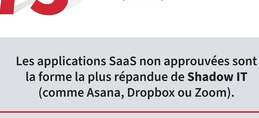
LastPass

Qu'est-ce que le **Shadow IT ?**

(Et pourquoi s'en soucier).

Le Shadow IT désigne l'utilisation d'appareils, d'applications ou de logiciels qui n'ont pas été approuvés par votre service informatique ou par la direction de l'entreprise. Pour faire simple, il s'agit des technologies non autorisées.



75% des employés utiliseront des outils à l'insu de l'IT d'ici à 2027 (*Gartner*)

Les applications SaaS non approuvées sont la forme la plus répandue de **Shadow IT** (comme Asana, Dropbox ou Zoom).

Le Shadow AI, l'utilisation non approuvée de l'IA, est également de plus en plus courant chez les employés qui se tournent vers des outils comme ChatGPT pour améliorer la productivité.

38% des employés ont partagé des informations professionnelles sensibles avec des outils d'IA non approuvés. (*CybSafe*)

Quel est le problème avec le Shadow IT et le Shadow AI ? Lorsque les employés choisissent leurs propres outils et applications pour faire leur travail, **ils contournent souvent des protocoles de sécurité essentiels, exposant votre entreprise à différents types de risques de sécurité et financiers.**

Pourquoi les employés utilisent le **Shadow IT et le Shadow AI**

Frustrations générées par les outils existants
Les employés prennent souvent les choses en main si l'IT met du temps à répondre aux demandes de nouveaux outils. Cela signifie qu'ils se procurent par eux-mêmes les applications SaaS (non sanctionnées) pour résoudre un problème urgent ou pour augmenter la productivité, inconscients des risques associés.

Résultat plus rapide et accès plus simple
Les employés gravitent vers les applications SaaS qui sont simples à télécharger, utiliser et intégrer. Toutefois, ces outils sont utilisés à l'insu de l'IT et donc sans supervision.

Une main-d'œuvre en pleine évolution
Les nouvelles générations d'employés qui rejoignent une main-d'œuvre dispersée géographiquement (en télétravail, hybride ou au bureau) sont plus susceptibles de recourir à des appareils personnels et des applications collaboratives pour améliorer leur productivité, ce qui peut mettre les données sensibles en danger.

80% des employés adoptent le Shadow IT pour des raisons de commodité ou de productivité. (*Forbes*)

Pourquoi se soucier du **Shadow IT et du Shadow AI**

La tentation de contourner les procédures officielles de l'IT est forte. Mais ces raccourcis, et l'utilisation du Shadow IT et du Shadow AI, peuvent exposer votre entreprise à des dommages importants.

Partage et fuites de données involontaires

76%

des PME déclarent que les déploiements de Shadow IT présentent des risques de cybersécurité « modérés ou graves ». (*Capterra*)

Conformité et risques juridiques

Le Shadow IT et le Shadow AI peuvent contrevenir aux règlements comme le PCI-DSS, GDPR, HIPAA ou SOX.

Failles de sécurité invisibles dans vos infrastructures informatiques

5x

Les organisations sont 5 fois plus susceptibles de subir un incident de sécurité si elles n'ont pas une visibilité centralisée du SaaS. (*Gartner*)

Prolifération coûteuse du SaaS

53%

des applications sont sous-utilisées, et les organisations dépensent environ 21 millions de dollars par an sur les licences SaaS inutilisées. (*Zylo*)

Comment **reprendre le contrôle** du Shadow IT et du Shadow AI

La meilleure défense pour votre entreprise ?
Une visibilité sur le SaaS et un gestionnaire de mots de passe.

Les outils de gestion SaaS peuvent détecter les applications, suivre l'utilisation et optimiser les dépenses logicielles, mais ils ne permettent pas de voir comment les utilisateurs s'authentifient et partagent et protègent les identifiants.

Un gestionnaire de mots de passe comme LastPass peut combler ces failles pour conférer une protection totale à votre organisation contre les risques liés au Shadow IT et au Shadow AI. LastPass :

- Impose des mots de passe forts et uniques et empêche la réutilisation des mots de passe sur les comptes SaaS, réduisant considérablement les risques de fuites.
- Permet le partage sécurisé d'identifiants, le contrôle d'accès basé sur les rôles et la visibilité sur les comptes dotés de privilèges, empêchant les accès non autorisés.
- Impose les meilleures pratiques de sécurité de l'authentification, diminuant les risques de vol d'identifiants et liés à l'hameçonnage.
- Aide l'IT à imposer une authentification forte, y compris pour les outils non autorisés, limitant les risques liés au Shadow IT.
- Assure l'application des règles de mot de passe, consigne les accès et contribue au respect des normes réglementaires.

Demander une démo