CLOUDFLARE

SOLUTION OVERVIEW

Discover workforce use of shadow AI and IT

Extend visibility over unsanctioned AI and SaaS tools with Cloudflare's traffic inspection

Unmask the unseen

Shadow IT is not a new problem, but rapid adoption of unapproved AI tools is driving a modern crisis:

- **20%** of organizations suffered a breach due to security incidents with shadow AI in 2025[1]
- **85%** of IT leaders say employees are adopting AI tools before IT can assess them[2]

Cloudflare restores visibility for organizations to manage this expanding attack surface:

- **Review app status:** Categorize AI and SaaS apps as approved, unapproved, or still in review
- **Enforce policies based on app status:** Allow, block, isolate, apply DLP detections to interactions, restrict file uploads, and more
- **Analyze app usage:** Monitor aggregate trends and conduct granular investigations
- **Evaluate app risk:** Assess trustworthiness via application confidence scores

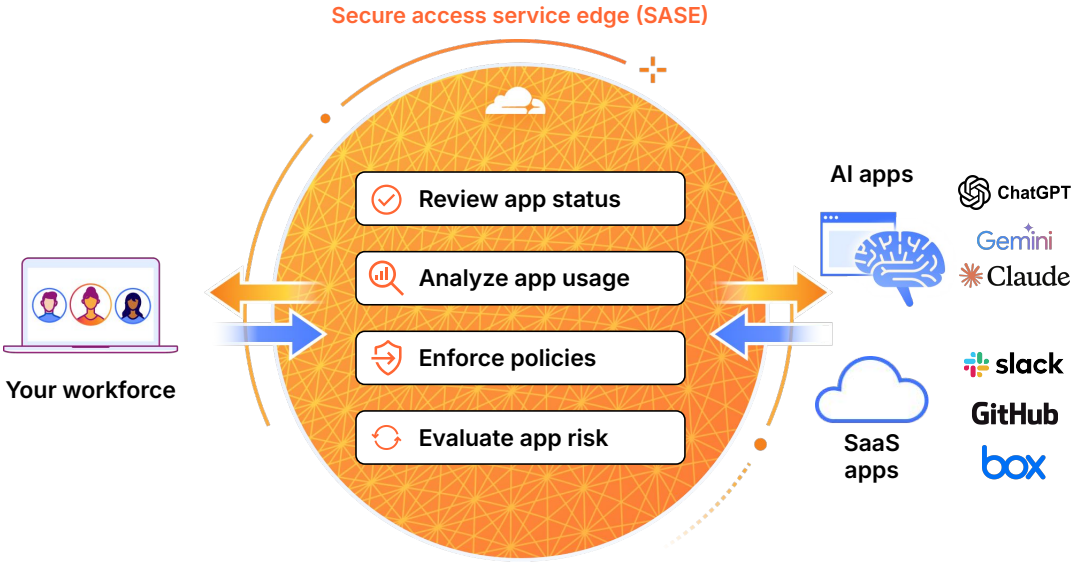
Unique risks of shadow AI

Shadow AI is different from traditional shadow IT. While SaaS apps mainly store or share files, AI tools transform and learn from any employee input..

This means that sensitive IP, customer data, or source code can be irreversibly absorbed for model training, with no possibility of removal.

How it works

Cloudflare's SASE platform sits inline between your workforce and resources to unify visibility and controls.



Additionally, integrate Cloudflare's CASB via API to scan for misconfigurations, user activity, and sensitive data. Manage security posture across AI apps (ChatGPT, Claude, Google Gemini) and other SaaS apps. Use CASB with your identity provider to see when users authenticate to any unsanctioned third-party apps.

Example dashboards

Filter this high-level overview of app usage based on:

- Application and app type
- Approval status
- Secured behind ZTNA
- Number of users

For more detail, click on the name of any AI app to see specific users or groups accessing it, their usage frequency, location, and the amount of data transferred.

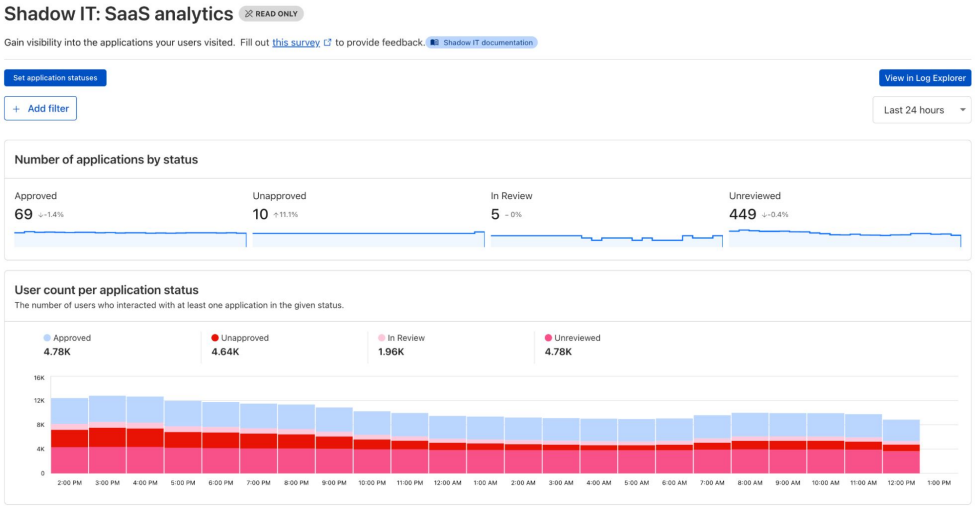


Figure 1: Shadow IT analytics dashboard

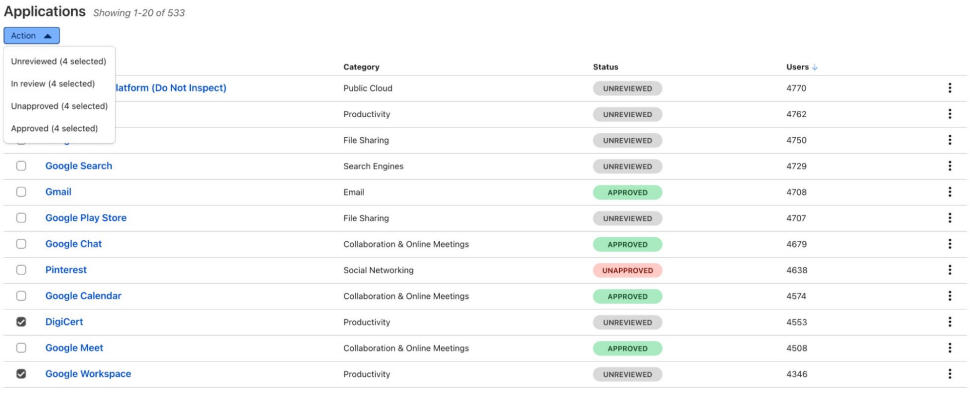


Figure 2: Mark application statuses

Organize apps and set access policies based on approval status:

- Approved (sanctioned)
- Unapproved (unsanctioned)
- In review
- Unreviewed

Want more technical guidance? Learn how to build policies with this learning path.

Want to go deeper on how to secure your AI adoption?

Explore more use cases | Request a workshop

1. 2025 IBM, Cost of a Data Breach report: Source
2. 2025 Manage Engine research: Source