Livre blanc

Novembre 2021

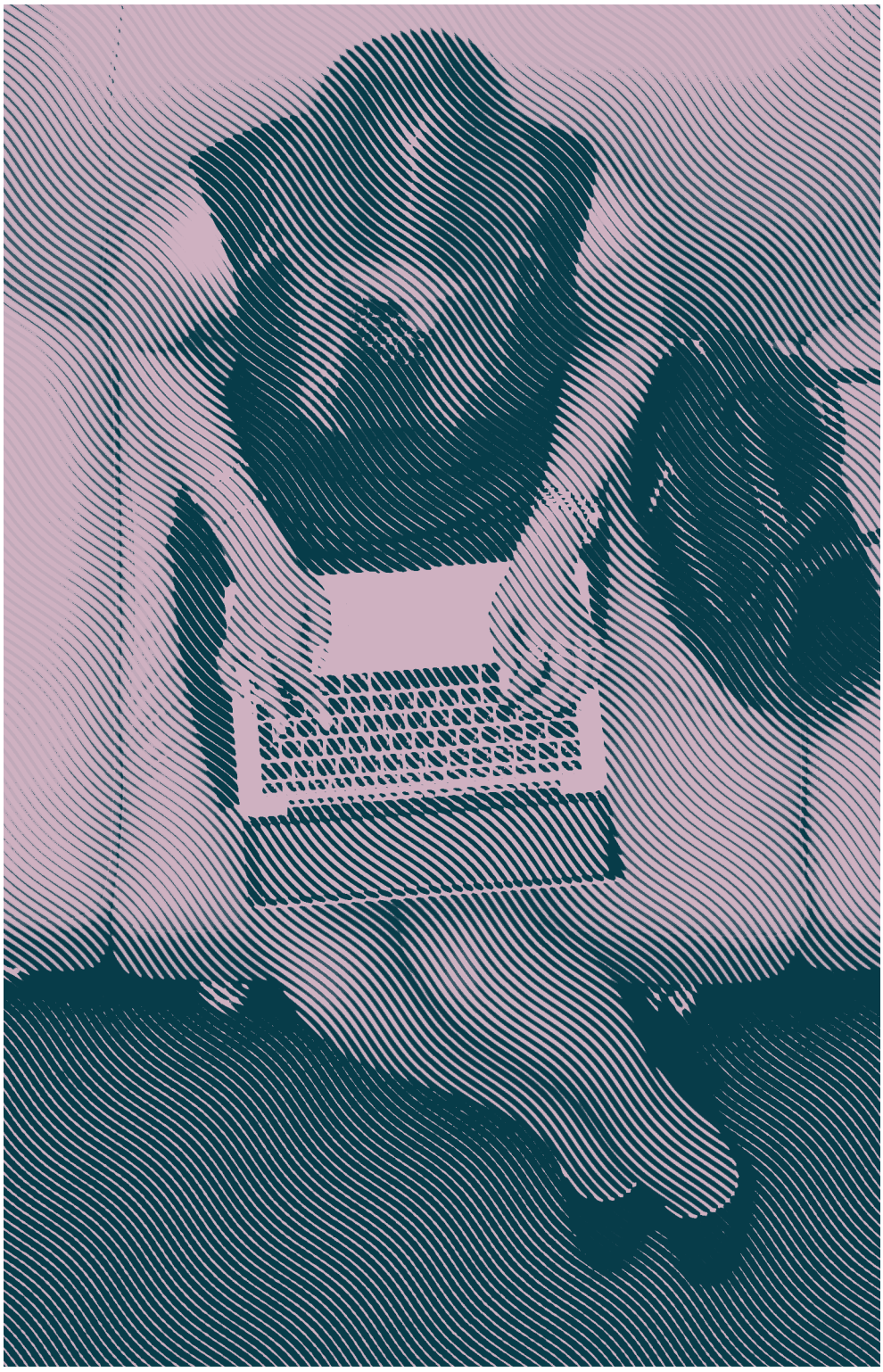
Comprendre la différence entre Customer IAM (CIAM) et IAM

Okta France

Paris

paris@okta.com

01 85 64 08 80



okta

Contenu

Introduction

Le domaine de la gestion des identités et des accès (IAM, Identity and Access Management) est rarement sujet à controverse. Mais aujourd'hui, la façon d'aborder les cas d'usage orientés client de l'IAM fait débat. D'aucuns commencent à parler de « Customer IAM » ou « Consumer IAM », d'où l'acronyme CIAM.

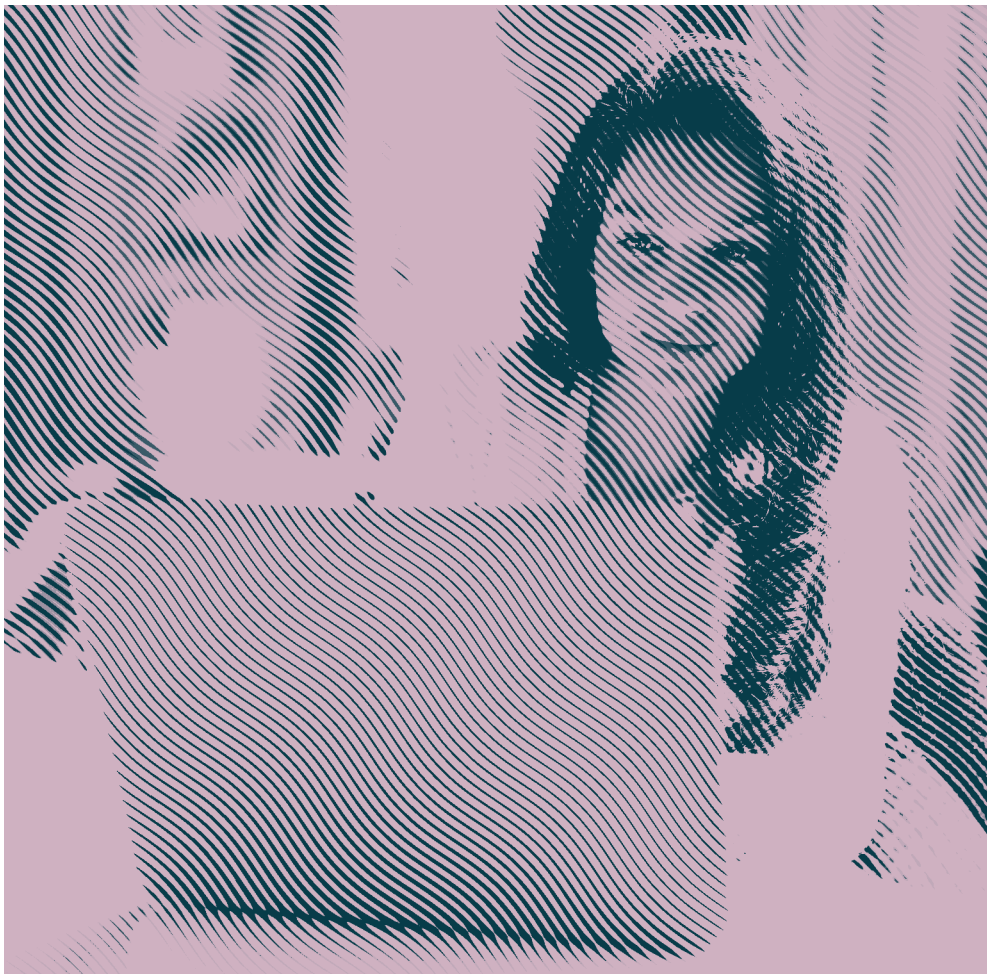
Le CIAM impose certes des exigences particulières, mais cela ne signifie pas que vous devez utiliser un produit uniquement axé sur le CIAM. L'approche d'Okta consiste à proposer un service cloud IAM global, avec une plateforme de base solide et des fonctionnalités permettant des cas d'usage CIAM. Nous pensons que ce choix est préférable à long terme.

Tout d’abord, qu’est-ce que l’IAM ou le CIAM ?

Si vous n’êtes pas familier des logiciels de gestion des identités, voici quelques rudiments. D’après Wikipédia, il s’agit de « l’ensemble des processus mis en oeuvre par une entité pour la gestion des habilitations de ses utilisateurs à son système d’information ou à ses applications ». Cette définition est large et peut s’appliquer à pratiquement tout processus informatique.

Pour la plupart des applications, il s’agit en quelque sorte d’une table de base de données qui stocke les profils et les mots de passe. Elle peut également contenir des données relatives aux autorisations. Pour les applications plus complexes ou les déploiements à grande échelle, il est possible d’avoir recours à une solution packagée de gestion des identités et des accès (IAM) qui renforce la sécurité et comporte des frameworks préintégrés permettant de gérer des autorisations plus complexes, éventuellement pour de nombreuses applications.

En général, les logiciels IAM prennent en charge de nombreux cas d’usage. Par exemple, si les utilisateurs sont des collaborateurs, l’autorisation pourra être basée sur un rôle dans l’entreprise, alors que si les utilisateurs sont des clients, elle reposera sur le statut d’adhésion à un programme de fidélité. Ce dernier cas de figure nous plonge dans l’univers du Customer IAM, ou CIAM.



Qu’est-ce que le CIAM et l’IAM ont en commun ?

En résumé, la sécurité, l’évolutivité et la haute disponibilité.

S’il est sans doute vrai que les solutions IAM ne répondent pas toutes aux exigences des cas d’usage orientés client (dits B2C), les composants fonctionnels et les protocoles de base de l’IAM restent les mêmes en matière d’authentification, d’autorisation, d’annuaires et de gestion du cycle de vie des comptes utilisateurs. Un fournisseur qui utilise des fonctionnalités IAM clés (telles que la prise en charge d’OpenID Connect et d’OAuth) dans tous les cas d’usage impliquant des collaborateurs, des sous-traitants, des partenaires, des clients et le grand public sera bien mieux armé que celui qui met au point une technologie propriétaire répondant à un seul cas d’usage. Cela se traduira au final par davantage d’innovation et une réussite durable sur le marché, et vous aurez trouvé un partenaire à long terme pour vos projets de développement applicatif. Vous avez tout intérêt à vous appuyer sur un socle solide et pérenne.

Les systèmes IAM détiennent les clés du royaume. Par conséquent, quel que soit le cas d’usage, la sécurité d’un produit IAM est de première importance. Les mêmes contrôles de sécurité que pour un service d’authentification ou de fédération s’appliquent, que le cas d’usage concerne des collaborateurs fédérés dans Office 365, des clients fédérés dans un portail d’assistance ou des consommateurs fédérés sur plusieurs sites web d’une grande entreprise du secteur hôtelier, comme MGM Resorts International. Si le compte d’un collaborateur est compromis, les systèmes internes peuvent être piratés, et dans le cas de comptes de consommateurs, une communication publique est généralement inévitable, ce qui peut avoir de mauvaises répercussions en termes d’image, même si votre entreprise n’est pas cotée en bourse.

L’évolutivité touche à un domaine où les fournisseurs spécialisés en CIAM peuvent se prévaloir de conditions particulières. Et d’une certaine façon, ils ont raison. Si vous comparez un service cloud CIAM spécialisé avec un produit IAM on-premise d’ancienne génération, il est évident que le service CIAM doit être capable de gérer un client unique avec des dizaines de millions d’identités. Nombre de produits on-premise plus anciens, voire des produits IDaaS (Identity-as-a-Service) génériques, n’ont pas été conçus pour fonctionner à cette échelle. Cependant, un produit IDaaS qui répond à tous les cas d’usage et dessert des milliers de clients avec des centaines de millions d’authentification par mois peut facilement évoluer pour gérer un nouveau client comptant des millions d’utilisateurs. L’argument selon lequel le CIAM est différent devient discutable lorsque votre fournisseur gère déjà un service cloud multitenant à grande échelle.

Enfin, la haute disponibilité est essentielle pour tous les cas d’usage. Si le système IAM tombe en panne, votre activité en pâtit.

Les collaborateurs sont certes nettement moins productifs, mais l’indisponibilité de votre site d’e-commerce est, quant à elle, synonyme de manque à gagner. Une fois encore, un service cloud évolué avec une redondance extrême garantit la haute disponibilité nécessaire dans tous les cas d’usage.

Alors, quelle est la différence entre CIAM et IAM ?

Les systèmes IAM axés collaborateurs servent généralement à accéder à des services internes et peuvent inclure un portail utilisateur. En revanche, la base d'utilisateurs des services CIAM est en principe constituée d'internautes ou d'utilisateurs d'applications mobiles qui souhaitent se connecter à un site web sans passer par le portail d'un fournisseur IAM tiers. Dans cette optique, les produits CIAM doivent être orientés développeurs et faciles à utiliser. Si le fournisseur CIAM ne permet pas aux développeurs de s'inscrire, de se connecter et de gérer facilement les comptes utilisateurs de leurs applications, ils vont aller voir ailleurs. Le service IAM doit comporter une API REST suffisamment granulaire pour permettre un accès par programmation à toutes ces fonctionnalités et fournir des outils de développement évolués, notamment des kits SDK pour plusieurs langages de programmation et des widgets intégrables.

Le CIAM exige plus de souplesse dans l'authentification selon le cas d'usage, de la fédération des clients B2B à l'authentification native, en passant par l'authentification sociale et même l'authentification sans mot de passe. Un service cloud IAM évolué toujours à la pointe des technologies et protocoles d'authentification aura un avantage dans cette situation, car il comportera tout cet éventail d'options. Avec l'authentification sociale, l'association et la dissociation d'un profil social avec le profil de base d'un utilisateur sont importantes, notamment dans les cas d'usage grand public. Très souvent, les développeurs auront besoin de personnaliser le comportement de ces données sociales, et le système IAM offrira la souplesse nécessaire pour exécuter par programmation diverses opérations sur les profils utilisateur.

Le modèle d'autorisation d'une solution CIAM peut s'avérer plus simple que les cas d'usage IT. Les rôles des clients sont souvent plus limités que ceux qu'on retrouve dans une grande entreprise. Dans ce domaine, un système IAM doté d'une fonctionnalité d'autorisation suffisamment robuste pour les scénarios d'entreprise pourra certainement gérer les critères d'autorisation CIAM, à condition que des éléments tels que les appartenances à des groupes et les attributs utilisateur puissent être modifiés par programmation.

La gestion des identités des clients exige une plus grande vigilance en matière de conformité aux réglementations, telles que le RGPD qui régit la protection des données à caractère personnel. Pour les applications grand public, il s'agit de prévoir les bonnes cases à cocher pour recueillir le consentement des utilisateurs. Cependant, la condition qui sous-tend l'IAM est la gestion sécurisée des données des utilisateurs. Il s'agit d'un critère de sécurité fondamental qui revêt une importance capitale dans tous les cas d'usage de l'IAM. La décision importante à prendre revient donc à privilégier une plateforme offrant la meilleure sécurité possible. L'utilisation des cases à cocher est relativement facile à mettre en oeuvre dans votre code, et devra sans doute faire l'objet d'une configuration sur mesure.

Et le Marketing Intelligence dans tout cela ?

Certains fournisseurs CIAM ont commencé à mettre au point leurs services à une époque où la transformation numérique n'en était qu'à ses premiers balbutiements. Sans doute étaient-ils visionnaires, mais leur objectif initial était plutôt de suivre le comportement des utilisateurs et de réaliser des analyses marketing. Ce sont des critères importants, mais le marché de ces produits a mûri et un directeur marketing a désormais le choix entre de nombreuses solutions d'analytique.

En parallèle, la technologie IAM n'est pas restée au point mort. De nouveaux protocoles comme OpenID Connect et OAuth permettent de proposer une architecture applicative évoluée (applications mobiles ou web monopage qui appellent des API REST backend) et des microservices (communication de serveur à serveur par API). Les développeurs ont besoin d'une plateforme IAM capable de sécuriser ces applications évoluées à l'aide de ces protocoles. Un service IAM évolué est plus susceptible de prendre en charge tous ces scénarios que des produits CIAM spécialisés plus orientés marketing.

La perspective globale pour l'informatique d'entreprise

Comme on le voit au travers des cas d'usage B2C pour l'IAM, les raisons ne manquent pas de porter son choix sur un produit IDaaS leader du marché comme Okta. Okta offre des fonctionnalités IAM d'avant-garde et est conçu de A à Z pour répondre aux exigences de sécurité, d'évolutivité et de haute disponibilité des cas d'usage impliquant des clients.

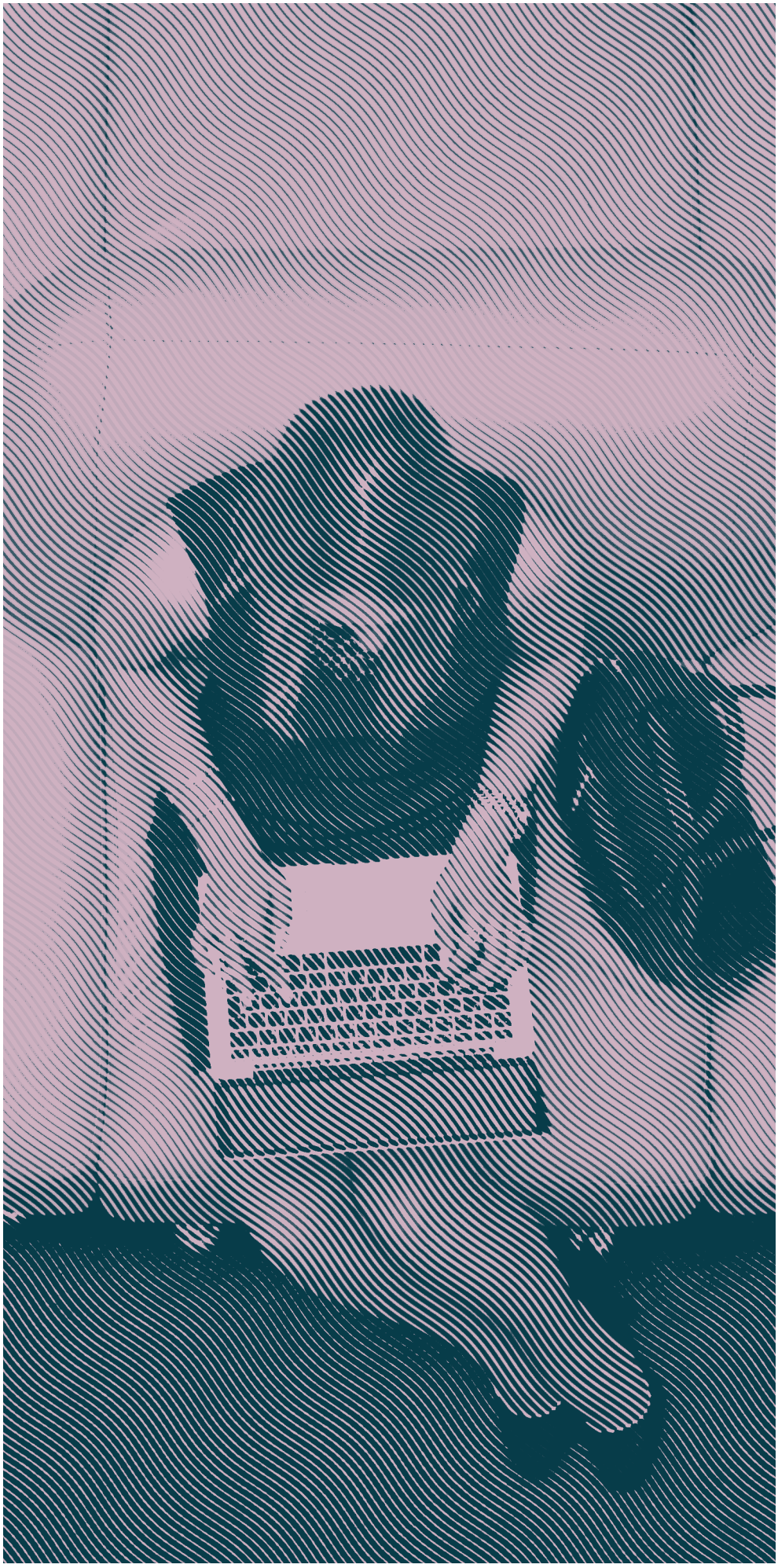
Mais le business numérique et l'informatique d'entreprise ne relèvent pas exclusivement du B2C. Les cas d'usage et les conditions requises varient énormément. Les clients d'Okta sont représentatifs de cette diversité : applications grand public, applications B2B, collaboration entre partenaires B2B, intégration de la chaîne d'approvisionnement, portails d'assistance, applications internes conçues pour la productivité des collaborateurs distants, intégration fluide entre sites d'e-commerce orientés client, connexion des collaborateurs à des applications SaaS, accès à vie aux ressources universitaires pour les anciens élèves, déploiement rapide d'un e-commerce sécurisé et enfin, aide aux entreprises souhaitant monétiser leurs données et développer leur activité dans l'économie des API.

Nous voyons dans tous ces cas d'usage des directeurs des systèmes d'information, des directeurs des données, des directeurs techniques et des directeurs du marketing d'entreprises très différentes. Et le meilleur moyen de prendre en compte ce panorama varié consiste à faire appel à un partenaire IAM ayant l'envergure nécessaire. Tout autre choix freinerait considérablement l'innovation future.

En savoir plus sur la gestion des identités des consommateurs pour le directeur du marketing, le RSSI et le DSI : **https://www.okta.com/resources/whitepaper-consumer-identity-management-for-the-cmo-ciso-and-cio/**

À propos d'Okta

Okta est le leader indépendant des solutions de gestion des identités destinées aux entreprises. Okta Identity Cloud permet aux entreprises de connecter en toute sécurité les bonnes personnes aux bonnes technologies au bon moment.Grâce à plus de 7 500 intégrations préconfigurées avec des applications et fournisseurs d'infrastructures, les clients d'Okta peuvent utiliser facilement et en toute sécurité les technologies de pointe répondant à leurs besoins. Plus de 13 000 entreprises font confiance à Okta pour les aider à protéger l'identité de leurs collaborateurs, partenaires et clients. **okta.com/fr**



okta