据进行加密等属性。

GenAI app 的最终风险评分是 SaaS 一般风险（根据 SaaS 属性计算）和 GenAI 风险（根据 GenAI 属性计算）的组合。风险评分计算在确定最终风险评分时给予 GenAI 风险额外权重。

STEP 1 | 登录 Strata Cloud Manager

STEP 2 | 要导航到 Activity Insights 仪表板，请选择 **Insights**（见解） > **Activity Insights** > **Applications**（应用程序）。

STEP 3 | 在表格中找到 GenAI app。如有必要，您可以筛选表格，仅显示 GenAI app。

1. **Add Filter**（添加过滤器）并添加 **GenAI Application**（**GenAI** 应用程序）过滤器。
2. 将 **GenAI Application**（**GenAI** 应用程序）过滤器设置为 **TRUE**。

STEP 4 | 要识别出构成最大威胁的 GenAI app，请检查 **Risk**（风险）列中的风险评分值。

风险评分	含义
4-5	高风险 — 很可能存在风险。
3	中风险 — 代表中等风险。
1-2	低风险 — 不太可能存在风险。

STEP 5 | 对风险最高的 app 采取措施。

例如，您可以创建策略规则来阻止这些 app，或者将 app 标记为 Unsanctioned（未认可）。

为 GenAI App 使用应用程序过滤器

应用程序过滤器根据您定义的应用程序属性动态地对应用程序进行分组。您可以在安全策略规则中使用应用程序过滤器，根据应用程序属性控制对 GenAI app 的访问，而不是在安全策略规则中显式定义 GenAI app 或应用程序组。

AI Access Security 包含以下预定义的 GenAI 应用程序过滤器。预定义的应用程序过滤器基于支持的 AI Access Security 用例。

- 音频生成器
- 对话代理
- 代码助手和生成器
- 开发人员平台
- 企业搜索
- 图像编辑器和生成器
- 会议助手
- 生产力助手
- 视频编辑器和生成器
- 写作助手

上述过滤器仅为显示标签。它们不能在安全策略规则中使用。

- Strata Cloud Manager
- Panorama

在 Strata Cloud Manager 上为 GenAI App 使用应用程序过滤器

STEP 1 | 登录 Strata Cloud Manager

STEP 2 | 选择 **Manage**（管理） > **Configuration**（配置） > **Objects**（对象） > **Application**（应用程序） > **Application Filters**（应用程序过滤器） 和 **Add Application Filter**（添加应用程序过滤器）。

STEP 3 | 输入描述性的 **Name**（名称）。

STEP 4 | 对于 **Tag**（标签），选择 **Generative AI**（生成式 **AI**）。

NGFW 或 Prisma Access 检查的所有 GenAI app 在检查时均带有 `genai` 标记。在为 GenAI app 创建自定义应用过滤器时，Palo Alto Networks 建议选择 **Generative AI**（生成式 **AI**）标签，以确保添加应用程序过滤器的安全策略规则适用于 GenAI app 流量。

STEP 5 | 配置额外的 类别过滤器，以缩小受影响的 GenAI app 的范围。创建 GenAI 应用程序过滤器时，请考虑以下标签。

- 风险 — 指定 **Risk**（风险）分数，以便安全策略规则操作仅应用于具有所选风险分数的 GenAI app。

  例如，您希望编写一条安全策略规则，无论 GenAI app 的使用情况如何，都阻止对其所有风险 app 的访问。在这种情况下，您可以为 GenAI app **4** 和 **5** 创建应用程序过滤器，因此安全策略规则仅适用于具有这些风险分数的 GenAI app。

- **Tag**（标签）— 指定安全策略规则操作是否适用于 标记为 **Sanctioned**（已认可）、**Tolerated**（可容忍） 或 **Unsanctioned**（未认可）的 GenAI app。此外，您还可以根据 GenAI app的用例应用标签。

  例如，您想编写一条安全策略规则，以允许访问已认可的代码助手和生成器 GenAI app。在这种情况下，您可以创建一个应用程序过滤器，其中包含 **Sanctioned**（已认可）和 **Code Assistant & Generator**（代码助手和生成器 ）标签，以便安全策略规则仅适用于具有此应用程序标签且符合用例的 GenAI app。

STEP 6 | 查看 **Matching Applications**（匹配应用程序）的列表。

STEP 7 | **Save**（保存）。

STEP 8 | **Push Config**（推送配置）并 **Push**（推送）。

STEP 9 | 创建自定义安全策略规则以控制 GenAI 访问.

在 Panorama 上为 GenAI App 使用应用程序过滤器

STEP 1 | 登录到 Panorama™ management server Web 界面。

STEP 2 | 选择 **Object**（对象） > **Application Filters**（应用程序筛选器）并 **Add**（添加）新的应用程序筛选器。

STEP 3 | 输入描述性的 **Name**（名称）。

STEP 4 | 对于 **Tag**（标签），选择 **Generative AI**（生成式 **AI**）。

NGFW 或 Prisma Access 检查的所有 GenAI app 在检查时均带有 `genai` 标记。在为 GenAI app 创建自定义应用过滤器时，Palo Alto Networks 建议选择 **Generative AI**（生成式 **AI**）标签，以确保添加应用程序过滤器的安全策略规则适用于 GenAI app 流量。

STEP 5 | 配置额外的 类别过滤器，以缩小受影响的 GenAI app 的范围。创建 GenAI 应用程序过滤器时，请考虑以下标签。

- 风险 — 指定 **Risk**（风险）分数，以便安全策略规则操作仅应用于具有所选风险分数的 GenAI app。

  例如，您希望编写一条安全策略规则，无论 GenAI app 的使用情况如何，都阻止对其所有风险 app 的访问。在这种情况下，您可以为 GenAI app **4** 和 **5** 创建应用程序过滤器，因此安全策略规则仅适用于具有这些风险分数的 GenAI app。

