1Password

EBOOK

Extending Access Management

Pourquoi le zero trust nécessite d'aller au-delà de l'IAM traditionnel - et comment le faire

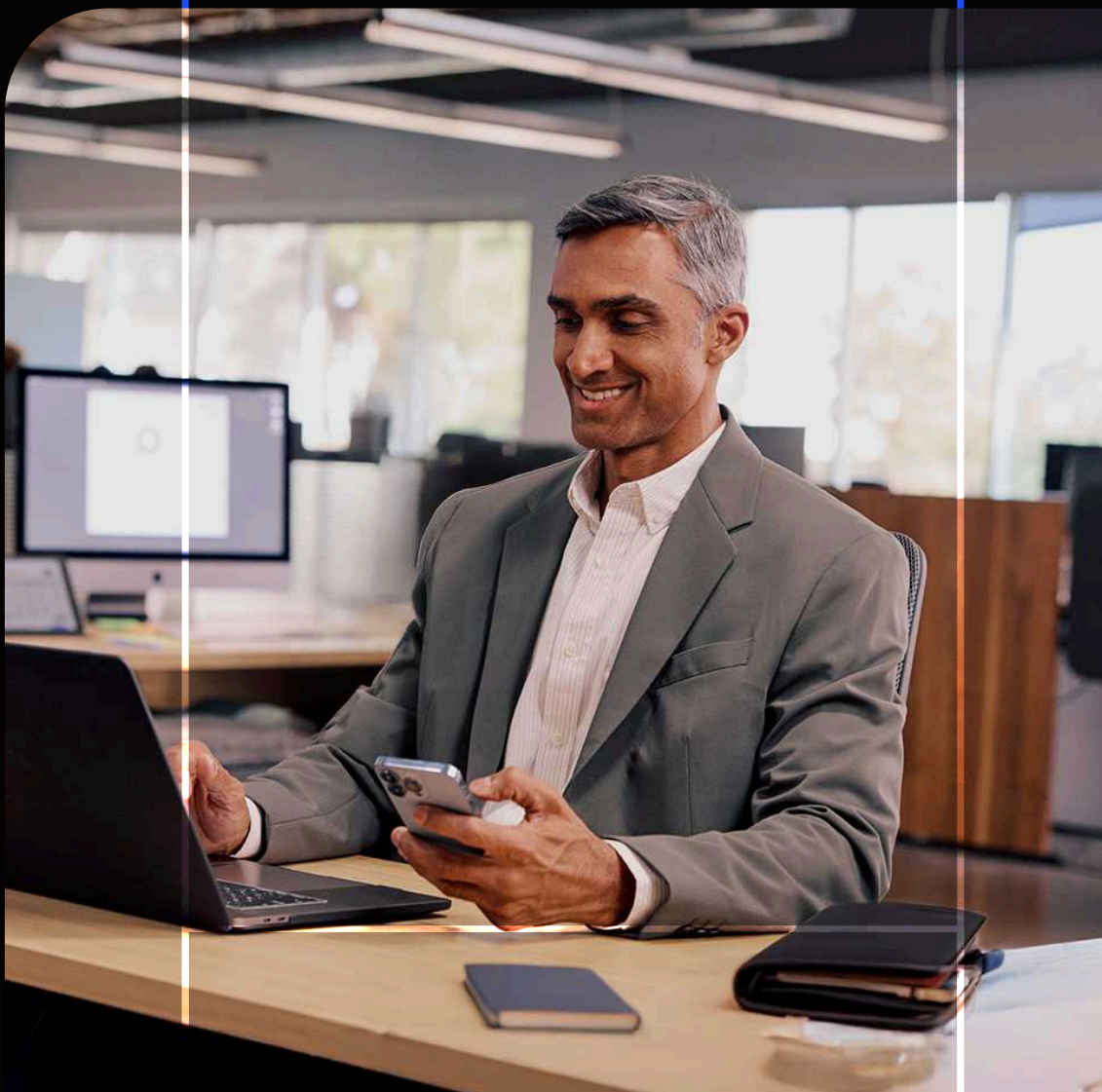


Table des matières

Introduction :

