L'APPRENTISSAGE FACILE

Édition spéciale Okta

L'IDaaS (Identity-as-a-Service)

pour les nuls

Comprendre l'IDaaS (Identity-as-a-Service)

Relever les défis liés à la sécurité

Adopter une gestion des identités en phase avec notre époque

Ces conseils vous sont offerts par

okta

Lawrence C. Miller

Frederico Hakamine

À propos d'Okta

Okta est le leader indépendant des solutions de gestion des identités. Okta Identity Cloud permet aux entreprises de connecter en toute sécurité les bonnes personnes aux bonnes technologies au bon moment. Grâce à plus de 6 500 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 7 950 organisations (dont la 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America et Twilio) font confiance à Okta pour les aider à protéger les identités de leurs collaborateurs et de leurs clients. Pour plus d'informations, consultez le site **www.okta.com/fr** ou suivez Okta à la page **www.okta.com/fr/blog**.

L'IDaaS (Identity-as-a-Service)

Édition spéciale Okta

Lawrence C. Miller et Frederico Hakamine

pour les nuls®

L'IDaaS (Identity-as-a-Service) pour les nuls®, une édition spéciale Okta

Publié par
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 070305774
www.wiley.com

ISBN 978-1-119-77029-9 (pbk); ISBN 978-1-119-77034-3 (ebk)

Imprimé aux États-Unis

10 9 8 7 6 5 4 3 2 1

Remerciements de l'éditeur

Nous remercions chaleureusement toutes les personnes qui ont contribué à la rédaction de ce livre. Cet ouvrage a été réalisé avec la participation de :

Rédacteur projet : Martin V. Minner

Directeur éditorial : Rev Mengle

Éditrice associée : Katie Mohr

Représentants du développement commercial :
Frazer Hossack, Karen Hattan

Éditeur de production :
Mohammed Zafar Ali

Table des matières

Introduction

À mesure qu'une entreprise se développe et évolue, elle adopte de nouvelles applications pour optimiser ses opérations et son environnement informatique. Et si par le passé, chaque utilisateur ne disposait que d'un identifiant et d'un mot de passe, les équipes IT gèrent désormais des centaines de données d'identification destinées à accéder aux multiples applications on-premise et cloud qui s'exécutent sur différentes plateformes et d'innombrables terminaux.

De même, de nombreuses entreprises proposent désormais des produits et services en ligne qui exigent une connexion à un compte sécurisé. L'IT est ainsi appelé à gérer des millions de données d'identification de clients du monde entier.

Pour couronner le tout, les utilisateurs constituent l'une des principales cibles des cyberattaques. Comme l'a révélé le récent rapport de Verizon *Data Breach Investigations Report* (DBIR), 81 % des compromissions de données impliquent l'utilisation abusive d'identifiants volés ou trop faibles. Pour limiter ces risques, les entreprises doivent mettre en œuvre différentes méthodes d'authentification de l'identité d'un utilisateur, au-delà des simples mots de passe.

Tout manquement en matière de sécurité peut signifier la fin d'une entreprise. Les solutions de gestion des identités et des accès (IAM, Identity and Access Management) répondent à cette problématique : elles permettent aux équipes IT de renforcer la sécurité et de gérer les identités et les accès à la fois des collaborateurs et des clients de l'entreprise – et ce, avec une rapidité, une fiabilité et une simplicité d'une constance remarquable, qu'elles prennent en charge dix ou cent mille utilisateurs internes, dix mille ou des centaines de millions de clients. D'une part, elles protègent les identifiants et les données sensibles des utilisateurs. D'autre part, elles libèrent l'équipe IT des tâches manuelles chronophages (telles que les réinitialisations de mots de passe ou le provisionnement de comptes), lui permettant ainsi de se consacrer à des projets plus stratégiques qui stimulent la croissance et la rentabilité de l'entreprise.