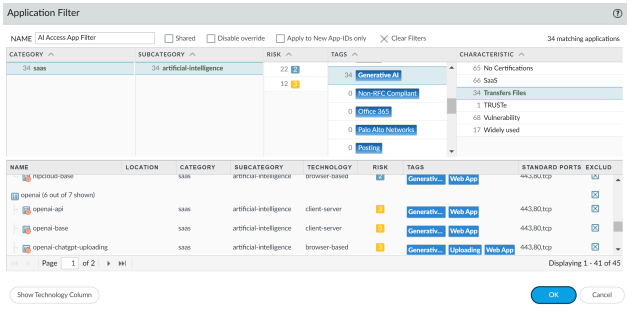
STEP 6 | 查看匹配的应用程序列表。

STEP 7 | 单击 **OK**（确定）。

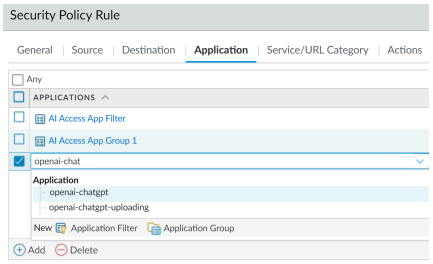
STEP 8 | 选择 **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 9 | 创建自定义安全策略规则以控制 GenAI 访问.

STEP 10 | 在以下示例中，**AI Access App Filter**（**AI** 访问 **App** 过滤器）应用程序过滤器具有 类别：SaaS，子类别：人工智能，标签：生成式 AI和 特征：传输文件。这将创建一个包含 34 个匹配的 GenAI 应用程序的过滤器。



STEP 11 | 在以下示例中，选择 openai-chatgpt 作为 **Application**（应用程序）。



STEP 12 | 通过从与对话式 AI 相关的“ “类别”、“子类别”、“技术”、“风险”、“特征”和“标签”部分中选择属性值来定义过滤器。例如，当您选择与对话聊天相关的值时，请注意对话框底部的匹配应用程序列表会缩小。调整了筛选器属性以匹配要安全启用的应用程序类型后，单击 **Save**（保存）。

修改默认 GenAI App 访问策略规则以控制 GenAI 访问

修改 Strata Cloud Manager 中的默认 GenAI App 策略规则，以控制企业中 GenAI App 的使用。

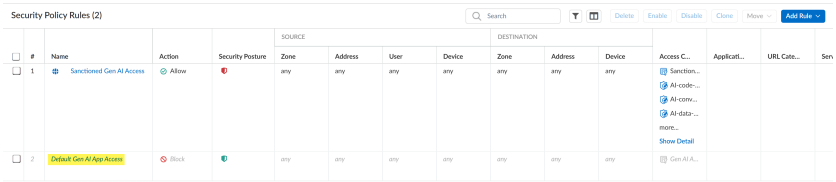
- 在 *Strata Cloud Manager* 中，虽然您可以通过 *GenAI App* 的安全策略创建策略规则，但 *Palo Alto Networks* 建议您使用互联网访问安全策略规则来高效地创建策略规则。
- *Palo Alto Networks* 不建议在 *Enterprise Data Loss Prevention (E-DLP)* 许可证未激活的情况下，将 *GenAI app* 和非 *GenAI app* 放在同一策略中。

对于 Strata Cloud Manager，AI Access Security 包含预定义的 默认 `GenAI app` 访问，以控制对企业中所有未明确允许的 GenAI app 的访问，该策略为开箱即用的策略。默认情况下，此策略规则会阻止企业内所有 GenAI app。要修改此策略：

STEP 1 | 登录 Strata Cloud Manager

STEP 2 | 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW & Prisma Access** > **Security Services**（安全服务） > **Security Policy**（安全策略），然后选择目标 **Configure Scope**（配置范围）（*Gen-AI-Best-Practice* 代码段）。

STEP 3 | 单击预定义的 `Default GenAI App Access`（默认 `GenAI App` 访问）策略规则。此策略规则阻止访问所有 GenAI app。



STEP 4 | **Enable**（启用） `Default GenAI App Access`（默认 `GenAI App` 访问）策略规则。默认情况下禁用。

STEP 5 | 在 Web 应用程序部分，根据需要配置 **Application**（应用程序）和 **URL Category**（**URL** 类别）。默认情况下，`Default GenAI App Access`（默认 `GenAI App` 访问）策略规则阻止访问所有 GenAI app。但是，您可以通过选择个人、应用程序组或应用程序过滤器来修改预定义的策略规则，以阻止特定应用程序。

- 应用程序 — 添加一个或多个 GenAI app。
- 应用程序组 — 应用程序组是您创建的单个应用程序的静态分组。
- 应用程序过滤器—应用程序过滤器根据您定义的 app 过滤器动态地对应用程序进行分组。

  例如，您可以使用预定义或自定义 GenAI app 筛选器动态控制对组织中 GenAI app 的访问，而不是添加单个 GenAI app 或创建每次需要更改时都必须手动更新的应用程序组。

STEP 6 | **Save**（保存）。

STEP 7 | **Push Config**（推送配置）并 **Push**（推送）。

创建自定义安全策略规则以控制 GenAI 访问

您可以创建自定义安全策略规则来控制 GenAI app 的使用，并防止敏感数据泄露到已认可的 GenAI app。使用标签、源（基于来源的流量）、用户组和其他特定参数来构建您的自定义策略。这有助于您在组织内为 GenAI app 实施自定义安全策略规则。