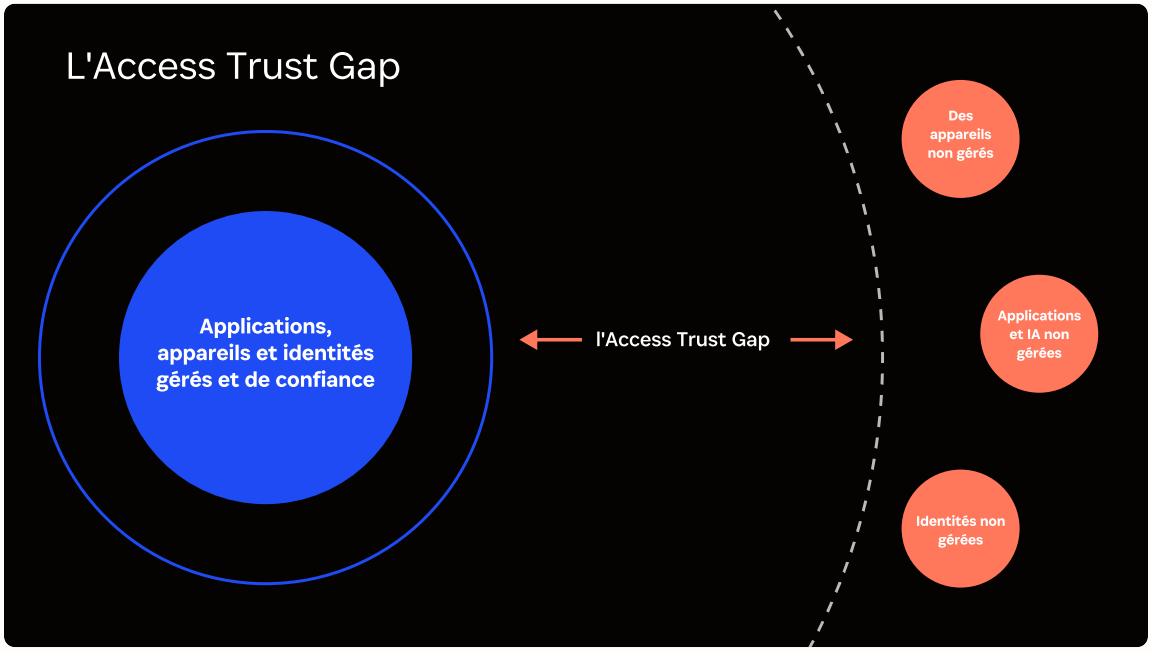
L'Access Trust Gap

Le télétravail et le travail hybride sont devenus la norme et non l'exception. Il est clair que le travail ne redeviendra jamais ce qu'il était. La flexibilité devient de plus en plus courante. Elle ne concerne pas que les lieux et méthodes de travail, mais également les appareils et les applications qui sont quotidiennement en usage.

Les approches traditionnelles de la gestion des identités et des accès (IAM) ont été conçues pour une autre époque — une époque où le travail nécessitait la présence des employés au bureau, sur un réseau d'entreprise, et à partir d'un appareil fourni par l'entreprise. Le nouveau mode de travail rend pratiquement impossible l'utilisation de ces outils existants pour répondre aux besoins du travail à distance et hybride, du BYOD, et pour sécuriser les applications introduites à la périphérie.

Comme nous le verrons ci-dessous, les procédés conventionnels d'IAM laissent des lacunes critiques dans votre stratégie de sécurité. Ce sont ces lacunes qui constituent **l'Access Trust Gap.**

L'Access Trust Gap est l'écart entre ce que les appareils, applications et connexions que les outils de sécurité actuels peuvent gérer, et ce qu'ils ne peuvent pas.



Qu'est-ce que l'Access Trust Gap?

Dans la plupart des entreprises, un grand décalage est présent entre l'objectif et la réalité en matière de sécurité. Le dessein est de sécuriser la totalité des appareils, applications et identités dans l'organisation, mais dans la pratique, les outils de sécurité en usage ne peuvent protéger qu'une fraction de ces appareils, applications et identités.

C'est ce que nous appelons l'Access Trust Gap.

