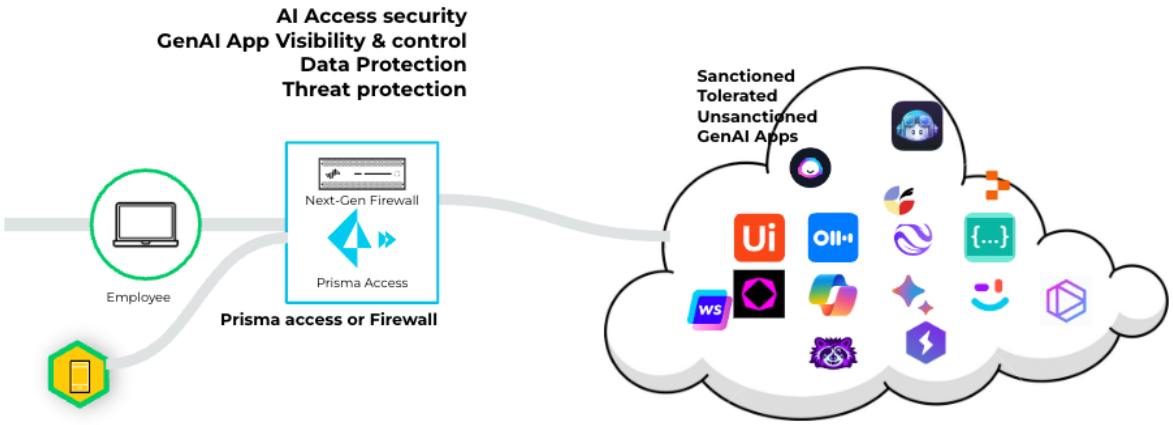
TÀI LIỆU
GIỚI THIỆU VÀ THỬ NGHIỆM GIẢI PHÁP AI ACCESS (AIAS)

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

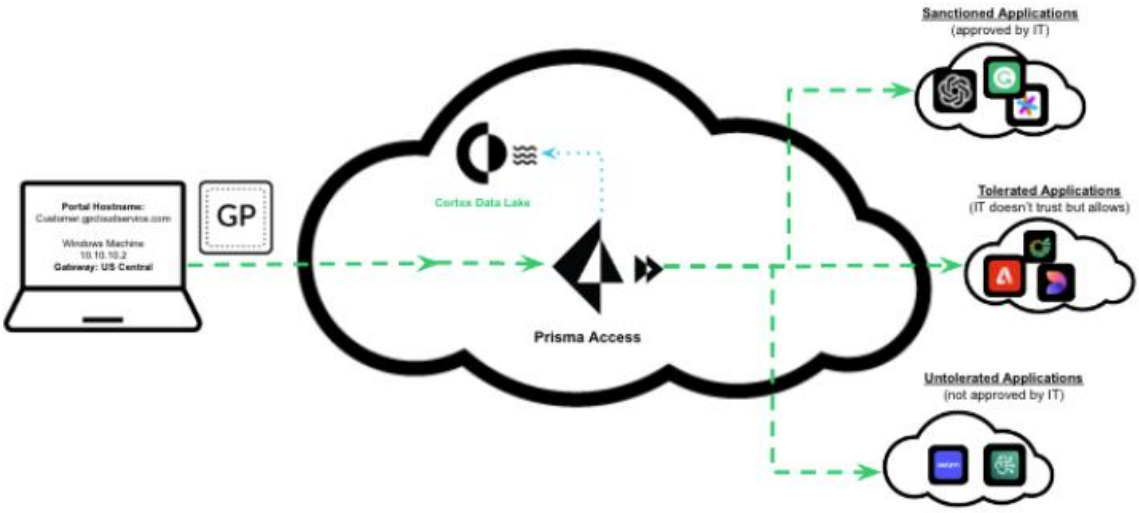
1 Giới thiệu chung

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

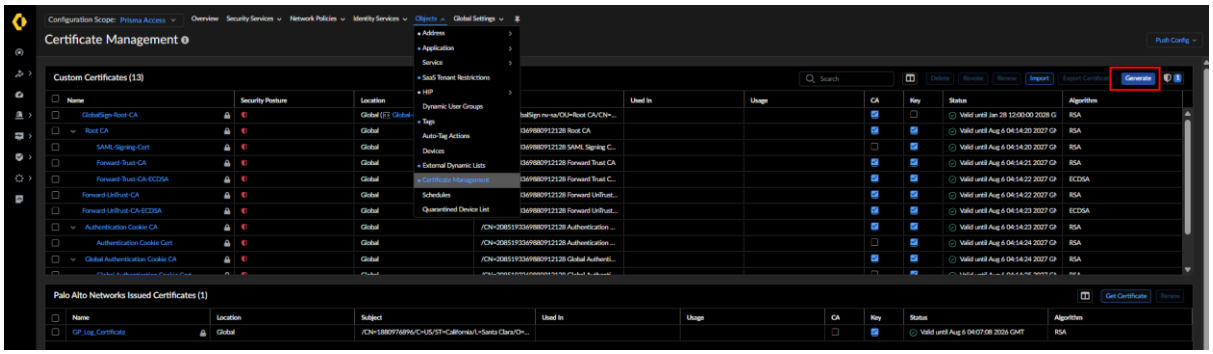
3.1 Thiết lập kết nối GP

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

3.2 Cấu hình SSL Decryption

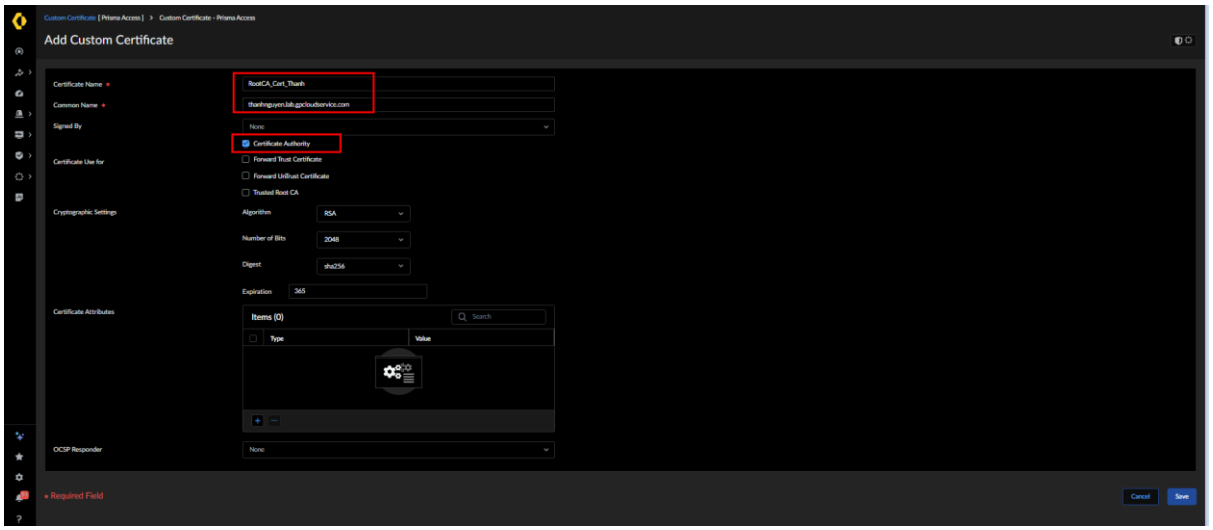
3.2.1 Tạo Self-Sign Root CA

Truy cập Objects – Certificate Management – Generate để tạo Cert



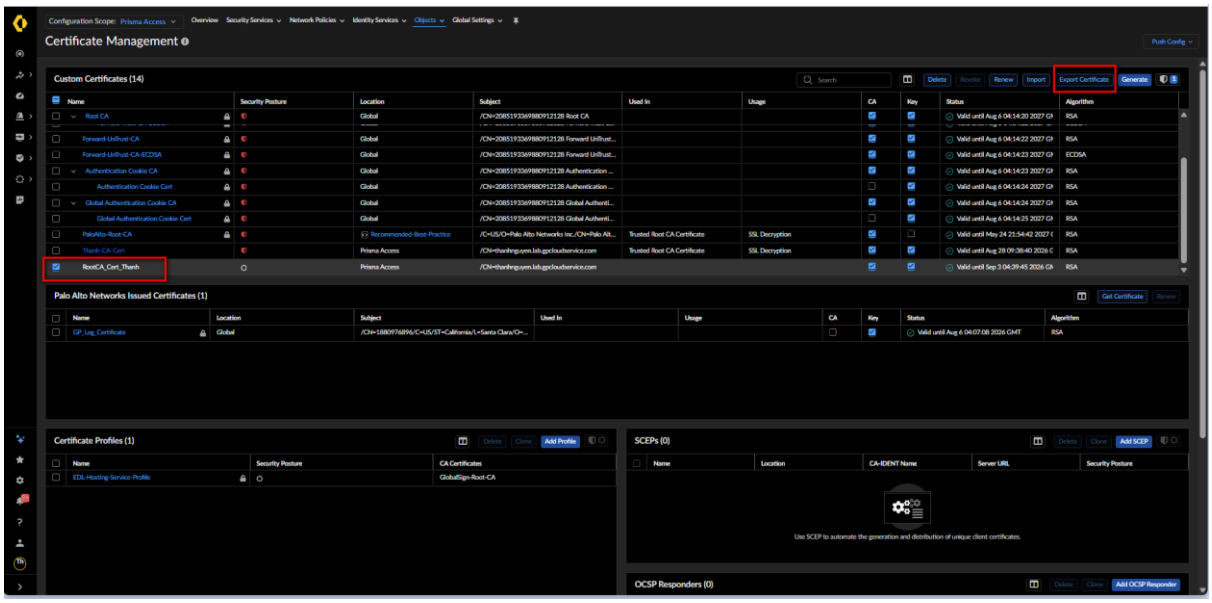
Khai báo thông tin Root CA Cert:

- 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 Sefl-Sign Cert Root CA.