Pour tirer parti des multiples avantages de l'IAM à grande échelle, la plupart des entreprises optent pour des services d'identité hébergés dans le cloud, ou IDaaS (Identity-as-a-Service). L'IDaaS offre une

gestion des identités robuste et évolutive assurant le contrôle des accès des utilisateurs et des clients à leurs applications et services, où qu'ils se trouvent dans le monde et sur n'importe quel terminal. Grâce à ce livre, vous découvrirez les principaux aspects de l'identité moderne, les différentes facettes de sa gestion et les atouts qu'offre une solution IDaaS pour votre entreprise.

À propos de ce livre

Les cinq chapitres de ce livre explorent les questions suivantes :

- Le concept d'identité, son évolution et son importance (chapitre 1)
- Les principes de l'IDaaS, solution moderne et novatrice de gestion des identités, comment elle permet de relever les défis actuels liés à l'identité et différents cas d'usage (chapitre 2)
- Les éléments constitutifs de l'IDaaS (chapitre 3)
- Les nouvelles tendances et innovations qui permettront de faire face à l'évolution de l'identité (chapitre 4)
- Les fonctionnalités et les avantages d'une gestion moderne des identités (chapitre 5)

Chaque chapitre est rédigé comme un tout, indépendant du reste de l'ouvrage. Si un sujet vous intéresse, vous pouvez donc vous y référer directement.

Les icônes utilisées dans ce livre

Ce livre est émaillé de différentes icônes destinées à attirer l'attention du lecteur sur des informations importantes. En voici le détail :


RAPPEL

Cette icône signale des informations importantes à retenir – ou, si vous nous permettez l'analogie, à inscrire dans votre mémoire non volatile.


TECHNIQUE

Si le jargon et les explications techniques vous enchantent, vous serez au paradis. Cette icône signale les informations un peu plus pointues que ne manqueront pas d'apprécier tous les technophiles.


CONSEIL

Un petit conseil est toujours le bienvenu : nous espérons que vous apprécierez ces informations utiles.

DANS CE CHAPITRE

- Principes fondamentaux et importance de l'identité
- Domaines associés à l'identité
- Historique des services d'identité

Chapitre 1
Qu'est-ce que l'identité ?

Ce chapitre explore les principes fondamentaux de l'identité en informatique, son importance, les différents domaines dont relève la gestion des identités et l'évolution du concept d'identité.

Comprendre l'identité et son importance

La technologie informatique au sens large a toujours constitué un bien précieux. De tout temps, l'accès à cette ressource a donc fait l'objet d'un contrôle plus ou moins rigoureux.

Ainsi, les premiers réseaux locaux ont été créés pour permettre le partage de fichiers et d'imprimantes au sein de l'entreprise. Mais seuls les cadres supérieurs et l'équipe marketing avaient le droit de partager les fichiers importants et les imprimantes laser couleur, très onéreuses à l'époque. Le département IT devait donc pouvoir identifier ces utilisateurs privilégiés et s'assurer que personne d'autre dans l'entreprise ne puisse accéder aux prévisions de vente ou effectuer des impressions en couleur.

Et si l'on remonte encore plus loin dans le temps, l'accès aux grands ordinateurs mainframes, dans les années 1960, était réservé à un très petit nombre de personnes. Naturellement, une salle verrouillée était en général la seule mesure de sécurité en place et, pour y avoir accès, il suffisait de montrer patte blanche et, de manière générale, d'avoir « la tête de l'emploi ».

L'identité et l'informatique ont donc toujours marché de pair (voir la figure 1-1).

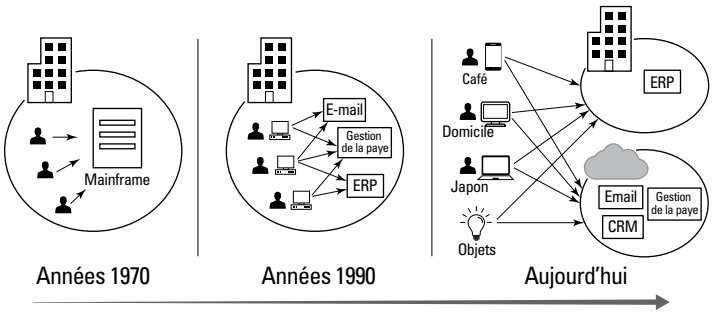

FIGURE 1-1 : L'identité et l'informatique ont toujours marché de pair. Avec l'évolution de l'IT, il est de plus en plus important de sécuriser la connexion aux technologies par les personnes et les objets.