Le fossé entre les accès et la fiabilité L'Access Trust Gap mesure le pourcentage de connexions qui ne sont pas approuvées parmi toutes les connexions d'une entreprise. Elle englobe les connexions à des applications non gérées et celles qui se font à partir d'appareils non approuvés. Plus la valeur de cette mesure est grande, plus le risque de fuites de données est élevé.

En matière de sécurité, les stratégies modernes, comme la confiance zéro, exigent de ne rien croire et de tout vérifier. Cependant, l'Access Trust Gap montre clairement qu'avec les procédés conventionnels d'IAM, les principes fondamentaux de la confiance zéro ne sont pas respectés. Un certain nombre d'éléments permettent de l'affirmer :

- Les applications et sites web non agréés, en dehors du périmètre de gestion des services informatiques et de sécurité, ne sont pas protégés.
- Des appareils non gérés, ou potentiellement vulnérables ou compromis, sont considérés comme fiables.
- La vérification des identités ne se limite pas à la saisie d'identifiants et de mots de passe.

Dans de nombreux cas, il est possible de résoudre certains des problèmes mentionnés ci-dessus, mais il demeure très improbable qu'une organisation puisse les résoudre tous dans leur intégralité. En fait, ce sont les informations d'identification compromises qui sont à l'origine de 70 % des fuites de données engendrant des répercussions financières.

Examinons en détail chacun des problèmes posés.

Applications : à la périphérie du réseau

Pour une large part, l'évolution récente de la situation a été impulsée par l'arrivée du SaaS, qui en est venu à dominer l'univers des applications professionnelles. Et les employés veulent en profiter. Ils adoptent de plus en plus leurs propres applications en provenance de la périphérie des réseaux, afin de parfaire leurs méthodes de travail. Voici quelques faits mentionnés dans le rapport de 1Password sur l'état de la sécurité des entreprises :

- Malgré des années de formation des employés et le déploiement de logiciels de gestion de la sécurité, un employé sur trois (34 %) utilise des applications ou des outils non agréés — qui constituent l'« informatique fantôme ».
- Selon 64 % des professionnels de la sécurité, l'informatique fantôme entrave la recherche d'un équilibre entre, d'une part, la sécurisation des outils et applications et, d'autre part, leur aisance d'usage par les employés.
- Les personnes qui recourent à l'informatique fantôme utilisent en moyenne cinq applications ou outils non agréés.

Ajoutons que la problématique s'étend au-delà de l'informatique fantôme. Les outils d'authentification unique (SSO) sont souvent utilisés pour gérer les accès aux applications, mais ils souffrent de leur complexité, de leurs coûts élevés et de la « taxe sur l'authentification unique », pratique qui oblige les organisations à payer encore plus à chaque fois qu'elles veulent sécuriser une nouvelle application.

BYOD

Ce ne sont pas seulement les nouvelles attentes qui alimentent cette tendance. Elle provient aussi des souhaits des employés concernant leur mode de travail. Les organisations continuent de fournir des appareils à usage professionnel, mais leurs employés se servent tout de même de leurs propres appareils pour le travail, que ces appareils soient agréés ou non.

65 % **Selon près des deux tiers des professionnels de la sécurité (65 %),** l'usage d'appareils personnels a contribué à obstruer considérablement la visibilité sur les habitudes des employés en matière de sécurité.

84 % **84 % des professionnels de la sécurité** affirment que leur entreprise oblige ses employés à utiliser exclusivement les appareils qu'elle leur fournit pour leur travail.

17 % **Pourtant, 17 % des employés** admettent ne jamais se servir des appareils fournis pour leur travail, préférant se limiter à l'usage d'ordinateurs personnels ou publics.

56 % **Plus de la moitié des employés (56 %)** ont utilisé un appareil personnel au cours de l'année écoulée.

20 % **Un employé sur cinq (20 %)** a travaillé sur un ordinateur public ou appartenant à un ami ou à un membre de sa famille.