(Strata Cloud Manager) 您可以使用或修改预定义的 **Sanctioned GenAI Access**（认可的 **GenAI** 访问） 自定义互联网访问策略规则，或者创建您自己的自定义互联网访问策略规则。

(Panorama™ management server) 创建安全策略规则以控制组织中 GenAI app 的使用。

您必须创建安全策略规则，以将已认可和可容忍的 GenAI app 与未认可的 GenAI app 分开控制。例如，如果组织中存在只能由特定用户访问的可容忍 GenAI app，您可以创建一个安全策略规则，仅允许这些特定用户访问。您可以将 Enterprise Data Loss Prevention (E-DLP) 数据配置文件与安全策略规则关联，以防止敏感数据外泄；还可以将漏洞保护配置文件与安全策略规则关联，以防止利用系统缺陷或未经授权访问系统的行为，从而阻止允许的用户进行此类尝试。此外，您还可以在规则库层次结构的较低层级创建第二个安全策略规则，以拒绝其他所有人的访问。

- 在 *Strata Cloud Manager* 中，即使您可以通过 *GenAI app* 的安全策略创建自定义策略规则，也建议您使用互联网访问策略规则来高效地创建策略规则。
- 如果 *Enterprise Data Loss Prevention (E-DLP)* 许可证未激活，则不建议在同一策略中同时存在 *GenAI app* 和非 *GenAI app*。

- Strata Cloud Manager
- Panorama

创建自定义策略规则以控制 GenAI App 的使用 (Strata Cloud Manager)

您的互联网访问安全策略规则将优先于您的安全策略规则进行评估和执行。如果互联网访问策略规则和安全策略规则都适用于同一流量，则互联网访问策略规则操作和 *Enterprise DLP* 检查配置优先于安全策略规则。成功匹配到互联网访问策略规则后，不再进行进一步的策略规则评估。

例如，您可以创建适用于用户组 *A* 和多个 *GenAI app* 的互联网访问策略规则和安全策略规则。

- 互联网访问策略规则 *A* 允许用户组 *A* 访问指定的 *GenAI app*，并且与 *GenAI app* 关联 *Enterprise DLP* 数据配置文件 *A*，以防止敏感数据外泄。
- 安全策略规则 *B* 阻止用户组 *A* 访问相同的指定 *GenAI app*。

在这种情况下，当用户组 *A* 中的任何用户访问互联网访问和安全策略规则中指定的 *GenAI app* 时，他们将被允许，并且将执行 *Enterprise DLP* 检查和判决渲染，因为互联网访问策略规则 *A* 在策略规则库评估顺序中更高。

STEP 1 | 使用 AI Access Security Insights 仪表板来 发现 GenAI app 带来的风险。

AI Access Security Insights 仪表板可详细全面地显示 GenAI app 在您组织中的使用情况。您可以发现存在风险的 GenAI app 使用案例、存在风险的 GenAI app，以及访问 GenAI app 的风险用户。

STEP 2 | 如果您想在代码片段中使用现有策略，请执行初始 AI Access Security 配置。

在 Strata Cloud Manager 中，这包括创建 Enterprise Data Loss Prevention (E-DLP) 数据配置文件以定义敏感数据匹配标准，关联预定义的 `Gen-AI-Best-Practice` 和 `Application-Tagging` 代码片段，以及用于阻止利用系统缺陷或未经授权访问系统的漏洞保护配置文件。

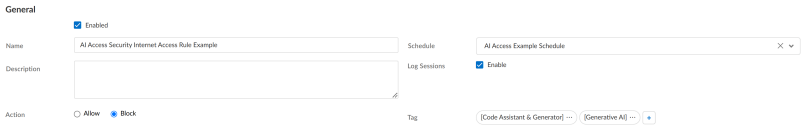
对于 NGFW，这还包括创建内部信任区域和出站非信任区域。

STEP 3 | 如果要构建自己的自定义策略，请登录到 Strata Cloud Manager。

STEP 4 | 创建自定义互联网访问策略规则。

- 在 *Strata Cloud Manager* 中，即使您可以通过 *GenAI app* 的安全策略创建自定义策略规则，也建议您使用互联网访问策略规则来高效地创建策略规则。
- 如果 *Enterprise Data Loss Prevention (E-DLP)* 许可证未激活，则不建议在同一策略中同时存在 *GenAI app* 和非 *GenAI app*。

1. 选择 **Add Rule**（添加规则） > **Internet Access Rule**（互联网访问规则）。
2. **Enable**（启用）互联网访问策略规则。
3. 输入描述性的 **Name**（名称）。
4. （可选）为互联网访问策略规则添加 **Description**（描述），并添加预定义的 **Tag**（标签）或创建一个新标签。
5. 配置 **Action**（操作）（**Block**（阻止）或 **Allow**（允许））。
6. （可选）配置 **Schedule**（计划）以指定互联网访问策略规则处于活动状态的时间。



7. 在“匹配条件”部分，根据流量 **Source**（源）（流量的来源）定义要强制执行的流量。

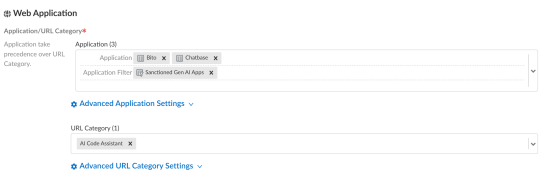
   例如，根据您的风险发现调查，您确定与 用户组 A 关联的未经授权的用户访问了经 用户组 B 认可的 GenAI app。在这种情况下，您可以创建一个互联网访问策略规则来阻止对 GenAI 的访问，并将 用户组 A 添加为用户组 **Source**（源）。

8. 在 Web 应用程序部分，配置 **Application**（应用程序）或 **URL Category**（**URL** 类别），以定义要阻止或允许访问哪些 GenAI app 或 GenAI app URL。

