

**A world where each day
is safer and more secure
than the one before**

TÀI LIỆU GIỚI THIỆU VÀ THỬ NGHIỆM GIẢI PHÁP AI ACCESS (AIAS)

Prepared by: thanhnguyen@paloaltonetworks.com (CCIE, PCNSE, NSE7)

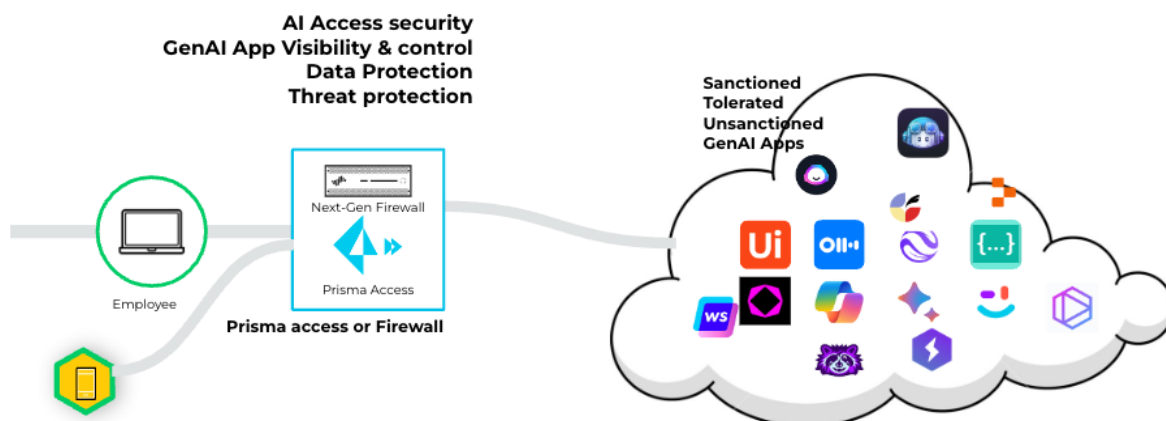
Liên hệ **Zalo 0904829879** để được hỗ trợ tư vấn các giải pháp của Palo Alto Network tại thị trường Việt Nam.

Contents

1	Giới thiệu chung	3
2	Mô hình thử nghiệm	3
3	Thiết lập môi trường PoC.....	4
3.1	Thiết lập kết nối GP	4
3.2	Cấu hình SSL Decryption	4
3.2.1	Tạo Self-Sign Root CA.....	4
3.2.2	Export Root CA Cert và cài đặt trên máy Client.	5
3.2.3	Tạo Cert Forward Trust	5
3.2.4	Tạo Cert Forward Untrust	6
3.2.5	Cài đặt Cert cho GP Portal	6
3.2.6	Cấu hình SSL Decrypt Rule	7
4	Kết quả chi tiết các Test Cases.....	7
4.1	Phát hiện tất cả các GenAI Apps đang được sử dụng trong tổ chức	7
4.2	Xem thuộc tính (Attributes) của AI Apps	9
4.3	Kiểm soát cho phép/ngăn chặn các GenAI Apps.....	10
4.4	Sử dụng cấu hình có sẵn (Predefined Snippet) trên Prisma Access	14
4.5	Phát hiện dữ liệu nhạy cảm gửi qua GenAI Apps	14
4.6	Phát hiện dữ liệu chứa mã độc gửi qua GenAI Apps.....	18
4.7	Đề xuất cấu hình tối ưu chính sách	19
4.8	Báo cáo GenAI Report	21

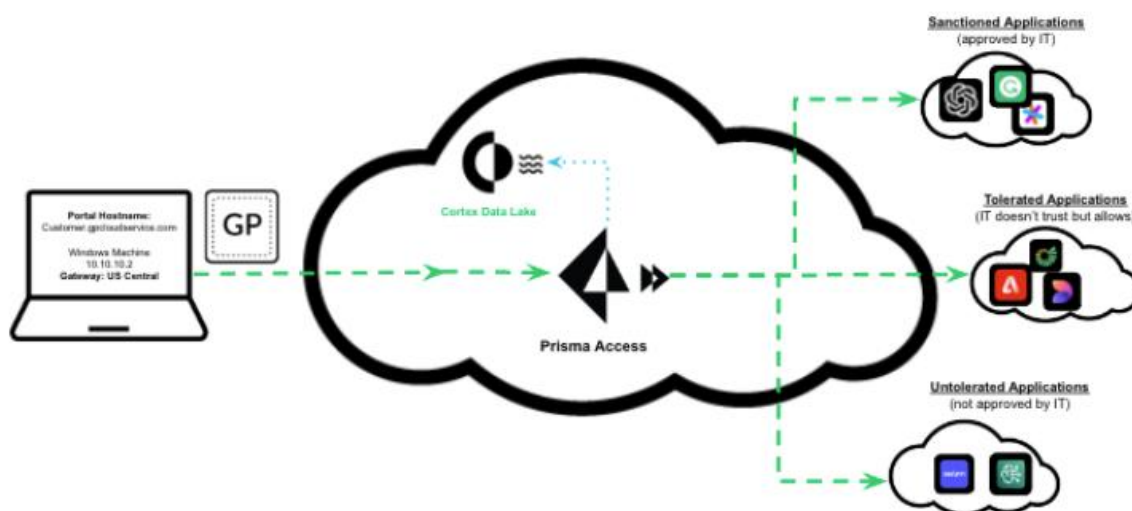
1 Giới thiệu chung

AI Access là tính năng chạy trên NGFW hoặc giải pháp SSE (Prisma Access) của Palo Alto Networks để quản lý các GenAI application, cung cấp khả năng visibility, access control, data và threat protection, cho phép khách hàng sử dụng các ứng dụng GenAI nhưng vẫn ngăn chặn các nguy cơ tấn công và thất thoát dữ liệu.



2 Mô hình thử nghiệm

Client (with GP installed) ----- Prisma access ----- Internet



3 Thiết lập môi trường thử nghiệm

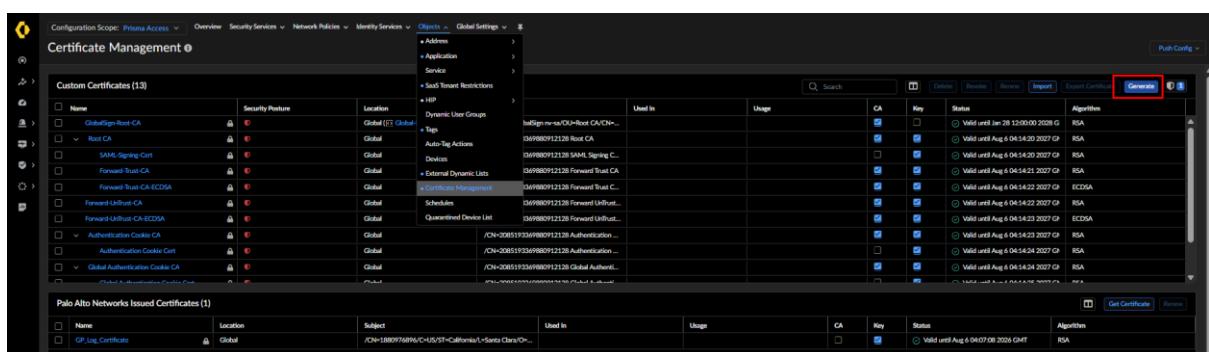
3.1 Thiết lập kết nối GP

Thiết lập kết nối Remote VPN sử dụng Global Protect trên máy Client tới Prisma Access.