La fiabilité des appareils

Certains employés se servent de leurs propres appareils, mais ce n'est pas tout. Pour les appareils qu'elles fournissent à leurs employés, les entreprises peuvent s'assurer qu'ils sont maintenus à jour, que les correctifs émis pour leur système d'exploitation et leurs applications sont appliqués, que la protection des terminaux y est activée et qu'ils sont correctement configurés. Toutefois, ce contrôle ne couvre que les appareils enregistrés dans un système de gestion des terminaux mobiles (MDM). Qu'en est-il donc des appareils personnels dont les employés se servent à des fins professionnelles ?

Malheureusement, les équipes informatiques et de sécurité ne disposent pas des ressources qu'il leur faudrait pour gérer à distance tous les appareils utilisés pour le travail. De plus, n'oublions pas que ces équipes n'ont aucun accès aux appareils personnels utilisés par les employés. En conséquence, les entreprises se trouvent dans l'impossibilité de surveiller les accès à leurs systèmes qui proviennent d'appareils peu fiables. A fortiori, elles ne peuvent pas bloquer ces accès.

Des équipes de sécurité désarmées

L'incapacité à répondre aux besoins signifie une chose : des risques sont pris. Malheureusement, les équipes informatiques et de sécurité se sentent souvent mal équipées pour résoudre les problèmes.

- Selon 92 % des professionnels de la sécurité, la politique de leur entreprise exige que tout logiciel et toute application soit agréé par le service informatique avant d'être utilisé pour le travail.
- Cependant, 59 % des professionnels de la sécurité déclarent ne pas être en mesure de s'assurer que les employés respectent cette politique.
- Les équipes de sécurité ne peuvent ni gérer tous les appareils à distance, ni contrôler les accès des appareils personnels aux applications professionnelles.

De plus, comme si toutes ces difficultés ne suffisaient pas, les outils actuels sont coûteux et leur usage nécessite souvent des compétences spécialisées, ce qui les rend inenvisageables pour un grand nombre d'entreprises. Le résultat ? Pour les équipes informatiques et de sécurité, les procédés conventionnels de gestion des identités et des accès sont inefficaces : ils ne permettent pas de gérer convenablement tous les accès depuis tous les appareils.

92 %

des professionnels de la sécurité, la politique de leur entreprise exige que tout logiciel et toute application soit agréé par le service informatique avant d'être utilisé pour le travail.

La gestion moderne des accès a des exigences modernes

De nouveaux cadres de cybersécurité ont été élaborés pour faire face à la problématique constatée. Par exemple, Le modèle de maturité Zero Trust de la CISA un modèle de confiance zéro catégorise les exigences selon cinq piliers distincts : les identités, les appareils, les réseaux, les applications et charges de travail et, pour finir, les données.

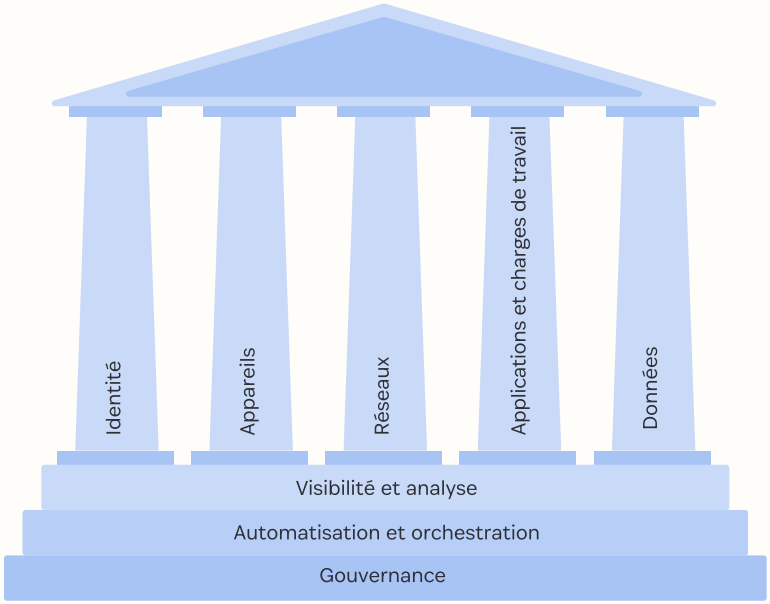


Fig. 1: Pilliers du modèle de maturité Zero Trust

Pour la gestion des accès, les piliers essentiels à prendre en compte sont les identités, les appareils et les applications et charges de travail. Dans le contexte du fossé entre les accès et la fiabilité, les problèmes apparaissent clairement. Les nécessités sont énoncées comme suit dans le modèle de maturité de confiance zéro de la CISA :

