Le Guide d'achat de l'identité des Collaborateurs

Ce qu'il faut prioriser dans une solution de gestion des identités et des accès des collaborateurs pour prendre les décisions les mieux adaptées à vos besoins

GUIDE D'ACHAT

INTRODUCTION

La transformation digitale s'accélère dans tous les secteurs, et les organisations de toutes tailles luttent pour accroître leurs parts de marché. Mais de nombreuses initiatives de transformation numérique ne parviennent pas à atteindre les résultats visés. Pourquoi ? Car la plupart des systèmes de gestions des accès et de l'identité existants ne sont pas compatibles avec les exigences d'une entreprise axée sur le numérique.

Prenons par exemple le transfert vers le cloud. Toutes les applications sur site n'ont pas d'alternative SaaS adaptée ou capable de migrer. La plupart des entreprises réalisent qu'elles doivent conserver un environnement informatique hybride pour les applications sur cloud et sur site. Mais leur ancien système d'IAM n'est pas compatible avec cette architecture hybride sans engendrer de coûts, de retards et de risques significatifs.

Un ancien IAM pose aussi des difficultés lorsqu'il s'agit de permettre aux collaborateurs d'accéder aux ressources. Au fil du temps, vous avez certainement cumulé des silos d'identité qui sont épars et déconnectés. En l'absence de base d'identité moderne, vous aurez du mal à fournir l'accès fluide dont un nombre croissant de collaborateurs en télétravail a besoin, tout en maintenant la sécurité des ressources et des données.

> « La vision des accès à distance a toujours été axée sur le télétravail ou au moins neutre vis-à-vis du télétravail, pour garantir que 'n'importe quel utilisateur puisse travailler n'importe où, sur n'importe quelle application, depuis n'importe quel appareil'. Toutefois, la crise sanitaire actuelle et les fermetures qui ont suivi dans le monde ont fait de cette approche une réalité plus rapidement que prévu, et de manière plus définitive que n'importe quelle technologie conventionnelle ou moteur d'activité ».
>
> Gartner 2020 Magic Quadrant for Access Management

Pour permettre la transformation numérique, vous avez besoin de plus de flexibilité que celle que les anciennes solutions peuvent vous fournir. Vous devez vous assurer que vos collaborateurs, dynamiques et mobiles, restent productifs en leur donnant accès aux ressources dont ils ont besoin depuis n'importe où et sur n'importe quel appareil. Vous devez garantir la sécurité contre des menaces croissantes et accroître l'agilité pour être réactif aux changements de priorités et d'exigences.

En bref, vous avez besoin d'une autorité d'authentification des collaborateurs. Une autorité d'authentification vous donne la puissance dont vous avez besoin pour trouver le juste équilibre entre un accès sécurisé et pratique pour vos collaborateurs. Et vous la trouverez dans une solution d'identité intelligente des collaborateurs.

La réussite d'une transformation numérique ne coule pas de source. Vous avez besoin d'une base d'identité intelligente sur laquelle bâtir la réussite de la transformation numérique. Poursuivez votre lecture pour découvrir :

- Les fonctionnalités indispensables nécessaires pour construire la base de votre identité des collaborateurs
- Comment quantifier la valeur commerciale d'un investissement dans l'identité des collaborateurs
- La procédure étape par étape pour prendre la meilleure décision adaptée à vos besoins

LES AVANTAGES DE LA TRANSFORMATION DE L'IDENTITÉ DES COLLABORATEURS

Lorsque vous continuez à vous appuyer sur l'ancienne identité et sur les silos, vous vous exposez à divers problèmes tels que la superposition de systèmes informatiques de plusieurs générations, de systèmes fragiles résultant d'une maintenance décousue, l'absence de fonctionnalités en self-service pour les développeurs (ayant entraîné des délais dans l'intégration d'applications) et l'émergence de solutions informatiques « shadows » alors que les unités commerciales se développent en étant frustrées par la rigidité informatique.

