Discovering AI Usage with Cloudflare ZTNA and CrowdStrike Exposure Management

Author: Travis G. Kench, CISSP
Title: Security Services Team Manager, SUNY ITEC
Version: 1.0
Date: February 10, 2026
LinkedIn: Connect

Table of Contents

Introduction

A security program cannot protect what it cannot identify, and this is especially important as new technology tools continue to appear across modern environments. The first step is to establish clear visibility into which applications are being used, who is using them, and how much data they handle. Cloudflare ZTNA and CrowdStrike Exposure Management support this effort by identifying both approved and unapproved applications, along with the data moving through them. With this insight, organizations can begin enforcing appropriate policies, limiting the use of highrisk tools, and allowing those that meet business and security requirements.

The purpose of this document is to help you identify the AI solutions currently active within your environment. It also provides a brief look at how to review these tools and apply policies to allow or block unapproved applications. If you need more advanced security controls such as monitoring prompt inputs, defending against prompt injection attacks, preventing sensitive data leaks, securing AI agents, protecting both locally hosted and SaaSbased language models, or enforcing detailed access and governance policies, you will need to explore the additional paid features offered by the vendors.

Cloudflare Zero Trust Network Access (ZTNA)

The following locations within Cloudflare ZTNA will help you identify AI solutions used within your environment, who is using them, and the amount of data that is being uploaded and downloaded from them.

Shadow IT: SaaS Analytics Dashboard

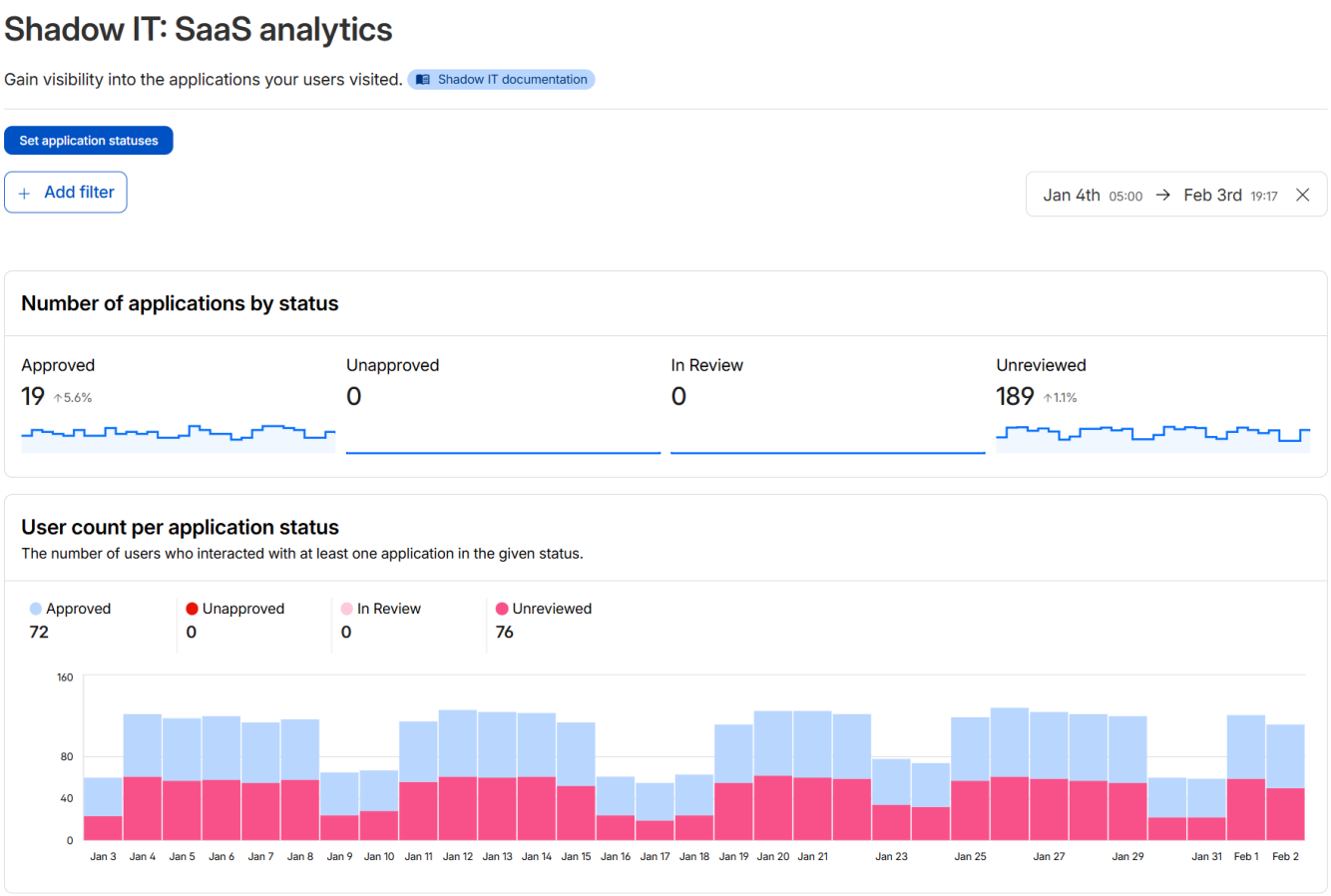
Identify AI Solutions Used Within Your Environment