3.2 Cấu hình SSL Decryption

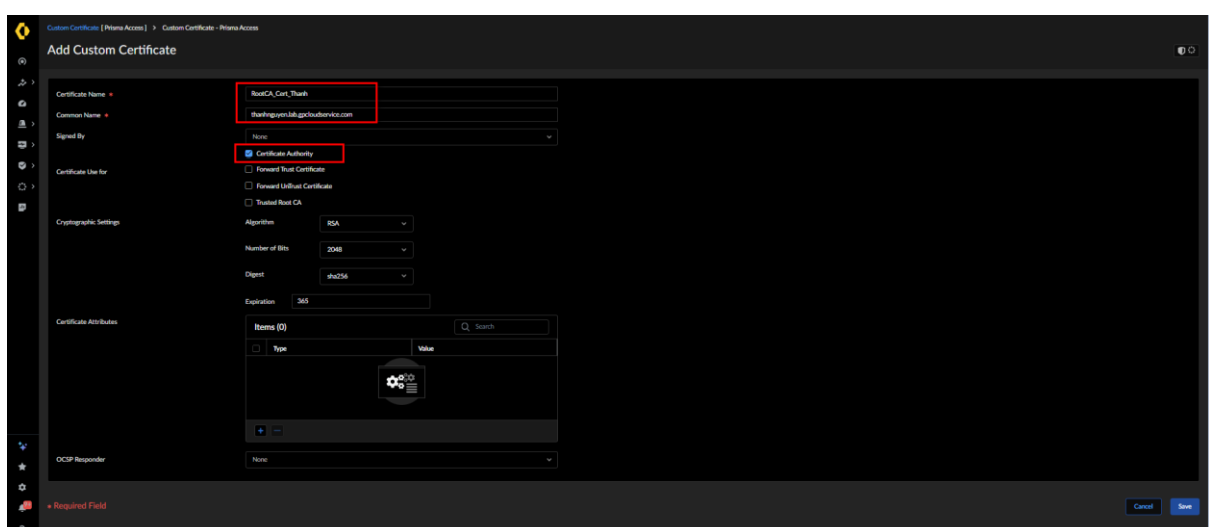
3.2.1 Tạo Self-Sign Root CA

Truy cập Objects – Certificate Management – Generate để tạo Cert



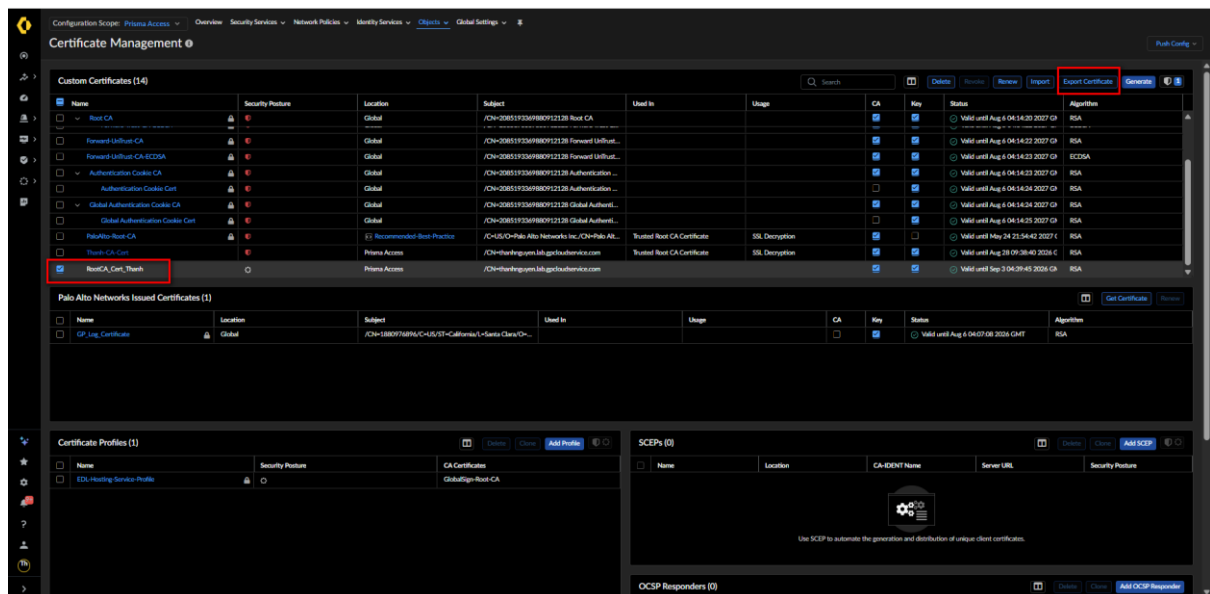
Khai báo thông tin Root CA Cert:

- Certificate Name: Tùy ý
- Common Name: Trùng với Domain Name (khuyến nghị) hoặc địa chỉ IP của service sẽ dùng Cert này.
- Chọn “Certificate Authority” để xác định đây là Self-Sign Cert Root CA.



3.2.2 Export Root CA Cert và cài đặt trên máy Client.

Chọn Cert muốn export và click “Export Certificate”:



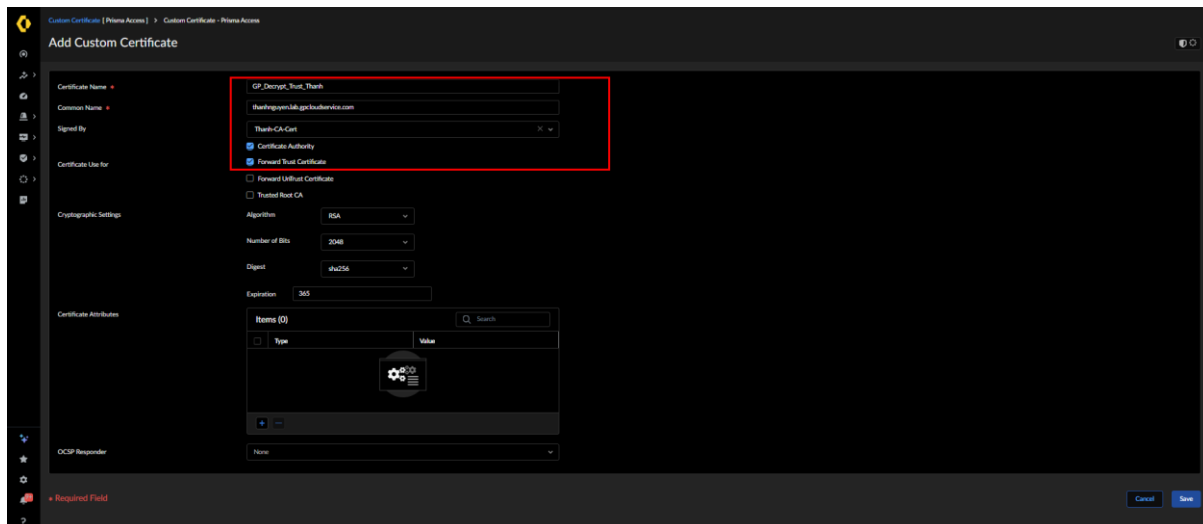
Chọn DER format:



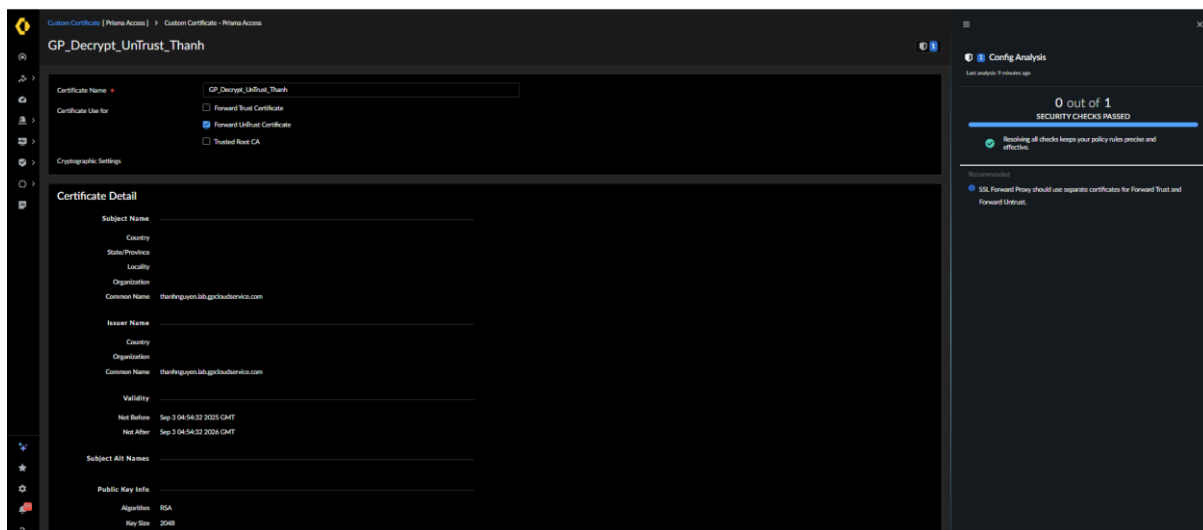
Sau khi export, cài đặt Cert trên vào danh sách Trusted Root CA trên máy.

3.2.3 Tạo Cert Forward Trust

Truy cập Objects – Certificate Management – Generate để tạo Cert

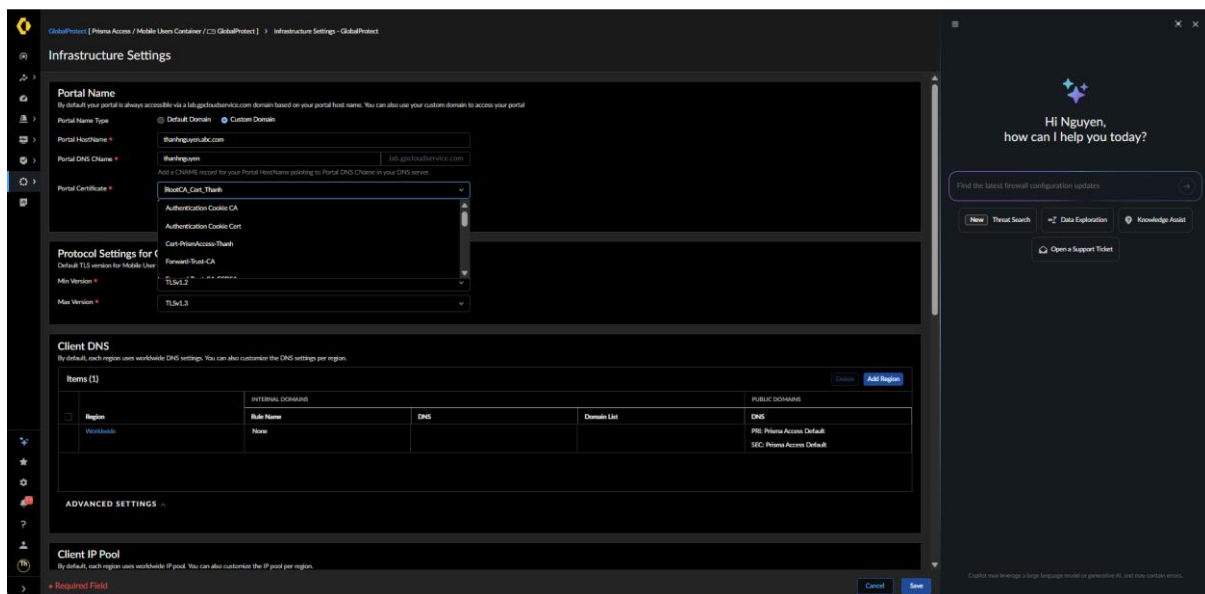
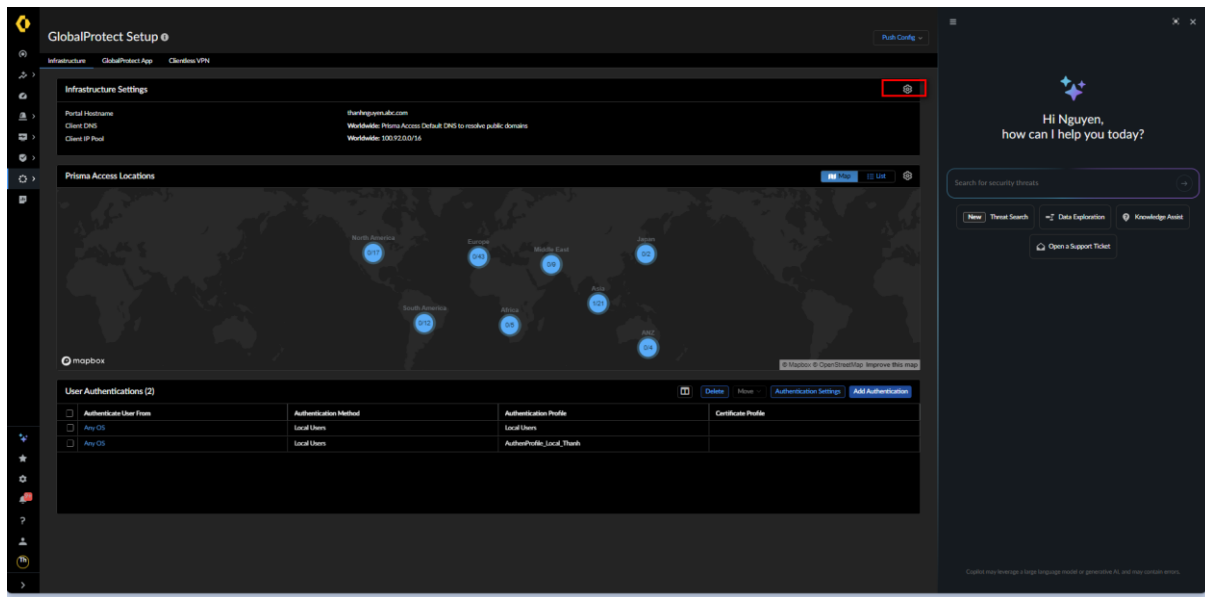