En revanche, une base d'identité durable procure divers avantages nécessaires pour réussir la transformation numérique. Lorsque vous vous libérez de vos anciens systèmes pour mettre en place des fonctionnalités modernes d'IAM, vous récupérez des fonctionnalités essentielles qui vous procurent :

- Un gain de temps, d'argent et de ressources
- Une meilleure productivité dans toute l'entreprise
- Une sécurité renforcée

Une administration centralisée

Une solution d'identité avec administration centralisée vous donne une vision consolidée de votre infrastructure d'identité. Vous pouvez sensiblement rationaliser l'administration en gérant toute votre entreprise grâce à un portail unique d'administration.

Authentification forte

Vous devez procurer une expérience utilisateur fluide et sécurisée, tout en assurant une défence contre des menaces et des vulnérabilités de sécurité qui évoluent. Cela est possible grâce à une solution d'identité compatible avec une authentification forte. Lorsque vous pouvez compter sur des politiques d'authentification qui utilisent un certain nombre de facteurs (l'intelligence artificielle et l'apprentissage automatisé, les risques de score, la biométrie et bien plus encore), vous pouvez faire correspondre les exigences d'authentification au risque de l'action réalisée, sans ajouter de frictions inutiles.

Des fonctionnalités intuitives pour les développeurs

Les développeurs d'applications doivent proposer rapidement de nouveaux projets, mais la sécurité ne peut pas être sacrifiée dans ce processus. Vous pouvez accompagner leurs besoins en termes de vitesse ET garantir que l'identité soit intégrée à leurs applications lorsque votre solution d'identité des collaborateurs fournit des fonctionnalités et des API en self-service, et que les standards ouverts sont pris en charge.

Compatibilité des intégrations

Une solution d'identité moderne doit être compatible avec le travail réalisé sur tous les types d'applications et tous les annuaires, y compris Microsoft Active Directory (AD). Elle devrait également fournir des fonctionnalités de synchronisation vous permettant d'utiliser les investissements existants.

Un déploiement flexible sur le cloud

Lorsque vous vous déployez sur le cloud ou le centre de données, vous avez besoin des options et de l'indépendance nécessaires pour atteindre les objectifs de votre organisation. Une solution d'identité moderne permet de consommer ou de déployer l'identité n'importe où.

Une meilleure expérience

Une solution d'identité moderne devrait considérablement améliorer votre expérience utilisateur. Lorsque vous réduisez les frictions et les incitations à se connecter grâce à une authentification avancée et intelligente, vous proposez le genre d'expérience qui fait que vos employés sont satisfaits et sécurisés.

QUANTIFIER LA VALEUR COMMERCIALE DE L'IDENTITÉ DES COLLABORATEURS

Lorsque vous définissez les besoins d'identité, vous pouvez commencer par évaluer vos économies en termes de coût total de possession (TCO). Mais ne vous arrêtez pas là. Vous devrez aussi examiner l'impact plus large sur l'entreprise. L'identité des collaborateurs apporte des améliorations quantifiables en termes de productivité, de sécurité et d'agilité. Les questions suivantes vous aideront à calculer la valeur que vous créez.

Productivité

- Combien de temps les employés perdent-ils à passer d'une application à l'autre ?
- Combien de temps pourraient-ils économiser s'ils pouvaient utiliser le single sign-on (SSO) pour toutes leurs applications ?
- Combien d'heures sont passées chaque semaine ou chaque mois à réinitialiser les mots de passe ?
- Combien de temps est consacré à la résolution des tickets d'assistance et à traiter les appels ?
- Quels sont les autres coûts cachés dus à l'absence de solution d'identité de bout en bout ?

Sécurité

- Combien de mots de passe un employé moyen doit-il gérer ?
- Comment les mots de passe et les silos d'authentification multiples affectent-ils vos risques de faille de sécurité ?
- Combien de ressources essentielles sont actuellement protégées par l'authentification multi-facteurs (MFA) ?
- À quel point vos ressources essentielles sont-elles exposées à des utilisateurs non autorisés dans votre propre entreprise ?
- Comment les collaborateurs sont-ils désinscrits lorsqu'ils quittent l'entreprise ?