   （允许的 GenAI app）仅将支持的 GenAI app 添加到允许的 app 列表中。

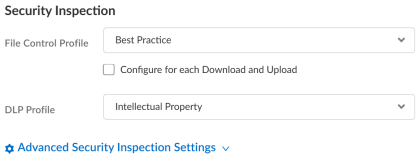
   - 应用程序 — 添加一个或多个 GenAI app。
   - 应用程序组 — 应用程序组是您创建的单个应用程序的静态分组。
   - 应用程序过滤器—应用程序过滤器根据您定义的 app 过滤器动态地对应用程序进行分组。

     例如，您可以使用预定义或自定义 GenAI app 筛选器动态控制对组织中 GenAI app 的访问，而不是添加单个 GenAI app 或创建每次需要更改时都必须手动更新的应用程序组。



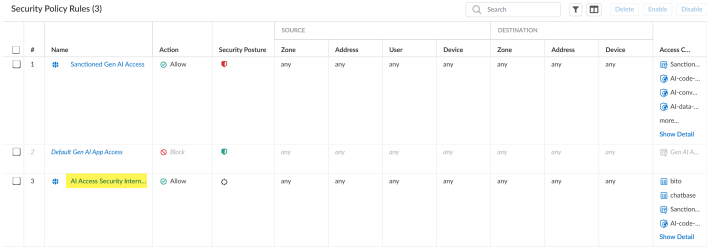
9. （允许的 GenAI app）在安全检查部分，选择文件阻止和 Enterprise DLP 配置文件，以防止敏感数据外泄。

- 文件控制配置文件 — 文件阻止配置文件 允许您识别要阻止或监视的特定文件类型。您可以创建自定义文件阻止配置文件，也可以使用默认的最佳实践文件阻止配置文件。
- **DLP** 配置文件 —Enterprise DLP 数据配置文件允许您定义要检测和阻止的敏感数据匹配条件，从而防止敏感数据外泄。当发现 GenAI app 带来的风险 时，必须分配数据配置文件以生成 **Sensitive Assets**（敏感资产）数据。



10. 配置根据需要配置其余的自定义 Internet 访问策略规则。
11. **Save**（保存）。

STEP 5 | 请确认您的访问策略规则已成功创建，并根据需要在策略规则库中对其进行排序。



STEP 6 | **Push Config**（推送配置）并 **Push**（推送）。

创建自定义策略规则以控制 GenAI App 的使用 (Panorama)

STEP 1 | 使用 AI Access Security Insights 仪表板来 发现 GenAI app 带来的风险。

AI Access Security Insights 仪表板可详细全面地显示 GenAI app 在您组织中的使用情况。您可以发现存在风险的 GenAI app 使用案例、存在风险的 GenAI app，以及访问 GenAI app 的风险用户。

STEP 2 | 执行初始 AI Access Security 配置。

这包括创建 Enterprise Data Loss Prevention (E-DLP) 数据配置文件，以定义敏感数据匹配标准，以及漏洞保护配置文件，用于阻止利用系统缺陷或未经授权访问系统的尝试。

对于 NGFW，这还包括创建内部信任区域和出站非信任区域。

STEP 3 | 登录到 Panorama™ management server Web 界面。

STEP 4 | 选择 **Policies**（策略） > **Security**（安全），然后指定 Device Group（设备组）。

STEP 5 | **Add**（添加）新安全策略规则。

STEP 6 | 配置安全策略规则 **General**（常规）、**Source**（源）和 **Destination**（目标）设置。

有关编写安全策略规则的详细信息，请参阅《安全策略管理指南》。

- **General**（常规）— 为安全规则提供一个描述性的 **Name**（名称）。您还可以选择为安全策略规则提供 **Description**（说明），并应用标签来帮助确定安全策略规则的用途。
- **Source**（源）— 定义安全策略规则应用时流量必须来自的位置。

  对于 **Source Zone**（源区），您可以选择内部信任区域。如果您希望安全策略规则应用于所有流量，而不论其源自何处，请为所有源设置选择 **Any**（任何）。

  例如，根据您的风险发现评估，您确定对 GenAI app 的访问过度配置，必须缩小到特定用户。在这种情况下，您可以编写 **Allow**（允许）策略规则并添加所需的 **Source User**（源用户）。
- **Destination**（目标）— 定义安全策略规则将应用的流量目标位置。

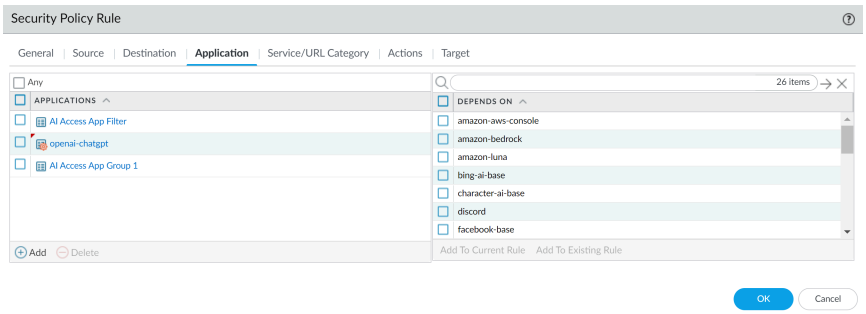
  对于 **Destination Zone**（目标区），您可以选择出站不信任区。如果您希望安全策略规则适用于所有流量，而不管流量目标是什么，请为所有目标设置选择 **Any**（任何）。