3.2.4 Tạo Cert Forward Untrust



3.2.5 Cài đặt Cert cho GP Portal

Vào Workflow – Prisma Access Setup:



Kết quả, khi kết nối GP không còn cảnh báo Cert

3.2.6 Cấu hình SSL Decrypt Rule

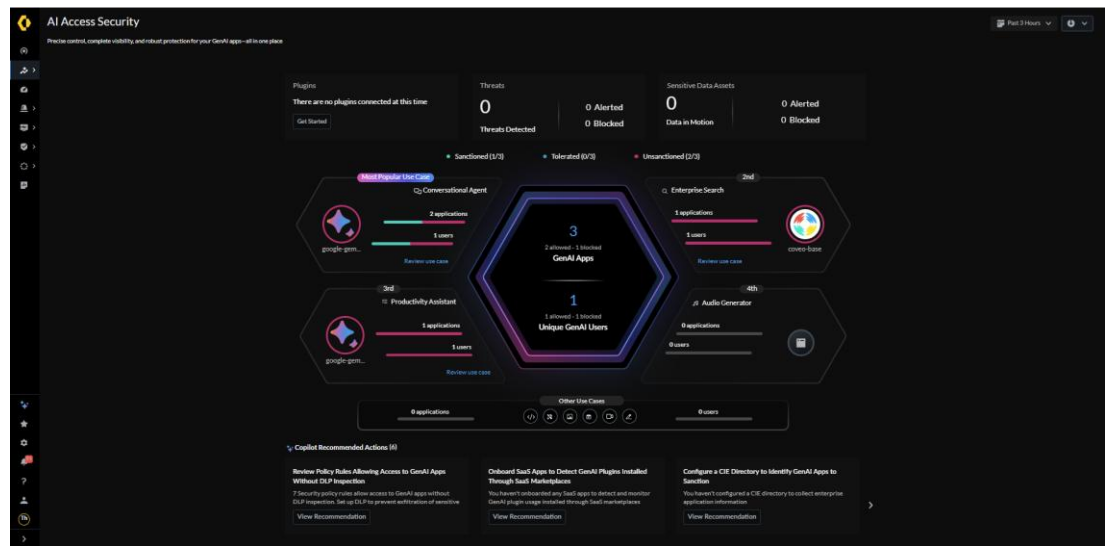
4 Kết quả chi tiết các Test Cases

4.1 Phát hiện tất cả các GenAI Apps đang được sử dụng trong tổ chức

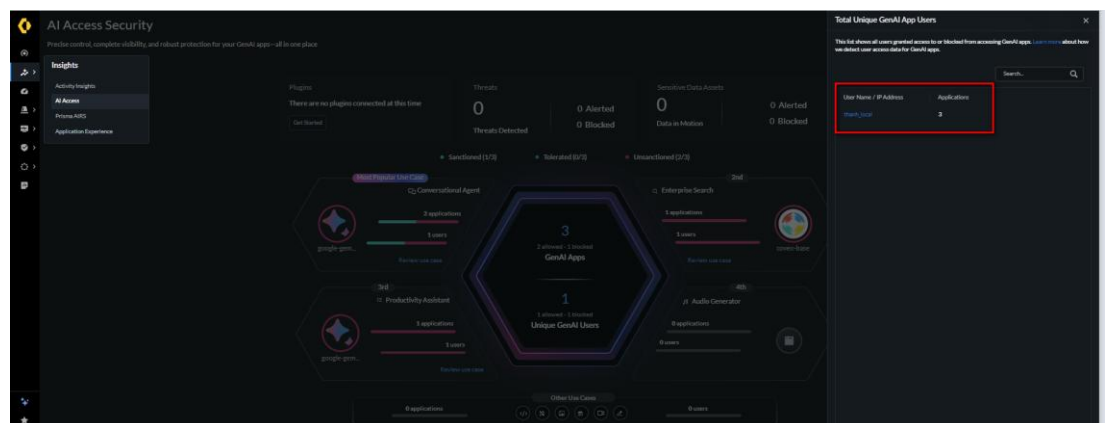
Mục tiêu	Xác định tất cả các GenAI Apps đang được sử dụng trong tổ chức, từ đó sử dụng làm căn cứ để phân loại và thiết lập chính sách kiểm soát các GenAI Apps này.
Các bước thực hiện	Kết nối người dùng GP tới Prisma Access, truy cập 1 số ứng dụng GenAI như ChatGPT, Gemini...để hệ thống có log.

Kết quả thực tế

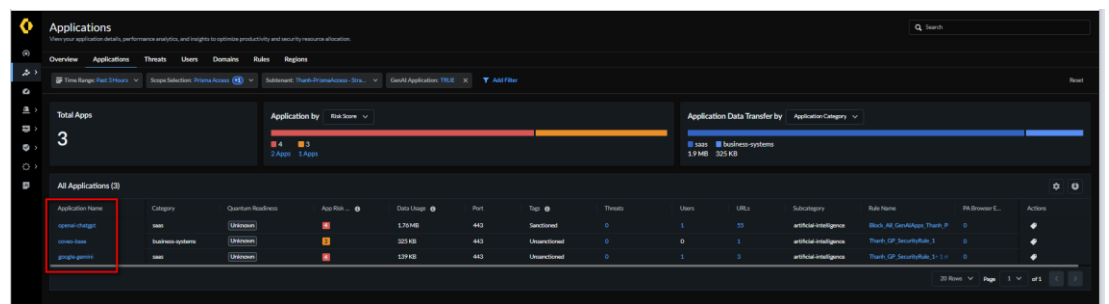
Truy cập AI Insight sẽ thấy được danh sách các GenAI Apps và người dùng trong hệ thống:



Danh mục GenAI Users:



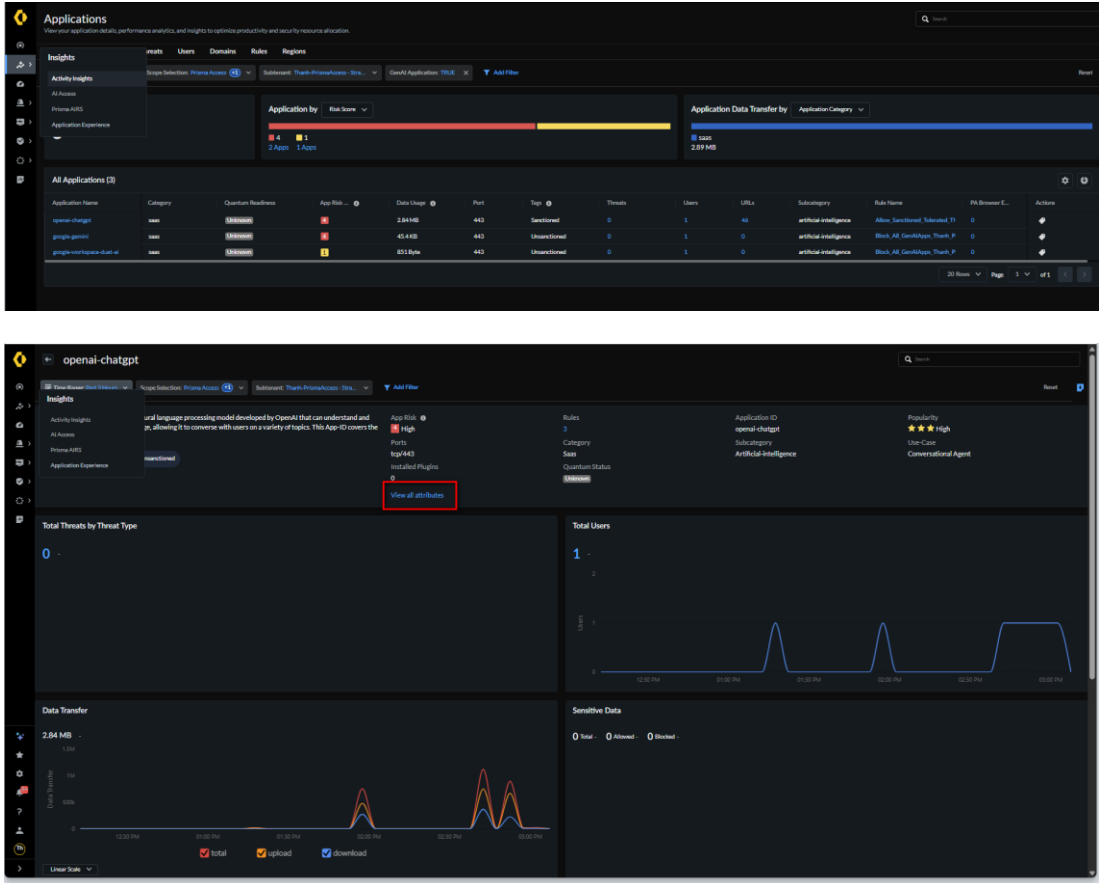
Danh mục GenAI Apps:

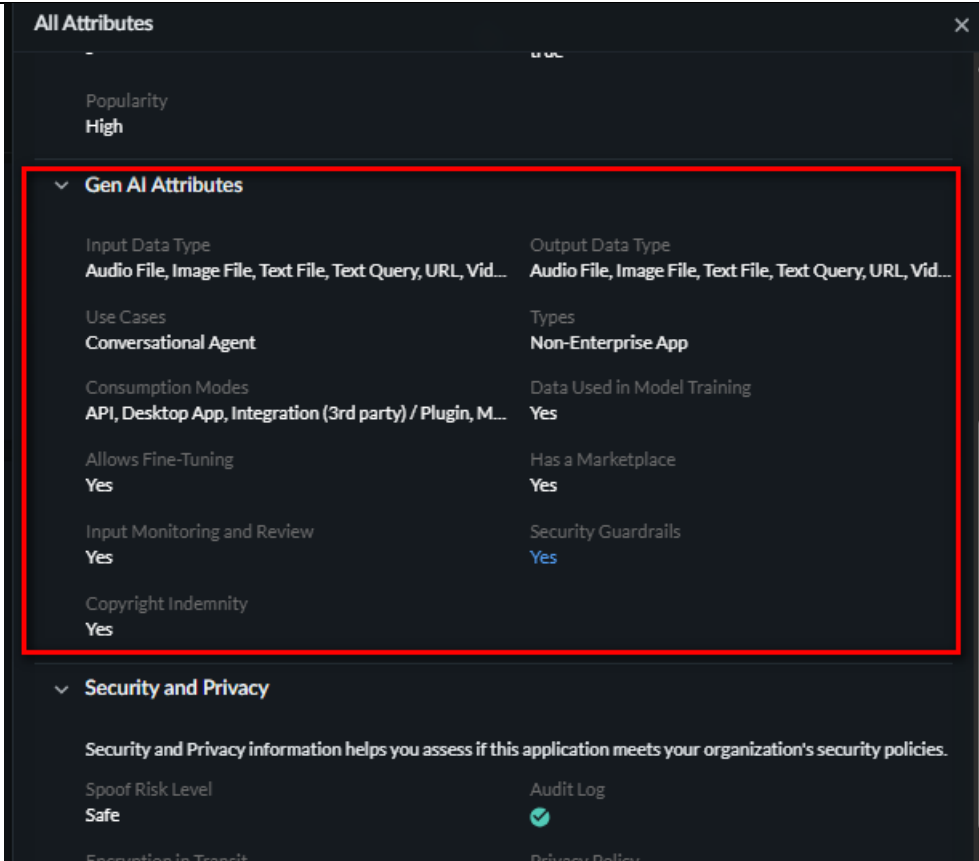


Đánh giá

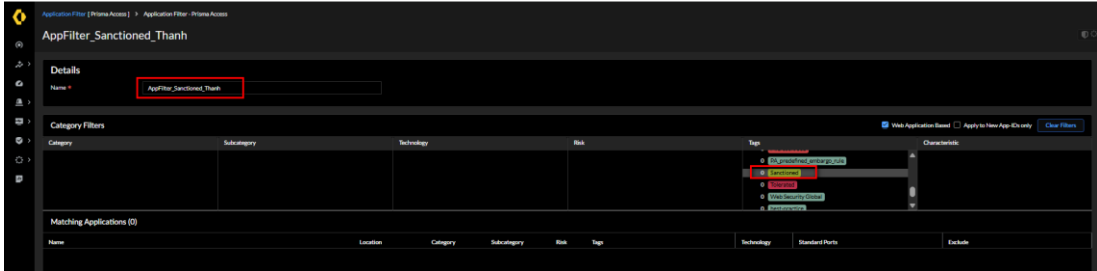
- Kết quả: ☐ Pass ☐ Fail
- Ghi chú:

4.2 Xem thuộc tính (Attributes) của AI Apps

Mục tiêu	Dựa vào các thuộc tính này, quản trị viên có thể cân nhắc và quyết định xem nên xếp AI Apps này vào thể loại nào, tương ứng là chính sách cho phép hay ngăn chặn AI App này.
Các bước thực hiện	Vào Activity Insight, lọc các App GenAI và chọn 1 App cụ thể (ví dụ: openai-chatgpt):  Xem thuộc tính:

	
Kết quả thực tế	
Đánh giá	- Kết quả: ☐ Pass ☐ Fail - Ghi chú:

4.3 Kiểm soát cho phép/ngăn chặn các GenAI Apps

Mục tiêu	Kiểm soát cho phép/ngăn chặn GenAI Apps
Các bước thực hiện	Cấu hình khai báo Application Filter, match với các Apps được tag là “Sanctioned” và “Tolerated”.  Ngoài các tag được gán thêm, tất cả các GenAI Apps đều được gán tag mặc định “GenerativeAI”, cấu hình gán nhãn cuối cùng như sau:

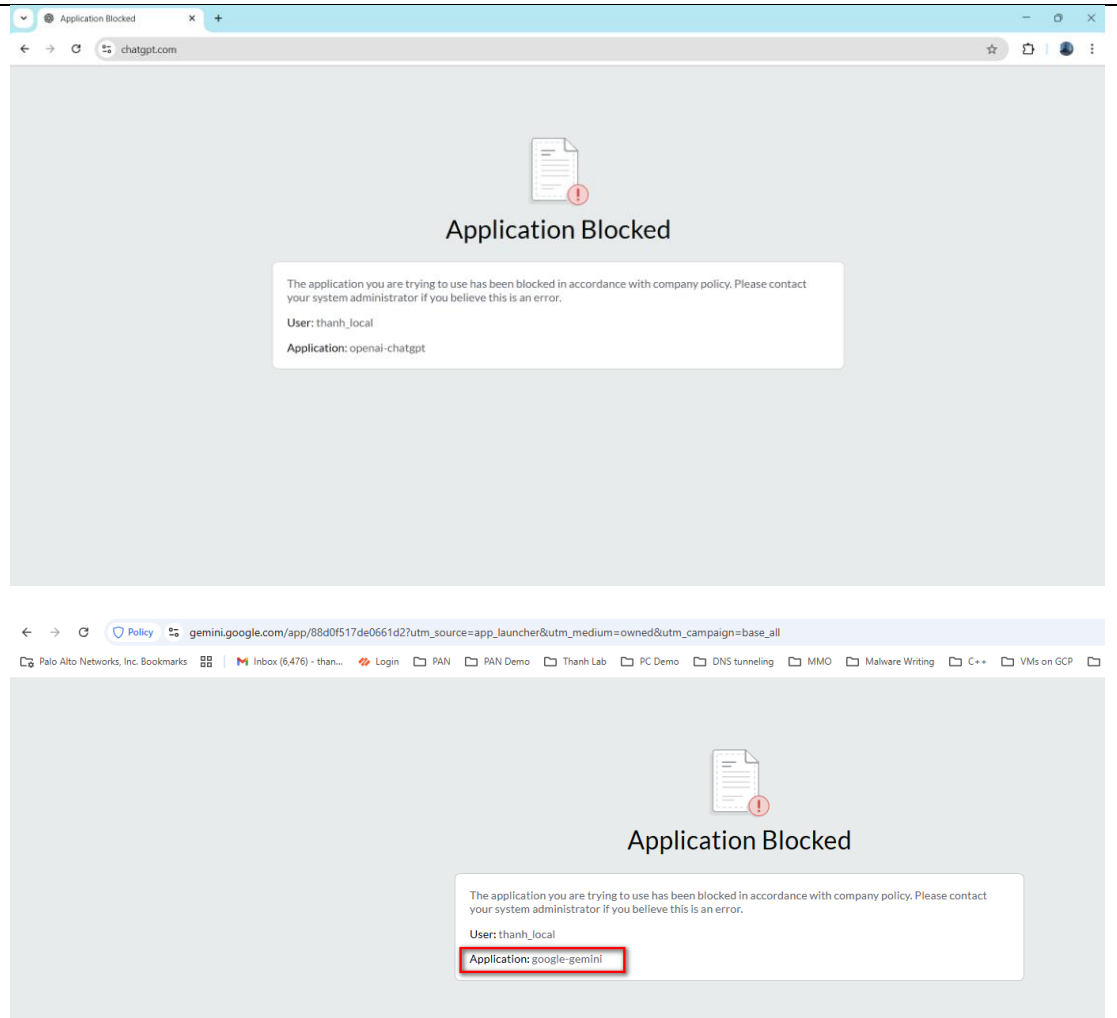
☐	AppFilter_Sanctioned_Thanh	☐	Prisma Access							Generation-AI Web-App Sanctioned		yes	
☐	AppFilter_Sanctioned_Thanh	☐	Prisma Access							Generation-AI Web-App Tolerated		yes	
☐	AppFilter_AI_GenAIApps_Thanh	☐	Prisma Access							Web-App Generation-AI	☒	yes	

Cấu hình Internet Access Rule, chỉ cho phép các App được tag là “Sanctioned” và “Tolerated”.

Thêm 1 Rule bên dưới, chặn tất cả các App GenAI còn lại (không phải Sanctioned và Tolerated):

Kết quả thực tế

Mặc định tất cả các GenAI Apps đều được phân loại là Unsanctioned nên ban đầu các ứng dụng như ChatGPT, Gemini...đều bị chặn lại:



Log ghi nhận chặn ứng dụng ChatGPT, Gemini:

Log Viewer

2025-09-08 13:19:05 - 2025-09-08 14:19:05 | 9 results | Page 1 of 1 | Export | Refresh

Subtype	From Zone	Source Address	Source User	To Zone	Destination Address	Destination User	Destination Port	Application	Action
deny	trust	100.10.0.2	thanh_local	untrust	44.201.170.113		443	google-gemini	deny
deny	trust	100.10.0.2	thanh_local	untrust	44.201.170.113		443	google-gemini	deny
deny	trust	100.10.0.2	thanh_local	untrust	44.201.170.113		443	google-gemini	deny
deny	trust	100.10.0.2	thanh_local	untrust	74.125.46.95		443	google-workspace-chat-ai	deny
deny	trust	100.10.0.2	thanh_local	untrust	104.18.52.47		443	openai-chatgpt	deny
deny	trust	100.10.0.2	thanh_local	untrust	104.18.52.47		443	openai-chatgpt	deny
deny	trust	100.10.0.2	thanh_local	untrust	104.18.52.47		443	openai-chatgpt	deny
deny	trust	100.10.0.2	thanh_local	untrust	172.64.155.209		443	openai-chatgpt	deny
deny	trust	100.10.0.2	thanh_local	untrust	172.64.155.209		443	openai-chatgpt	deny

Đánh dấu và phân loại lại ChatGPT thành ứng dụng Sanctioned:

Applications

View your application details, performance analytics, and insights to optimize productivity and security resource allocation.