- **Les identités :** Dans la mesure du possible, les entreprises doivent totalement intégrer leurs dispositifs de gestion des identités, des identifiants de connexion et des accès. Les objectifs visés sont d'appliquer des politiques d'authentification rigoureuses, d'accorder les autorisations au cas par cas sur la base des contextes et, en dernier lieu, d'évaluer les risques liés aux identités pour les utilisateurs et entités couverts par les systèmes de sécurité.
- **Les appareils :** Il convient de sécuriser tous les appareils couverts par les systèmes de sécurité, de gérer les risques liés aux appareils autorisés non couverts et d'empêcher les appareils non autorisés d'accéder aux ressources.
- **Les applications et charges de travail :** Il convient de gérer et de sécuriser les applications déployées et de s'assurer que leur distribution est sûre.

Sur la base du modèle de maturité, les piliers ci-dessus donnent lieu à un certain nombre d'exigences à satisfaire pour combler le fossé entre les accès et la fiabilité :

Exigence	Définition
Identité de l'utilisateur	Capacité à gérer les identités de l'ensemble du personnel, ainsi que les accès associés.
Connexion universelle	Procédure de connexion fluide qui va au-delà de l'authentification unique pour inclure les sites web, comme ceux des comptes bancaires et des réseaux sociaux, et les applications de SaaS non gérées.
La fiabilité des appareils	Visibilité sur l'état de tous les appareils utilisés pour accéder aux applications professionnelles, qu'ils soient détenus par l'entreprise ou par des individus ; capacité à indiquer aux utilisateurs les actions à mener pour maintenir le système d'exploitation et les applications de leurs appareils à jour et en bon état.
Gestion contextuelle des accès	Politiques dynamiques qui prennent en compte le contexte des demandes — par exemple l'heure, le lieu, l'état des appareils et la robustesse des identifiants — avant d'autoriser les accès.
Visibilité des applications	Visibilité sur toutes les applications gérées, héritées et non gérées/fantômes utilisées pour les affaires, avec la possibilité de voir la robustesse de l'authentification, l'étendue de l'utilisation et la fréquence d'utilisation.
Gestion des mots de passe d'entreprise	Gestion sécurisée des identifiants pour la totalité des applications et sites web, que ces éléments soient gérés ou non.

Il est presque impossible de satisfaire ces exigences avec les produits de gestion des identités existants. Dans la plupart des cas, ces produits permettent aux organisations de gérer les identités, mais ils sont loin de convenir pour la facilitation des accès, la sécurisation des appareils et la prise en charge des applications de périphérie.

Les produits de gestion des identités existants ne répondent pas aux nécessités de la confiance zéro

Exigence	Produits existants pour la gestion des identités d'un personnel
Identité de l'utilisateur	✓
Connexion universelle	✗
La fiabilité des appareils	✗
Gestion contextuelle des accès	✗
Visibilité des applications	✗
Gestion des mots de passe d'entreprise	✗

Les procédés et outils conventionnels d'IAM présentent des carences critiques lorsqu'ils s'agit d'appliquer la confiance zéro.

Bienvenue dans l'ère de la gestion étendue des accès

La confiance zéro constitue désormais un cadre primordial pour la sécurité moderne. Dans les environnements de travail modernes, la réponse apportée aux besoins n'a fait qu'accélérer la nécessité d'adopter ce cadre. « Ne vous fiez à rien, vérifiez tout ». Avec ces lignes directrices, une chose est devenue claire : il convient d'étendre la portée des méthodes de gestion des accès, afin de sécuriser la totalité des appareils, applications et identités en usage.

C'est ce que nous appelons la gestion étendue des accès, ou Extended Access Management (XAM).

