1Password

1PASSWORD® EXTENDED ACCESS MANAGEMENT

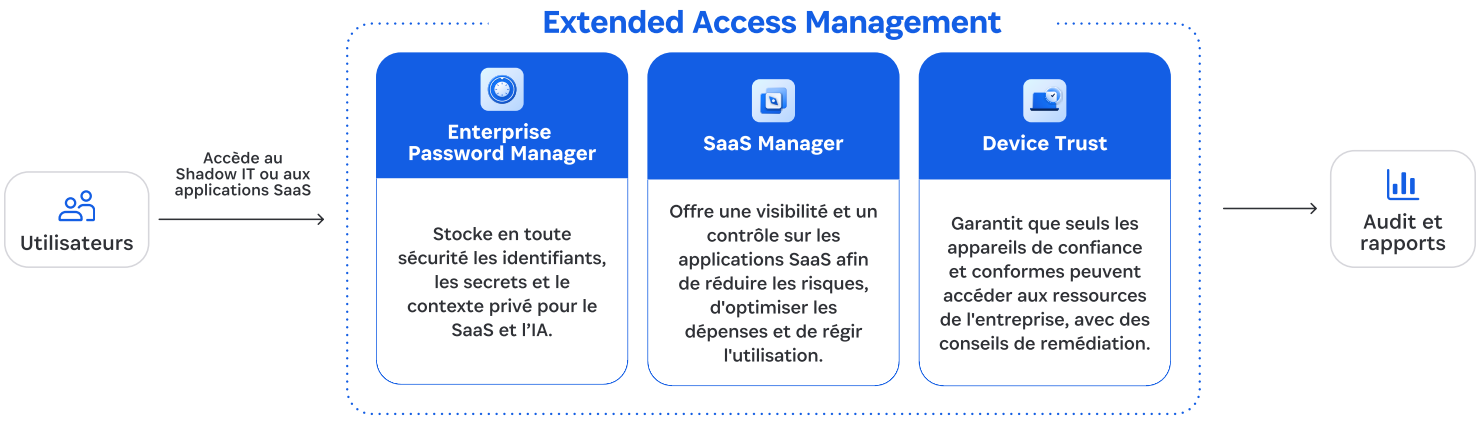
Sécurisez toutes les connexions, quels que soient l'application et l'appareil utilisés

La productivité et la sécurité se heurtent. Mais ce n'est pas inévitable.

Les entreprises d'aujourd'hui ont un problème de prolifération : prolifération du SaaS, des appareils et des identités. Conjointement, l'accès décentralisé au SaaS et la nouvelle familiarité des travailleurs avec la technologie ont produit des effets : les employés disposent désormais de l'assurance qu'il leur faut pour reconnaître les outils adaptés à leurs tâches, et pour se les procurer. Ils ne se limitent plus à l'usage des outils et appareils fournis par leur entreprise.

Alors que les organisations s'efforcent de maximiser la productivité de leurs salariés et de les responsabiliser, elles sont confrontées aux risques accrus causés par le **« fossé entre les accès et la fiabilité ».** Ce fossé représente les risques que certains éléments posent pour la sécurité lorsqu'ils accèdent aux données d'une entreprise sans être soumis à des contrôles adéquats. Les éléments préoccupants sont les identités non fédérées ainsi que les appareils, applications et outils d'IA non gérés. Lorsque ces éléments ne sont pas couverts par des garanties et une visibilité coordonnées et contextuelles, les entreprises sont confrontées à un accroissement de leurs risques en matière de sécurité et de conformité.

Au-delà de l'IAM et du MDM : l'Extended Access Management



Capacités d'admin

1. Découvrir et identifier les applications SaaS et le Shadow AI
2. Activer des workflows pour intervenir sur les applications découvertes
3. Répondre aux exigences de conformité et consigner les accès SaaS

L'Extended Access Management permet de sécuriser les appareils, les applications et les agents d'IA qui sont impossibles à gérer par les outils existants conçus pour la gestion des identités et des accès (IAM), l'authentification unique (SSO) ou la gestion des appareils mobiles (MDM). Elle aide les organisations à combler le fossé entre les accès et la fiabilité. En conséquence, **les risques sur la sécurité et ceux de non-conformité sont réduits** et, en parallèle, les entreprises **bénéficient de gains de productivité significatifs et d'économies financières notables.** De plus, **les employés disposent des moyens qu'il leur faut pour faire preuve d'initiative** en ce qui concerne la rectification des problèmes constatés et la conformité.

Pour les équipes informatiques et de sécurité modernes, l'Extended Access Management est indispensable

1Password Extended Access Management est une plateforme composée est une plateforme de gestion étendue des accès. Elle est composée du gestionnaire de mots de passe de 1Password pour entreprise (Enterprise Password Manager), de l'outil de 1Password consacré à la conformité des appareils (Device Trust) et de 1Password SaaS Manager. Cette plateforme 1Password XAM permet de sécuriser les accès aux données sensibles détenues par une entreprise. Pour ce faire, elle donne à ses utilisateurs les moyens de gérer :

- **Les applications non agréées et non gérées (Shadow IT)** qui ne sont pas sécurisées par un dispositif d'authentification unique (SSO)
- **Les appareils non gérés** qui échappent à la protection des systèmes de MDM (gestion des appareils mobiles)
- **Les agents d'IA** qui disposent d'un accès à une multiplicité de systèmes et de la capacité d'effectuer des tâches par eux-mêmes

1Password Extended Access Management, pourquoi ?

- **Bénéficiez d'une visibilité intégrale**
  Combinez dans une interface unique la gestion et la sécurité des identités, des applications et des appareils.
- **Rectifiez plus rapidement vos problèmes de sécurité**
  Faites appliquer des mesures de protection des identités, et assurez-vous que les accès aux données de votre entreprise sont limités aux utilisateurs de confiance qui se servent d'un appareil sécurisé.
- **Simplifiez les accès**
  Gérez les accès de vos administrateurs, utilisateurs finaux et agents d'IA à tous les types d'applications.

Principales fonctionnalités de 1Password Extended Access Management

- **Sécurisez toutes les connexions.** Assurez-vous que les méthodes d'authentification employées par vos utilisateurs finaux et par vos agents d'IA sont sécurisées, qu'il s'agisse d'accéder à des applications gérées ou non gérées via le SSO, les mots de passe, l'authentification multifacteur (MFA) ou les passkeys.
- **Réduisez les risques liés à Shadow IT.** Détectez et sécurisez les accès de vos employés à toutes les applications, qu'elles soient gérées par votre entreprise ou non. Tirez parti des renseignements fournis sur l'usage du SaaS, optimisez vos dépenses sur le SaaS et rationalisez vos flux de gestion des accès.
- **Maintenez vos appareils en bon état.** Surveillez l'état et la sécurité de vos appareils en temps réel, afin d'empêcher les appareils inconnus ou en mauvais état d'accéder à des ressources. Aidez vos utilisateurs finaux à remédier eux-mêmes aux problèmes sans l'intervention de votre service informatique.
- **Mettez en œuvre une gestion contextuelle des accès.** Bloquez les accès aux applications jusqu'à ce que les utilisateurs aient mené à bien certaines tâches de sécurité critiques, par exemple en répondant à une alerte de Watchtower, en mettant à jour un navigateur ou en résolvant un problème de non-conformité sur un appareil.

En savoir plus sur la gestion étendue des accès et sur **1Password Extended Access Management.**

1Password