

従業員によるシャドーAIとIT 使用を検出

Cloudflareのトラフィック検査で、無許可のAIツールやSaaSツールの可視性を拡大させる

見えないものを可視化

シャドーITの解明は新しい問題ではありません。しかし、未承認のAIツールの急速な利用は、現代の危機を脅かしています。

- 20%の組織で2025年、シャドーAIを使用したセキュリティインシデントによる被害に遭遇¹
- 85%のITリーダーは、IT部門による評価前のAIツールを従業員が使っていると報告²

Cloudflareは、拡大する攻撃対象領域を管理するための可視性を回復させます。

- **アプリのステータスを評価**：AIとSaaSアプリを承認済み、未承認、またはレビュー中として**分類**
- **アプリのステータスに基づくポリシーの適用**：許可、ブロック、分離、インタラクションへのDLP検出の適用、ファイルアップロードの制限**など**
- **アプリの使用状況を分析**：**集約されたトレンドを監視**、詳細な調査を実施
- **アプリケーションのリスクを評価**：信頼性を評価
アプリケーションの信頼度スコアによる



シャドーAIの固有リスク

シャドーAIは、従来のシャドーITとは異なります。SaaSアプリは主にファイルの保存または共有を行います。AIツールは従業員のあらゆる入力から変換し、学習します。

つまり、機密性の高いIP、顧客データ、ソースコードがモデルのトレーニングのために不可逆的に吸収され、取り外される可能性がまったくないことを意味します。

仕組み

CloudflareのSASEプラットフォームは、従業員とリソースの間に位置し、可視性と制御を一元化します。



さらに、[CloudflareのCASBをAPI経由で統合](#)し、設定ミス、ユーザーアクティビティ、機密データをスキャンします。AIアプリ ([ChatGPT](#)、[Claude](#)、[Google Gemini](#)) とその他のSaaSアプリのセキュリティ体制を管理します。

CASBとIDプロバイダーを使うと、ユーザーが無許可のサードパーティアプリに対して認証するかどうかを確認できます。

ダッシュボードの例

以下に基づいて、アプリの使用状況の概要をフィルタリングします：

- アプリケーションとアプリの種類
- 承認ステータス
- ZTNAの背後で保護
- ユーザー数

詳細は、任意のAIアプリの名前をクリックすると、それらを利用している特定のユーザーやグループ、利用頻度、場所、データ転送量が表示されます。

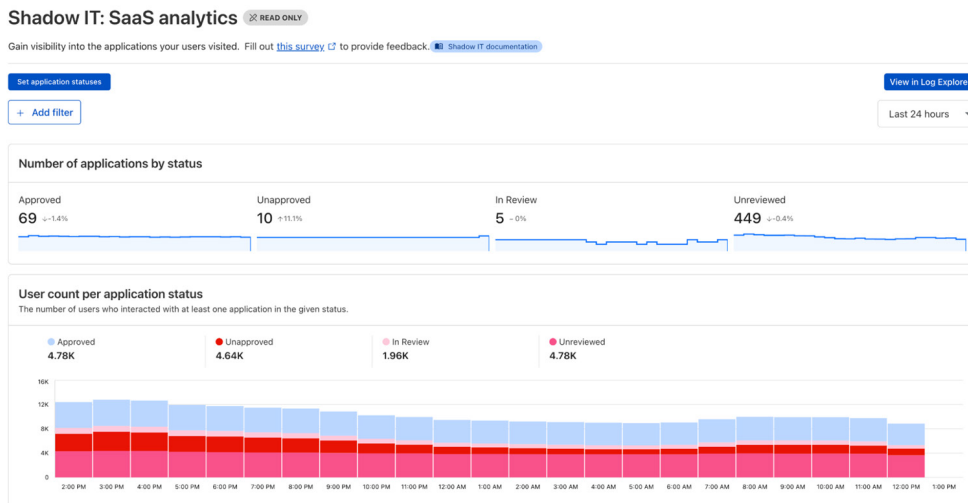


図1：シャドーIT分析ダッシュボード

Applications Showing 1-20 of 533

Action Unreviewed (4 selected) In review (4 selected) Unapproved (4 selected) Approved (4 selected)

Application	Category	Status	Users
latform (Do Not Inspect)	Public Cloud	UNREVIEWED	4770
	Productivity	UNREVIEWED	4762
	File Sharing	UNREVIEWED	4750
<input type="checkbox"/> Google Search	Search Engines	UNREVIEWED	4729
<input type="checkbox"/> Gmail	Email	APPROVED	4708
<input type="checkbox"/> Google Play Store	File Sharing	UNREVIEWED	4707
<input type="checkbox"/> Google Chat	Collaboration & Online Meetings	APPROVED	4679
<input type="checkbox"/> Pinterest	Social Networking	UNAPPROVED	4638
<input type="checkbox"/> Google Calendar	Collaboration & Online Meetings	APPROVED	4574
<input checked="" type="checkbox"/> DigiCert	Productivity	UNREVIEWED	4553
<input type="checkbox"/> Google Meet	Collaboration & Online Meetings	APPROVED	4508
<input checked="" type="checkbox"/> Google Workspace	Productivity	UNREVIEWED	4346

承認ステータスに基づいてアプリを整理し、アクセスポリシーを以下のように設定しました。

- 承認（認可）
- 未承認（無許可）
- レビュー中
- レビュー待ち

より詳細な技術ガイダンスが必要ですか？このラーニングパスで、ポリシーの構築方法について学びましょう。

図2：アプリケーションのステータス設定状況

AIの導入をセキュアにする方法についてさらに深く掘り下げてみませんか？

[その他のユースケースを見る](#) [ワークショップを依頼する](#)

1. 2025年 IBM、「Cost of a Data Breach」レポート：出典
 2. 2025年Manage Engine調査：出典