La XAM est une stratégie de gestion des accès qui part du principe que l'usage d'appareils personnels et la présence de l'informatique fantôme font partie du cours normal des choses. Ces tendances ne sont pas à combattre activement et à éliminer par les équipes informatiques et de sécurité. Ce point de départ crée un environnement de travail où :

Les employés sont mobilisés pour jouer un rôle actif dans le renforcement de la sécurité — en particulier, ils s'assurent que leurs informations d'identification sont sécurisées et que les appareils utilisés sont en bon état.	La confidentialité des employés est respectée — des pratiques transparentes précisent clairement quelles données sont recueillies et à quelles fins, ce qui instaure un climat de confiance où le personnel accepte volontiers la présence d'outils de sécurité.
Les employés font usage des outils de sécurité déployés, contrairement à ce qui se passe quand des outils suscitent tellement de tensions que des employés les court-circuitent.	La productivité des employés est assurée, les outils de sécurité faisant en sorte que le moyen le plus simple d'accomplir les tâches soit aussi le plus sûr.

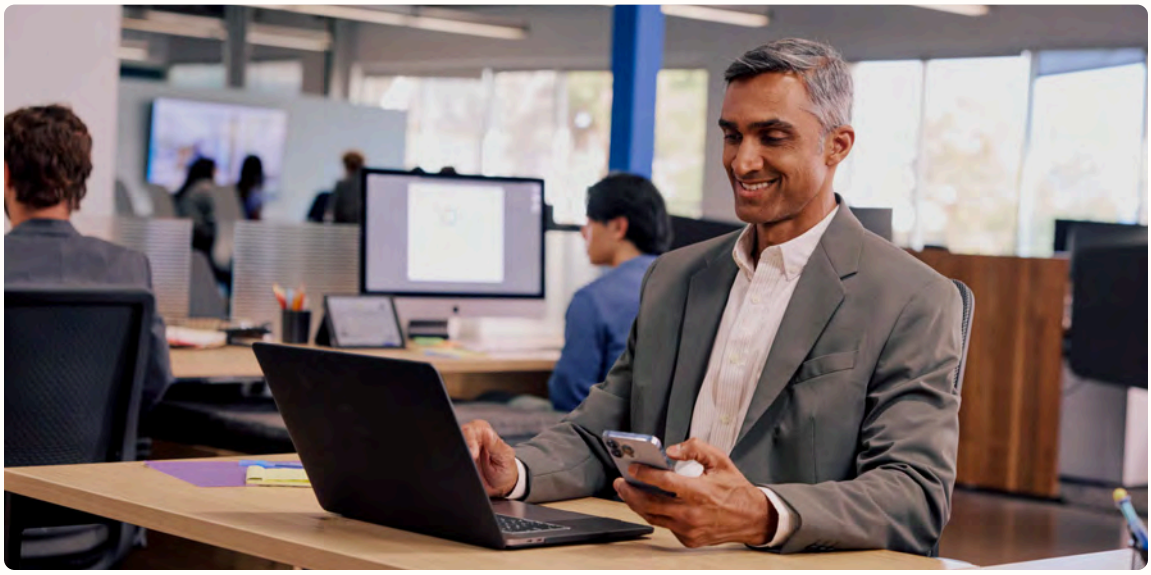
Il convient d'étendre la portée des méthodes de gestion des accès, afin de sécuriser la totalité des appareils, applications et identités en usage.

Un aspect distingue la gestion étendue des accès (XAM) des procédés couramment utilisés par les entreprises pour la gestion des identités : la XAM couvre tout ce dont les employés se servent pour leurs tâches quotidiennes, c'est-à-dire toutes les applications (y compris celles qui ne sont pas gérées et les applications fantômes), tous les sites web et tous les appareils. Et ce n'est pas tout : les procédés de XAM permettent aux employés d'utiliser les appareils et applications qu'il leur faut pour être continuellement les plus productifs possible.

XAM représente une nouvelle catégorie de logiciels de sécurité pour :

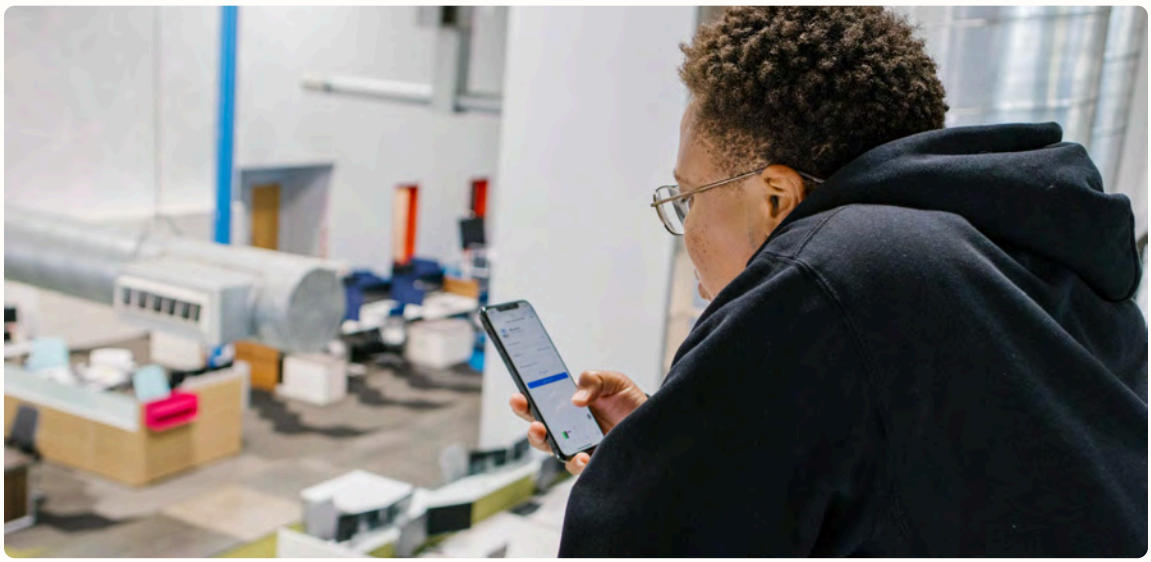
	Sécuriser toutes les applications — qu'elles soient gérées, fantômes ou anciennes.
	Mettre en œuvre globalement une procédure unique de connexion pour toutes les applications — facilitant ainsi l'usage des identifiants les plus sûrs possible à chaque fois qu'un employé se connecte à une application.
	Maintenir tous les appareils en bon état – qu'ils s'agisse d'appareils d'entreprise, gérés ou non par l'organisation propriétaire, ou d'appareils mobiles personnels (ordinateurs portables ou autres) appartenant à des employés — et bloquer ou restreindre les tentatives d'accès provenant d'appareils peu fiables.
	N'autoriser que les appareils en bon état à accéder aux applications — contrairement aux outils d'IAM, qui ne peuvent pas restreindre les accès des appareils en mauvais état.
	Apporter une expérience d'une élégante simplicité aux utilisateurs — ces outils fonctionnent aussi bien sur les appareils professionnels que sur ceux appartenant à des individus, ce qui encourage les employés à sécuriser leurs appareils personnels avec la XAM car cette méthode constitue le moyen le plus simple d'accéder aux applications.

XAM représente une nouvelle catégorie de logiciels de sécurité pour garantir la santé de tous les appareils.