STEP 7 | 在 **Application**（应用程序）设置中，指定 GenAI 应用程序组、应用程序过滤器或应用程序。

（允许的 Web 应用程序）仅将支持的 GenAI app 添加到允许的应用程序列表中。

- 应用程序 — 添加一个或多个 GenAI app。
- **Application Category**（应用程序类别）— 应用程序类别（也称为应用程序过滤器）可根据您定义的应用程序过滤器动态地对应用程序进行分组。

  例如，您可以使用预定义或自定义 GenAI app 筛选器动态控制对组织中 GenAI app 的访问，而不是添加单个 GenAI app 或创建每次需要更改时都必须手动更新的应用程序组。
- 应用程序组 — 应用程序组是您创建的单个应用程序的静态分组。



STEP 8 | 配置安全策略规则 **Actions**（操作）。决定要对策略规则执行哪些操作。最佳实践是附加安全配置文件，使防火墙能够扫描所有允许的流量以发现威胁。从 **Profile Type**（配置文件类型）下拉列表中选择 **Profiles**（配置文件），然后选择要附加到规则的各个安全配置文件。请为您的 GenAI app 选择以下设置所需的操作：

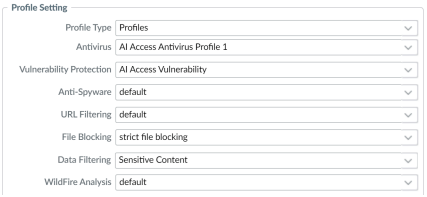
1. 对于 **Action**（操作），配置 NGFW 在检测到从安全策略规则 **Source**（源）到 **Destination**（目标）的流量时采取的 Action（操作）。

   例如，如果要允许访问一个或多个 GenAI app，请选择 **Allow**（允许），如果要阻止对一个或多个 GenAI app 的所有访问，请选择 **Deny**（拒绝）。
2. 对于 **Profile Type**（配置文件类型），选择 **Profiles**（配置文件）。

   您至少必须添加 **Vulnerability Protection**（漏洞防护）和 **Data Filtering**（数据过滤）配置文件。在发现 GenAI app 带来的风险时，需要这些来生成 **Threats**（威胁）和

Sensitive Assets（敏感资产）数据。其余配置文件是可选的，可以根据需要配置。对于以下每种安全配置文件类型，您可以选择现有配置文件或创建新配置文件。

- 反病毒
- 漏洞保护
- 防间谍软件
- URL 筛选
- 文件传送阻止
- 数据筛选
- WildFire Analysis



在 ***Actions***（操作）选项卡中，***Profile Setting***（配置文件设置）优先于 ***Action Setting***（操作设置）。因此，最佳做法是确保两种设置正确匹配。例如，即使将 *Action Settings*（操作设置）设置为 *Allow*（允许），并将其中一个 *Profile Settings*（配置文件设置）设置为 *Block*（阻止）*ChatGPT*，它仍会被阻止。

STEP 9 | 提交并将新配置推送到您的受管防火墙，以完成 Enterprise DLP 插件的安装。

此步骤是使 Enterprise DLP 数据过滤配置文件名称出现在数据过滤日志中的必要步骤。

不建议对*Enterprise DLP*配置更改使用 ***Commit and Push***（提交并推送）命令。使用 ***Commit and Push***（提交并推送）命令需要额外且不必要的操作开销，即在推送范围选择中手动选定受影响的模板和受管防火墙。

- **Panorama** 的完整配置推送
  1. 选择 **Commit**（提交） > 提交到 **Panorama**以及 **Commit**（提交）。
  2. 选择 **Commit**（提交） > **Push to Devices**（推送到设备），然后选择 **Edit Selections**（编辑选择）。
  3. 选择 **Device Groups**（设备组），并选择 **Include Device and Network Templates**（包含设备和网络模板）。
  4. 单击 **OK**（确定）。
  5. 将您的配置更改 **Push**（推送）到使用 Enterprise DLP 的受管防火墙。
- **Panorama** 的部分配置推送

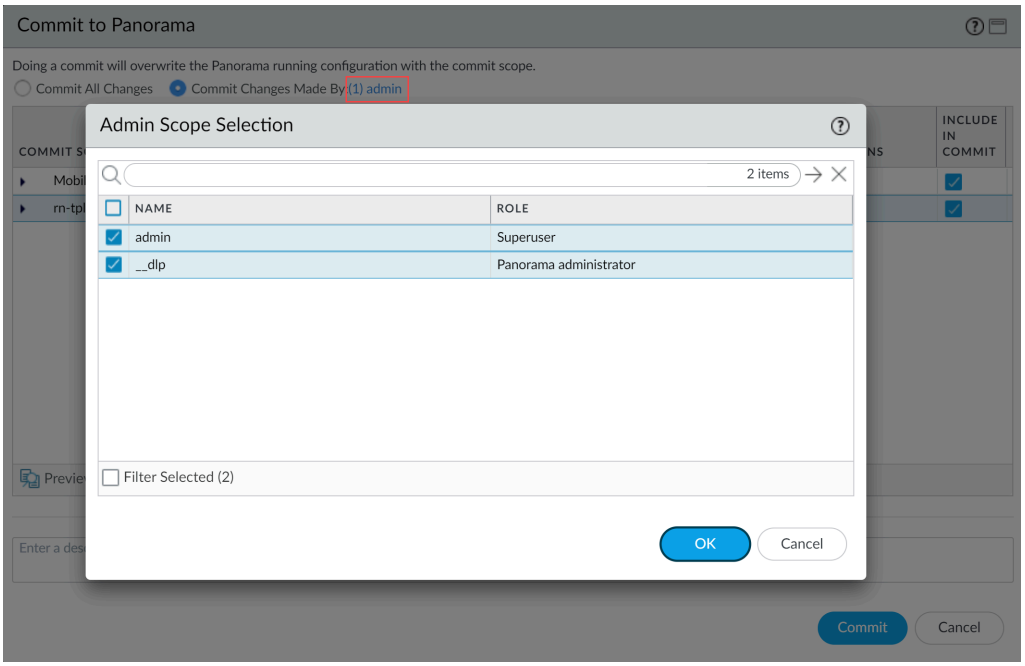
  执行部分配置推送时，务必包含临时 *__dlp* 管理员。这是保持 *Panorama* 和 *DLP* 云服务同步所必需的。