Overview Applications Threats Users Domains Rules Regions

Time Range: Past 24 hours | Scope Selection: Private-ASIS | Subdomain: Thanh-Framwork-Dev... | Source Type: User | Search Application: 190K | Add Filter

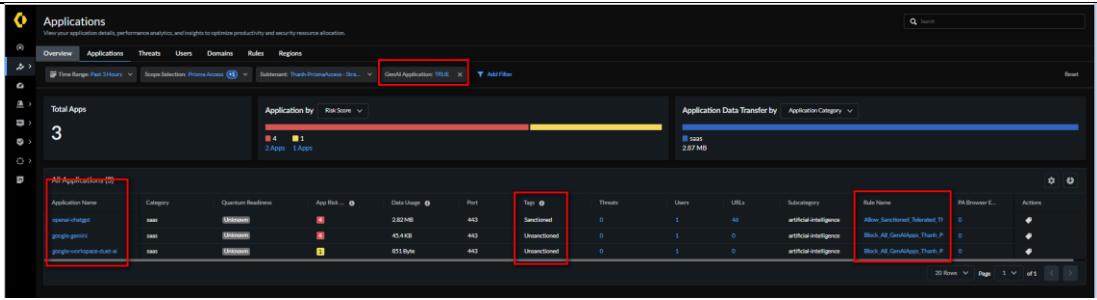
Total Apps: 4

Application by Risk Score: 4 Apps (2 Apps) | Application Data Transfer by Application Category: 0 Apps (Business-systems: 1.79 MB, 325 KB)

All Applications (4)

Application Name	Category	Quantum Readiness	App Risk	Data Usage	Port	Tags	Threats	Users	URLs	Subcategory	Rule Name	Risk Score	Actions
openai-chatgpt	user	Unmonitored	High	1.03 MB	443	Unsanctioned	0	1	50	artificial-intelligence	Threat_CP_SecurityRule.1	0	Sanctioned Threatened Unsanctioned
google-gemini	business-systems	Unmonitored	High	323 KB	443	Unsanctioned	0	0	1	artificial-intelligence	Threat_CP_SecurityRule.1	0	Sanctioned Threatened Unsanctioned
google-gemini	business-systems	Unmonitored	High	310 KB	443	Unsanctioned	0	1	1	artificial-intelligence	Threat_CP_SecurityRule.1	0	Sanctioned Threatened Unsanctioned
google-gemini	business-systems	Unmonitored	High	49.3 KB	443	Unsanctioned	0	0	0	artificial-intelligence	Threat_CP_SecurityRule.1	0	Sanctioned Threatened Unsanctioned

13

	
Đánh giá	- Kết quả: ☐ Pass ☐ Fail - Ghi chú:

4.4 Sử dụng cấu hình có sẵn (Predefined Snippet) trên Prisma Access

Mục tiêu	Trên Prisma Access có 02 snippet “GenAI Best Practices” và “Application Tagging), chứa sẵn các cấu hình phân loại AI App và Policy mặc định. Người quản trị chỉ cần áp dụng mà không cần phải cấu hình lại từ đầu.
Các bước thực hiện	
Kết quả thực tế	
Đánh giá	- Kết quả: ☐ Pass ☐ Fail - Ghi chú:

4.5 Phát hiện dữ liệu nhạy cảm gửi qua GenAI Apps

Mục tiêu	Với các GenAI App được phép sử dụng, quản trị viên có thể thiết lập chính sách để quét luồng dữ liệu của các App này để phát hiện các dữ liệu nhạy cảm dựa vào DLP engine.
Các bước thực hiện	Thực hiện upload 1 file chứa dữ liệu nhạy cảm (ví dụ chứa mã nguồn python) lên 1 ứng dụng GenAI được phép sử dụng (ví dụ: ChatGPT), khi chưa cấu hình ngăn chặn, việc upload file chứa mã nguồn python thành công.

ChatGPT ▾

1+2=

1 + 2 = 3 ✓

📄 👍 🗨️ 📤 🔄 ...

 **python-sample.txt**
Document

Tôi đã xem file bạn tải lên (python-sample.txt) và thấy trong đó có nhiều đoạn code Python trộn lẫn:

1. Web scraping với Scrapy + BeautifulSoup

- Lớp `HnsSpider` dùng để crawl Hacker News (`news.ycombinator.com`) qua 15 trang đầu.
- Trích xuất `id`, `title`, `url`, `rank` từ mỗi bài viết.

2. Game Blackjack (Casino)

- Sử dụng `random` để xáo bài.
- Người chơi và Dealer được chia bài, có logic xử lý "hit" hoặc "stay".
- Có điều kiện thắng/thua/hòa.

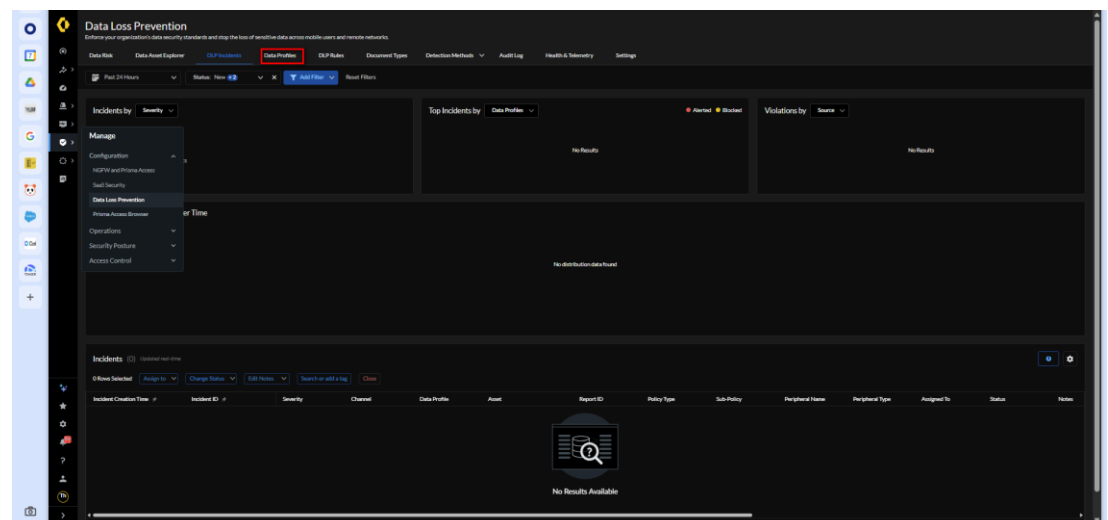
3. Automation với Selenium + BeautifulSoup

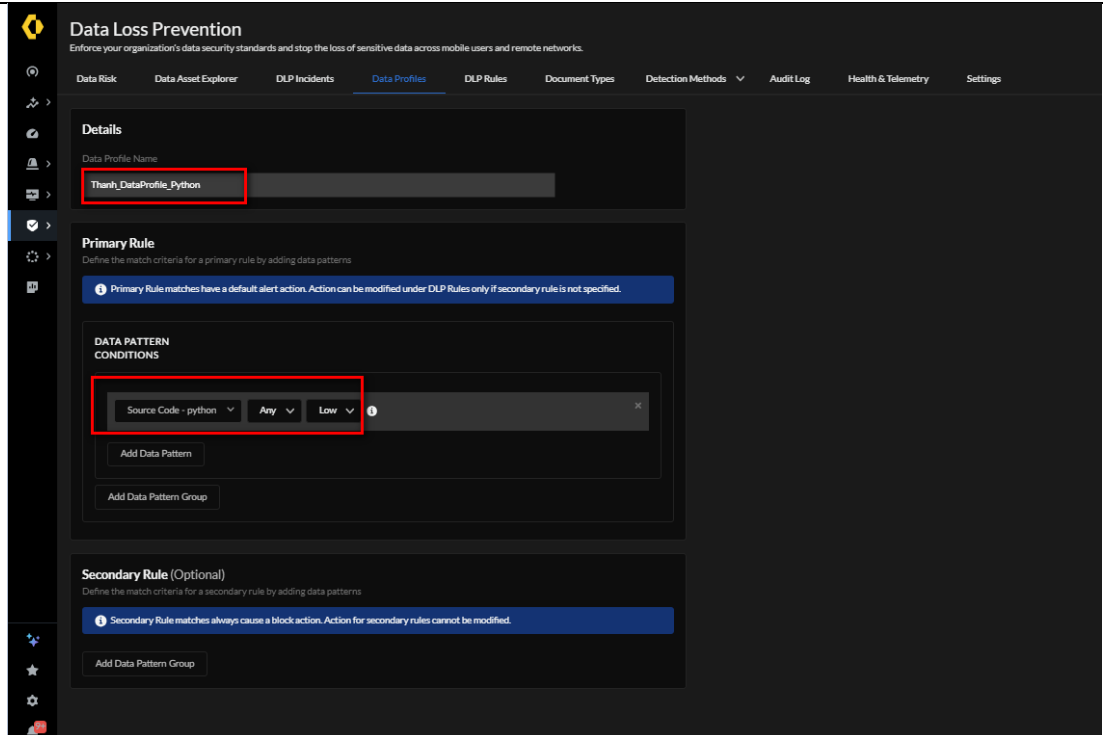
- Khởi chạy `headless Chrome`.

