CLOUDFLARE

APERÇU DE LA SOLUTION

Identifiez la manière dont vos collaborateurs se servent des outils de Shadow AI et de Shadow IT

Étendez votre visibilité aux outils IA et SaaS non approuvés grâce aux fonctionnalités d'inspection du trafic proposées par Cloudflare

Dévoiler l'invisible

L'informatique fantôme (Shadow IT) n'est pas un problème récent, mais l'adoption rapide d'outils IA non approuvés est à l'origine d'une crise moderne :

- **20 %** des entreprises ont subi une violation résultant d'incidents de sécurité liés à l'IA fantôme (Shadow AI) en 2025.[1]
- **85 %** des responsables informatiques déclarent que leurs collaborateurs adoptent des outils d'IA avant que le service IT ne puisse les évaluer.[2]

Cloudflare restaure la visibilité des entreprises afin de leur permettre de gérer cette surface d'attaque en pleine expansion :

- **Examen du statut des applications :** classez vos applications IA et SaaS comme approuvées, non approuvées ou toujours en cours d'examen.
- **Application des politiques en fonction du statut de l'application :** autorisez, bloquez, isolez, appliquez des mesures de détection DLP aux interactions et limitez les importations de fichiers parmi bien d'autres possibilités.
- **Analyse de l'utilisation des applications :** surveillez les tendances cumulées et procédez à des investigations granulaires.
- **Évaluation des risques liés aux applications :** estimez la fiabilité de vos applications à l'aide de scores de confiance

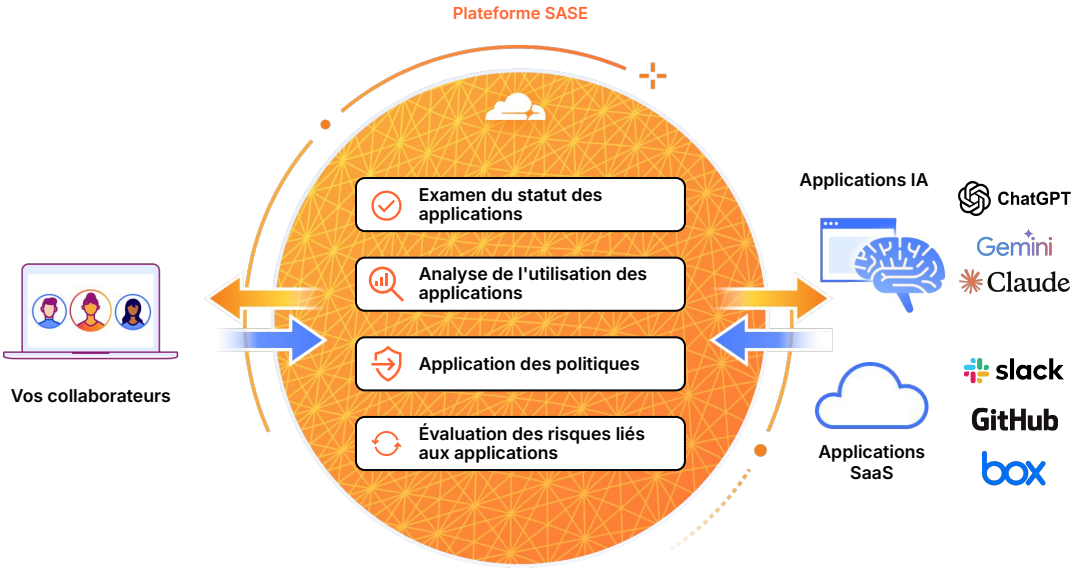
Les risques uniques liés à l'IA fantôme

L'IA fantôme diffère de l'informatique fantôme « traditionnelle ». Les applications SaaS servent principalement à stocker ou à partager des fichiers, mais les outils IA sont capables de transformer et d'apprendre de n'importe quelle entrée saisie par un collaborateur.

Vos données sensibles, comme vos éléments de propriété intellectuelle, les données concernant vos clients ou votre code source, peuvent être absorbées de manière irréversible à des fins d'apprentissage des modèles, sans possibilité de suppression.

Fonctionnement

La plateforme SASE de Cloudflare s'intègre (en inline) entre vos collaborateurs et vos ressources afin d'unifier la visibilité et les mesures de contrôle.



Vous pouvez également intégrer le CASB Cloudflare par l'intermédiaire d'une API afin d'analyser les erreurs de configuration, l'activité des utilisateurs et les données sensibles. Gérez la stratégie de sécurité de l'ensemble de vos applications IA, (ChatGPT, Claude, Google Gemini) et de vos autres applications SaaS. Utilisez le CASB en combinaison avec votre fournisseur d'identité afin de découvrir à quel moment vos utilisateurs s'authentifient auprès d'applications tierces non autorisées.