Agilité

- Combien de temps est perdu à entretenir votre solution d'identité actuelle ?
- De quelle façon l'absence d'options d'identité ralentit-elle l'entreprise et l'installation d'application ? Le cas échéant, combien d'heures sont passées à résoudre ces problèmes ?
- Quelles opérations informatiques peuvent être simplifiées grâce à une nouvelle plateforme d'identité ?

Vous pouvez également utiliser cette calculatrice de valeur commerciale pour élaborer une solide analyse de rentabilité sur l'investissement dans l'identité des collaborateurs. Vous découvrirez la valeur exacte que vous pouvez créer en rendant vos employés plus productifs, en garantissant que les ressources essentielles de votre entreprise soient plus sécurisées et en vous assurant que votre entreprise soit plus agile. Faîtes dès maintenant le calcul.

DÉFINIR LES OBJECTIFS DE VOTRE ENTREPRISE

Investir dans l'identité est souvent un projet stratégique qui sollicite plusieurs parties prenantes et unités commerciales. Lorsque vous associez l'identité des collaborateurs aux initiatives existantes, vous créez un alignement avec des objectifs organisationnels plus larges et gagnez plus facilement en popularité. Ci-dessous figurent certains des objectifs les plus courants inclus dans les investissements dans l'identité des collaborateurs.

Migration vers le cloud

Les organisations travaillent de plus en plus dans un monde hybride, multi-cloud et elles ont besoin de solutions d'identité qui peuvent s'adapter avec elles. L'identité moderne peut être déployée dans un environnement cloud public, privé ou managé.

La transformation numérique

Un projet ou une feuille de route explicites pour la transformation numérique constituent un bon point de départ. L'identité fournit la base nécessaire à une intégration rapide des applications, une meilleure expérience utilisateur et une intégration facilitée.

Zero Trust & CARTA

Les initiatives de télétravail se sont accélérées en 2020. En réponse à l'évolution des menaces et du nombre croissant de ressources situées en dehors du réseau de l'entreprise, les organisations abandonnent le concept de périmètres pour adopter Zero Trust et CARTA. Une solution d'identité moderne permet d'authentifier n'importe quel utilisateur, sur n'importe quel appareil et dans n'importe quelle situation, en utilisant des politiques adaptatives pour garantir une expérience utilisateur optimale.

DevOps

La vitesse apporte un avantage concurrentiel, qui est la raison pour laquelle DevOps est la méthode préférée pour le développement logiciel. Pour garantir que votre organisation profite de tous les avantages de DevOps, il faut une identité facilement consommable dans un environnement DevOps.

Connexion sans mot de passe

Afin que vos employés travaillent en toute sécurité et de manière productive, vous devez limiter les risques et éliminer les frictions de leurs taches quotidiennes. La connexion sans mot de passe vous permet de fournir un accès fluide, tout en procurant une plus grande assurance du fait que vos utilisateurs sont bien ceux qu'ils prétendent être.

CE QU'IL FAUT REGARDER DANS UNE SOLUTION D'IDENTITÉ DES COLLABORATEURS

Lorsque vous avez clarifié vos objectifs commerciaux et emporté l'adhésion pour aller de l'avant, vous devez identifier les fournisseurs à examiner. Lorsque vous évaluez un fournisseur, prenez les éléments suivants en considération :

- Depuis combien de temps ce fournisseur travaille-t-il dans ce secteur ?
- Ce fournisseur est-il un leader du secteur ?
- Ce fournisseur a-t-il fait preuve d'expertise sous la forme d'exemples de réussite des clients et de témoignages ?
- Ce fournisseur est-il impliqué dans la recherche et le développement continus pour améliorer les produits et satisfaire l'évolution des exigences du secteur et des clients ?
- Ce fournisseur propose-t-il une formation solide, une assistance et une communauté d'utilisateurs active ?

Pour construire l'avenir sur une base d'identité durable dont vous avez besoin pour réussir votre transformation numérique, vous avez aussi besoin d'un ensemble de fonctionnalités essentielles. En réalité, l'absence de ces fonctionnalités est souvent la goutte d'eau qui fait déborder le vase et ce qui pousse au final les entreprises à commencer à chercher une solution d'identité moderne.