+ Ask anything

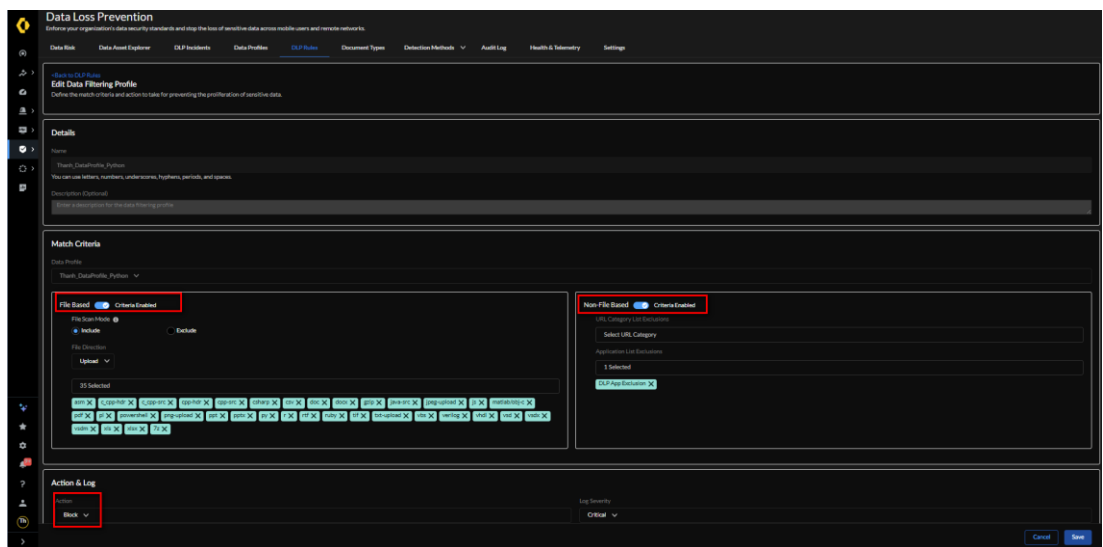


Cấu hình DLP, tạo Data Profile match với các loại file Python

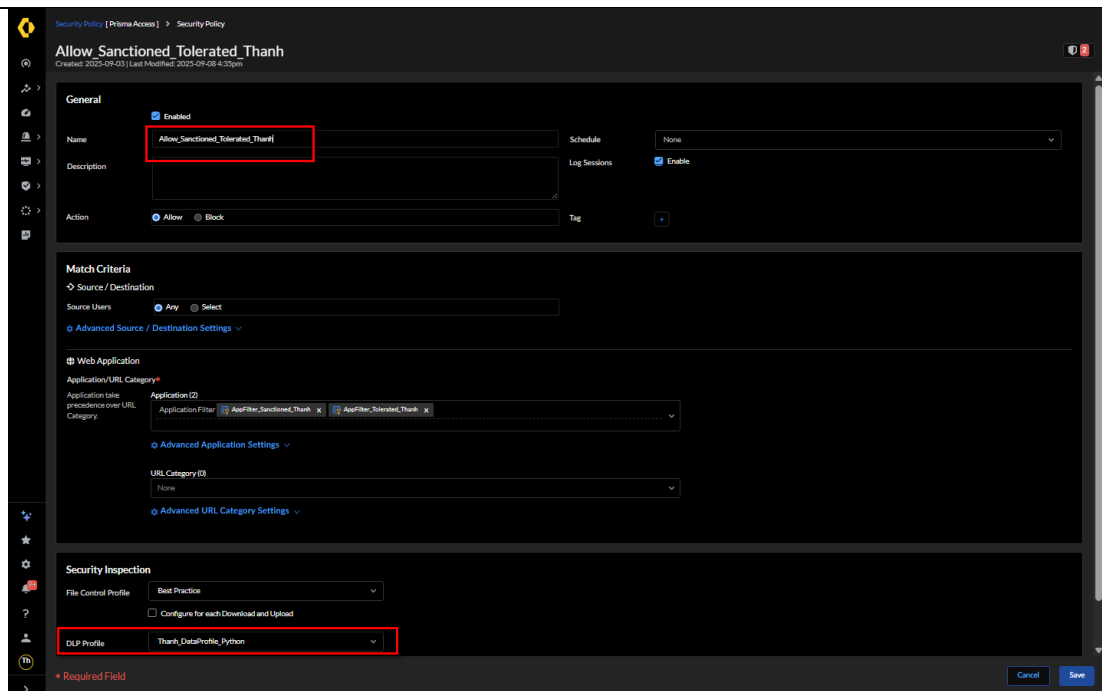




Cấu hình DLP rule cho cả 2 loại File Based và Non-File Based, Action là “Block”

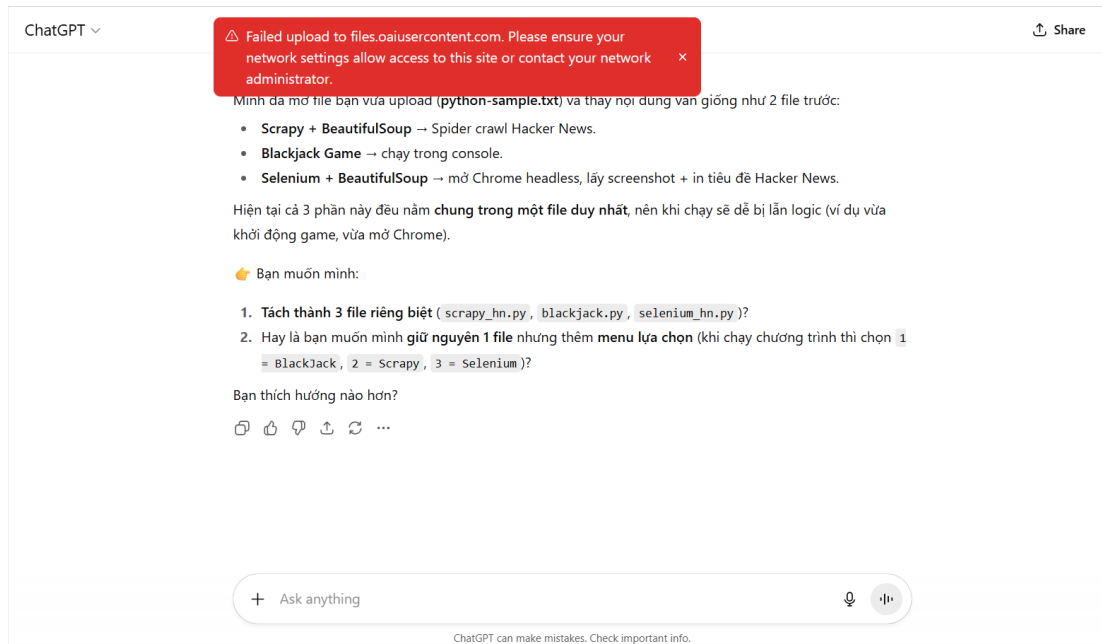


Sử dụng DLP Profile vừa tạo, áp dụng vào Security Policy, thực hiện Push để áp dụng cấu hình.

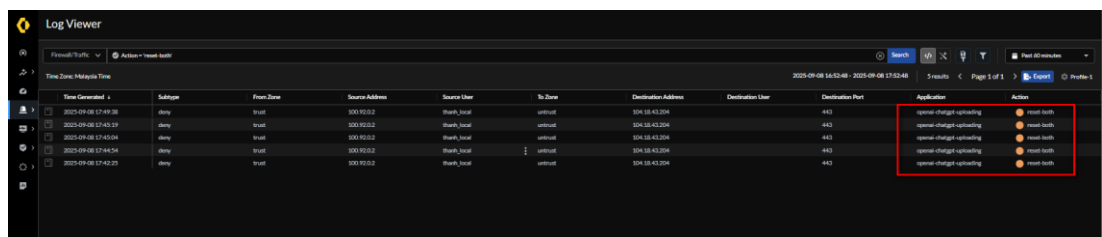


Kết quả thực tế

Khi thực hiện upload lại file chứa python code sẽ không thành công:

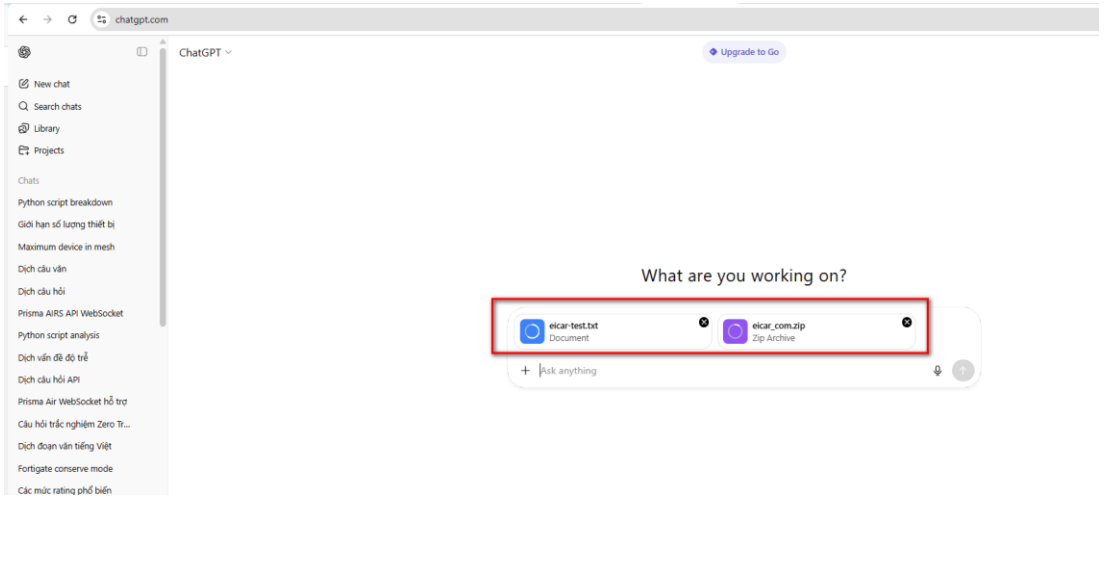
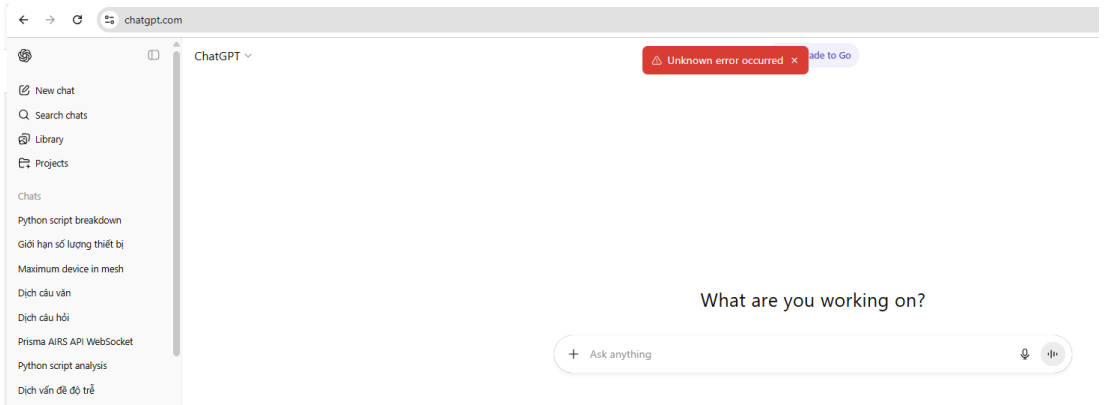