  例如，您有一个 *admin Panorama* 管理员用户，允许其提交和推送配置更改。*admin* 用户对 *Enterprise DLP* 配置进行了更改，并且只想提交这些更改并将其推送到受管防火墙。在这种情况下，*admin* 用户还需要在部分提交和推送操作中选择 *__dlp* 用户。

  1. 选择 **Commit**（提交） > 提交到 **Panorama**。
  2. 选择 **Commit Changes Made By**（提交更改者）然后单击当前 Panorama 管理员用户，选择要包含在部分提交中的其他管理员。

     在本例中，admin 用户当前已登录并正在执行提交操作。管理员用户必须单击 **admin**，然后选择 __dlp 用户。如果其他 Panorama 管理员进行了其他配置更改，也可以在此处选择。

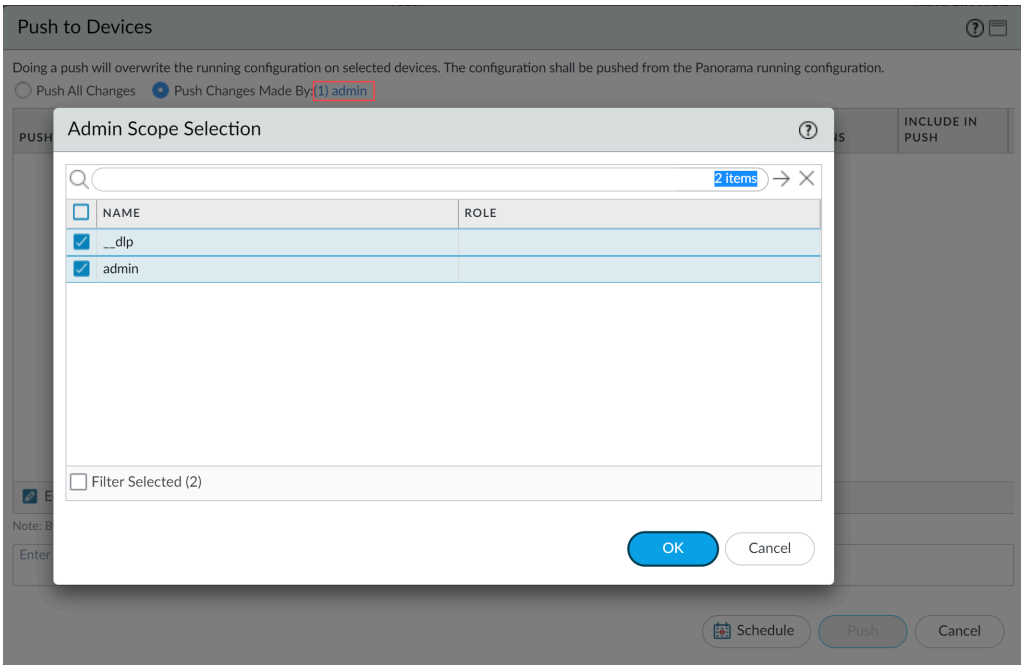
     单击 **OK**（确定）继续。



3. **Commit**（提交）。
4. 选择 **Commit**（提交） > **Push to Devices**（推送到设备）。
5. 选择 **Push Changes Made By**（推送更改者），然后单击当前 Panorama 管理员用户，选择要包含在部分推送中的其他管理员。

   在本例中，`admin` 用户当前已登录并正在执行推送操作。管理员用户必须单击 **admin**，然后选择 `__dlp` 用户。如果其他 Panorama 管理员进行了其他配置更改，也可以在此处选择。

   单击 **OK**（确定）继续。



6. 选择 **Device Groups**（设备组），并选择 **Include Device and Network Templates**（包含设备和网络模板）。
7. 单击 **OK**（确定）。
8. 将您的配置更改 **Push**（推送）到使用 Enterprise DLP 的受管防火墙。

AI Access Security 建议

您的网络安全管理员可以通过AI Access Security 仪表板和 Strata Command Center 获得有关 GenAI app 在您组织网络上的使用情况的宝贵数据。为了使您的网络安全管理员能够在采用 GenAI app 时快速解决漏洞并加强安全态势，Palo Alto Networks 引入了 AI Access Security 建议。

AI Access Security 提供手动和自动建议。手动建议是指需要您手动实施的建议。AI Access Security 提供分步说明，并提供所有相关文档的链接，以帮助您成功实施建议的更改。Strata Cloud Manager 上的 Palo Alto Networks Copilot 实现的是自动化推荐，而不是管理员操作。但是，提出 AI Access Security 建议的管理员必须批准所有更改。

- 针对 **NGFW** 和 **Prisma Access** 的建议（由 **Strata Cloud Manager** 管理）— AI Access Security 建议会随着管理员进行配置更改而实时更新，并且 AI Access Security 会分析您网络上的流量。这样一来，您可以快速响应任何配置更改或可能危及您组织的风险 GenAI app 流量，如果不立即处理，这些更改或流量可能会危及您的组织。任何分析网络流量的建议都会回顾过去七天的数据，以此作为建议的依据。