Voici les fonctionnalités que vous souhaiteriez prioriser pour vous aider à réduire la liste de fournisseurs. Bien sûr, chaque organisation a ses propres besoins uniques. Aussi vous souhaiterez peut-être ajuster ou ajouter d'autres fonctionnalités à celles-ci pour satisfaire vos cas d'utilisation et vos exigences spécifiques.

SINGLE SIGN-ON	CONDITIONS
Évolutivité	Le fournisseur prend-il en charge l'évolutivité sur tous les types d'applications (sur site, internes, SaaS) ?
Fédération	Le fournisseur fournit-il une authentification fédérée et une assertion basée sur des standards avec des politiques illimitées et flexibles ?
Source de confiance unique	Le fournisseur gère-t-il en direct l'agrégation d'attributs depuis plusieurs annuaires sur site et sur cloud ?
Architecture simplifiée	Ce fournisseur prend-il en charge les déploiements sur cloud, sur site et hybrides pouvant être pré-configurés avec Docker et Kubernetes ?
Migration	Le fournisseur prend-il en charge les chemins de migration et la coexistence avec d'anciens fournisseurs de WAM grâce à des outils prêts à l'emploi ?

SINGLE SIGN-ON	CONDITIONS
Intégrations	Ce fournisseur propose-t-il des kits d'intégration au serveur complets, des adaptateurs et une assistance pour vos applications existantes ?
Gestion centralisée	Ce fournisseur vous offre-t-il de la visibilité sur tous les clients et toutes les connexions par le biais d'un portail de gestion centralisé ?

UNE AUTHENTIFICATION INTELLIGENTE	CONDITIONS
Plusieurs méthodes d'authentification	Ce fournisseur fournit-il une gamme d'options d'authentification pour prendre en charge vos cas d'usage ? • Appli mobile avec balayage, saisie, OTP • Appli de bureau protégée par un code PIN • Notifications push pour iOS et Android • Empreinte digitale et reconnaissance faciale • Notifications sur Apple Watch • Absence de mot de passe certifiée FIDO • Authentifiants tiers • Clés de sécurité • Authentification hors-ligne
Politiques d'authentification qui s'adaptent	Ce fournisseur fournit-il des politiques adaptatives basées sur des facteurs contextuels tels que l'emplacement, l'adresse IP et le geofencing pour prendre en charge l'authentification basée sur les risques ?
Posture de l'appareil	Ce fournisseur vous permet-il d'identifier les attributs de l'appareil tels que les réglages de sécurité ? Pouvez-vous dire si un appareil a été rooté/jailbreaké ?
Connexion sans mot de passe	Ce fournisseur propose-t-il des options qui limitent ou qui éliminent les mots de passe avec des politiques basées sur la durée, ou des architectures FIDO, Zero Trust, etc. ?
Intégration	Ce fournisseur prend-il en charge les intégrations avec les VPN, les MDM et les autres MFA ?
Facilité de gestion	Ce fournisseur fournit-il des tableaux de bord, des rapports détaillés des événements, des suivis d'audit et une gestion par le biais d'une interface utilisateur administrative et des API ?

ANNUAIRE & DATA STORE	CONDITIONS
Sécurité	Ce fournisseur fournit-il le chiffrement des données dans tous les états, le hashing moderne des mots de passe, les alertes aux administrateurs, leur enregistrement et le contrôle des attributs aux données ?
Source de confiance unique	Ce fournisseur fournit-il des champs et des attributs utilisateurs illimités pouvant se synchroniser sur plusieurs annuaires ?
Flexibilité	Ce fournisseur fournit-il l'évolutivité avec peu de temps d'interruption pour des millions d'identités et des milliards d'attributs ?
Architecture simplifiée	Ce fournisseur prend-il en charge les déploiements sur cloud, sur site et hybrides pouvant être pré-configurés avec Docker et Kubernetes ?
Intégration	Ce fournisseur s'intègre-t-il à plusieurs annuaires (sur site et sur cloud), en proposant une synchronisation des données en temps réel et bidirectionnelle ?
Délégation d'administration	Ce fournisseur fournit-il une console de gestion pour surveiller les performances et les infrastructures avec une délégation d'administration des profils utilisateurs ?

EXPÉRIENCE DES EMPLOYÉS	CONDITIONS
Expérience utilisateur	Ce fournisseur procure-t-il une expérience cohérence sur tous les types d'appareils et d'applications ?
Accès en un clic	Ce fournisseur fournit-il un dock complet pour les employés leur permettant d'accéder à toutes les applis ?
Le libre-service	Ce fournisseur fournit-il des options pour que les utilisateurs réinitialisent les mots de passe et réalisent des actions similaires sans devoir appeler le service d'assistance ?
Méthodes d'authentification faciles	Ce fournisseur fournit-il des méthodes d'authentification pratiques telles que la biométrie des appareils ?

Utilisez cette check-list pour évaluer les solutions pour les collaborateurs proposées par les fournisseurs. Des lignes blanches ont été ajoutées à la fin pour y inscrire vos éventuelles exigences supplémentaires.

Conditions	Ping Identity	Fournisseur 2	Fournisseur 3
Single Sign-On			
Évolutivité			
Fédération			
Source de confiance unique			
Architecture simplifiée			
Migration			
Intégrations			
Gestion centralisée			
Une authentification intelligente			
Plusieurs méthodes d'authentification			
Méthodes d'authentification adaptative			
Posture de l'appareil			
Connexion sans mot de passe			
Intégration			
Facilité de gestion			
Annuaire et magasin de données			
Sécurité			
Source de confiance unique			
Flexibilité			
Architecture simplifiée			
Intégration			
Facilité de gestion			
Expérience des employés			
Expérience utilisateur			
Accès en un clic			
Le libre-service			
Méthodes d'authentification faciles			
Considérations supplémentaires			

PRENDRE LES MEILLEURES DÉCISIONS D'IDENTITÉ POUR LES COLLABORATEURS ADAPTÉES À VOS BESOINS

Choisir les solutions d'identité pour vos collaborateurs est une décision importante. La bonne solution vous donnera la base dont vous avez besoin pour être sûr de réussir votre transformation numérique, sans parler du fait qu'elle simplifiera sensiblement votre travail.

La plateforme Ping Intelligent Identity augmente l'efficacité opérationnelle pour que vous puissiez répondre rapidement à l'évolution des besoins de votre entreprise. Plus de 60 sociétés du Fortune 100 font confiance à Ping pour ses services d'identité centralisés et flexibles. Accompagnés par des fonctionnalités performantes telles que l'authentification dynamique et l'accès adaptatif, ils fournissent aux bonnes personnes l'accès fluide et sécurisé aux bonnes ressources, et vous aussi vous pouvez le faire.

Pour en savoir plus sur les fonctionnalités de Ping et comparer nos scores par rapports aux autres fournisseurs d'IAM, consultez le 2020 Gartner Magic Quadrant for Access Management.

Pour obtenir plus d'informations sur les fonctionnalités d'identité des collaborateurs de Ping, consultez le 2020 Gartner Critical Capabilities Report.

À PROPOS DE PING IDENTITY : Ping Identity est pionnier des solutions intelligentes de gestion des identités. Nous aidons les entreprises à mettre en place une sécurité des identités définie par Zero Trust et des expériences utilisateur plus personnalisées et plus fluides. La plate-forme Ping Intelligent Identity™ fournit aux clients, employés, partenaires et, de plus en plus, aux objets connectés, un accès aux API et aux applications cloud, mobiles, SaaS et sur site, tout en gérant les données d'identité et de profil à l'échelle de l'entreprise. Plus de la moitié des entreprises du classement Fortune 100 fait confiance à notre expertise en matière d'identités, à notre position de leader sur les standards ouverts, et à notre partenariat avec des sociétés comme Microsoft et Amazon. Nous proposons des options flexibles permettant d'étendre les environnements hybrides et d'accélérer les projets de transformation digitale grâce à des fonctionnalités d'authentification multifacteur, de gestion des accès, de sécurisation intelligente des API, de répertoire et de gouvernance des données. Rendez-vous sur www.pingidentity.com.

#3552 | 16.20 | v03