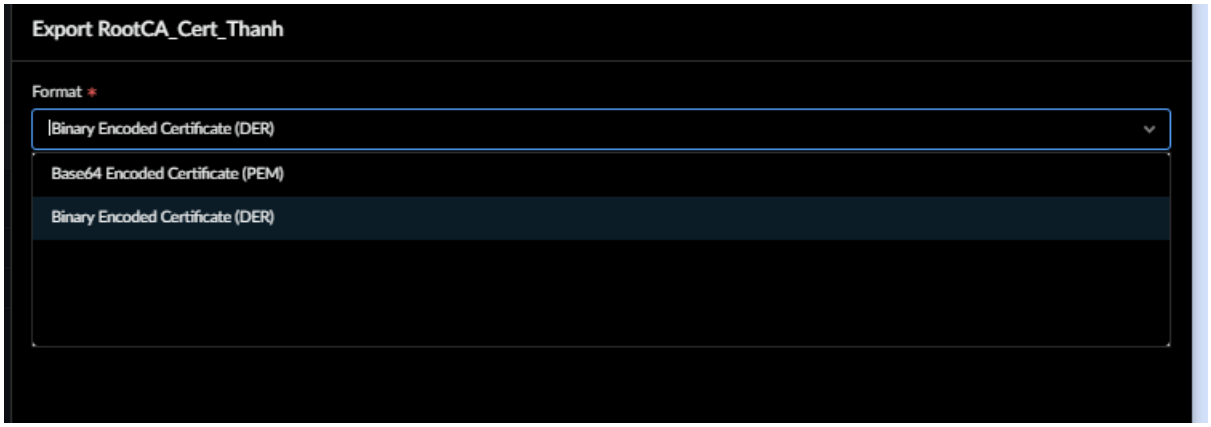


3.2.2 Export Root CA Cert và cài đặt trên máy Client.

Chọn Cert muốn export và click “Export Certificate”:



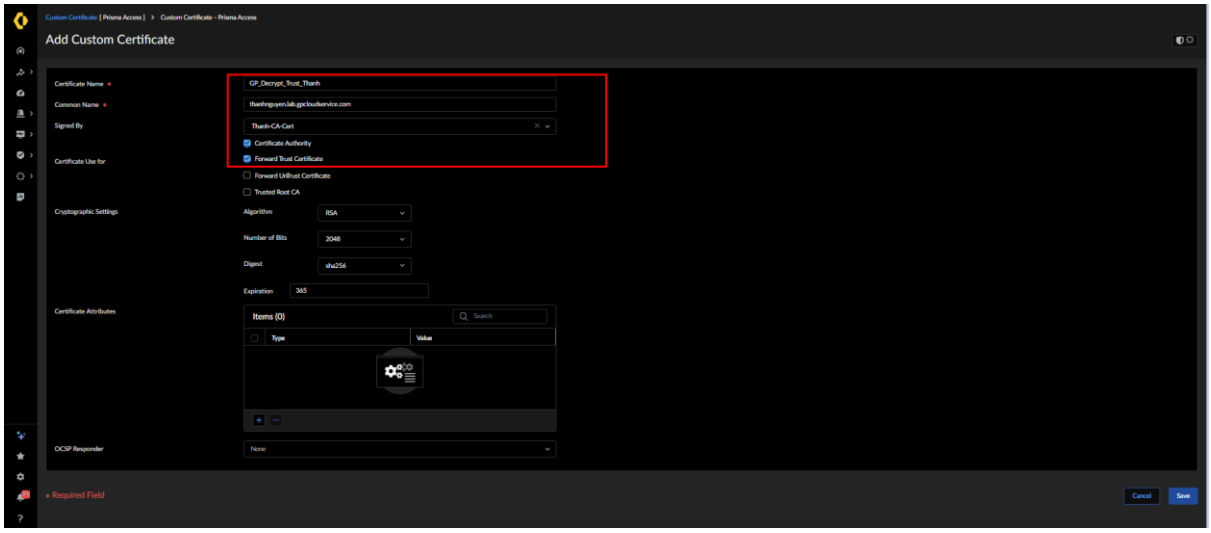
Chọn DER format:



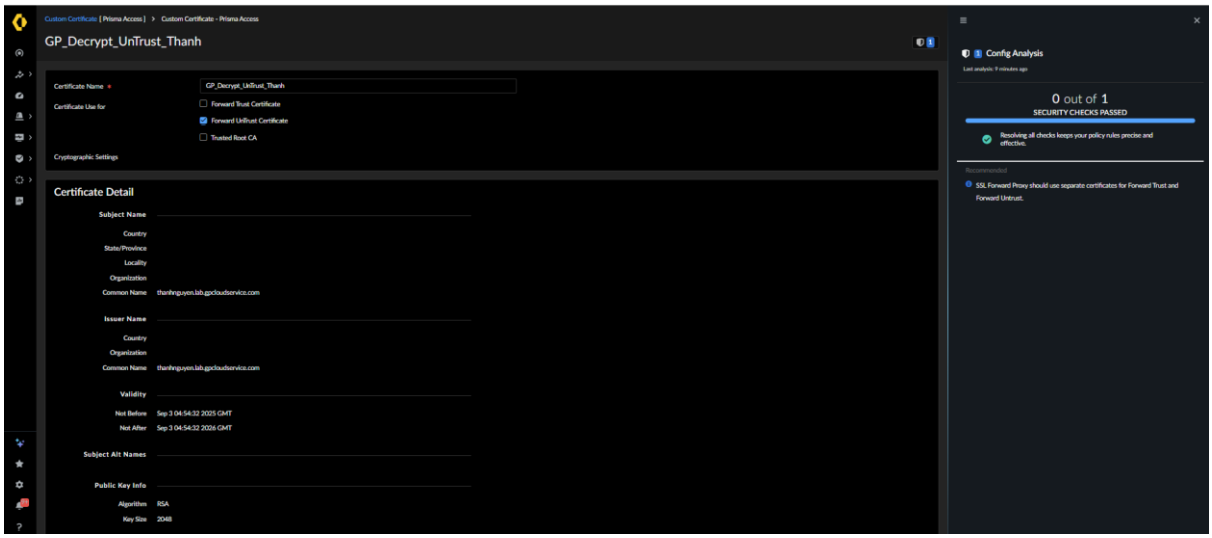
Sau khi export, cài đặt Cert trên vào danh sách Trusted Root CA trên máy.

3.2.3 Tạo Cert Forward Trust

Truy cập Objects – Certificate Management – Generate để tạo Cert

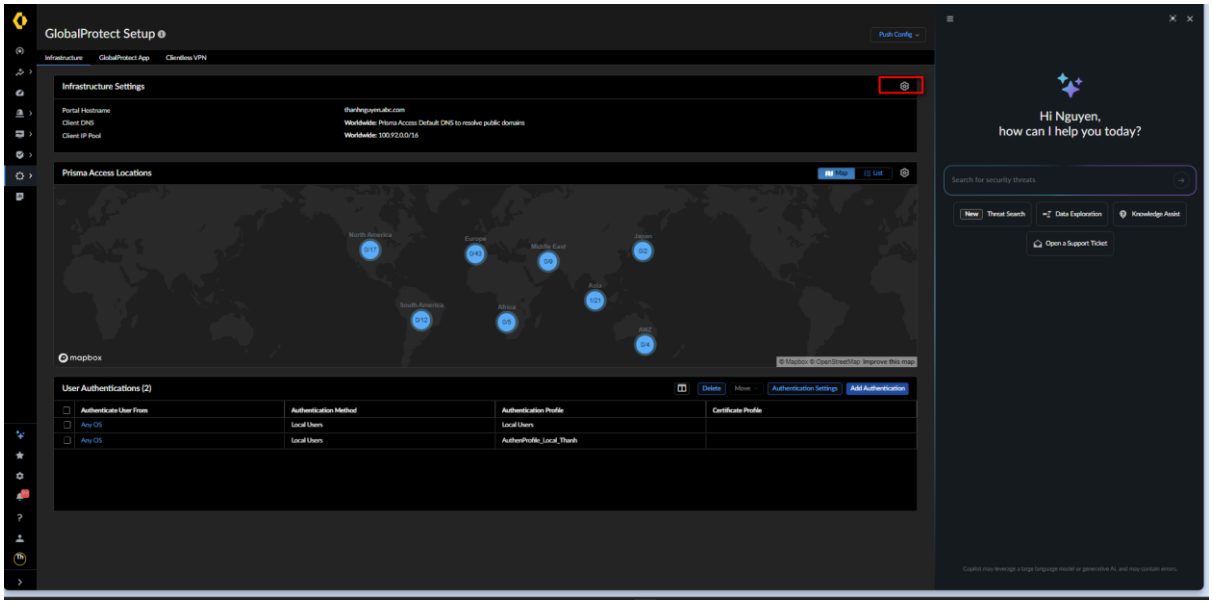


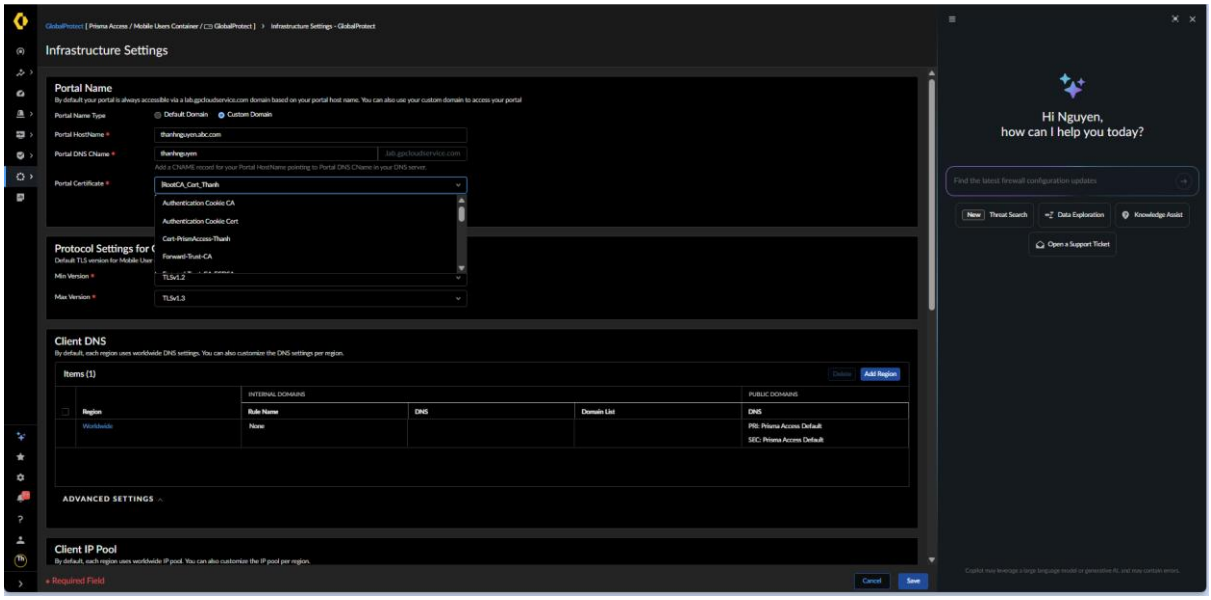
3.2.4 Tạo Cert Forward Untrust



3.2.5 Cài đặt Cert cho GP Portal

Vào Workflow – Prisma Access Setup:





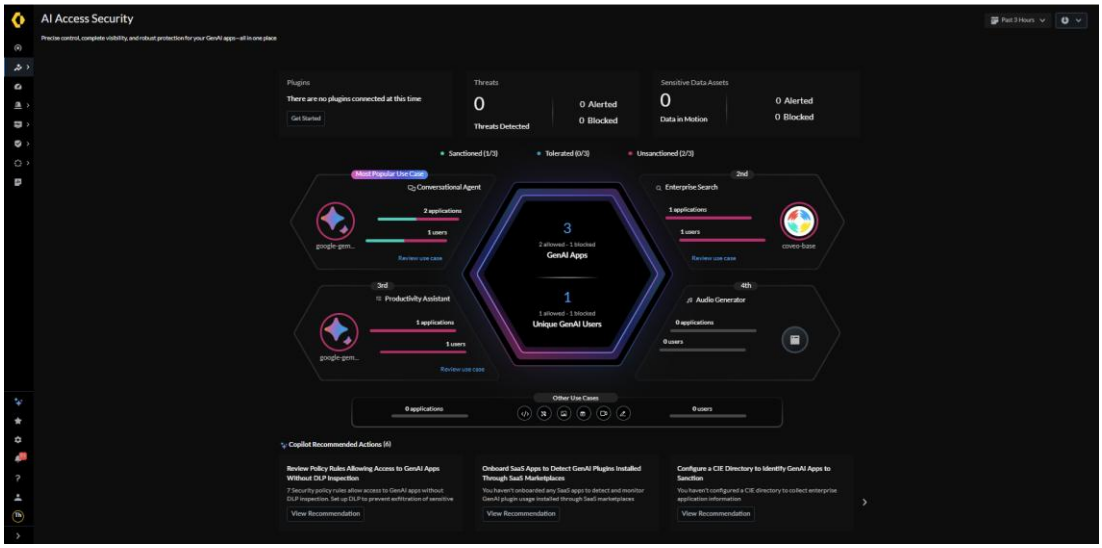
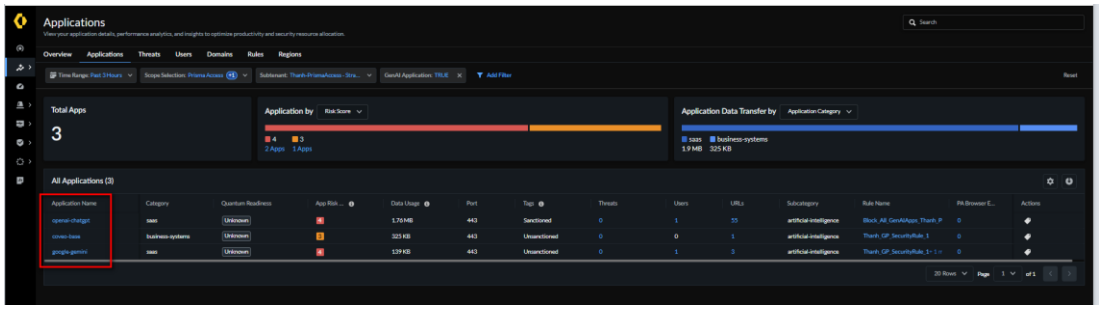
Kết quả, khi kết nối GP không còn cảnh báo Cert

3.2.6 Cấu hình SSL Decrypt Rule

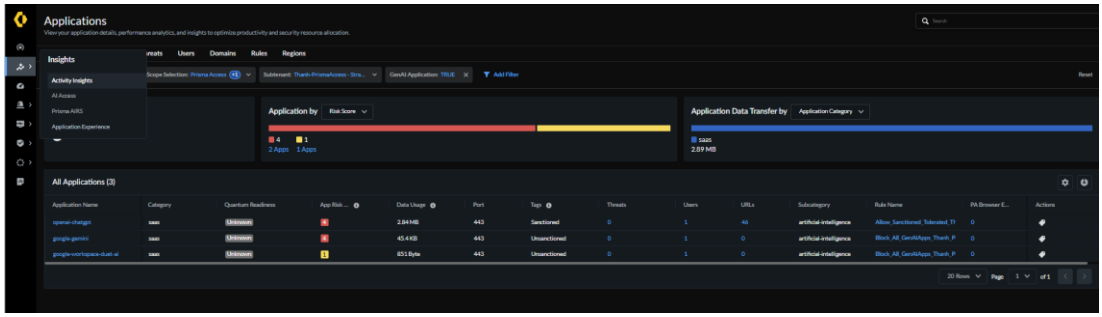
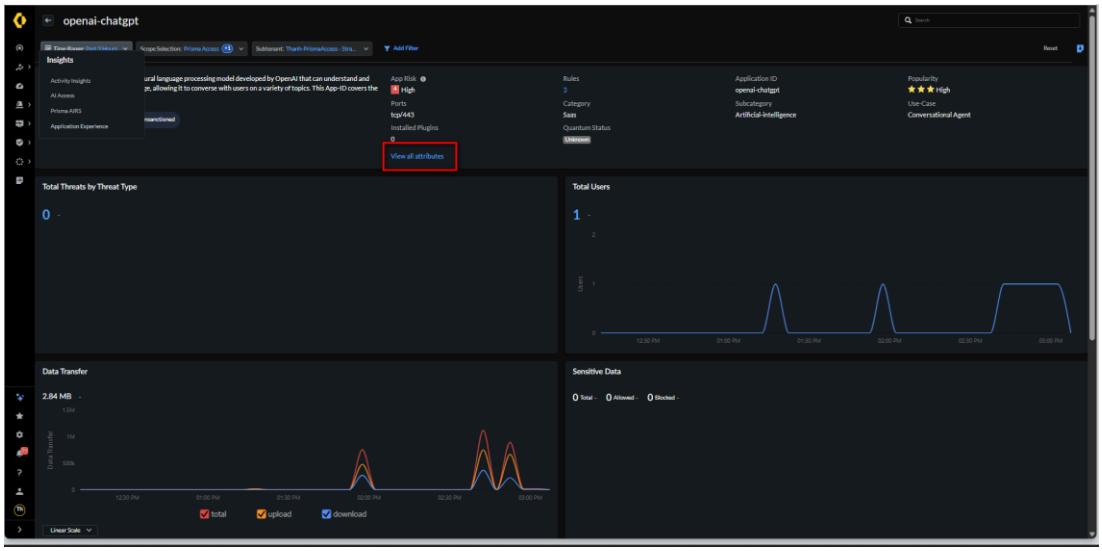
4 Kết quả chi tiết các Test Cases

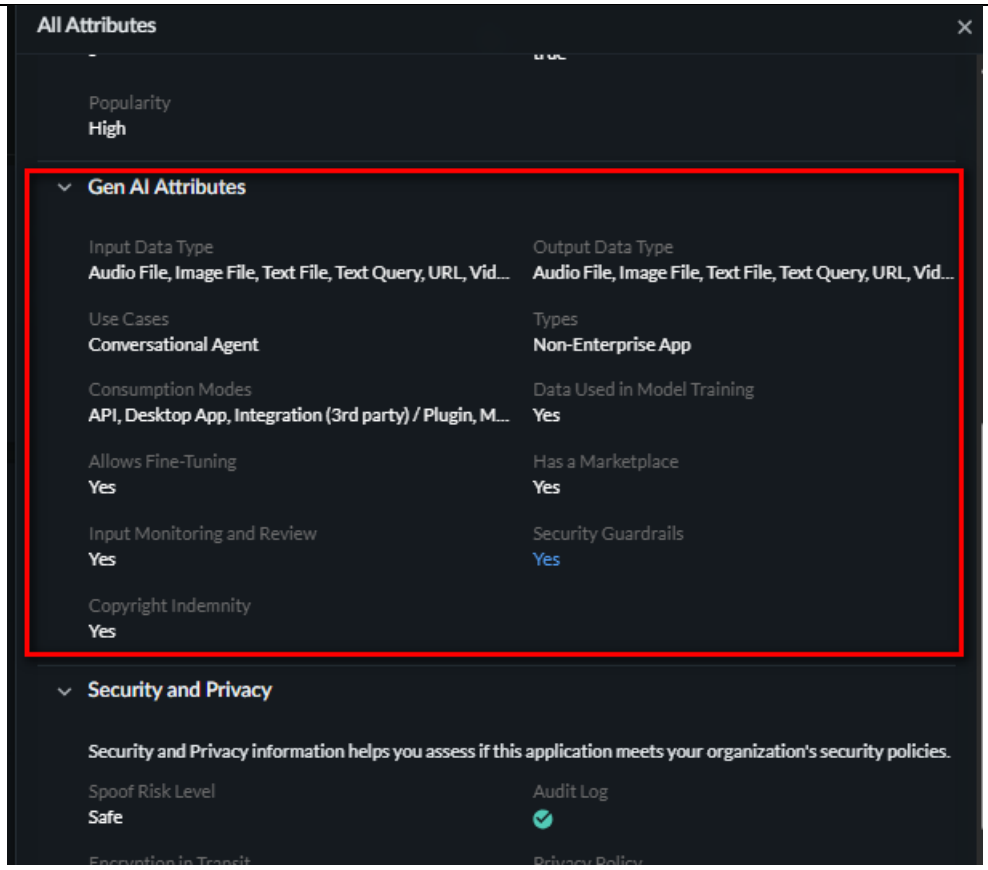
4.1 Phát hiện tất cả các GenAI Apps đang được sử dụng trong tổ chức

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.

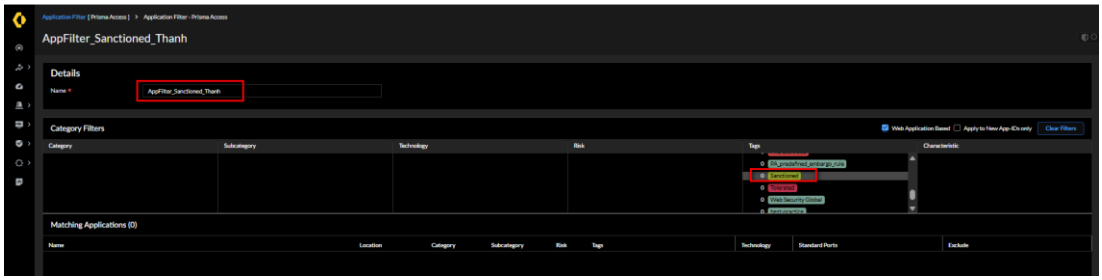
Kết quả thực tế	Truy cập AI Insight sẽ thấy được danh sách các GenAI Apps và người dùng trong hệ thống:  Danh mục GenAI Users:  Danh mục GenAI Apps: 
Đánh giá	- Kết quả: ☐ Pass ☐ Fail - Ghi chú:

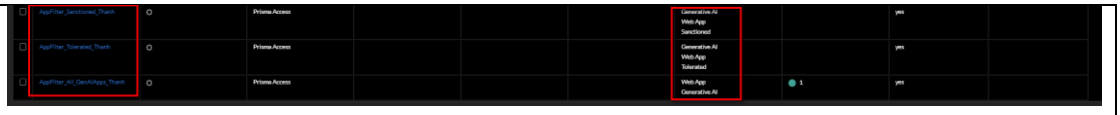
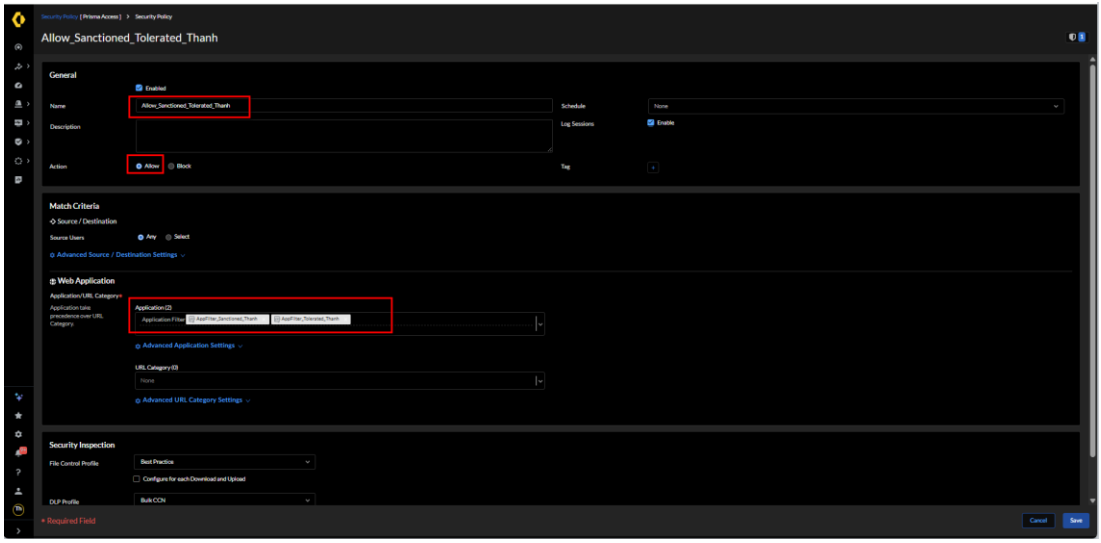
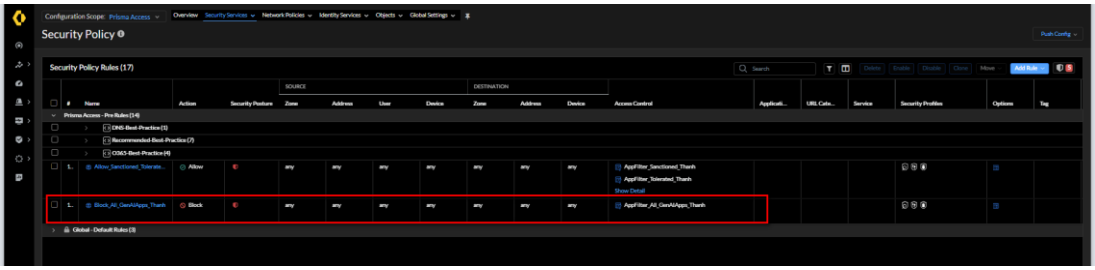
4.2 Xem thuộc tính (Attributes) của AI Apps

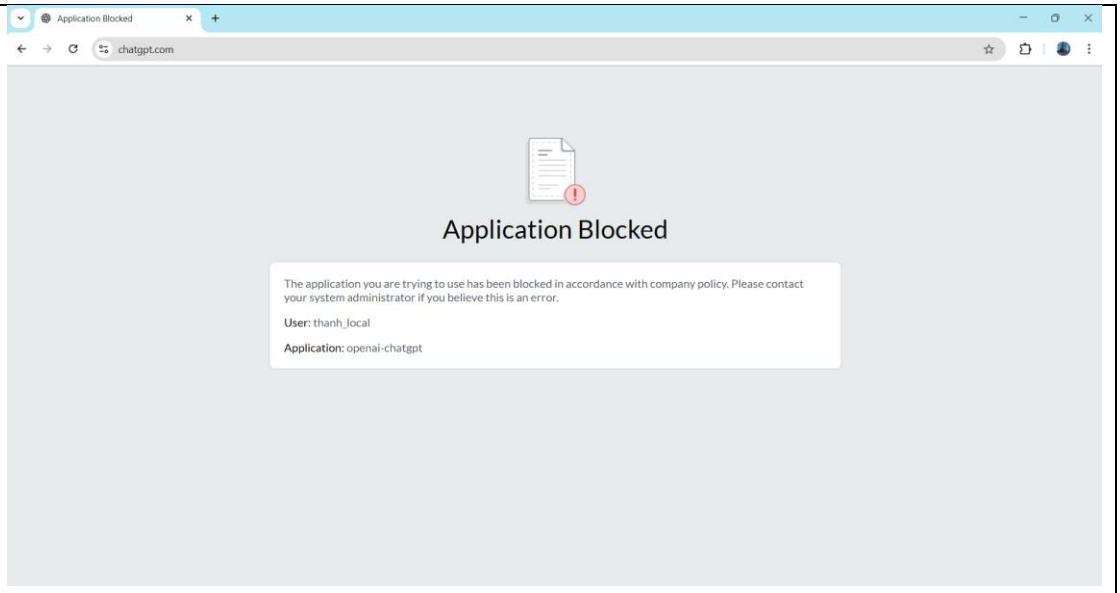
Mục tiêu	Dựa vào các thuộc tính này, quản trị viên có thể cân nhắc và quyết định xem nên xếp AI Apps này vào thể loại nào, tương ứng là chính sách cho phép hay ngăn chặn AI App này.
Các bước thực hiện	Vào Activity Insight, lọc các App GenAI và chọn 1 App cụ thể (ví dụ: openai-chatgpt):   Xem thuộc tính:

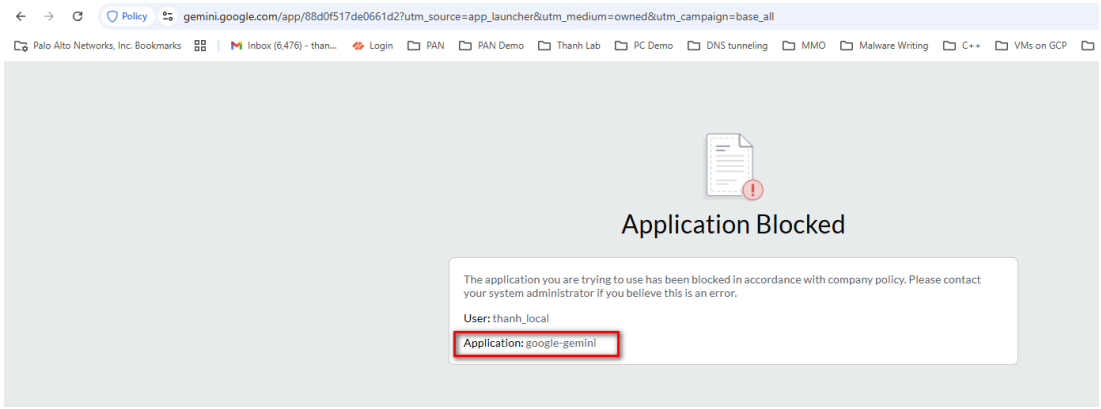
	
Kết quả thực tế	
Đánh giá	- Kết quả: ☐ Pass ☐ Fail - Ghi chú:

4.3 Kiểm soát cho phép/ngăn chặn các GenAI Apps

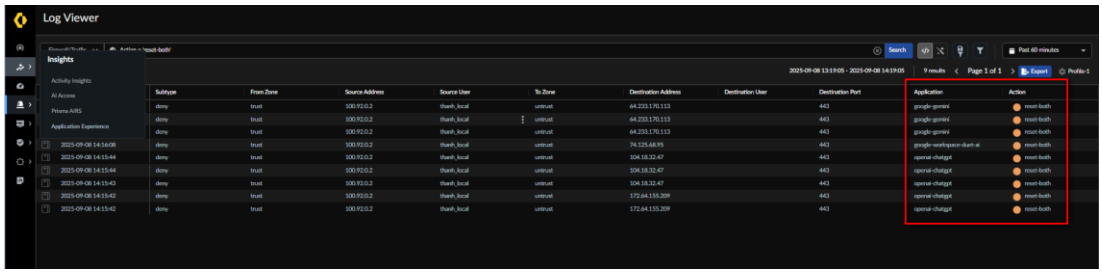
Mục tiêu	Kiểm soát cho phép/ngăn chặn GenAI Apps
Các bước thực hiện	Cấu hình khai báo Application Filter, match với các Apps được tag là “Sanctioned” và “Tolerated”.  Ngoài các tag được gán thêm, tất cả các GenAI Apps đều được gán tag mặc định “GenerativeAI”, cấu hình gán nhãn cuối cùng như sau:

	 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:

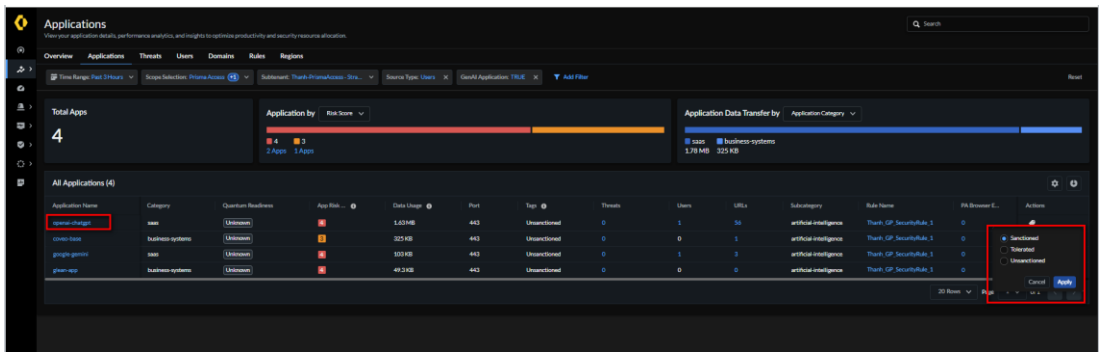




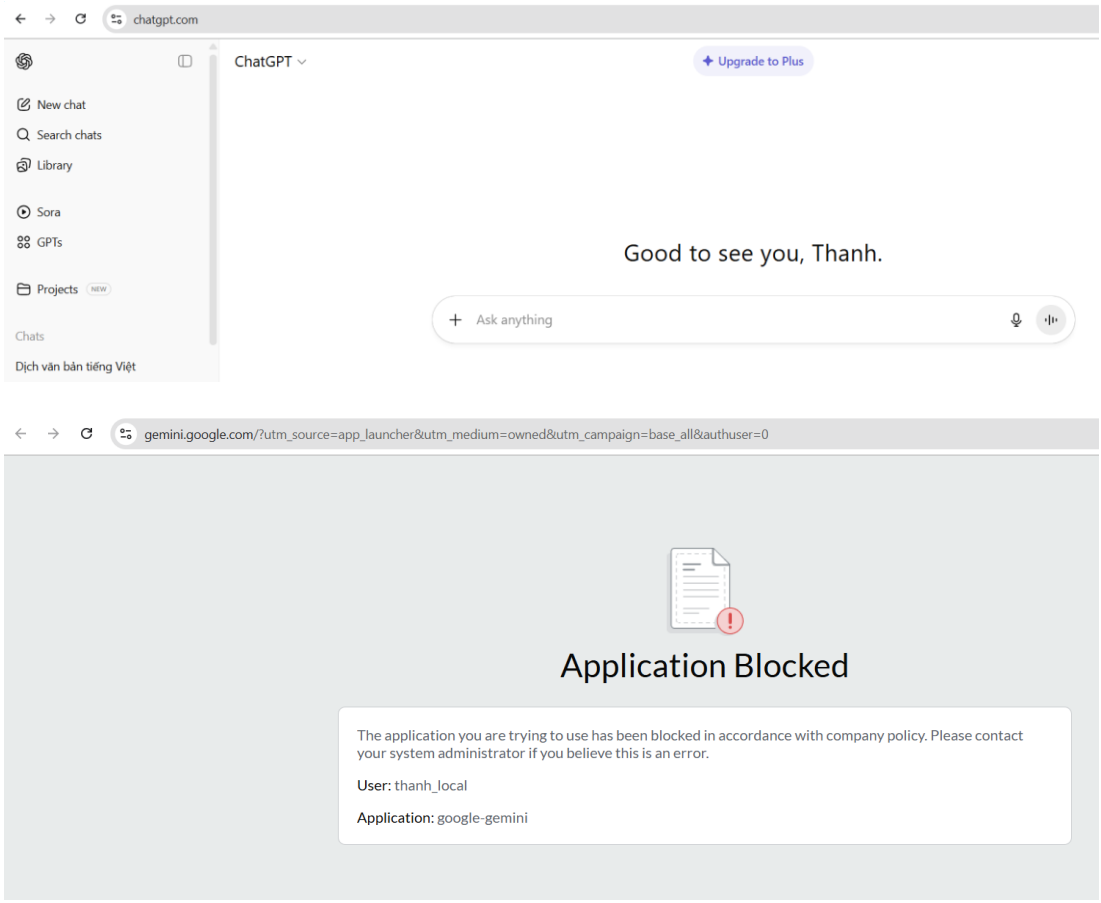
Log ghi nhận chặn ứng dụng ChatGPT, Gemini:



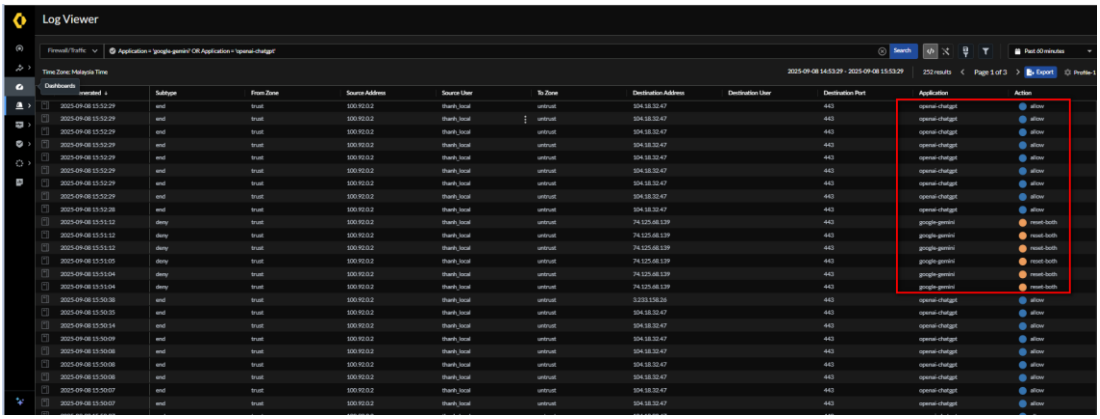
Đánh dấu và phân loại lại ChatGPT thành ứng dụng Sanctioned:

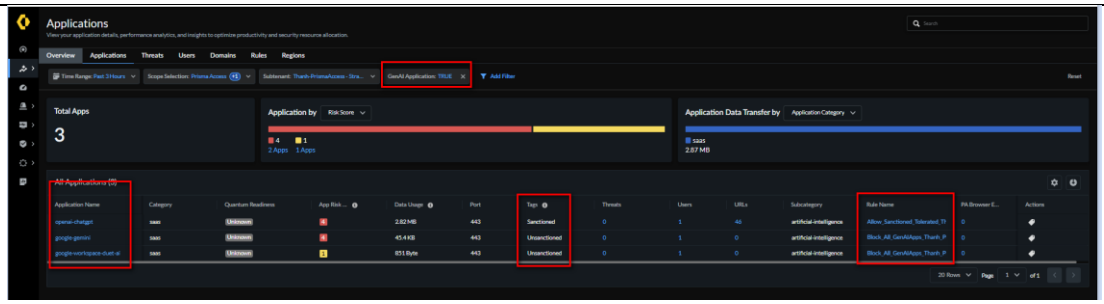


Lúc này, ứng dụng ChatGPT vừa được đánh dấu là Sanctioned được cho phép đi qua, còn các ứng dụng còn lại (ví dụ: Gemeni) vẫn bị chặn lại.



Log:



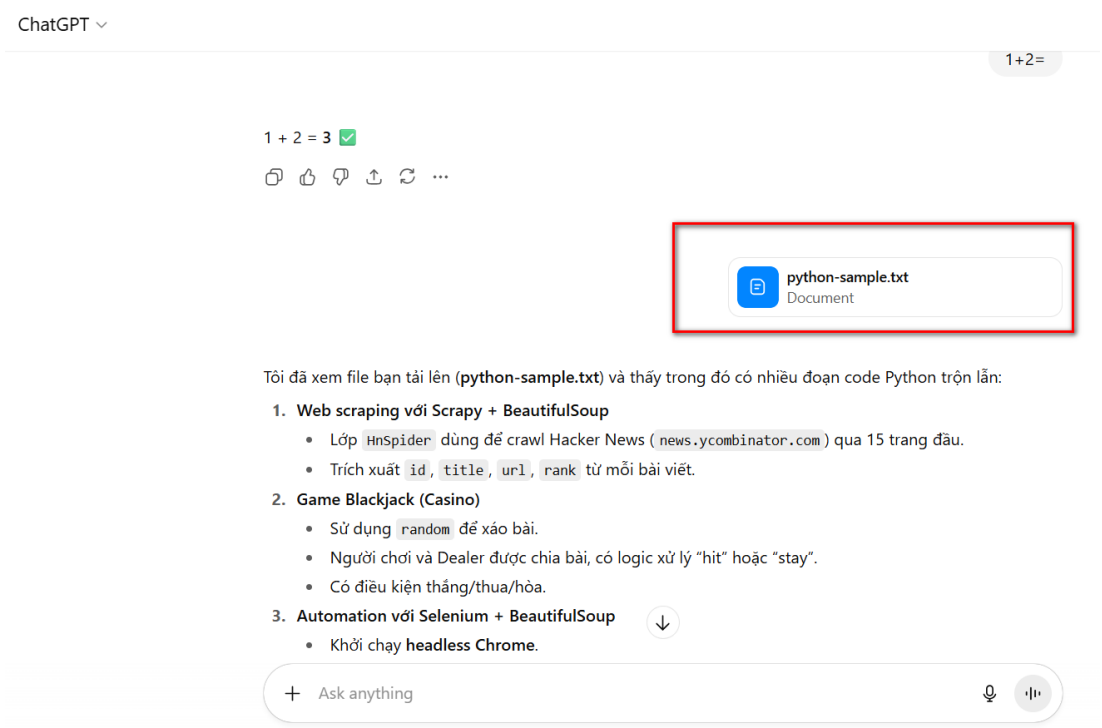
	
Đánh giá	- Kết quả: ☐ Pass ☐ Fail - Ghi chú:

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

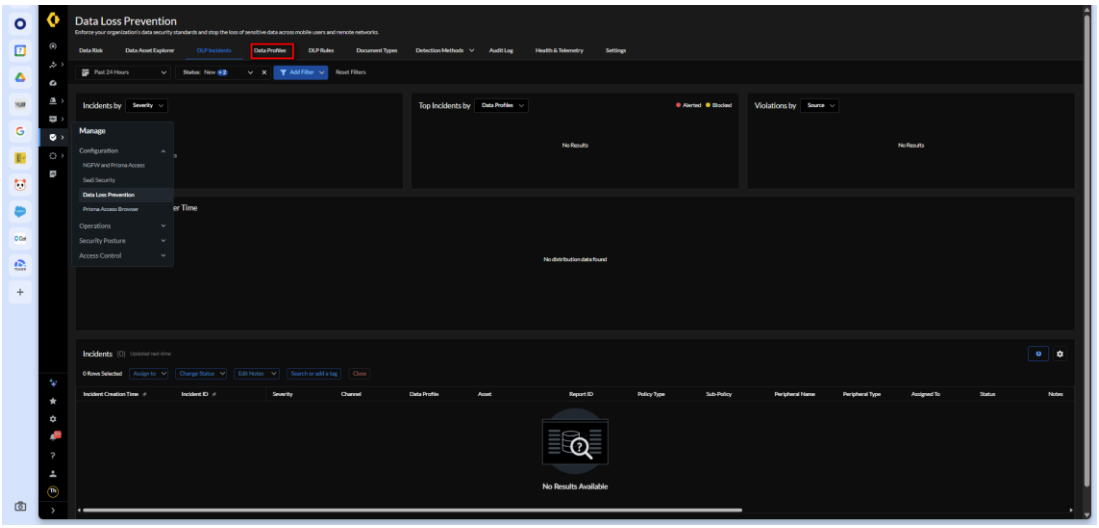
Mục tiêu	Trên Prisma Access có 02 snippet "GenAI Best Practices" và "Application Tagging), chứa sẵn các cấu hình phân loại AI App và Policy mặc định. Người quản trị chỉ cần áp dụng mà không cần phải cấu hình lại từ đầu.
Các bước thực hiện	
Kết quả thực tế	
Đánh giá	- Kết quả: ☐ Pass ☐ Fail - Ghi chú:

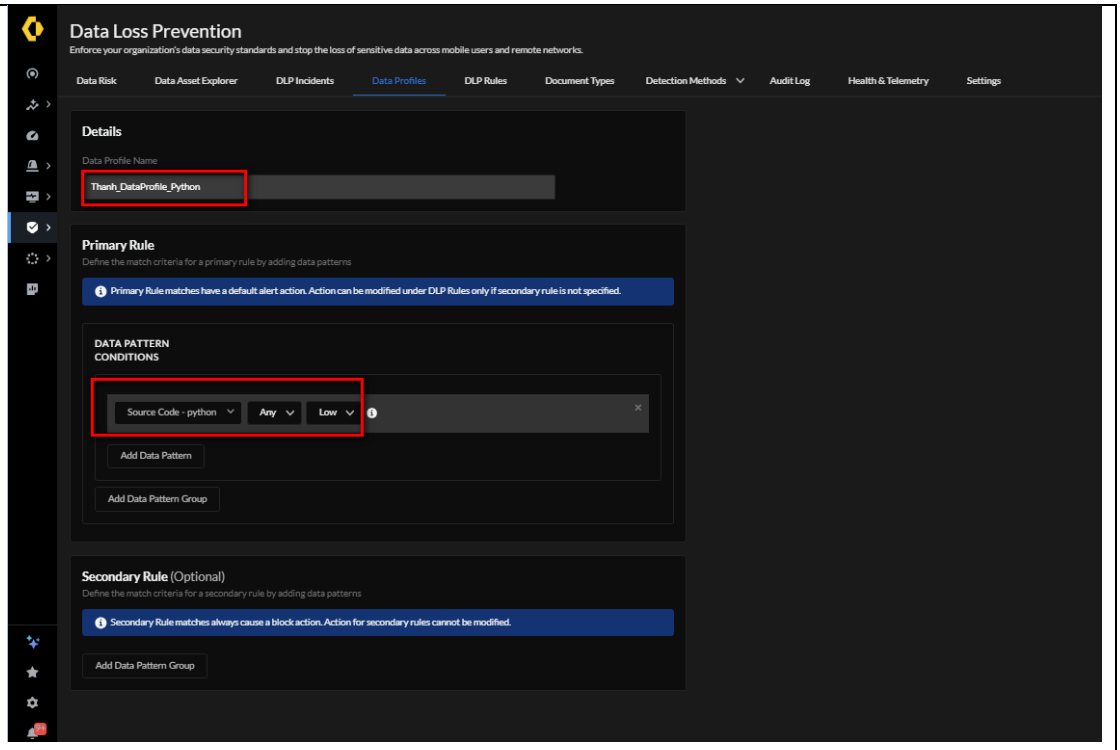
4.5 Phát hiện dữ liệu nhạy cảm gửi qua GenAI Apps

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.

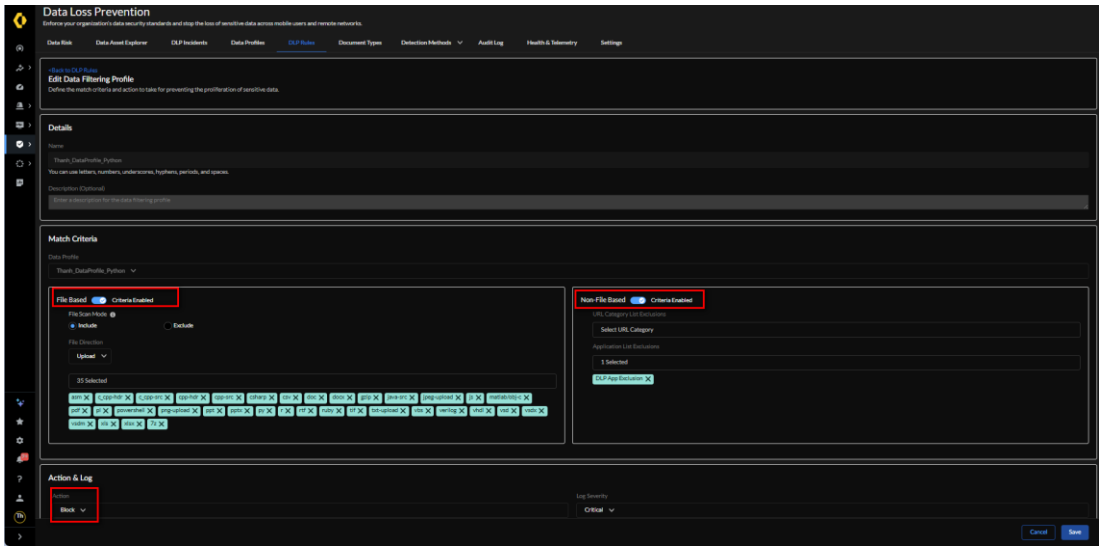


Cấu hình DLP, tạo Data Profile match với các loại file Python

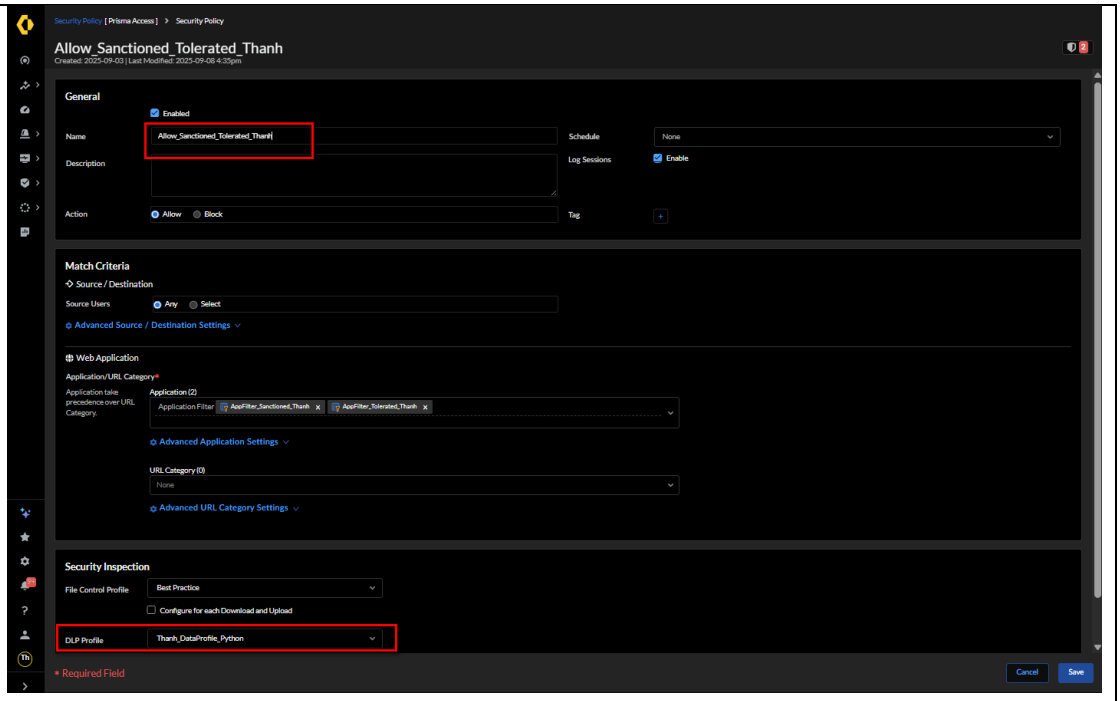




Cấu hình DLP rule cho cả 2 loại File Based và Non-File Based, Action là "Block"

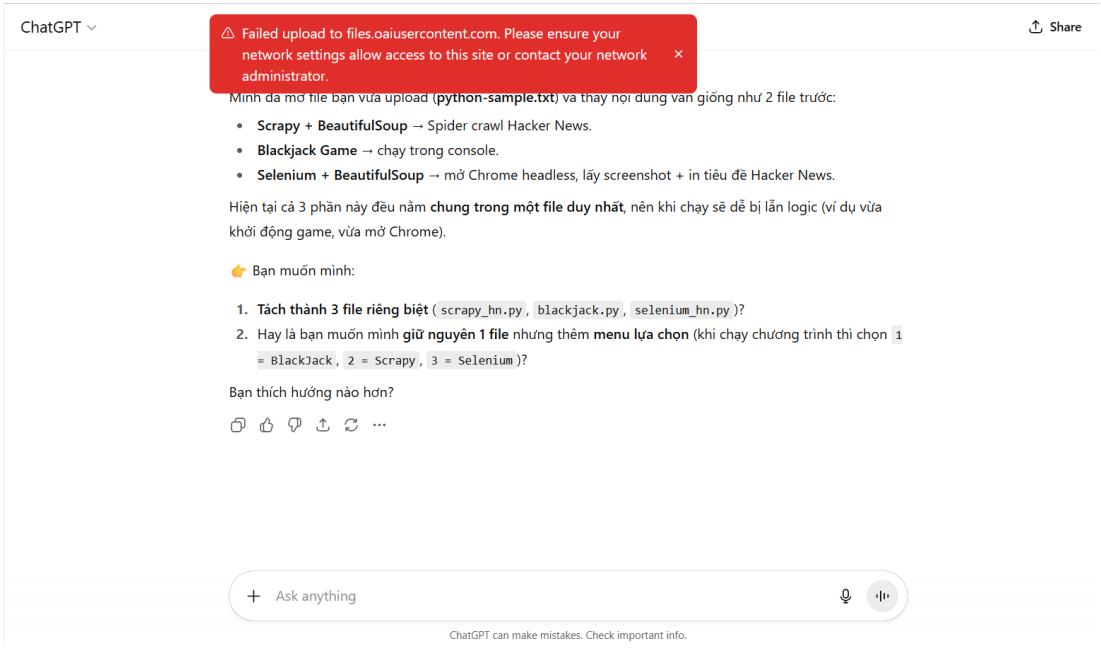


Sử dụng DLP Profile vừa tạo, áp dụng vào Security Policy, thực hiện Push để áp dụng cấu hình.