  如果您有 NGFW 和 Prisma Access（由 Strata Cloud Manager 管理）以及 Prisma Access Browser，则 AI Access Security 仅显示针对您的 NGFW 和 Prisma Access 租户的建议。在这种情况下，AI Access Security 不显示 Prisma Access Browser 建议。
- 针对 **NGFW** 和 **Prisma Access** 的建议（由 **Panorama** 管理）— AI Access Security 建议每 24 小时在 Strata Cloud Manager 上更新一次。

  如果您有 NGFW 和 Prisma Access（由 Panorama 管理）以及 Prisma Access Browser，则 AI Access Security 仅显示针对您的 NGFW 和 Prisma Access 租户的建议。在这种情况下，AI Access Security 不显示 Prisma Access Browser 建议。
- 针对 **Prisma Access Browser** 的建议 — AI Access Security 建议是静态的，在您实施后仍然有效。Palo Alto Networks 建议您在实施后继续监控这些建议，以确保您的安全管理员能够解决 GenAI app 采用策略中的任何漏洞。

  AI Access Security 仅在您拥有独立 Prisma Access Browser 许可证且未部署任何 NGFW 或 Prisma Access 租户时才会显示 Prisma Access Browser 的建议。

  如果您有 NGFW 和 Prisma Access（由 Panorama 或 Strata Cloud Manager 管理）以及 Prisma Access Browser，则 AI Access Security 仅显示针对您的 NGFW 和 Prisma Access 租户的建议。在这种情况下，AI Access Security 不显示 Prisma Access Browser 建议。

AI Access Security 针对以下场景提供建议。

- **GenAI App** 分类建议

  专注于根据您网络及其 app 中 GenAI app 的使用情况提供建议。

  例如，如果 AI Access Security 注意到您的组织允许流量访问未认可的 GenAI app。在这种情况下，AI Access Security 建议将这些 GenAI app 重新分类为 Sanctioned（已认可）或 Tolerated（可容忍）。

- 最佳实践检查和政策建议

  AI Access Security 使用 最佳实践评估 (BPA) 服务来分析您现有的 NGFW 和 Prisma Access 策略规则库，以提供建议来加强您的安全态势，从而安全地采用 GenAI app。

  例如，如果 BPA 服务发现您有一条安全策略规则允许访问未认可的 GenAI app。

- **Data Loss Prevention**（数据丢失防护-**DLP**）建议

  为了防止敏感数据泄露到已认可和可容忍的 GenAI app，AI Access Security 分析您的安全策略规则，以确定您是否将流量转发到 Enterprise DLP 进行在线检查和静态数据检查。这还可以包括将流量转发到 Enterprise DLP 所需的配置建议

- 接入并最大化 **AI Access Security**

  这些建议侧重于提供可操作的建议，以更好地利用平台的各项功能。这些建议侧重于用户与各种市场的连接，或者针对支持静态数据的 GenAI app。

- **Prisma Access Browser** 建议

  针对 Prisma Access Browser 的建议侧重于提供有针对性的指导，以帮助 Prisma Access Browser 独立用户保护和优化其 GenAI app 的使用。这些建议包括配置 GenAI app 访问权限、激活预定义的安全策略规则以保护通过 Prisma Access Browser 访问的 GenAI app 的访问权限，以及审查疑似敏感数据泄露到未认可的 GenAI app 的事件。

生成 AI Access Security 报告

AI Access Security报告全面概述您组织的 GenAI app 和插件使用情况以及安全状况。本报告旨在帮助您理解并管理您所处环境中快速发展的 GenAI app 所带来的风险。本报告包含大量可操作的见解和量身定制的建议，使您的安全管理员能够就 GenAI app 采用策略和安全做出明智的决策。

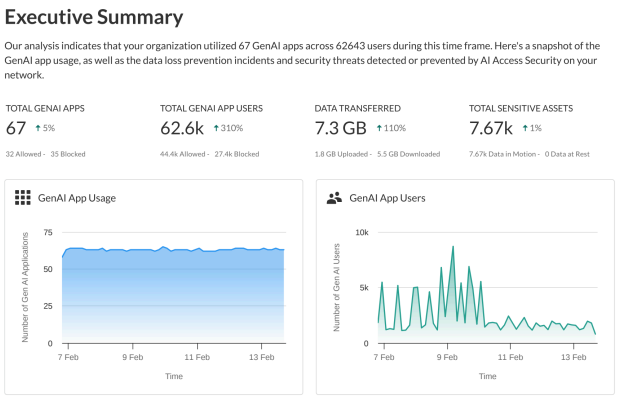
AI Access Security 报告的关键组成部分包括：

- 执行摘要

  执行摘要部分概述您组织中 GenAI app 和插件的关键指标。它简要概述了以下内容：

  - GenAI app 使用情况，您快速了解组织内用户访问这些 app 的广泛程度。
  - GenAI app 上传和下载的数据量（以千兆字节 (GB) 为单位）。
  - 检测到的动态和静态敏感数据资产数量。

  执行摘要部分为您的安全管理员提供了一个快速、一目了然的视角，了解您组织内的 GenAI app 概况。它作为进入报告后续章节中提供的更详细信息的入口点，使您的安全管理员能够快速掌握组织的整体 GenAI 安全状况，并确定可能需要进一步关注或调查的领域。