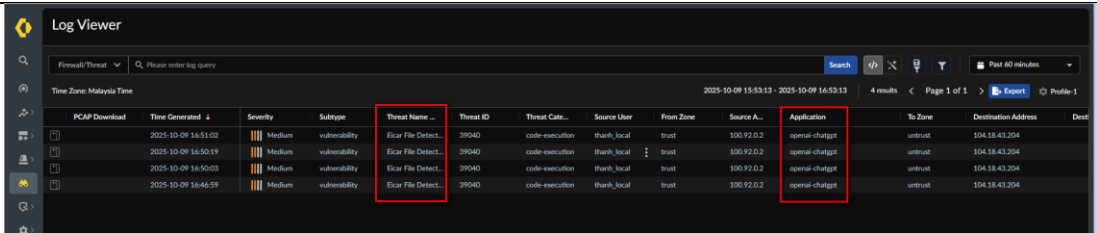
Log ngăn chặn upload file qua ChatGPT:



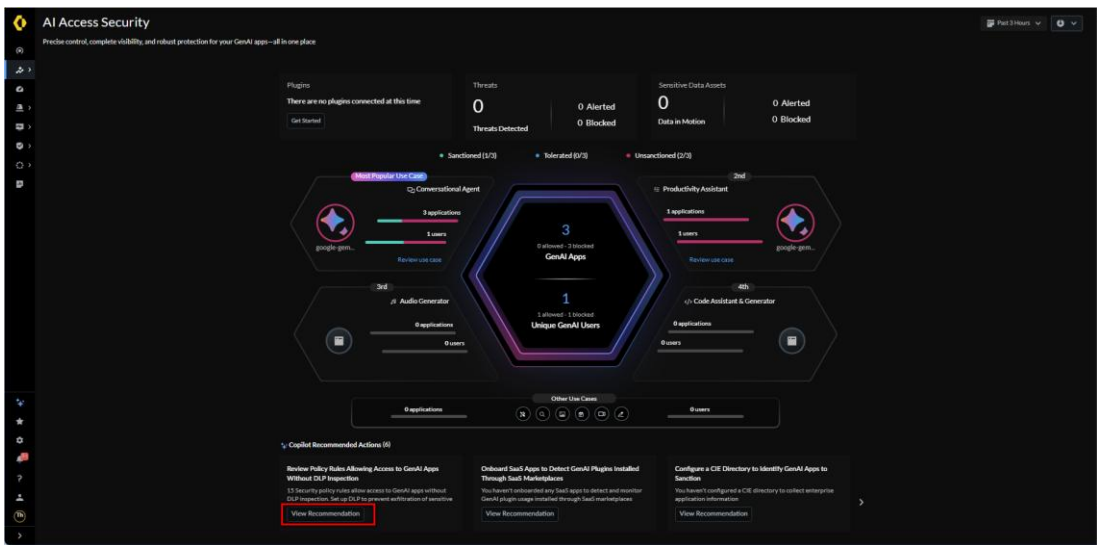
Đánh giá	- Kết quả: ☐ Pass ☐ Fail - Ghi chú:
-----------------	---

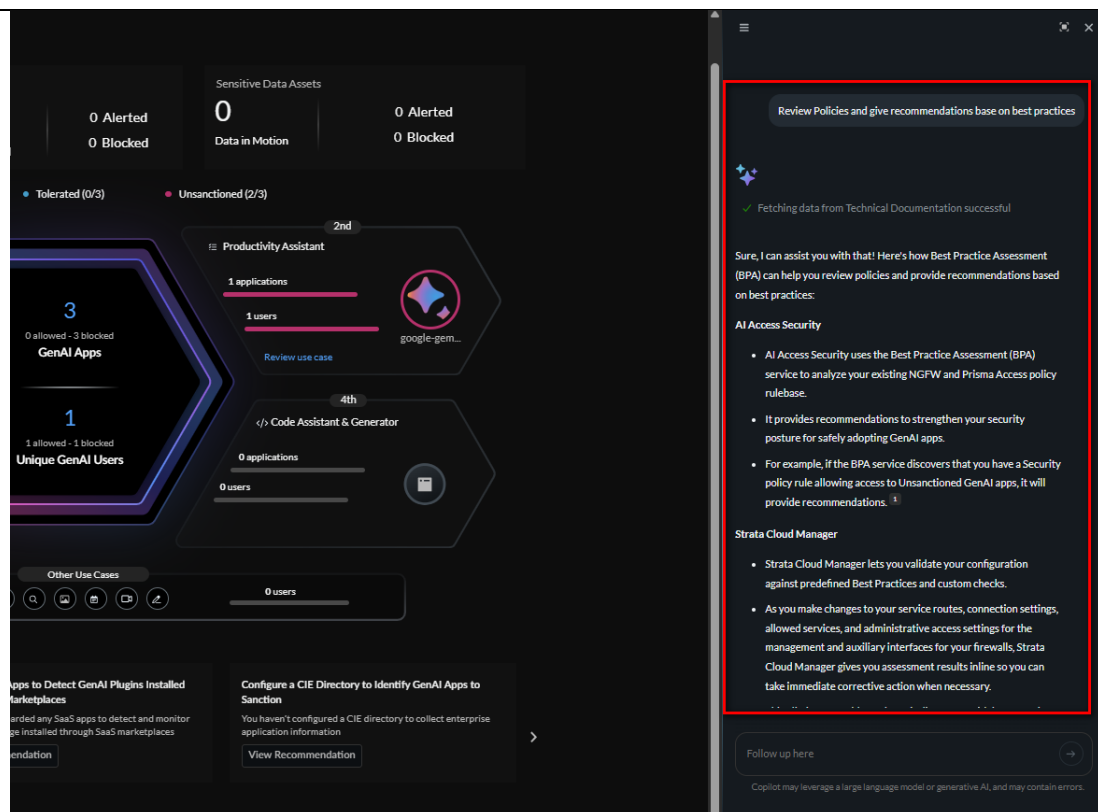
4.6 Phát hiện dữ liệu chứa mã độc gửi qua GenAI Apps

Mục tiêu	Với các GenAI App được phép sử dụng, quản trị viên có thể thiết lập chính sách để quét luồng dữ liệu của các App này để phát hiện các dữ liệu chứa mã độc gửi qua GenAI Apps
Các bước thực hiện	Upload file mã độc mẫu (Eicar file) 
Kết quả thực tế	Không thể upload file chứa mã độc:  Log ghi nhận:

	
Đánh giá	- Kết quả: ☐ Pass ☐ Fail - Ghi chú:

4.7 Đề xuất cấu hình tối ưu chính sách

Mục tiêu	Hệ thống đưa ra các đề xuất cấu hình tối ưu Policy kiểm soát các ứng dụng GenAI
Các bước thực hiện	Truy cập Insight → AI Access, chọn “View Recommendation”  Đặt câu hỏi tương tác với Copilot và thực hiện theo các Steps trong khuyến nghị.
Kết quả thực tế	Hệ thống trả lời và đưa ra khuyến nghị, hướng dẫn cấu hình:



Sensitive Data Assets

0 Alerted
0 Blocked

0 Data in Motion

0 Alerted
0 Blocked

• Tolerated (0/3) • Unsanctioned (2/3)

GenAI Apps

3
0 allowed - 3 blocked

Unique GenAI Users

1
1 allowed - 1 blocked

Productivity Assistant

2nd

1 applications
1 users

Review use case

google-gem...

Code Assistant & Generator

4th

0 applications
0 users

Other Use Cases

0 users

Apps to Detect GenAI Plugins Installed Marketplaces

boarded any SaaS apps to detect and monitor ge installed through SaaS marketplaces

Configure a CIE Directory to Identify GenAI Apps to Sanction

You haven't configured a CIE directory to collect enterprise application information

View Recommendation

Review Policies and give recommendations base on best practices

✓ Fetching data from Technical Documentation successful

Sure, I can assist you with that! Here's how Best Practice Assessment (BPA) can help you review policies and provide recommendations based on best practices:

AI Access Security

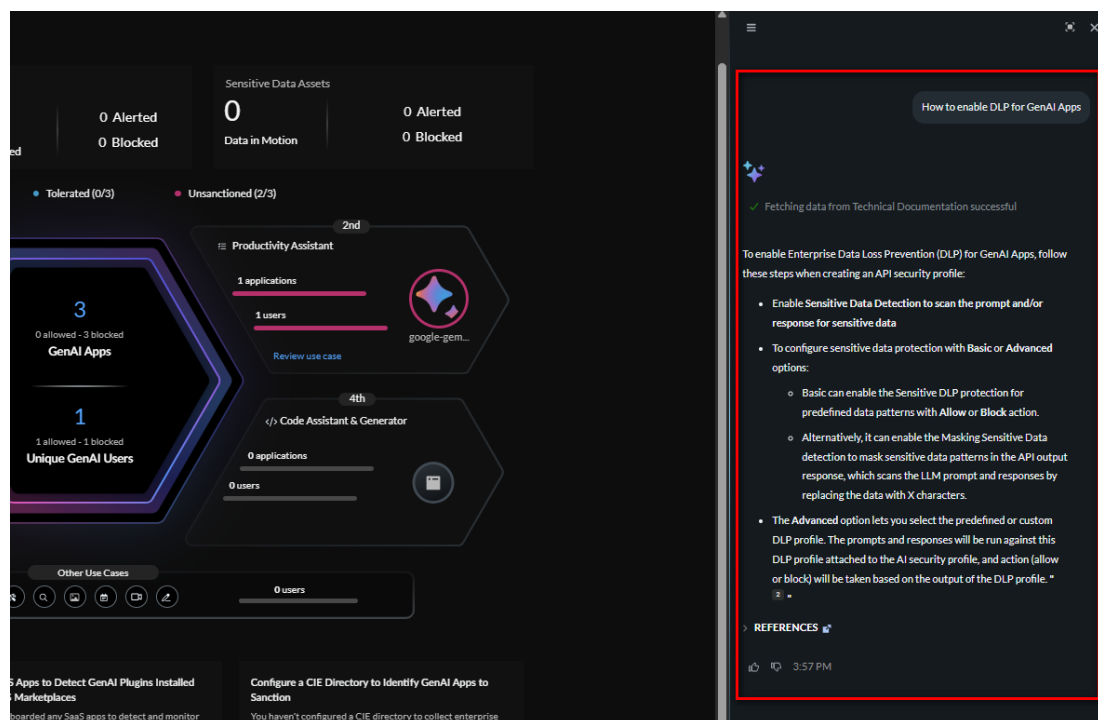
- AI Access Security uses the Best Practice Assessment (BPA) service to analyze your existing NGFW and Prisma Access policy rulebase.
- It provides recommendations to strengthen your security posture for safely adopting GenAI apps.
- For example, if the BPA service discovers that you have a Security policy rule allowing access to Unsanctioned GenAI apps, it will provide recommendations. ¹

Strata Cloud Manager

- Strata Cloud Manager lets you validate your configuration against predefined Best Practices and custom checks.
- As you make changes to your service routes, connection settings, allowed services, and administrative access settings for the management and auxiliary interfaces for your firewalls, Strata Cloud Manager gives you assessment results inline so you can take immediate corrective action when necessary.

