Livre blanc

Guide du parcours de maturité de l'identité

Une feuille de route pour améliorer la productivité, optimiser l'expérience utilisateur et renforcer la sécurité grâce à l'identité

Sommaire

L'identité au service des objectifs métier

L'identité numérique a longtemps été un simple service chargé de la gestion des noms d'utilisateur et des mots de passe. Aujourd'hui, elle est un levier stratégique pour les entreprises modernes. C'est un véritable moteur qui permet aux entreprises d'interagir de façon sécurisée avec leurs collaborateurs, clients et partenaires, où qu'ils soient et quel que soit l'équipement utilisé, et de surveiller et contrôler ces interactions. L'identité fait partie intégrante de notre monde connecté. Elle peut contribuer à la qualité ou à la médiocrité de l'expérience utilisateur, clarifier ou complexifier les investigations de sécurité, faire gagner ou perdre du temps et de l'argent à l'IT, et faciliter ou compliquer les initiatives de gouvernance, gestion des risques et conformité. L'identité participe donc à la bonne marche de l'entreprise, notamment en contribuant à l'efficacité opérationnelle et à la maîtrise des coûts, à la croissance des revenus et au renforcement de la cybersécurité. Au vu de l'ampleur des enjeux, il n'est guère surprenant que de nombreuses entreprises éprouvent des difficultés à moderniser et à optimiser leurs services d'identités clients et collaborateurs.

L'identité peut transformer les interactions des entreprises avec les utilisateurs et, ce faisant, contribuer à la réalisation des objectifs métier suivants :

Augmentation du chiffre d'affaires

Dans de nombreux secteurs, les entreprises rivalisent d'efforts pour séduire la clientèle grâce à l'expérience client, et l'identité a son rôle à jouer pour optimiser cette expérience.

60 %

des utilisateurs sont plus susceptibles d'augmenter leurs dépenses lorsque la connexion est simple, sûre et fluide[1]

Maîtrise des coûts et efficacité accrue :

Les possibilités de consolidation, d'intégration et d'automatisation offertes par une plateforme d'identité contribuent à améliorer l'efficacité des collaborateurs et de l'équipe IT, à mieux maîtriser les dépenses en logiciels et à lancer plus rapidement de nouvelles offres.

22 %

des entreprises qui investissent massivement dans l'automatisation parviennent à réduire les coûts de 22 % par rapport à celles qui sont à la traîne à cet égard[2]

Cybersécurité renforcée :

Devenue le premier vecteur d'attaque du paysage actuel des menaces, l'identité joue un rôle crucial dans votre pile de sécurité.

61 %

des entreprises considèrent désormais la gestion et la sécurisation des identités numériques comme l'une des trois grandes priorités de leur programme de sécurité[3]

[1] Okta Customer Identity Trends Report, 2023

[2] Bain and Company, 2023

[3] 2023 Trends in Securing Digital Identities Report, Identity Defined Security Alliance

Modèle de maturité de l'identité

Une étude[4] révèle que les entreprises les plus matures dans le domaine de l'identité collaborateur sont

3,9 x

plus susceptibles d'affirmer que leurs solutions d'identité contribuent à leur agilité

3,4 x

plus susceptibles de déclarer que leurs solutions d'identité leur apportent une aide précieuse pour la résolution des incidents

3,6 x

plus susceptibles d'affirmer que leurs solutions d'identité contribuent à la productivité des collaborateurs

3,2 x

plus susceptibles d'affirmer que leurs solutions d'identité permettent d'atténuer considérablement les menaces

Le modèle de maturité de l'identité d'Okta est un cadre mis au point pour évaluer vos capacités actuelles de gestion des identités et leur efficacité, proposer un plan d'amélioration et mesurer la valeur et la réussite des mesures prises. Prendre conscience de la maturité de votre environnement d'identités et de l'intérêt d'une progression en ce sens pour améliorer les résultats métier et en retirer plus de valeur vous aidera à mieux cibler vos efforts et vos investissements.

Sur la base des comportements et des bonnes pratiques collectives observés chez les milliers de clients Okta, nous avons développé un modèle de maturité complet qui propose à la fois un parcours et des critères d'évaluation pour l'ensemble des activités liées à l'identité. Ce livre blanc s'intéresse à la maturité de l'identité collaborateur (personnel, prestataires et partenaires) et de l'identité client (consommateurs, fournisseurs et autres acteurs). Les recherches et les témoignages de nos clients montrent que plus les entreprises ont atteint un stade de maturité avancé, plus l'identité joue un rôle important dans le succès de l'entreprise.

Évaluation de la maturité de l'identité et de sa progression

La première étape d'un parcours de maturité consiste à réaliser une évaluation réaliste et approfondie de l'approche actuelle de votre entreprise en matière d'identité. Notre évaluation examine l'identité au travers de trois critères : agilité opérationnelle, expérience utilisateur et, enfin, sécurité et conformité. À mesure que votre infrastructure d'identités gagne en maturité, réfléchissez à la façon dont vos efforts contribuent aux résultats métier. En mesurant régulièrement les indicateurs clés de performance (KPI) et en les mettant en correspondance avec les résultats métier, tels ceux présentés dans le tableau 1, vous pourrez rendre compte des progrès réalisés et améliorer l'adhésion au projet au sein de l'entreprise.

Outre ces trois catégories, chaque stade suggère des actions pour définir, affiner, implémenter et évaluer la stratégie d'identité à l'échelle de l'entreprise.

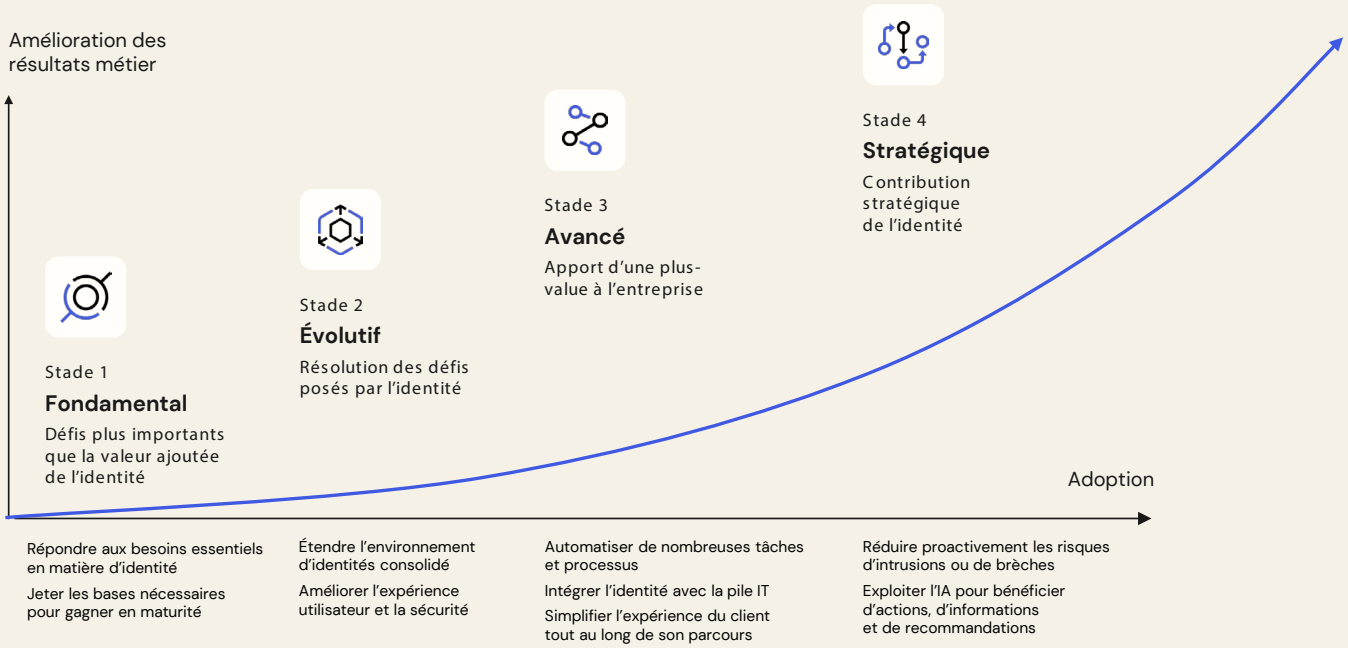
[4] Les avantages d'une approche unifiée de la gestion des identités et des accès, Enterprise Strategy Group, commandité par Okta

Catégorie	Description : capacité à	Métriques pour évaluer la performance de l'infrastructure d'identités	Contribution aux résultats métier
Agilité opérationnelle	**Développer, déployer et gérer des flux et services liés à l'identité,** p. ex. • Intégration de l'identité dans de nouveaux canaux numériques ou applications • Gestion du cycle de vie des effectifs • Déploiement de nouvelles améliorations ou fonctionnalités de gestion des identités • Lancement rapide de nouvelles offres aux clients • Évolutivité simple et rapide pour répondre aux fluctuations de la demande	• Équivalents temps plein en IT dédiés à l'administration et au support de l'identité • Délai nécessaire à l'adoption et au déploiement des applications • Coût ou temps consacré à la maintenance de l'infrastructure d'identités • Nombre de demandes d'assistance liées aux problèmes d'accès ou aux demandes relatives aux applications • Délai nécessaire à la résolution des problèmes d'identité par le service d'assistance • Délai de lancement des applications clients	Maîtrise des coûts et efficacité accrue • Création et gestion de l'identité plus simples et rapides • Simplification des fusions-acquisitions afin d'accélérer la rentabilisation Augmentation du chiffre d'affaires • Mise sur le marché accélérée
Expérience utilisateur	**Proposer des expériences utilisateurs fluides, pratiques et attrayantes,** p. ex. Pour tous : • Expériences fiables et cohérentes sur les canaux physiques et numériques Pour les collaborateurs : • Accès à distance fluide • Applications disponibles dès le premier jour • Libre-service efficace pour les demandeurs et les vérificateurs Pour les clients : • Expériences fluides pour l'inscription, la connexion, etc. • Libre-service • Personnalisation	• Scores de satisfaction des collaborateurs (eSAT) • Métriques de l'expérience client (p. ex. NPS, CSAT) • Temps passé par les utilisateurs à se connecter ou à répondre aux invites d'authentification renforcée • Temps attendu par les collaborateurs pour l'accès aux nouvelles applications ou l'onboarding • Taux d'abandon des clients lors de l'inscription et de la connexion • Taux de conversion client (du statut de visiteur au compte enregistré) • Minutes d'interruption non planifiée par mois	Efficacité accrue • Simplification de l'accès utilisateur Augmentation du chiffre d'affaires • Augmentation des conversions d'inscription et de connexion • Personnalisation des expériences clients • Création d'expériences omnicanales fluides • Simplification de l'onboarding des entreprises clientes
Sécurité et conformité	**Atténuer et neutraliser proactivement les menaces, respecter le principe du moindre privilège et la conformité réglementaire,** p. ex. • Accès sécurisé pour les collaborateurs et les clients • Réduction de la surface d'attaque des identités • Soutien d'initiatives de gouvernance des identités • Gestion de l'accès à privilèges • Soutien des pratiques Zero Trust • Respect des exigences en matière de confidentialité • Protection contre les fraudes à l'identité	• Nombre des incidents de sécurité liés à l'identité • Temps et coûts de détection et de réponse aux incidents de sécurité et brèches liés à l'identité • Temps et coûts associés au reporting des audits et de la conformité • Adoption de l'authentification avancée par les collaborateurs • Nombre d'incidents impliquant l'usurpation de compte (ATO)	Maîtrise des coûts et efficacité accrue • Simplification de la gouvernance et de la conformité • Optimisation des dépenses en logiciels • Augmentation du chiffre d'affaires • Amélioration de la confiance client sans nuire à l'expérience Cybersécurité renforcée • Atténuation proactive des menaces ciblant l'identité • Blocage des attaques de phishing • Renforcement de la confiance des clients

Planification du parcours, étape par étape

Le modèle de maturité de l'identité d'Okta comprend quatre stades progressifs qui précisent les fonctionnalités de gestion des identités nécessaires et comment les utiliser pour améliorer les résultats métier et la valeur pour l'entreprise. À chaque étape, le modèle décrit les difficultés généralement rencontrées par les entreprises, les recommandations sur les mesures à prendre pour surmonter ces difficultés et progresser jusqu'au niveau de maturité suivant, et enfin les avantages escomptés. Pour chaque stade, le modèle suggère des actions pour créer, implémenter et évaluer la stratégie d'identité à l'échelle de l'entreprise. Même s'il n'existe pas d'approche universelle en matière de gestion des identités, celle proposée par Okta est suffisamment flexible pour offrir des recommandations utiles à toute entreprise soucieuse de renforcer sa posture d'identité.

Modèle de maturité de l'identité



Stade 1– Fondamental

Envisager l'identité de façon globale et non comme un ensemble de fonctions

Au tout début du parcours vers la maturité de l'identité, il arrive souvent que l'entreprise connaisse les scénarios suivants :

- Elle commence à étendre les services numériques ou portails en ligne à l'intention de ses clients.
- Elle est confrontée à des inefficacités et à une grande surface d'attaque en raison du cloisonnement des solutions d'identité pour ses collaborateurs et partenaires.

Sans stratégie d'identité définie, les développeurs consacrent un temps et des ressources considérables à créer et à gérer en interne des services de gestion des identités « maison » ou on-premise. Les identités collaborateurs sont disséminées dans de multiples référentiels et systèmes à la suite de fusions et acquisitions, de l'extension des services cloud et des applications héritées. L'expérience utilisateur est médiocre : le processus d'inscription est basique et peu cohérent sur les divers canaux. Pour les collaborateurs, une fédération limitée et l'utilisation de nombreux mots de passe différents impactent la productivité. La fiabilité et la disponibilité de la solution de gestion des identités sont problématiques et l'automatisation est minimale ou inexistante. L'intégration avec d'autres systèmes est limitée ou compliquée et demande une intervention manuelle importante de la part des administrateurs. La prolifération des identités et le manque de visibilité qui en résulte accroissent les risques de sécurité, et la protection des identités est réactive.

À ce stade, il faut chercher avant tout à répondre aux besoins essentiels en matière d'identité (p. ex. onboarding des clients au sein d'un seul portail, implémentation de contrôles de sécurité de l'identité fiables) tout en posant des bases solides pour progresser dans le parcours de maturité.

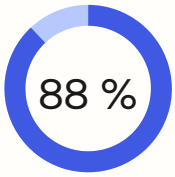
Mesures stratégiques à prendre à ce stade :

- Créer un inventaire complet de toutes les applications on-premise et cloud utilisées dans l'entreprise
- Envisager d'aligner les programmes de gestion des identités clients et collaborateurs autour d'objectifs métier et de gouvernance partagés

La création et la gestion en interne d'une solution d'identité impactent les délais de lancement[5]

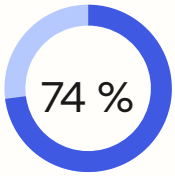
3e type d'application le plus chronophage

L'authentification se classe en 3e place des applications les plus chronophages à créer et à gérer en interne



des entreprises qui utilisent une plateforme SaaS tierce pour l'authentification ont réduit leurs délais de lancement

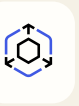
par rapport



à celles qui ont développé une solution d'authentification en interne

[5] Le point sur l'adoption des services SaaS par les équipes de développement, SD Times, commandité par Okta

Catégorie	Les enjeux de l'identité	Mesures à prendre	Avantages pour les entreprises
Agilité opérationnelle	• La création/gestion de services d'identité on-premise/développés en interne/fragmentés est difficile et prend beaucoup de temps aux administrateurs et développeurs	• Implémenter un annuaire d'utilisateurs unifié pour consolider et synchroniser les référentiels d'utilisateurs au niveau des différents annuaires et systèmes d'enregistrement hérités • Implémenter une interface de base d'administration des identités pour le cycle de vie des utilisateurs	Réduction du temps consacré par l'équipe IT aux tâches suivantes : • Gestion et synchronisation des référentiels d'utilisateurs • Gestion des accès des utilisateurs/groupes
Expérience utilisateur	• Problèmes de fiabilité/ disponibilité • Frictions considérables à la connexion, pas d'expérience utilisateur personnalisable • Solutions d'identité disparates par entité	• Adopter une infrastructure haute disponibilité avec basculement, reprise après incident et accords SLA supérieurs à 99,9 % • Déployer un SSO de base pour les collaborateurs et l'authentification sur les applications cloud • Déployer un SSO de base pour les clients avec quelques options d'authentification sociale pour tirer parti des identifiants existants • Implémenter des fonctions en libre-service simples (p. ex. la récupération des mots de passe)	• Amélioration de la productivité du personnel et/ou du taux d'utilisation client grâce à une adoption et à un accès aux applications plus rapides • Friction client réduite grâce aux options libre-service pour la gestion de base des comptes
Sécurité et conformité	• Risques de sécurité dus à la prolifération des mots de passe, manque de visibilité sur les contrôles d'accès aux applications, référentiels d'utilisateurs cloisonnés, pas d'application de politiques, etc.	• Installer un serveur d'autorisation conforme aux standards modernes et déployer des politiques d'accès de base pour les API • Sécuriser les données d'identité avec des fonctionnalités de chiffrement et de hachage de base • Implémenter une authentification multifacteur (MFA) pour les collaborateurs incluant RADIUS et/ ou LDAP pour prendre en charge les applications récentes et héritées • Mettre en place quelques politiques d'accès collaborateurs qui reflètent les besoins des groupes d'utilisateurs et les zones réseau	• Renforcement de la posture de sécurité du personnel • Diminution des verrouillages de comptes clients résultant d'attaques malveillantes



Stade 2 – Évolutif

Extension de l'environnement et des fonctionnalités de gestion des identités, début de l'automatisation

À ce stade, une entreprise peut avoir :

- Lancé plusieurs applications ou portails clients et s'est engagée à en fournir plus
- Progressé dans la consolidation des identités collaborateurs et cherche à l'étendre à d'autres applications et à implémenter des fonctionnalités de gestion des identités supplémentaires

À présent, l'accès est mis sur l'avancement des réalisations de la première phase et l'extension de l'environnement d'identités consolidé à de nouveaux services, cas d'usage, utilisateurs et applications. À l'heure où les entreprises proposent de nouveaux services numériques pour améliorer leur part de marché et étoffer leur clientèle, leurs priorités évoluent pour s'attacher à créer des expériences fiables et différenciées pour les particuliers et les entreprises clientes.

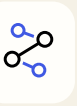
Pour les entreprises possédant des technologies propriétaires et une infrastructure IT critique on-premise, l'extension des fonctions d'identité à ces ressources permet d'améliorer l'expérience utilisateur, les processus d'administration et la posture de sécurité.

Avec l'extension de cet environnement, les entreprises doivent veiller à ce que leur infrastructure d'identités puisse gérer les augmentations de la demande sans compromettre la qualité du service ou exiger de l'équipe IT une gestion constante de l'extension du système et du support. Elles doivent également commencer à automatiser certains processus d'identité afin que l'extension ne sollicite pas trop l'équipe IT et les propriétaires d'applications. Comme de nombreuses entreprises adoptent l'approche Zero Trust en matière de cybersécurité, c'est le moment idéal de commencer à tirer parti de l'identité pour soutenir cette initiative.

Mesures stratégiques à prendre à ce stade :

- Aligner l'identité et mettre en place une communication entre les équipes IT, sécurité et technologies pour définir les domaines de compétence et l'expertise
- Évaluer les lacunes en matière d'identité pour encourager l'élaboration de plans d'investissement et de correction

Catégorie	Les enjeux de l'identité	Mesures à prendre	Avantages pour les entreprises
Agilité opérationnelle	• Onboarding et offboarding manuels du personnel, des clients et des partenaires • Difficulté à gérer des référentiels d'identités fragmentés, issus de systèmes hérités • Problèmes de performance ou de disponibilité liés aux pics/augmentations de la demande	• Commencer à automatiser le provisioning et la gestion du cycle de vie des utilisateurs pour l'onboarding et l'offboarding, et pour gérer les autorisations d'accès aux applications en aval, etc. • Limiter ou envisager d'éliminer certains systèmes hérités qui sont difficiles à gérer/mettre à niveau ; qui possèdent des référentiels d'utilisateurs distincts ; dont l'intégration est inexistante ou difficile ; qui ne permettent pas le SSO ou la fédération • Intégrer l'identité avec des applications utilisant des standards comme SAML, OIDC, Oauth2, etc. • Commencer à adopter certains kits SDK et API • Faire en sorte que l'infrastructure puisse gérer correctement les pics/augmentations de la demande sans nuire à la qualité des services	Diminution : • Coût ou temps consacré à la maintenance de l'infrastructure d'identités • Demandes d'assistance liées aux problèmes d'accès • Gestion et synchronisation des référentiels d'utilisateurs • Gestion des accès des utilisateurs/groupes • Temps passé à l'extension de l'environnement d'identités Provisioning et déprovisioning accélérés des utilisateurs Simplification des fusions et acquisitions pour vos collaborateurs et vos clients
Expérience utilisateur	• Applications/portails multiples avec expérience de connexion incohérente • Retard dans l'onboarding des nouveaux collaborateurs • Problème de disponibilité de l'authentification sécurisée en raison de la présence de serveurs RADIUS on-premise, etc.	• Étendre l'intégration de la connexion des clients à d'autres fournisseurs d'identité sociale, p. ex. Apple, Google, etc. • Prendre en charge la fédération du SSO pour les clients, partenaires et prestataires qui possèdent des identités existantes chez d'autres fournisseurs d'identité • Minimiser les points de friction de la connexion et de l'inscription des clients en ne demandant que les attributs nécessaires • Étendre le SSO des collaborateurs à des applications critiques hébergées on-premise • Implémenter l'authentification sans mot de passe pour les collaborateurs • Lancer d'autres fonctions en libre-service	• Limitation des points de friction utilisateurs avec des expériences d'inscription et de connexion plus fluides • Amélioration de la satisfaction et de la productivité des collaborateurs grâce à un accès immédiat aux applications clés et un accès plus rapide aux autres • Fiabilité accrue et limitation des interruptions dues à des serveurs non redondants ou on-premise
Sécurité et conformité	• Environnement d'accès collaborateurs trop permissif dû à des politiques d'accès globales • Failles de sécurité résultant d'un MFA trop limité pour les collaborateurs • Sécurité entravée par les objectifs à atteindre en matière d'expérience client	• Consolider le contrôle des accès collaborateurs entre les applications cloud et on-premise • Implémenter le contrôle d'accès basé sur les rôles (RBAC) • Étendre le MFA collaborateurs à facteurs forts (avec des facteurs biométriques ou de possession) aux partenaires et prestataires, ainsi que pour les applications critiques on-premise, ou implémenter l'accès sans mot de passe • Implémenter le MFA pour les clients avec des facteurs biométriques ou de possession, ou implémenter l'accès sans mot de passe • Prendre les mesures initiales en vue de l'adoption du Zero Trust (p. ex. politiques d'accès dynamiques) • Mettre en place l'intégration avec des API gateways standard pour bénéficier d'une vue uniforme de l'autorisation clients • Introduire quelques outils d'audit et de surveillance	• Renforcement de la sécurité • Amélioration de la conformité grâce à des droits d'accès basés sur le principe du moindre privilège et à des contrôles d'accès MFA (p. ex. SOX) • Diminution du temps et des coûts associés aux audits et aux évaluations de la conformité



Stade 3 – Avancé

Automatisation et intégration accrues, expérience optimisée

À ce stade, les entreprises retirent une valeur importante de l'identité. L'accès est mis sur :

- La simplification de l'expérience client pour optimiser les conversions
- L'intégration progressive de l'identité avec la pile technologique étendue de l'entreprise pour améliorer l'efficacité
- La proactivité en matière de sécurité

L'intégration de l'identité avec d'autres systèmes vous permet d'automatiser des tâches et des processus, et de bénéficier d'une visibilité accrue sur les utilisateurs et leur environnement. Par exemple, une intégration étroite avec des systèmes RH permet aux entreprises d'automatiser la création des identités utilisateurs, l'onboarding, l'offboarding et le provisioning du personnel, ce qui contribue à améliorer la productivité des collaborateurs, à accroître l'efficacité de l'administration IT et à réduire les coûts en logiciels ainsi que les risques de sécurité dus à un provisioning excessif. L'intégration de l'identité client avec les moteurs marketing et de données consolide les silos de données et offre une vue unique sur les profils utilisateurs afin d'offrir une expérience de marque cohérente sur tous les canaux. Les entreprises peuvent également apprendre à mieux connaître les clients et leurs préférences afin d'offrir une expérience plus personnalisée. Une automatisation accrue permet par ailleurs aux développeurs et aux équipes IT de se concentrer sur les priorités nécessaires à la croissance de l'entreprise.

Avec le développement des opérations et de l'empreinte numérique, les entreprises sont de plus en plus ciblées par des cyberattaques sophistiquées. En réponse au phénomène, les offres de sécurité se sont multipliées. Les outils ITDR (Identity Threat Detection and Response) et ISPM (Identity security posture management) permettent de combler les failles de sécurité et d'améliorer la réponse aux menaces. En intégrant ces outils avec votre système de gestion des identités, vous pouvez évaluer et répondre automatiquement aux fluctuations du risque lié à l'identité.

Mesures stratégiques à prendre à ce stade :

Collaborer avec les différentes équipes à l'élaboration d'une stratégie de l'identité client et collaborateur

Adopter des processus formels et continus pour évaluer la posture de sécurité des identités

Mesurer et prendre des décisions sur la base d'indicateurs liés à l'identité

Catégorie	Les enjeux de l'identité	Mesures à prendre	Avantages pour les entreprises
Agilité opérationnelle	• Processus métier peu efficaces qui n'intègrent pas les derniers progrès technologiques et ont encore recours à des activités manuelles à l'origine de retards et d'erreurs • Prise en charge d'un large éventail de cas d'usage d'identité sans pour autant augmenter la charge de travail des développeurs	• Automatiser la plupart des processus de gestion du cycle de vie des utilisateurs, dont le provisioning immédiat et les demandes d'accès afin de limiter l'intervention des équipes IT et développement • Tirer parti de certaines intégrations prêtes à l'emploi avec les systèmes métier et marketing • Automatiser la recertification de l'accès des collaborateurs en fonction des changements de rôle ou de poste • Prendre en charge divers kits SDK et API grâce à une documentation et à un support avancés	Réduction du temps • consacré par les équipes IT et d'ingénierie aux intégrations personnalisées • consacré par les équipes IT et GRC (Gouvernance, risque et conformité) à l'organisation et à l'exécution de campagnes de recertification et d'audits • consacré par les responsables et les propriétaires d'applications à vérifier les accès Adoption accélérée de nouveaux systèmes et applications d'entreprise
Expérience utilisateur	• Attentes élevées des clients qui veulent bénéficier d'expériences fluides et cohérentes • Friction de l'accès des collaborateurs en raison de politiques d'accès rigides, inadaptées aux utilisateurs ou au contexte, ou de la lenteur des processus d'accès aux applications	• Garantir la résilience à l'ide de serveurs redondants et d'équilibreurs de charge • Automatiser la liaison/fusion des comptes • Utiliser le progressive profiling pour capturer les attributs des utilisateurs au fil du temps et enrichir ainsi les profils • Implémenter l'accès sans mot de passe pour tous les points de contact des utilisateurs (terminaux, applications et comptes), et utiliser des passkeys et des authentificateurs logiciels ou matériels dans les cas requis • Améliorer l'onboarding des clients avec la vérification des identités et des comptes • Autoriser les demandes d'accès en libre-service des collaborateurs	• Création d'expériences clients omnicanales fluides • Amélioration des taux de conversion d'inscription et de connexion grâce à un ciblage plus fin et à une personnalisation améliorée • Productivité accrue des collaborateurs grâce à l'automatisation du libre-service et à un accès accéléré • Limitation de la fraude grâce à une vérification des comptes plus poussée
Sécurité et conformité	• Risques associés aux télétravailleurs, à leurs terminaux et aux réseaux • Cibles de cyberattaques plus avancées et en constante augmentation	• Étendre le MFA à niveau d'assurance élevé aux connexions via un ordinateur • Mettre en place un mécanisme MFA résistant au phishing pour les collaborateurs sur toutes les ressources • Implémenter un contrôle d'accès basé sur les attributs (ABAC) • Intégrer la solution avec des outils ITDR et ISPM • Implémenter l'accès sans mot de passe sécurisé à l'infrastructure critique (serveurs, clusters Kubernetes, bases de données, etc.) • Déployer une solution de gestion du niveau de sécurité des identités (ISPM) pour identifier les risques posés par de mauvaises configurations, des utilisateurs disposant d'autorisations excessives, etc. • Adopter l'authentification continue pour prendre en charge le Zero Trust et prendre des décisions d'octroi d'accès avec les données les plus récentes • Implémenter des réponses de sécurité automatisées par rapport aux risques identifiés vis-à-vis de l'identité • Adopter la recertification récurrente (planifiée) de l'accès utilisateur pour respecter le principe du moindre privilège • Intégrer la solution avec des outils de gestion de la confidentialité et de la conformité pour assurer le suivi des préférences clients	• Réduction de la surface d'attaque • Simplification de la gouvernance et de la conformité grâce à l'automatisation des vérifications des accès et des flux de demande d'accès • Blocage des attaques de phishing

Stade 4 – Stratégique

Utilisation de l'identité pour obtenir un avantage stratégique

À ce stade, les entreprises considèrent que l'identité joue un rôle stratégique dans leur réussite et contribue aux résultats métier. Elles ont souvent une présence numérique mondiale importante, avec des équipes qui travaillent en étroite collaboration pour peaufiner continuellement les initiatives d'identité destinées à offrir plus d'autonomie à leur personnel et à établir de meilleures relations avec leurs clients sur différents canaux.

À ce stade, les entreprises cherchent à :

- Optimiser l'infrastructure d'identités pour améliorer l'efficacité et les marges bénéficiaires
- Intégrer l'identité avec leur pile de sécurité pour détecter et répondre aux menaces en temps réel
- Tirer parti de l'intelligence artificielle et de leur empreinte cloud pour offrir une meilleure expérience utilisateur et améliorer proactivement la sécurité de l'identité

Lorsque l'identité est pleinement intégrée à la pile technologique, les entreprises peuvent collecter, normaliser et corréler les données à l'échelle de leur infrastructure. L'identité devient le principal point de contrôle pour gérer l'accès aux ressources et un élément clé des stratégies de cybersécurité. Du point de vue de la gouvernance, gestion des risques et conformité, l'intégration de l'identité offre une meilleure visibilité et un contrôle des accès plus granulaire sur les utilisateurs et terminaux autorisés à accéder à des ressources numériques spécifiques et sur les autorisations dans leur entreprise. De plus, cette même intégration permet d'assurer le suivi des préférences des clients en matière de confidentialité. Si l'identité est à la fois intégrée et automatisée et qu'elle exploite en plus l'IA pour bénéficier d'informations et de recommandations, les entreprises peuvent plus facilement s'adapter à l'évolution des attentes des clients, des exigences réglementaires, des contraintes métier et du paysage des menaces.

Mesures stratégiques à prendre à ce stade

Mettre en place des pratiques opérationnelles et de gouvernance matures pour que l'identité puisse continuellement s'adapter aux besoins métier et apporter une valeur ajoutée

Catégorie	Les enjeux de l'identité	Mesures à prendre	Avantages pour les entreprises
Agilité opérationnelle	• Vue unifiée des identités dans les environnements cloud, on-premise et cloud hybride • Adaptation aux besoins du marché, aux comportements utilisateurs et aux réglementations en constante évolution	• Centraliser toutes les données d'identité pour l'ensemble des utilisateurs, des applications et des droits • Automatiser complètement les politiques, la gestion du cycle de vie des utilisateurs, les opérations liées à l'identité et les workflows de réponse aux menaces • Tirer parti de l'IA pour formuler des recommandations destinées à améliorer la gouvernance et la sécurité de l'identité, à optimiser l'expérience utilisateur et à simplifier la configuration et le développement	• Mise sur le marché accélérée avec une efficacité accrue des équipes IT, d'administration et de développement
Expérience utilisateur	• Expériences clients peu homogènes sur les différents terminaux et canaux • Analyse des comportements des clients pour un ciblage précis et une sécurité renforcée	• Mettre en place des expériences d'accès client personnalisables et extensibles sur tous les canaux • Déclencher des questions contextualisées pendant l'inscription et la connexion des clients afin de collecter des données zero-party	• Création d'expériences omnicanales fluides • Expérience hautement personnalisée grâce à des données zero-party intégrées
Sécurité et conformité	• Privilèges permanents hérités au niveau des applications et de l'infrastructure • Mauvaise configuration du cloud ou des identités • Réponse rapide aux événements de sécurité	• Éliminer les privilèges permanents, gérer les identifiants partagés pour les ressources à privilèges dans des coffres-forts sécurisés • Unifier la sécurité de l'identité (IAM, PAM et IGA) • Ingérer les signaux des outils de sécurité tiers pour bénéficier d'informations plus précises sur les menaces • Déployer une autorisation fortement granulaire, basée sur les risques • Automatiser la recertification de l'accès utilisateur en fonction des signaux de risques • Faire en sorte que l'infrastructure puisse s'adapter dynamiquement aux pics de demande et démontrer la conformité aux réglementations en matière de fiabilité et sécurité	• Atténuation et neutralisation proactives des menaces ciblant l'identité • Réduction des délais de détection et de réponse aux menaces • Amélioration de la confiance sans sacrifier l'expérience client • Renforcement de la confiance des clients au moyen de fonctions avancées de sécurité et de protection contre la fraude

Valeur ajoutée de l'identité

Lorsque vous savez à quel stade se trouve votre entreprise dans son parcours de maturité de l'identité, vous pouvez déterminer plus facilement les prochaines étapes et surveiller sa progression. En comprenant comment l'identité contribue à offrir des expériences numériques innovantes, protège l'entreprise contre les menaces de sécurité et favorise sa croissance, vous pourrez garder une longueur d'avance sur la concurrence.

Partenaire stratégique indépendant dans le domaine de l'identité, Okta a collaboré avec des entreprises du monde entier et de multiples secteurs pour les aider à progresser dans leur transformation digitale et à réaliser leurs objectifs en matière d'accès, d'authentification et d'automatisation. Okta surveille le paysage de l'identité et de la sécurité et innove en permanence pour permettre à votre entreprise de se consacrer pleinement à son cœur de métier.

Pour consulter un glossaire des termes liés à l'identité, rendez-vous sur la page https://www.okta.com/resources/identity-and-access-management-glossary/.