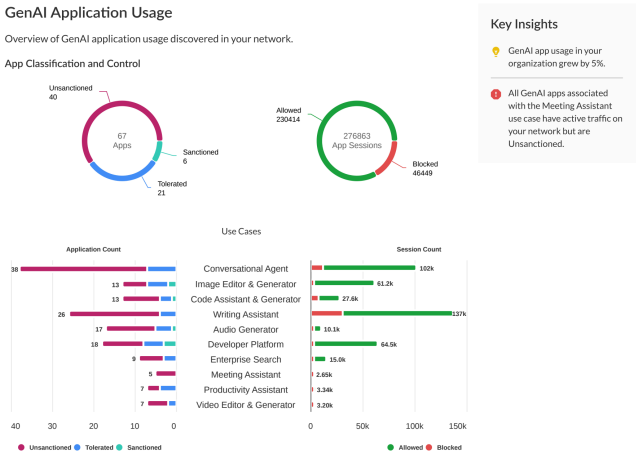


- **GenAI** 应用程序使用情况

  GenAI App 使用情况部分提供了组织内 GenAI app 使用情况的全面细分数据。其中包括：

  - GenAI App 总数，显示已允许和已阻止的 GenAI app，以及已认可、可容忍和未认可的 GenAI app 的分布情况。
  - GenAI 用例细分，按 app 分类（已认可、可容忍或认可）以及流量是否已允许或已阻止进行分类。
  - 未认可但已允许的 app 数，包括自报告期开始以来的更改。
  - 未认可但已允许的 GenAI app 的汇总使用数据，包括用户数量和传输的数据总量。
  - 前 5 个未认可但已允许的 GenAI app 的详细信息，包括 app 名称、用户数、会话数和相关风险因素。

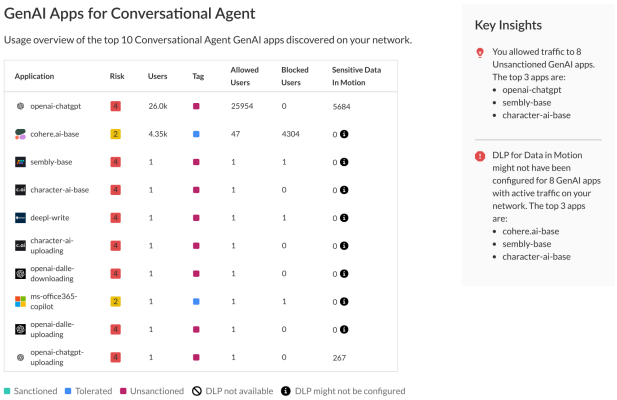
  本部分可帮助您的安全管理员快速识别潜在的安全风险，了解 GenAI app 在不同使用场景下的使用情况，并就应用使用策略规则和安全态势做出明智的决策。



- 热门用例的 **GenAI App**

  热门用例的 GenAI App 部分概述了您组织内使用最多的 10 个 GenAI app，并按 GenAI app 用例 进行分类。它详细列出了您组织中最常用的 GenAI app，并包含每个 GenAI app 的以下信息：

  - 使用的 GenAI app 的名称。
  - 与 GenAI app 相关的风险评分。
  - 使用 GenAI app 的唯一用户数。
  - GenAI app 分类，指明 app 是已许可、可容忍还是未认可。
  - GenAI app 允许和阻止的唯一会话数。
  - 用户访问 GenAI app 时生成的Enterprise DLP事件数。

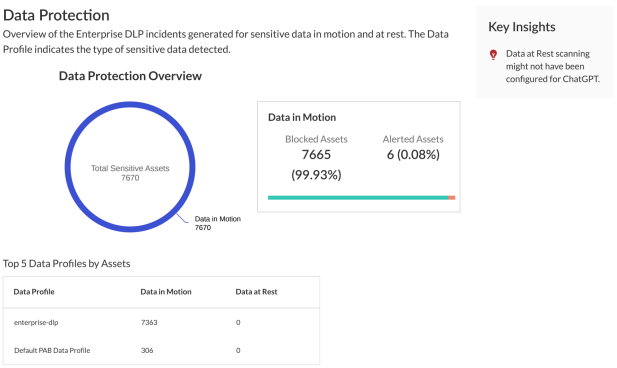


- 数据保护

  数据保护部分提供了有关组织 GenAI 生态系统中敏感数据处理的关键见解。本部分包括：

  - 检测到的敏感资产总数，分为已允许或已阻止两类。
  - 敏感资产在所有 GenAI app 中的分布情况，按敏感资产类型分组。
  - 排名前 5 的 GenAI app 中发现的敏感数据的详细信息。

  这些信息可以帮助您的安全管理员快速识别与组织内 GenAI app 使用相关的潜在数据安全风险。通过突出显示哪些 GenAI app 正在处理敏感信息以及正在处理哪些类型的敏感数据，您可以优先考虑数据保护工作，并根据需要调整安全策略规则。



STEP 1 | 登录 Strata Cloud Manager

STEP 2 | 选择 **Insights**（见解） > **SECURITY**（安全） > **AI Access**（**AI** 访问）。

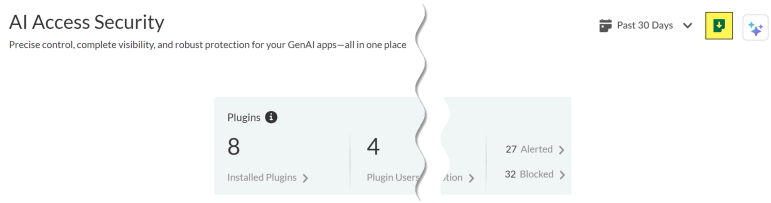
STEP 3 | 选择 AI Access Security 报告的时间范围。

AI Access Security 支持生成过去**24**小时、过去**7**天或过去**30**天的报告。

STEP 4 | 以 PDF 格式将 AI Access Security 报告 **Download**（下载）到您的本地设备。

默认文件名为 `AI Access Security Report <generation-date>.pdf`。

在 *AI Access Security* 报告下载完成之前不要离开或刷新页面。在下载完成之前离开或刷新页面会中断下载，您必须重新下载 *AI Access Security* 报告。



STEP 5 | 导航到您选择的下载文件夹并查看 AI Access Security 报告。