Comparaison entre les outils conventionnels de gestion des identités et la XAM

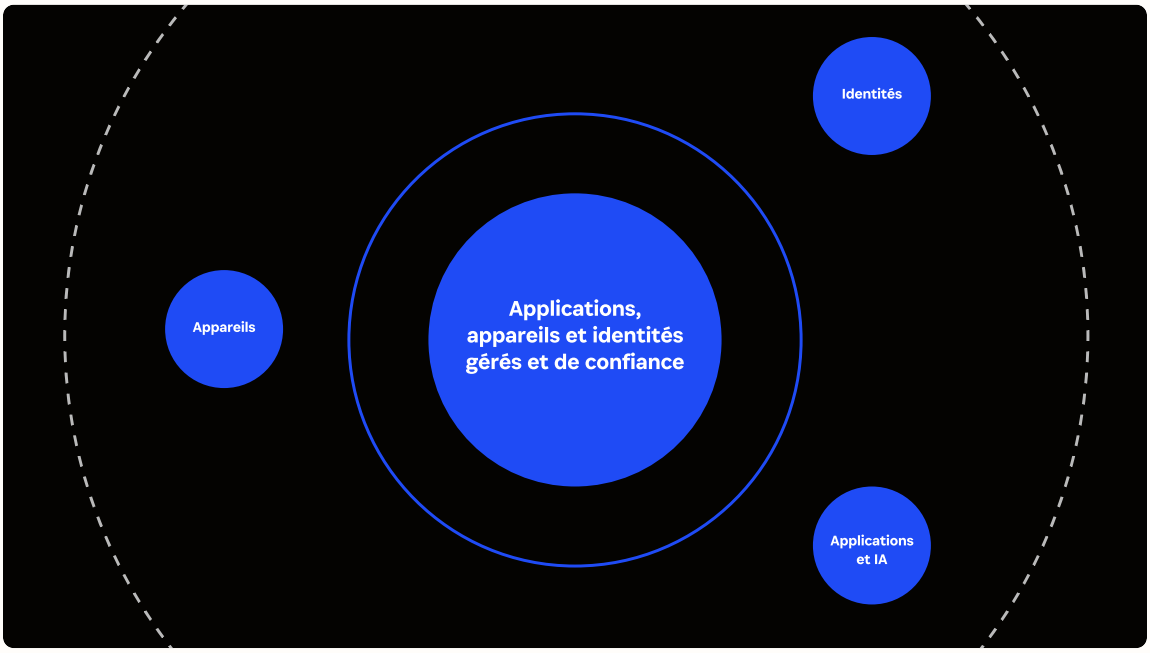
Exigence	Produits existants pour la gestion des identités d'un personnel	Gestion étendue des accès (XAM)
Identité de l'utilisateur	✓	✓
Connexion universelle	x	✓
La fiabilité des appareils	x	✓
Gestion contextuelle des accès	x	✓
Visibilité des applications	x	✓
Gestion des mots de passe d'entreprise	x	✓



1Password® Extended Access Management et l'avenir du zero trust

1Password XAM comble le fossé entre les accès et la fiabilité, qui est présent aussi bien avec la gestion des identités et des accès (IAM) qu'avec la gestion des accès privilégiés (PAM) et celle des appareils mobiles (MDM), et que les systèmes de détection et de réponse étendues (XDR) ne peuvent pas éliminer.
1Password XAM :

- Sécurise toutes les applications
- Incorpore une procédure de connexion unique de portée globale, qui couvre toutes les applications
- Garantit le bon état de tous les appareils
- Garantit que les accès aux applications sont limités aux seuls appareils en bon état
- Apporte une expérience d'une élégante simplicité aux utilisateurs



Conclusion -

Activer et sécuriser

La XAM représente un changement radical dans la manière dont les organisations abordent la gestion des identités et des accès. Il s'agit d'une approche globale qui couvre la sécurisation des identités, des appareils et des applications. Naguère, les employés n'accédaient aux systèmes de leur entreprise qu'à partir d'un parc de matériel tangible et maîtrisé. Il suffisait de sécuriser ce type d'accès. Aujourd'hui, l'ère du travail moderne donne lieu à des besoins fondamentalement différents. La XAM est une nouvelle approche de la cybersécurité qui permet aux organisations de répondre à ces besoins avec des outils faciles à utiliser.

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

Adopté par plus de 165 000 entreprises et des millions de consommateurs, 1Password propose des solutions de sécurité des identités et de gestion des accès conçues pour la façon dont les gens travaillent et vivent aujourd'hui. La mission de 1Password est d'éliminer le conflit entre sécurité et productivité tout en protégeant chaque connexion, pour chaque application, sur chaque appareil. En tant que fournisseur du gestionnaire de mots de passe d'entreprise le plus utilisé, 1Password continue d'innover sur sa solide base afin d'offrir des solutions de sécurité sur lesquelles comptent des entreprises de toutes tailles, dont Associated Press, Salesforce, GitLab, Under Armour et Intercom.

En savoir plus sur 1Password.