Exemples de tableaux de bord

Vous pouvez identifier la manière dont vos collaborateurs utilisent les applications en filtrant cette vue d'ensemble de haut niveau selon les critères suivants :

- Application et type d'application
- Statut d'approbation
- Sécurisation derrière une solution ZTNA
- Nombre d'utilisateurs

Pour plus de détails, cliquez sur le nom de n'importe quelle application IA afin de visualiser les utilisateurs ou les groupes spécifiques qui y accèdent, la fréquence à laquelle ils utilisent cette application, leur position géographique et la quantité de données transférées.

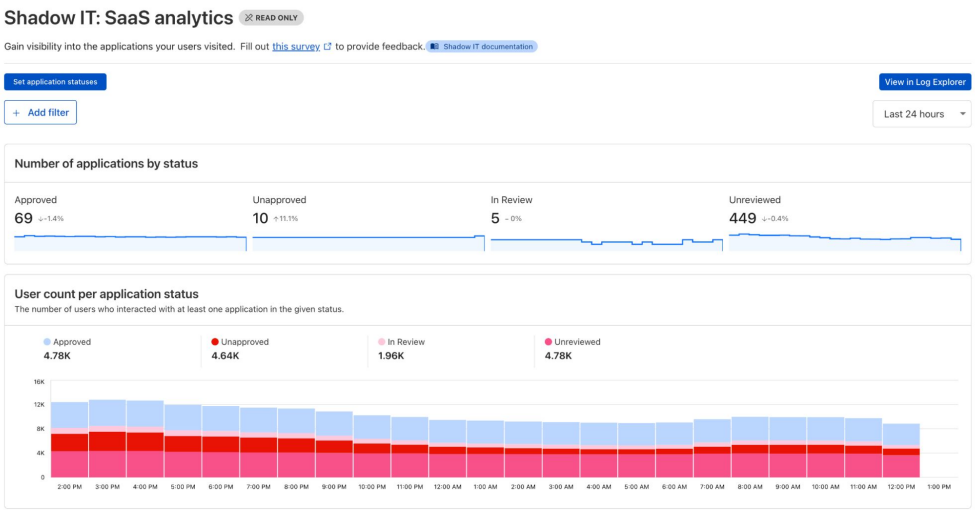


Figure 1 : tableau de bord de l'outil d'analyse de l'informatique fantôme

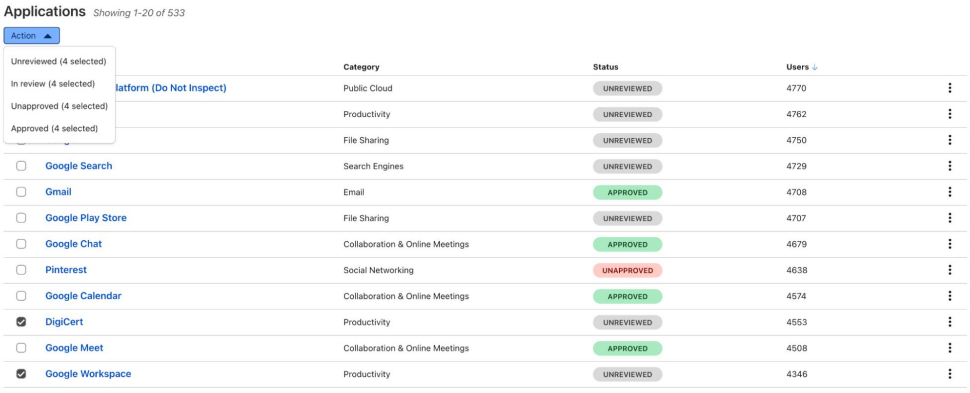


Figure 2 : identification du statut des applications

Organisez vos applications et définissez les politiques d'accès à ces dernières en fonction de leur statut d'approbation :

- Approuvée (autorisée)
- Non approuvée (non autorisée)
- En cours d'examen
- Non validée

Vous souhaitez bénéficier de davantage de conseils techniques ? Découvrez comment définir vos politiques dans ce parcours d'apprentissage.

Vous souhaitez aller plus loin quant à la manière dont sécuriser l'adoption de l'IA dans votre entreprise ?

Découvrir d'autres scénarios d'utilisation

Demander un atelier

1. IBM, Cost of a Data Breach Report 2025 (Rapport IBM sur le coût d'une violation de données en 2025) : source
2. Recherche ManageEngine 2025 : source