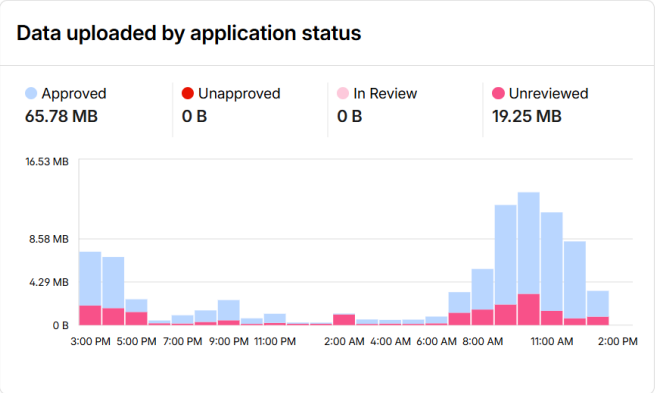
1. Navigate to the Cloudflare Dashboard
2. Protect & Connect > Zero Trust
3. Insights > Dashboards
4. Dashboard: "Shadow IT: SaaS analytics" - This dashboard gives you the ability to filter down into the solution and user data.
    a. Adjust the timeframe from the default "Last 24 hours" to fit the goal of your assessment.
    b. + Add filter
        i. "Application type" equals "Artificial Intelligence"
        ii. Click, Apply.
    c. + Add filter
        i. "Application type" equals "MCP Servers"
        ii. Click, Apply.
    d. Review report and do more filtering if necessary to identify users who are using AI resources. If you identify a solution that you want to do a deep dive into just hover over the name and select "Filter". That will supply you with the following granular information:
        i. User count.
        ii. Amount of data uploaded.
        iii. Amount of data downloaded.
        iv. Users by data uploaded.
        v. Users by data downloaded.
        vi. Countries by data uploaded.
        vii. Countries by data downloaded.
        viii. Top devices by data uploaded.
        ix. Top devices by data downloaded.
        x. Hostname by data downloaded.
        xi. Hostname by data uploaded.
    e. If you identify solutions that should be approved or marked as unapproved you can do so via the link at the top of the dashboard titled "Set application statuses".

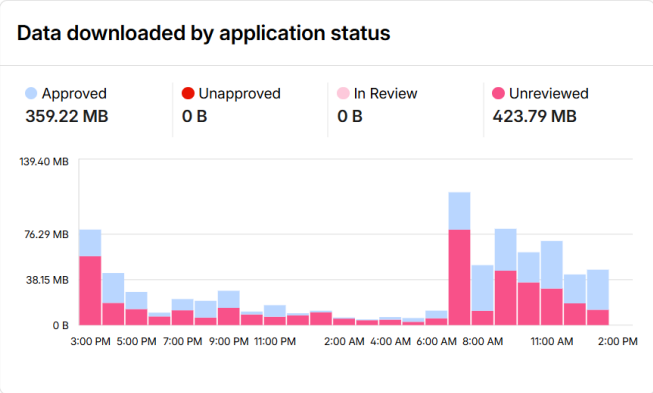
i. Based on your review you can then create a HTTP policy to allow or block traffic to the specific resources via the link at the top of the dashboard titled "Manage HTTP status policies".

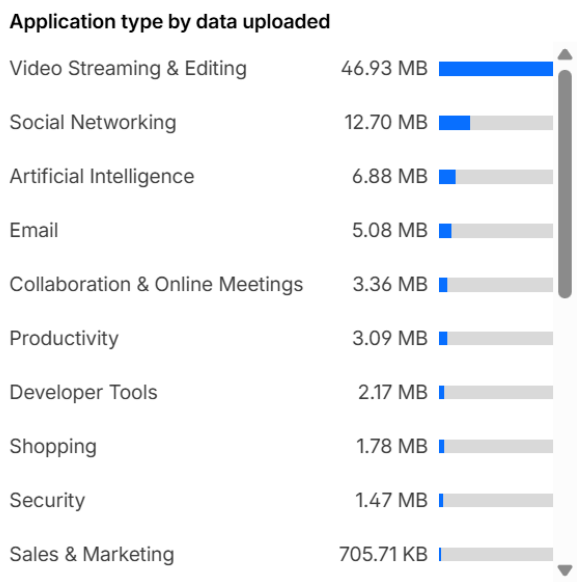
Identify Developer Tools Used Within Your Environment (common to have AI integrations)

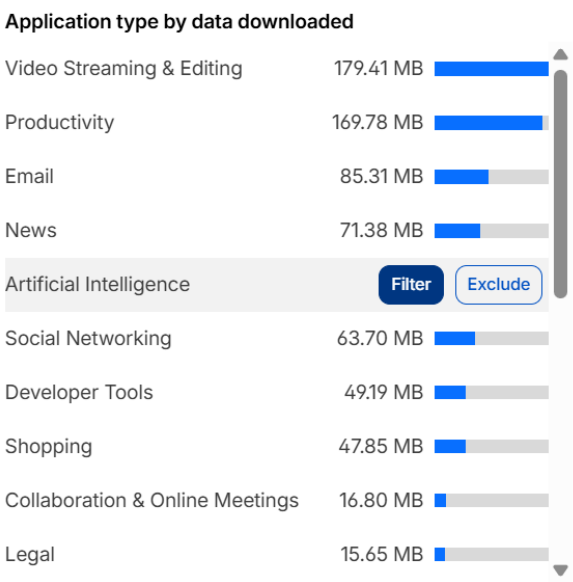
1. Navigate to the Cloudflare Dashboard
2. Protect & Connect > Zero Trust
3. Insights > Dashboards
4. Dashboard: "Shadow IT: SaaS analytics" - This dashboard gives you the ability to filter down into the solution and user data.
    a. Adjust the timeframe from the default "Last 24 hours" to fit the goal of your assessment.
    b. + Add filter
        i. "Application type" equals "Developer Tools"
        ii. Click, Apply.
    c. Review report and do more filtering if necessary to identify users who are using AI resources. If you identify a solution that you want to do a deep dive into just hover over the name and select "Filter". That will supply you with the following granular information:
        i. User count.
        ii. Amount of data uploaded.
        iii. Amount of data downloaded.
        iv. Users by data uploaded.
        v. Users by data downloaded.
        vi. Countries by data uploaded.
        vii. Countries by data downloaded.
        viii. Top devices by data uploaded.
        ix. Top devices by data downloaded.
        x. Hostname by data downloaded.
        xi. Hostname by data uploaded.
    d. If you identify solutions that should be approved or marked as unapproved you can do so via the link at the top of the dashboard titled "Set application statuses".
        i. Based on your review you can then create a HTTP policy to allow or block traffic to the specific resources via the link at the top of the dashboard titled "Manage HTTP status policies".