Follow up here

Copilot may leverage a large language model or generative AI, and may contain errors.



Sensitive Data Assets

0 Alerted
0 Blocked

0 Data in Motion

0 Alerted
0 Blocked

• Tolerated (0/3) • Unsanctioned (2/3)

GenAI Apps

3
0 allowed - 3 blocked

Unique GenAI Users

1
1 allowed - 1 blocked

Productivity Assistant

2nd

1 applications
1 users

Review use case

google-gem...

Code Assistant & Generator

4th

0 applications
0 users

Other Use Cases

0 users

Apps to Detect GenAI Plugins Installed Marketplaces

boarded any SaaS apps to detect and monitor

Configure a CIE Directory to Identify GenAI Apps to Sanction

You haven't configured a CIE directory to collect enterprise application information

How to enable DLP for GenAI Apps

✓ Fetching data from Technical Documentation successful

To enable Enterprise Data Loss Prevention (DLP) for GenAI Apps, follow these steps when creating an API security profile:

- Enable Sensitive Data Detection to scan the prompt and/or response for sensitive data
- To configure sensitive data protection with Basic or Advanced options:
 - Basic can enable the Sensitive DLP protection for predefined data patterns with Allow or Block action.
 - Alternatively, it can enable the Masking Sensitive Data detection to mask sensitive data patterns in the API output response, which scans the LLM prompt and responses by replacing the data with X characters.
- The Advanced option lets you select the predefined or custom DLP profile. The prompts and responses will be run against this DLP profile attached to the AI security profile, and action (allow or block) will be taken based on the output of the DLP profile. ¹

REFERENCES

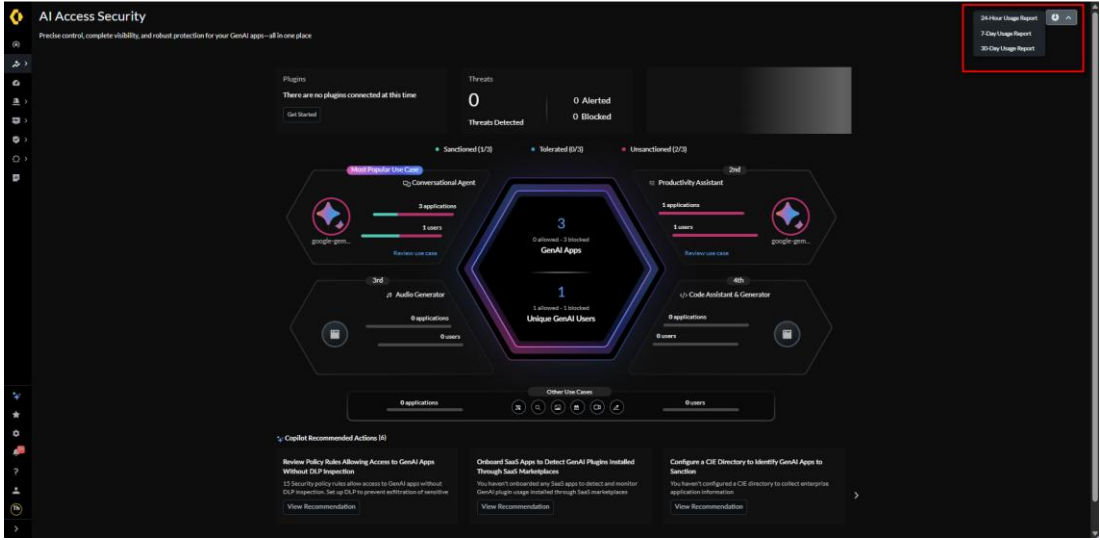
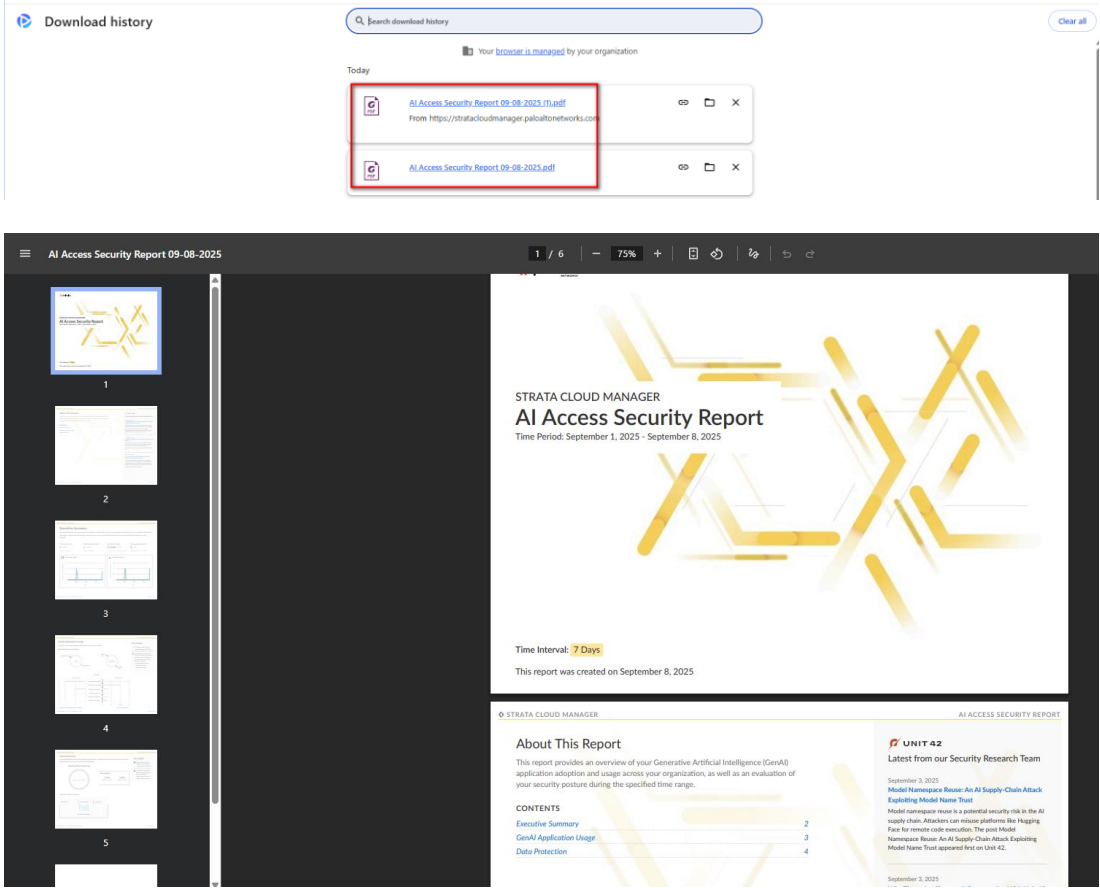
3:57 PM

Đánh giá

- Kết quả: ☐ Pass ☐ Fail

- Ghi chú:

4.8 Báo cáo GenAI Report

Mục tiêu	Cho phép tạo các báo cáo về GenAI Apps dạng Executive Summary, trong các khoảng thời gian Last 24h, 7 days, hoặc 30 days.
Các bước thực hiện	Truy cập Insight → AI Access, chọn khoảng thời gian để tạo Report 
Kết quả thực tế	Có thể download và xem Report. 

Executive Summary

Our analysis indicates that your organization utilized 5 GenAI apps across 1 users during this time frame. Here's a snapshot of the GenAI app usage, as well as the data loss prevention incidents and security threats detected or prevented by AI Access Security on your network.

TOTAL GENAI APPS

5 ↑ 100%

2 Allowed - 3 Blocked

TOTAL GENAI APP USERS

1 ↑ 100%

1 Allowed - 1 Blocked

DATA TRANSFERRED

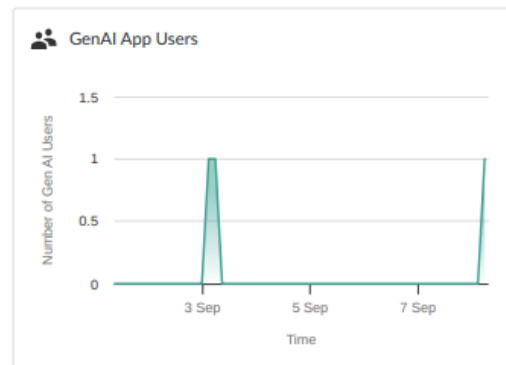
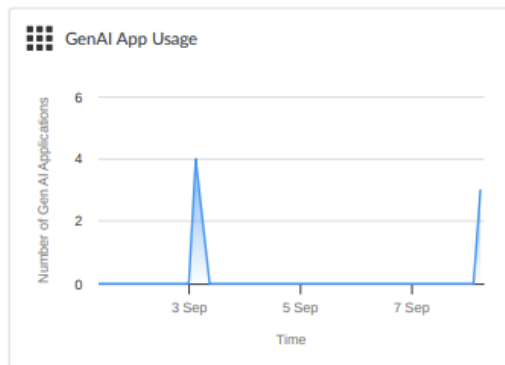
7.0 MB ↑ 100%

4.7 MB Uploaded - 2.2 MB Downloaded

TOTAL SENSITIVE ASSETS

0 ↓ 0%

0 Data in Motion - 0 Data at Rest



SEPTEMBER 1, 2025 - SEPTEMBER 8, 2025

PAGE 2 OF 4

STRATA CLOUD MANAGER

AI ACCESS SECURITY REPORT

GenAI Application Usage

Overview of GenAI application usage discovered in your network.

App Classification and Control



Key Insights

- GenAI app usage in your organization grew by 100%.
- All GenAI apps associated with 5 use cases have active traffic on your network but are Unsanctioned. Review the top use cases:
 - Productivity Assistant
 - Enterprise Search
 - Writing Assistant

Mẫu Report:

https://drive.google.com/file/d/1N6iGI_rHTwP7HTaPBiWNyDWILcNvMA39/view?usp=drive_link

Đánh giá

- Kết quả: ☐ Pass ☐ Fail
- Ghi chú: