Livre blanc

Juin 2022

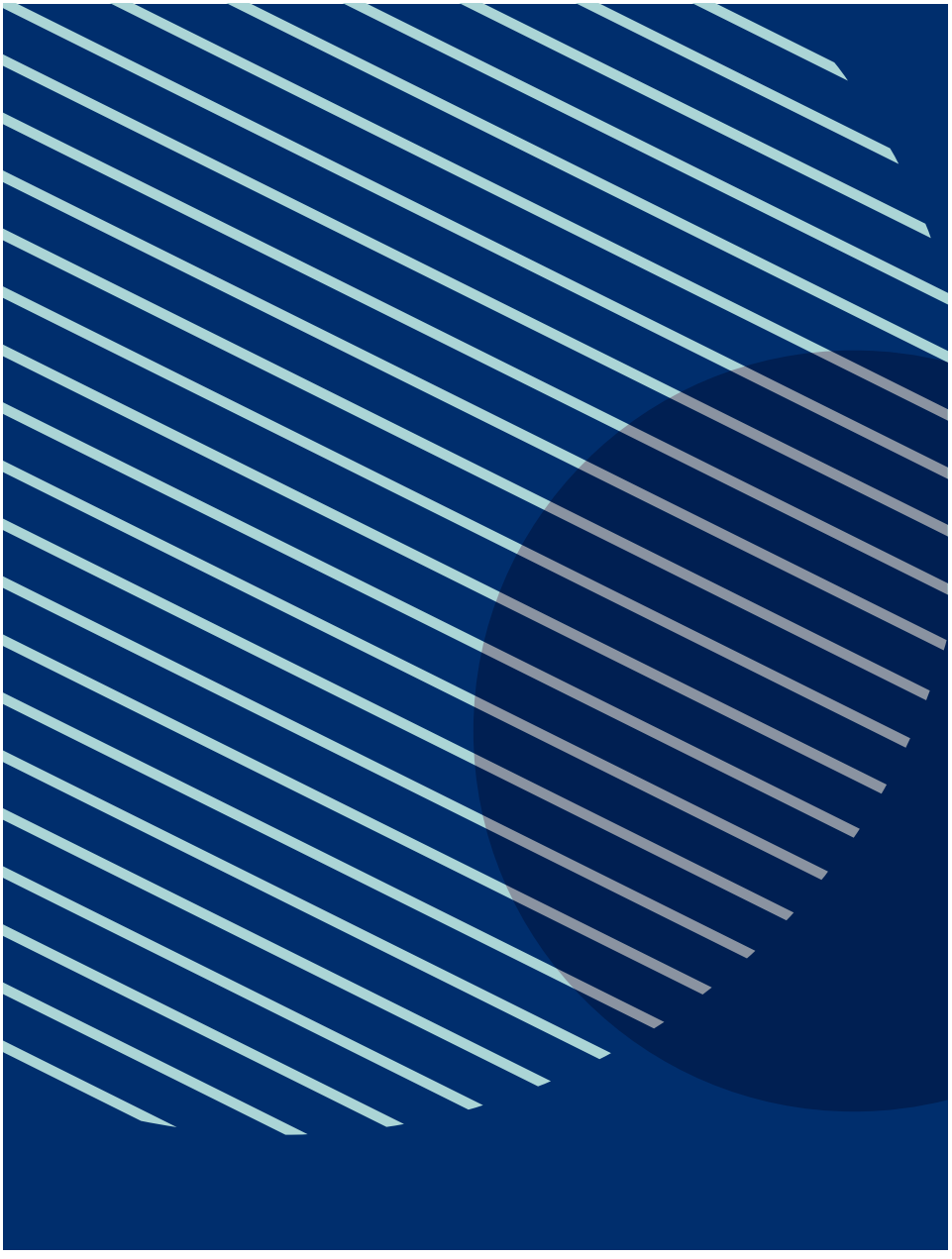
Guide d’achat de la gestion des identités et des accès

Comment choisir la solution d’identité la mieux adaptée à vos clients et collaborateurs

Okta France

paris@okta.com

+33 01 85 64 08 80



okta

Sommaire

3 Des enjeux importants
5 Un impact généralisé
7 Comment faire le bon choix
7 Attribut 1 : Neutralité et indépendance
9 Attribut 2 : Personnalisation
10 Attribut 3 : Facilité d'utilisation
11 Attribut 4 : Fiabilité et sécurité
12 Conclusion

Pourquoi ce guide ?

La gestion des identités et des accès (IAM) existe depuis de nombreuses années et n'a cessé de prendre de l'importance. Alors, pourquoi les divers départements et dirigeants des entreprises s'intéressent-ils particulièrement à cette question en ce moment ? Qu'est-ce qui explique l'importance croissante de la gestion des identités et des accès et quels sont les enjeux en cas d'erreur ? Quels critères devez-vous prendre en compte lors du choix d'une solution ?

Ce guide est destiné à vous aider à répondre à ces questions et à d'autres encore. Il évoque les tendances à l'origine de cet engouement pour la gestion des identités et des accès et met en évidence les éléments critiques de cette décision d'achat. En effet, ce sont ces leviers et les facteurs de risque qui déterminent les attributs auxquels vous devez être attentif lors du choix d'une solution IAM. Vous devez identifier les avantages et les inconvénients de chaque solution, ainsi que leur impact non seulement sur votre rôle particulier, mais aussi sur les autres parties prenantes stratégiques de votre entreprise. Après tout, les solutions IAM ne sont pas des systèmes isolés : elles impliquent un investissement coûteux à long terme et ont une incidence sur tous les éléments de votre entreprise — du conseil d'administration et l'équipe dirigeante, jusqu'aux nouvelles recrues de tous les départements et, dans de nombreux cas, vos clients et d'autres partenaires stratégiques externes.

Des enjeux importants

La gestion des identités et des accès (IAM) continue de s'imposer dans les entreprises de tous les secteurs à travers le monde. Mais quels sont les facteurs à l'origine de l'essor de l'IAM ?

La transition vers un modèle de travail hybride nécessite une solution IAM

Il y a maintenant plusieurs décennies qu'a émergé le concept du travail numérique. Cependant, l'accélération de notre transformation digitale collective s'est récemment amplifiée, notamment en raison de la pandémie.

> “
> Comme le Covid continue de circuler et que les taux de contamination augmentent dans les différents États qui encouragent le retour au bureau, nous allons devoir nous adapter à un mode de travail différent de ce à quoi nous nous étions préparés.
>
> EJ Widun, Chief Technology Officer,
> Oakland County Michigan

Les entreprises exigent plus de rapidité et d'agilité, souhaitent adopter librement des services à la demande, veulent pouvoir adapter leurs capacités à leurs besoins et désirent innover en permanence : pour répondre à toutes ces exigences, la migration vers le cloud devient inévitable. Et lorsque, pour suivre cette évolution, les entreprises créent et exécutent de nouveaux services dans le cloud, elles choisissent souvent la meilleure option disponible sur le marché pour chaque besoin. Cela se traduit par un environnement disparate, qui multiplie les fournisseurs d'infrastructures cloud, les applications SaaS, les outils de développement et de gestion, les services d'analyse et les plateformes de sécurité. Et quel est l'élément fédérateur qui permet d'assurer la cohésion de toutes ces solutions disparates ? L'identité. Les solutions IAM permettent aux entreprises d'octroyer à tous leurs utilisateurs un accès à l'ensemble de leurs applications, équipements et technologies de façon simple et sécurisée. Mais les solutions IAM héritées, conçues pour les environnements on-premise, ne sont pas à la hauteur de la tâche, car elles sont généralement isolées et difficiles à maintenir. De plus, les tentatives de modernisation de ces plateformes de gestion des identités laissent des lacunes dans la couverture, sans répondre à tous les besoins.

Les solutions héritées ne sont pas adaptées

	Solutions d'identité héritées on-premise	Solutions d'identité cloud avancées
Connexion avec les technologies cloud		X
Connexion avec les terminaux personnels		X
Gestion des personnes extérieures à l'entreprise		X
Expérience utilisateur optimale		X

Une sécurité de pointe nécessite une solution IAM

Au cours des deux dernières années, nous avons vécu une transition brutale vers un modèle de travail à distance/hybride — à dire vrai, le numérique a envahi notre mode de vie tout entier. Le modèle de sécurité fondé sur le périmètre réseau traditionnel est devenu obsolète du jour au lendemain. En effet, c'est l'identité qui constitue désormais le nouveau périmètre. Il n'est dès lors pas étonnant que les menaces et les attaques basées sur l'identité aient augmenté de façon spectaculaire.

Un rapport Verizon Data Breach Investigations a révélé que 89 % des attaques web sont dues à des compromissions d'identifiants.

Face à la multiplication des brèches de sécurité sophistiquées, les entreprises ont besoin de davantage de systèmes, protocoles et normes pour protéger leurs données. Et si les réglementations en matière de confidentialité, sécurité et conformité se sont renforcées, le temps, les ressources et l'argent nécessaires pour se conformer à ces exigences, et adopter un modèle de sécurité de type Zero Trust, ont également augmenté. En bref, l'accélération des roadmaps numériques a entraîné une augmentation des risques et des coûts associés, si bien qu'il est plus important que jamais de faire le bon choix dès le départ.

Les entreprises dont l'engagement client omnicanal est extrêmement fort conservent en moyenne 89 % de leurs clients, contre 33 % pour les entreprises dont l'engagement client omnicanal est faible.

Aberdeen Group

À qui ce guide est-il destiné et pourquoi ?

Les exigences des consommateurs nécessitent une solution IAM

Non seulement les entreprises doivent accroître leurs capacités numériques tout en repoussant une vague croissante d'attaques complexes liées à l'identité, mais les consommateurs exigent désormais des expériences fluides et transparentes, qu'il s'agisse des collaborateurs internes ou des clients externes. Au cours des deux dernières années, les entreprises ont dû repenser les modalités de leurs interactions avec leurs collaborateurs et clients. Maximiser les conversions grâce à une application mobile ou établir une relation individuelle avec les acheteurs, patients ou clients constitue une première étape importante pour maximiser les revenus et fidéliser les clients à long terme. Cela dit, il est essentiel d'instaurer une sécurité robuste, car elle favorise la confiance, un élément essentiel de la fidélisation à la marque. Les entreprises doivent trouver un équilibre délicat entre la sécurité et des expériences fluides et pratiques. Et elles doivent y parvenir dès la première tentative parce que leur concurrent le plus proche n'est qu'à un clic.

Un impact généralisé

Que vous décidiez de développer ou d'acheter votre solution, une chose est sûre : l'IAM a un impact considérable sur votre entreprise et vos relations avec vos clients. Il est donc primordial d'identifier vos parties prenantes clés et de constituer une équipe interfonctionnelle dont les responsabilités sont clairement définies pour le processus d'évaluation, d'achat et d'implémentation. En impliquant toutes les parties prenantes dès le début, vous augmenterez vos chances de réaliser le meilleur investissement stratégique à long terme pour votre entreprise.

> “
> Si vous n'avez pas l'adhésion de tous, jusqu'au CIO et au CISO, le projet est voué à l'échec.
>
> Trey Ray, Manager of Cybersecurity, FedEx

Quel que soit le promoteur de cette initiative, il est important de reconnaître les différentes parties prenantes et leurs objectifs respectifs tant pour les utilisateurs internes qu'externes.

Pour vous aider à réfléchir au type d'équipe qu'il vous faudra réunir, voici une liste des départements susceptibles de tirer profit d'un fournisseur d'identité stratégique. N'oubliez pas que la diversité des parties prenantes au sein d'une même équipe interfonctionnelle varie selon l'entreprise. Dans l'idéal, vous devriez privilégier l'inclusivité, et inclure autant de représentants de ces départements qu'il est pertinent pour votre entreprise.

Sécurité p. ex. CSO, CISO	• Réduction du risque d'incident de sécurité • Accélération des délais de détection et d'intervention • Réduction de l'impact d'un incident de sécurité	Intégration complète avec toutes les applications, tous les domaines et tous les terminaux et regroupement de tous ces éléments en un seul endroit pour gérer, visualiser et administrer la sécurité de façon centralisée.
Technologies de l'information et technologies métier p. ex. CIO	• Réduction des coûts IT et augmentation de l'efficacité opérationnelle • Amélioration des performances et de la fiabilité de l'infrastructure IT • Amélioration de la productivité, de la satisfaction et la rétention des collaborateurs • Facilitation et accompagnement de la transformation digitale • Accélération des fusions et acquisitions, coentreprises et cessions en toute efficacité	Recours à l'automatisation pour les actions administratives, entraînant une accélération du service aux collaborateurs et une réduction des coûts à long terme. Votre solution IAM doit raccourcir le cycle de vie de vos applications et de vos utilisateurs pour permettre un déploiement plus rapide.
Marketing et marketing numérique p. ex. CDO, VP Marketing	• Génération de revenus accélérée • Attraction et fidélisation de nouveaux clients • Amélioration de la collaboration avec les partenaires commerciaux • Amélioration de l'expérience client	Votre solution IAM doit proposer des options de connexion flexibles, telles que la connexion via les réseaux sociaux, tout en éliminant les points de friction du parcours du client grâce à des fonctionnalités de gestion des identités avancées, comme le progressive profiling et l'authentification biométrique.
Infrastructure et opérations p. ex. VP of I&O	• Migration d'une architecture on-premise vers une solution cloud pour réduire les coûts et simplifier la gestion • Systèmes hautement disponibles, résilients et performants (aucune interruption planifiée)	Architecture cloud-first qui s'intègre facilement avec les composants on-premise hérités permettant de fournir un service hautement résilient et disponible assorti d'un SLA d'au moins 99,99 %.
Produits et ingénierie p. ex. CPO, CTO, Director of Engineering	• Amélioration de l'efficacité opérationnelle permettant de concentrer les efforts de développement sur le cœur de métier • Réduction des délais de développement et de mise en service pour leurs clients	Mise à disposition des développeurs d'une plateforme d'identification et d'autorisation avancée, orientée développeurs.

Comment choisir une solution stratégique et non un simple outil

Comment faire le bon choix

Le choix d'une solution IAM peut s'avérer délicat, particulièrement au vu de l'importance des enjeux et de l'impact de cette décision sur votre entreprise. Mais en vous concentrant sur un nombre limité d'attributs essentiels, vous pourrez réduire vos options et identifier la solution répondant le mieux à vos besoins à long terme.

> "La gestion des identités est essentielle, la sécurité l'est tout autant, de même qu'il est essentiel de permettre aux utilisateurs autorisés d'avoir accès aux données dont ils ont besoin.
>
> Harry Moseley, CIO,
> Zoom

Bien qu'il existe incontestablement des fonctionnalités complémentaires intéressantes, nous nous concentrerons ici sur les caractéristiques absolument indispensables d'une solution IAM. Voici quatre attributs essentiels, leurs avantages et quelques questions qui vous aideront à déterminer leur importance pour votre entreprise.

Attribut 1 : Neutralité et indépendance

Votre solution IAM doit être indépendante sur le plan technologique afin de préserver l'agilité de l'entreprise, ce qui vous permet de choisir les meilleures solutions logicielles en fonction des besoins de votre activité et non de votre fournisseur d'identité.

Comme mentionné précédemment, suite à la migration vers le cloud, les entreprises se retrouvent souvent à devoir gérer des piles technologiques composées d'un large éventail de solutions de pointe pour ses différents départements. Ces piles technologiques sont suffisamment complexes à gérer sans que vous deviez subir le manque de flexibilité de votre fournisseur d'identité. Dans la mesure où l'identité est le seul élément qui assure la cohérence de toutes vos solutions et piles dans l'ensemble des départements de votre entreprise, la neutralité est un attribut indispensable pour préserver l'agilité de votre entreprise au fil du temps. Si votre plateforme de gestion des identités est présentée, d'une manière ou d'une autre, comme une solution tout-en-un de type guichet unique, il est probable qu'elle n'obtiendra pas de bons résultats en matière de neutralité.

Lorsque vous évaluez une solution IAM, assurez-vous qu'elle offre les fonctionnalités suivantes :	Pour bénéficier des avantages suivants :
• Large éventail de préintégrations performantes • Intégrations prenant en charge les dernières normes ouvertes les plus couramment utilisées • Écosystème de gestion des risques garantissant des partenariats solides entre les fournisseurs de solutions de sécurité réseau, de détection des menaces sur les terminaux et de gestion des terminaux mobiles • Intégrations d'annuaires permettant d'automatiser le cycle de vie des identités de bout en bout, c'est-à-dire du provisioning à la désactivation, en utilisant n'importe quel système de référence comme source fiable • Prise en charge de toutes les normes d'authentification ouvertes • Accès IT hybrides sécurisés pour les applications stratégiques et les environnements multicloud au sein d'une plateforme d'identité unique	• Liberté de choisir les meilleures solutions disponibles, aujourd'hui comme demain • Possibilité d'optimiser les investissements déjà réalisés (p. ex. fournisseurs de clouds publics) • Réduction des tâches manuelles pour les utilisateurs, les administrateurs IT et les développeurs • Déploiement et lancement plus rapides • Efficacité accrue des opérations et des tâches de développement • Niveau de sécurité élevé

Pour estimer l'importance de la neutralité pour votre entreprise, posez-vous les questions suivantes :

- Combien de départements de votre entreprise dépendront du fournisseur d'identité ?
- Combien de piles technologiques différentes votre solution IAM devra-t-elle prendre en charge ?
- À quelle fréquence une nouvelle technologie est-elle déployée par l'une de vos parties prenantes ou entités ?
- Quel est le délai moyen de déploiement d'une nouvelle application à l'échelle de l'entreprise ou d'une solution technologique nécessitant une approche Big Bang ? Et éprouvez-vous des difficultés à réduire ce délai ?
- Dans quelle mesure des délais de déploiement plus courts pourraient-ils réduire les coûts de votre entreprise ?

> "Toute nouvelle application adoptée par Sephora est immédiatement intégrée à Okta. Auparavant, le processus technique d'intégration d'une nouvelle application dans notre système prenait plusieurs semaines, voire plusieurs mois, mais il ne prend plus qu'une journée avec Okta.
>
> Arnaud Feyssaguet, IT Infrastructure Manager, Sephora

Attribut 2 : Personnalisation

Votre solution IAM doit s'adapter à vous pour que vous puissiez vous adapter à l'évolution des besoins métier.

Les entreprises ne sont pas immuables, alors pourquoi votre solution IAM devrait-elle l'être ? La gestion de l'accès des collaborateurs représente un enjeu majeur et les préférences des consommateurs évoluent en permanence. Une solution IAM stratégique doit pouvoir gérer l'identité de chaque utilisateur (collaborateurs, clients, partenaires et fournisseurs) tout au long de son cycle de vie, que ce soit dans les cas d'usage de gestion des identités liés aux collaborateurs ou aux clients. Votre entreprise doit réfléchir à la façon dont la gestion des identités permet d'optimiser l'orientation client sans compromettre l'efficacité opérationnelle.

Lorsque vous évaluez une solution IAM, assurez-vous qu'elle offre les fonctionnalités suivantes :	**Pour bénéficier des avantages suivants :**
• Options de personnalisation no-code or low-code • Architecture orientée API avec framework d'extensibilité complet • Workflows dynamiques permettant l'automatisation du cycle de vie des utilisateurs et des politiques d'accès • Visibilité sur l'identité de tous les terminaux pour créer des politiques de sécurité contextuelles • Moteur de politiques pour permettre des politiques d'accès dynamiques adaptées à l'utilisateur, au cas d'usage, au terminal, etc. • Langage d'expression permettant aux développeurs et aux administrateurs de référencer, de transformer et de combiner les attributs provenant de systèmes disparates et de les consolider au sein d'une source fiable unique	• Déploiement rapide de nouvelles expériences (p. ex. onboarding rapide des nouveaux collaborateurs, déploiement de nouvelles intégrations d'applications, etc.) • Renforcement de la sécurité • Diminution du travail de développement pour tout nouveau workflow • Amélioration de l'efficacité opérationnelle (c'est-à-dire « faire plus avec moins » en optimisant les ressources IT actuelles, le budget, etc.) • Amélioration de l'expérience client entraînant une augmentation du taux de fidélisation

Pour estimer l'importance de la personnalisation de la solution IAM pour votre entreprise, posez-vous les questions suivantes :

- Combien de temps et d'argent sont consacrés aux ressources de développement pour créer de nouveaux workflows et maintenir les workflows existants et en évolution ?
- Combien de temps d'ingénierie est consacré aux automatisations personnalisées ?
- Combien de ressources sont consacrées à la création de pages de destination personnalisées pour les applications orientées clients ou les portails B2B destinés aux partenaires ?
- Combien de temps est consacré à la mise en conformité avec les exigences réglementaires et d'audit (p. ex. FedRAMP, SOX, CCPA, RGPD, etc.) ?
- Où en êtes-vous dans votre démarche d'adoption d'un modèle de sécurité Zero Trust et que vous faut-il pour atteindre votre prochain objectif concernant ce projet ?

> Si nous ne détectons pas correctement une erreur et qu'elle est relevée par un audit SOX, nous devrons la signaler à la SEC (Securities and Exchange Commission). Il s'agit d'un risque majeur pour n'importe quelle entreprise.
>
> Curtis Salinas, Senior Director,
> Strategic Planning & Operations, Slack

Attribut 3 : Facilité d'utilisation

Votre solution IAM doit être conviviale pour que vous puissiez créer des expériences agréables pour vos collaborateurs, vos clients et tous les autres utilisateurs.

Une solution IAM qui s'intègre facilement à l'ensemble de vos applications, utilisateurs et terminaux tout au long du cycle de vie des identités peut rapidement s'avérer difficile à développer, coûteuse à maintenir et compliquée à utiliser. Une solution d'identité stratégique doit donc également être simple et intuitive à utiliser, tant pour les développeurs et les administrateurs que pour les utilisateurs. À défaut, vous risquez d'épuiser des ressources IT limitées et/ou d'avoir un impact négatif sur l'expérience des utilisateurs finaux, ce qui pourrait entraîner une attrition accrue des effectifs ou nuire à la réputation de la marque.

Lorsque vous évaluez une solution IAM, assurez-vous qu'elle offre les fonctionnalités suivantes :	**Pour bénéficier des avantages suivants :**
• Console d'administration centralisée pour gérer tous les utilisateurs, applications et politiques • Outils en libre-service pour les administrateurs, tels que des guides de démarrage rapide et des assistants d'intégration • Widgets, API et SDK couvrant l'authentification des utilisateurs, la configuration des ressources et le contrôle des accès • Possibilité pour les développeurs d'accéder à un ensemble complet de ressources pour les aider à intégrer rapidement et efficacement la gestion des identités dans n'importe quel projet de développement • Possibilité d'automatiser les processus complexes centrés sur l'identité sans code • Possibilité de s'intégrer simplement à chacun des systèmes et applications de votre entreprise • Options de personnalisation no-code ou low-code • Options de connexion via les réseaux sociaux pour offrir une grande liberté de connexion • Authentification sans mot de passe • Informations et visibilité pour maîtriser la gestion de la sécurité grâce à des rapports et une visibilité des activités au niveau des utilisateurs, des applications et des terminaux	• Réduction des coûts de maintenance et d'exploitation • Amélioration de l'expérience utilisateur • Intégrations plus rapides avec les systèmes et applications de sécurité de pointe • Réduction des points de friction dans le parcours numérique des utilisateurs finaux • Augmentation de l'adoption au sein de l'entreprise • Augmentation de la satisfaction et de la fidélité des utilisateurs finaux • Renforcement de la sécurité

Pour estimer l'importance de la facilité d'utilisation de la solution IAM pour votre entreprise, posez-vous les questions suivantes :

- Quel est le volume de code actuellement utilisé pour la personnalisation ?
- Quel est le processus d'intégration pour les nouveaux systèmes et applications ?
- Combien d'heures de travail manuel faut-il pour développer et gérer les processus axés sur l'identité ?
- Disposez-vous d'une vue centrale unifiée de tous les utilisateurs, applications et politiques ?
- Combien de ressources sont consacrées au développement de la gestion des identités ?
- Quel est l'impact de la pile d'applications métier sur la productivité des collaborateurs ?

> "L'implémentation d'une couche d'identités unifiée nous a aidés à toucher davantage de clients, à accélérer l'onboarding des nouveaux utilisateurs et à améliorer l'expérience.
>
> Emnet Gossaye, Security Software Engineer, Kensho

Attribut 4 : Fiabilité et sécurité

Votre solution IAM doit être fiable et sûre.

L'IAM est une fonction stratégique pour l'entreprise qui repose sur une base de confiance. Une solution IAM stratégique connecte les personnes aux technologies en toute sécurité et gère parfaitement les données les plus précieuses d'une entreprise : l'identité de ses utilisateurs. La confiance est primordiale et si vos clients ne peuvent pas compter sur vous en raison d'interruptions, planifiées ou non, ou à cause de risques de sécurité, c'est un problème. Ce problème entraîne une diminution des revenus et une augmentation des coûts, ce qui peut mener l'entreprise droit à la catastrophe.

Lorsque vous évaluez une solution IAM, assurez-vous qu'elle offre les fonctionnalités suivantes :	Pour bénéficier des avantages suivants :
• Aucune interruption planifiée • Nœuds à autorétablissement • SLA de 99,99 % pour le temps de disponibilité • Modèle de responsabilité partagée en matière de sécurité • Outils de sécurité proposant des recommandations proactives pour renforcer la sécurité • Possibilité de définir des périmètres de sécurité autour desquels l'accès peut être limité ou restreint	• Renforcement de la confiance de vos collaborateurs et clients • Continuité des activités • Absence d'incidents de sécurité préjudiciables à la marque • Renforcement de la sécurité

Pour estimer l'importance de la résilience de la solution IAM pour votre entreprise, répondez aux questions suivantes :

- Quelle serait la conséquence de pannes système fréquentes et/ou prolongées ? Perte de productivité, de revenus ou de clients ?
- Combien pourriez-vous économiser si vous bénéficiiez d'un temps de disponibilité de 99,99 % ou plus ?
- Établissez un classement des fournisseurs que vous envisagez en fonction de leur historique des indisponibilités. Qui arrive en tête ?

> "Par le passé, il est arrivé que les développeurs doivent réécrire du code parce qu'il n'était pas sûr. Aujourd'hui, ils sont en mesure de fournir un code sûr dès le départ, et c'est mieux pour tout le monde. Leur satisfaction au travail s'est améliorée, car ils peuvent offrir de la valeur plus rapidement et ne doivent pas consacrer des cycles de développement complets à corriger des problèmes de conformité.
>
> Justin Moore, IAM Manager,
> NOV Inc

Conclusion

La modernisation de l'environnement IT reste un objectif à long terme pour les départements IT de toutes les entreprises. Ces dernières années n'ont fait qu'accélérer le calendrier pour nombre d'entre elles et ont mis en évidence la prépondérance de cette initiative.

La migration vers le cloud, malgré tous ses avantages, se traduit également par un essor du Shadow IT, dans la mesure où de nombreux départements IT achètent des solutions de pointe disparates pour construire leurs piles technologiques en fonction des besoins de leur activité. Cela laisse les entreprises vulnérables au nombre croissant d'attaques complexes basées sur l'identité. Par ailleurs, en tant que consommateurs, nous attendons beaucoup de chaque entreprise avec laquelle nous interagissons, que ce soit en qualité de consommateur ou de collaborateur. Trouver le bon équilibre entre la sécurité, et donc la confiance, et une interaction fluide n'est pas une tâche facile pour les entreprises. Cependant, une solution de gestion des identités adaptée peut les y aider.

La gestion des identités et des accès constitue le ciment qui assure la cohésion de toutes les piles technologiques disparates afin de permettre aux marques de proposer des expériences omnicanales fluides, sûres et fiables, tant à leurs collaborateurs qu'à leurs clients.

Une solution IAM doit être au minimum neutre, personnalisable, facile à utiliser et, surtout, sûre et fiable. C'est précisément ce qu'offre Okta. Nous aimerions partager avec vous la façon dont nous avons aidé d'autres entreprises à gagner du temps, limiter les risques et réduire les coûts liés à la gestion des identités et des accès.

Pour en savoir plus sur la valeur de l'implémentation d'une solution IAM, consultez les calculateurs de ROI et d'avantages pour l'activité d'Okta.

Pour échanger directement avec nous quant à vos besoins spécifiques, contactez-nous dès aujourd'hui.