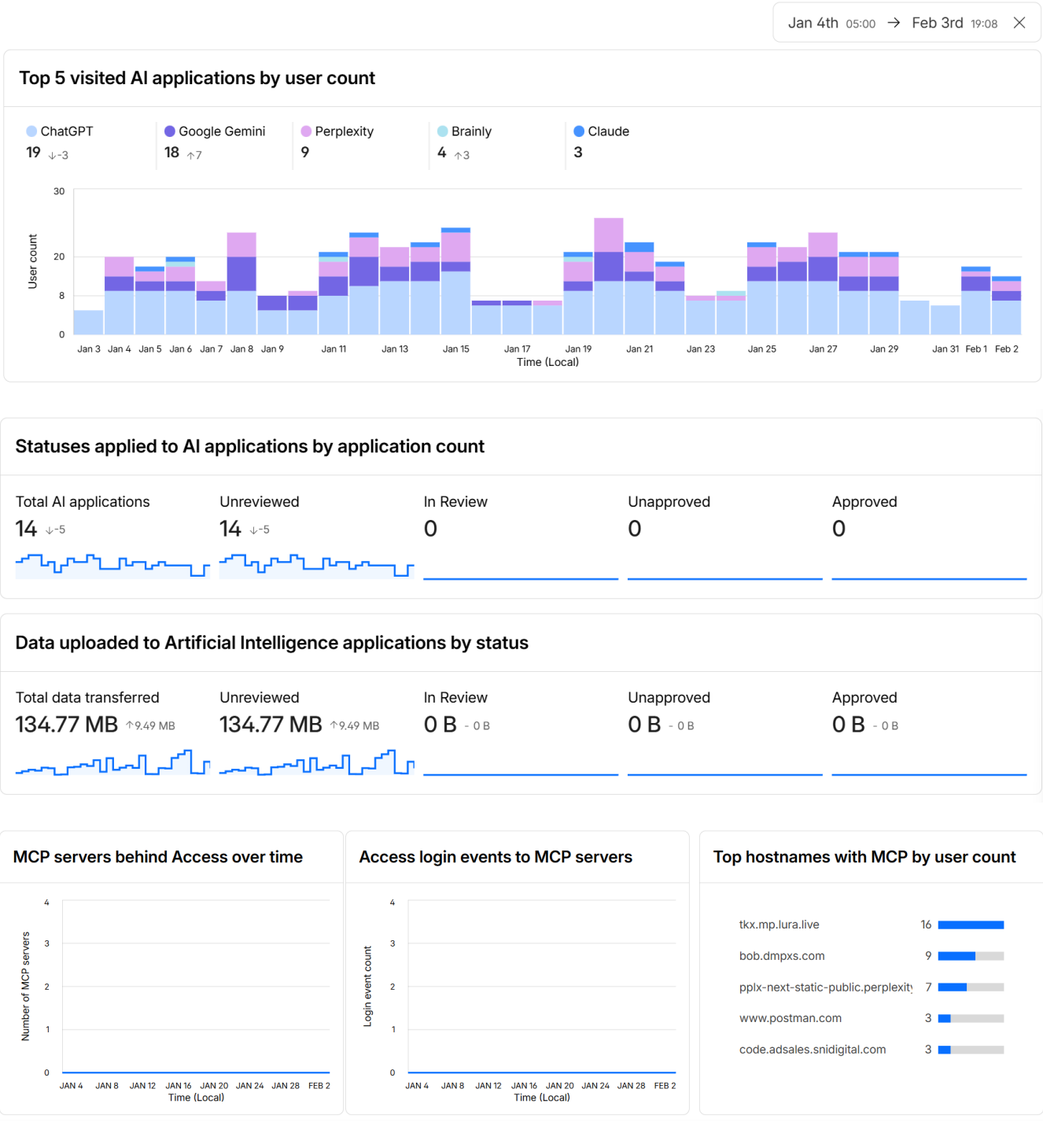






AI Security Report Dashboard

1. Navigate to the Cloudflare Dashboard
2. Protect & Connect > Zero Trust
3. Insights > Dashboards
4. Dashboard: "AI security report" - This dashboard gives you a high-level overview of the AI solutions used within your environment.
    a. Top 5 visited AI applications by user count.
    b. Statuses applied to AI applications by application count
    c. Data uploaded to Artificial Intelligence applications by status
    d. MCP servers behind Access over time
    e. Access login events to MCP servers
    f. Top hostnames with MCP by user count



CrowdStrike Exposure Management

Use Falcon Exposure Management to discover and control unsanctioned AI tools before they become a risk.

1. In the Falcon platform, navigate to Exposure management > Applications > All. Filter to show "AI" values only.
    a. Filter on "Category": Type "AI", and then select all of the category names that appear. Based on my experience I have come across the following options: "AI", "GenAI Assistants & Chatbots", "GenAI Development & Coding Tools", and "GenAI Image Generators & Editing" however you may encounter others based on what CrowdStrike has observed and categorized as AI usage within your environment.

2. Open the details panel for the items on the filtered list for suspicious activity indicators, related vulnerabilities, and usage data.
3. Use this information to strengthen policies.
4. You can create scheduled reports to proactively try to identify and address unapproved applications used within your environment.