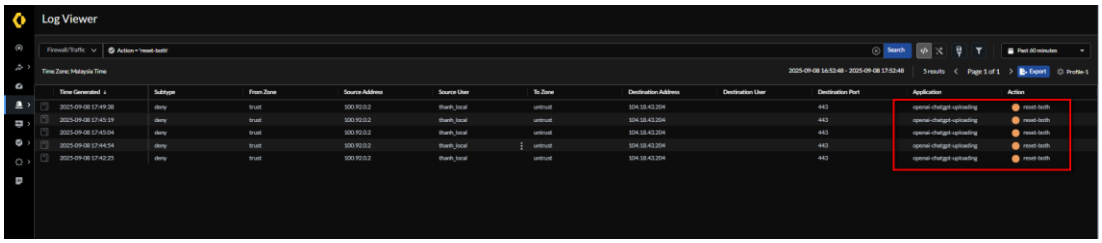


Kết quả thực tế

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

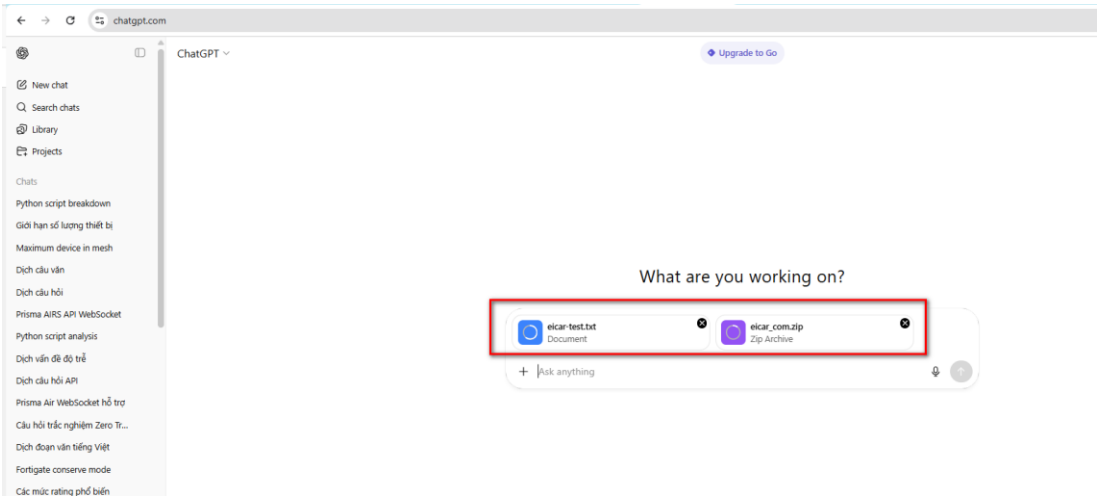
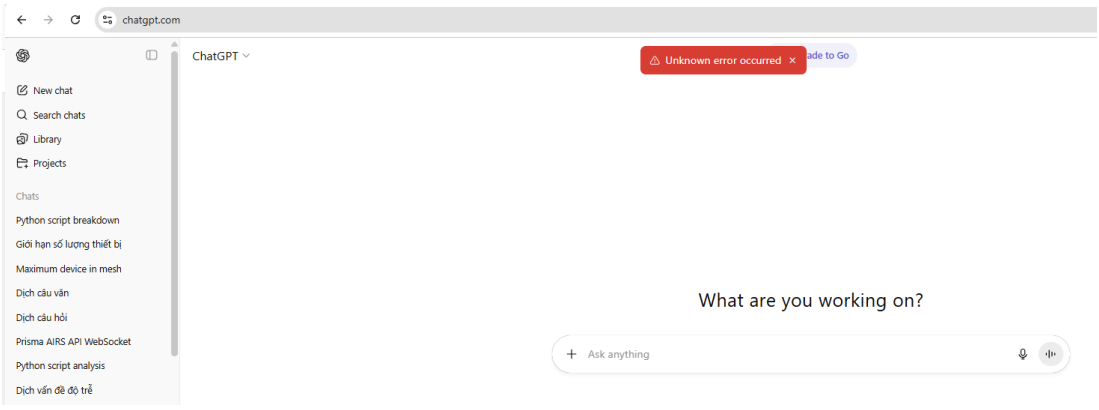


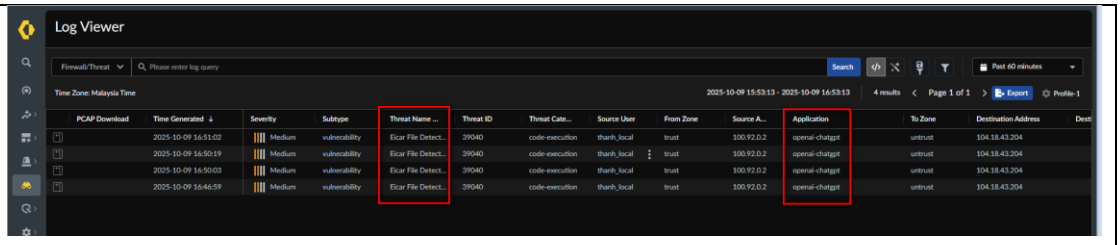
Log ngăn chặn upload file qua ChatGPT:



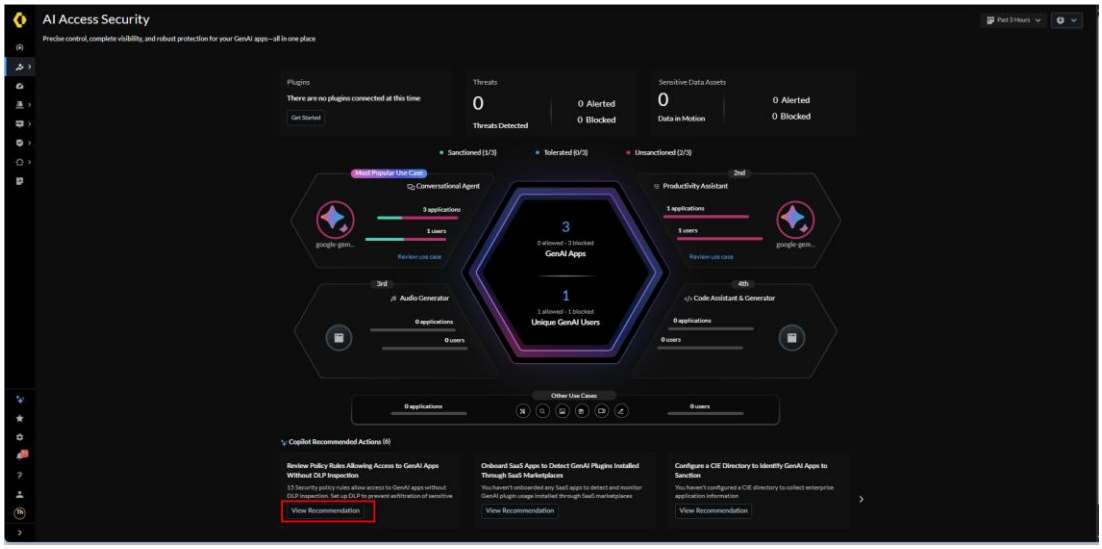
Đánh giá	- Kết quả: ☐ Pass ☐ Fail - Ghi chú:

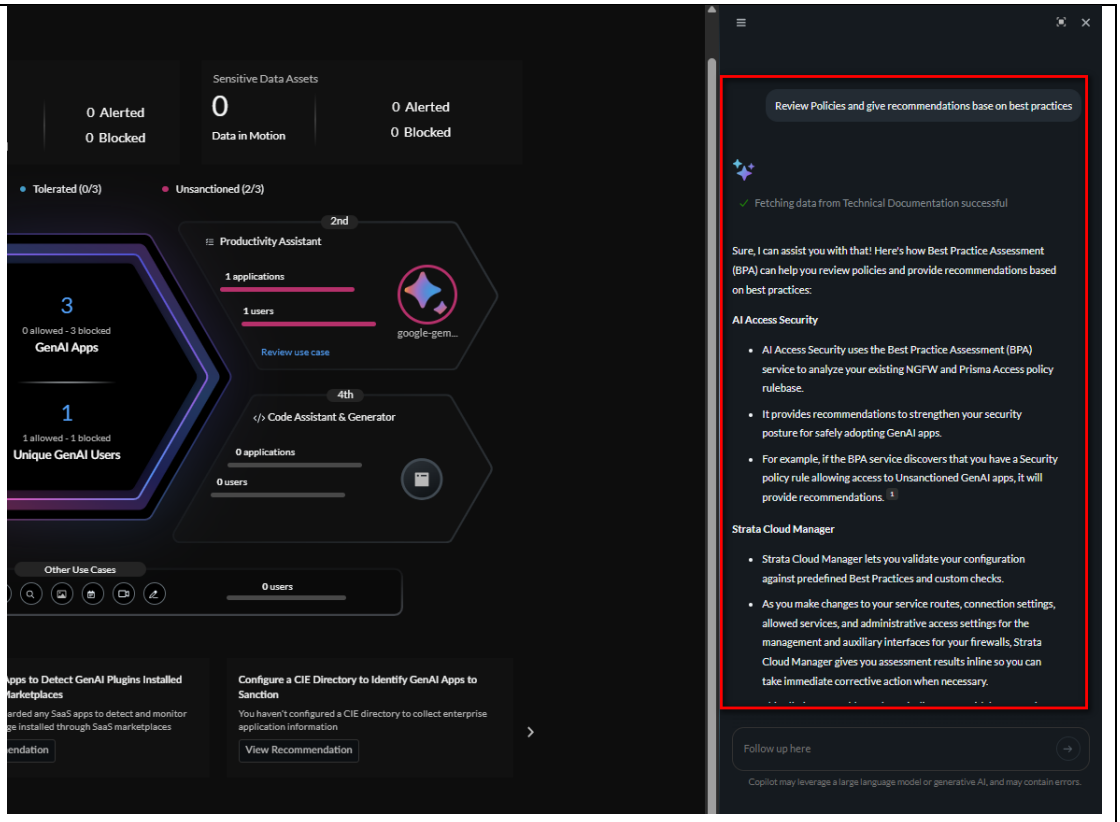
4.6 Phát hiện dữ liệu chứa mã độc gửi qua GenAI Apps

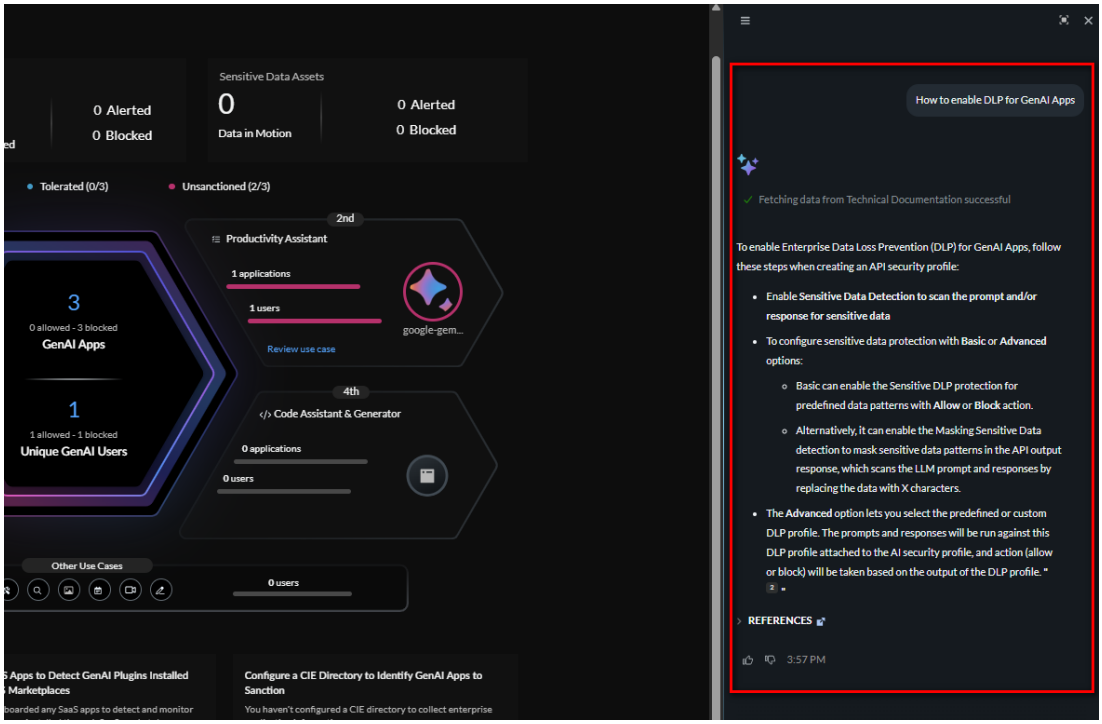
Mục tiêu	Với các GenAI App được phép sử dụng, quản trị viên có thể thiết lập chính sách để quét luồng dữ liệu của các App này để phát hiện các dữ liệu chứa mã độc gửi qua GenAI Apps
Các bước thực hiện	Upload file mã độc mẫu (Eicar file) 
Kết quả thực tế	Không thể upload file chứa mã độc:  Log ghi nhận:

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

4.7 Đề xuất cấu hình tối ưu chính sách

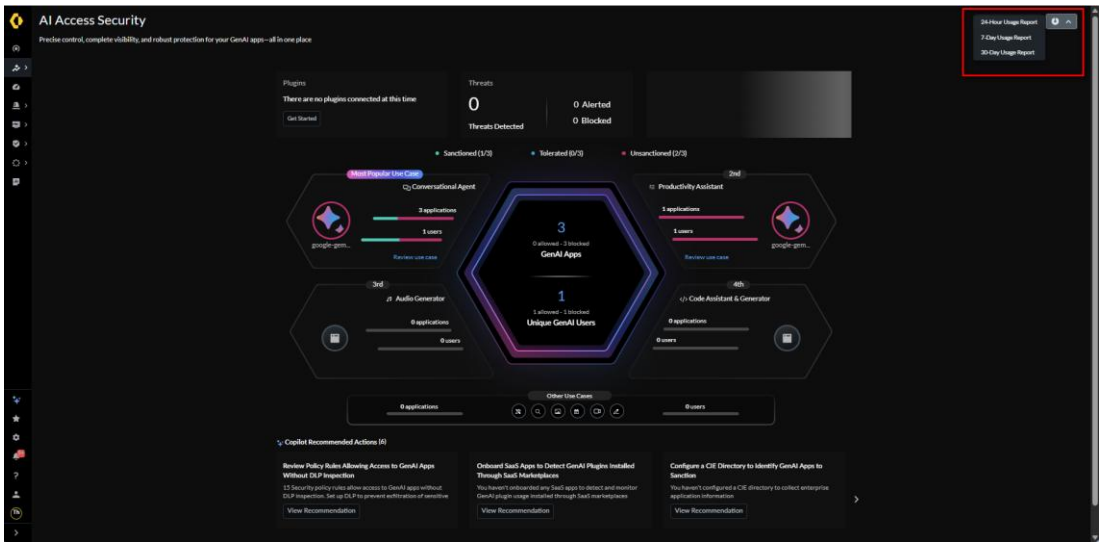
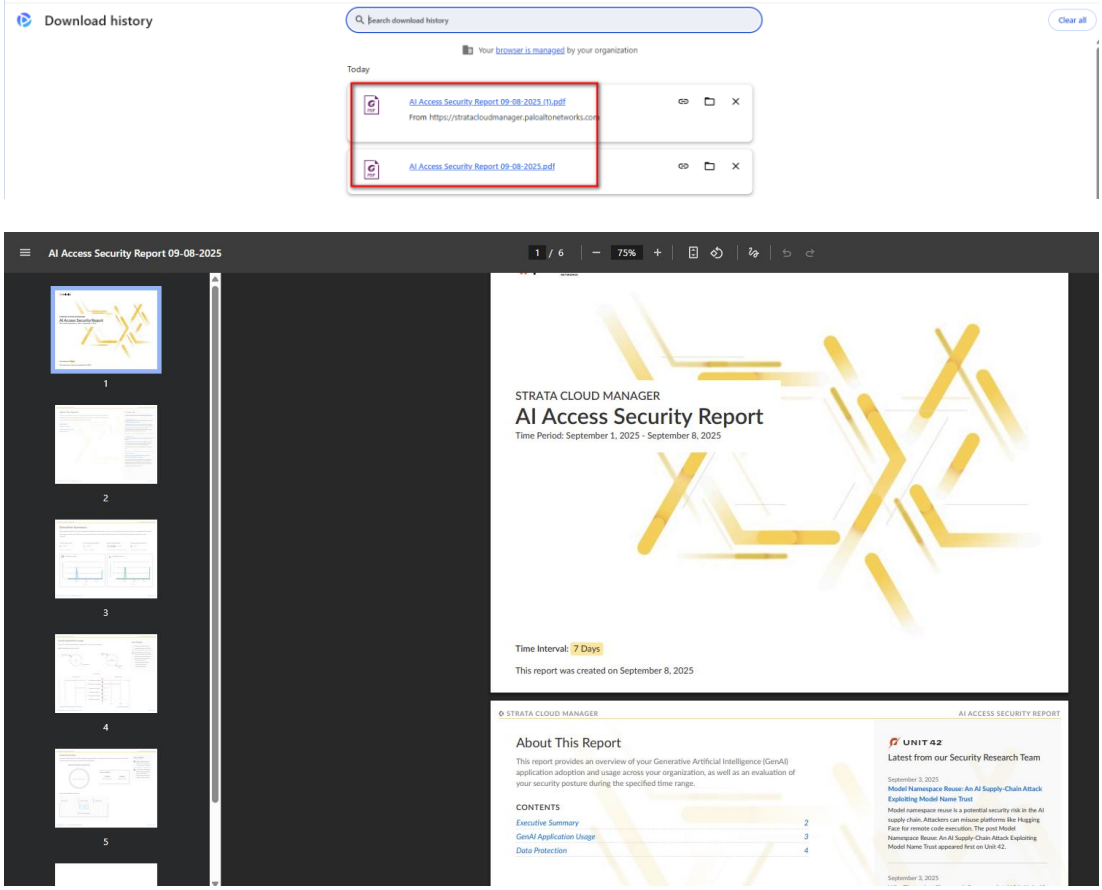
Mục tiêu	Hệ thống đưa ra các đề xuất cấu hình tối ưu Policy kiểm soát các ứng dụng GenAI
Các bước thực hiện	Truy cập Insight → AI Access, chọn "View Recommendation"  Đặt câu hỏi tương tác với Copilot và thực hiện theo các Steps trong khuyến nghị.
Kết quả thực tế	Hệ thống trả lời và đưa ra khuyến nghị,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

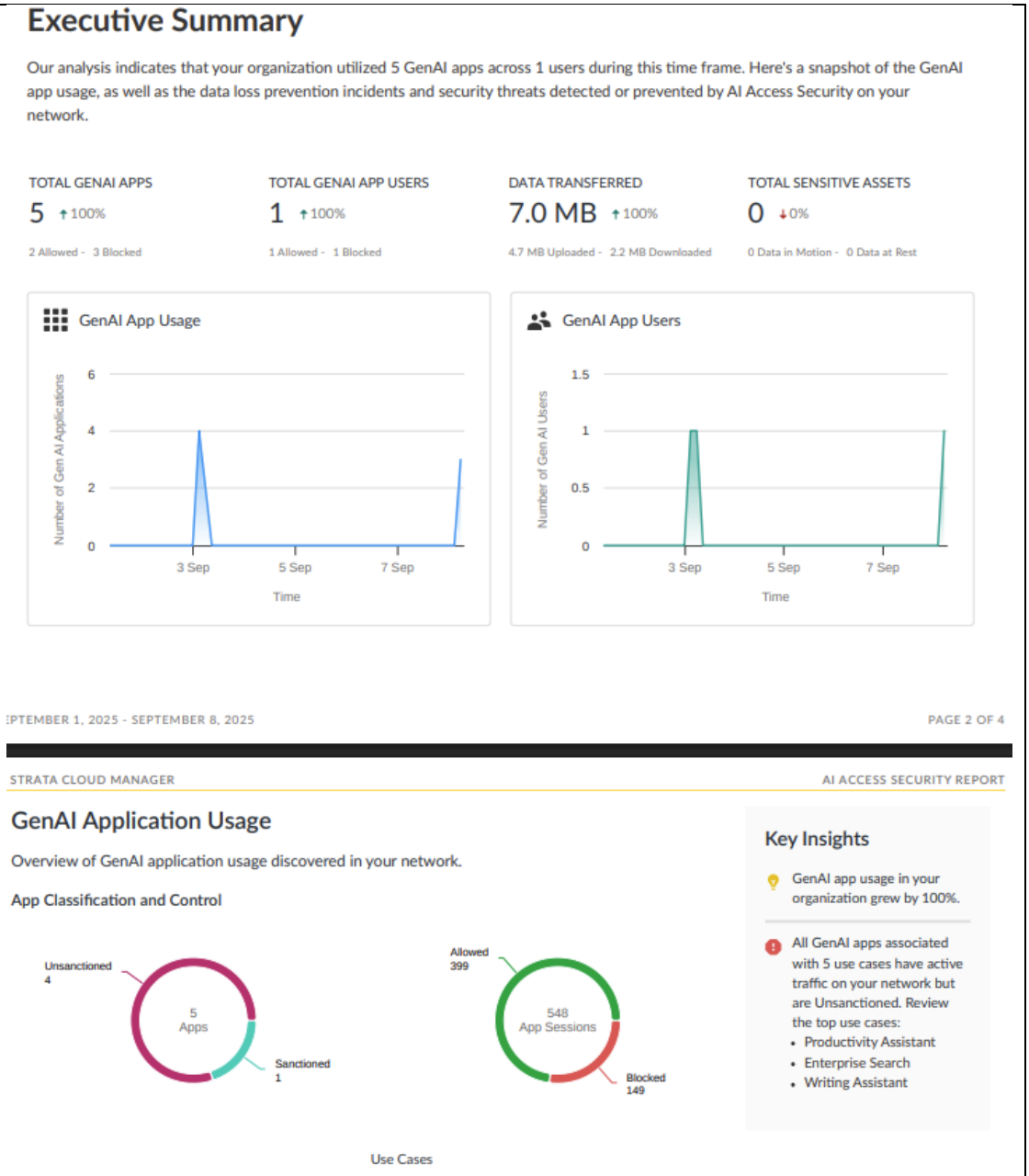




Đánh giá	- Kết quả: ☐ Pass ☐ Fail - Ghi chú:

4.8 Báo cáo GenAI Report

Mục tiêu	Cho phép tạo các báo cáo về GenAI Apps dạng Excutive 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. 



Mẫu Report:

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

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