À chaque nouvelle évolution de l'IT, les besoins en matière d'identité et de sécurité ont eux aussi évolué. Ainsi, dans les années 1990 et au début des années 2000, les collaborateurs d'une entreprise travaillaient dans ses locaux. Leurs données étaient protégées par un pare-feu installé au niveau du périmètre séparant le réseau de l'entreprise et Internet. Les employés se rendaient sur leur lieu de travail, pointaient et ouvraient une session sur leur ordinateur de bureau. À la fin de la journée, ils se déconnectaient de leur PC et rentraient chez eux pour se consacrer à leur vie personnelle.

Puis, les iPhones et les ordinateurs portables ont fait leur apparition et les gens ont commencé à travailler et collaborer de façon plus dynamique. Aujourd'hui, les collaborateurs lisent leurs e-mails professionnels sur leurs smartphones personnels, chattent en ligne avec leurs amis et envoient des liens sur les réseaux sociaux à partir de leurs ordinateurs portables d'entreprise connectés à des réseaux Wi-Fi ouverts dans des cafés, des aéroports et des halls d'hôtel. La réalité actuelle voit s'enchevêtrer vies privées et professionnelles, bien loin de l'environnement de travail et du périmètre réseau bien définis et bien contrôlés d'autrefois.

Étant donné que l'interaction avec l'informatique se fait désormais partout et depuis n'importe quel terminal, assurer la sécurité ne se limite plus simplement à isoler chaque personne sur son lieu de travail, sur un poste de travail spécifique, et à faire confiance à tous les intervenants au sein du périmètre réseau. Les entreprises doivent pouvoir sécuriser l'accès aux applications de chaque utilisateur tout en

appliquant des règles adaptées aux différents contextes de réseaux, systèmes et données. En outre, elles doivent pouvoir gérer ces identités à grande échelle, pour un vaste écosystème de collaborateurs et de clients, sur une multitude de systèmes, n'importe où dans le monde. L'IT continue à évoluer, mais c'est toujours l'identité qui sert à garantir votre sécurité.

RAPPEL

Dès l'instant où des ressources ou des informations confidentielles sont partagées, il faut identifier en toute sécurité l'individu qui utilise ces ressources ou consulte ces informations. Vous pouvez ainsi limiter ce qu'un utilisateur donné peut faire (par exemple, qui peut utiliser l'imprimante laser couleur) et empêcher d'autres utilisateurs d'accéder aux données ou de commettre des actions qui pourraient nuire à autrui (par exemple, utiliser frauduleusement le numéro fiscal d'un tiers, relevé à partir d'une déclaration de revenus électronique, ou effectuer des achats en ligne en utilisant le numéro de carte de crédit de quelqu'un d'autre).

Définition des trois domaines de l'identité

Diverses technologies permettent de résoudre trois grands problèmes liés à l'identité :

- Établir et vérifier une identité
- Déterminer à quoi peut accéder une identité et ce qu'elle peut faire
- Définir les politiques et processus utilisés pour gérer les identités au sein des réseaux et systèmes d'une organisation

Ces technologies s'articulent en trois domaines présentés en figure 1-2 et décrits dans les trois sections suivantes.

Gestion des identités et des accès (IAM)

De manière générale, la gestion des identités et des accès, ou IAM (Identity and Access Management), est la technologie qui sert à classifier les utilisateurs et les groupes dans un système logiciel, ainsi que les ressources auxquelles ils peuvent accéder et les fonctions qu'ils peuvent exécuter. L'IAM gère l'authentification, l'autorisation, la gestion des comptes et le contrôle d'accès.

L'IAM aide les entreprises à contrôler qui sont les utilisateurs de leur entité (*composant de gestion des identités*) et à quels services ceux-ci peuvent accéder ou non, et selon quelles modalités (*composant de gestion des accès*).

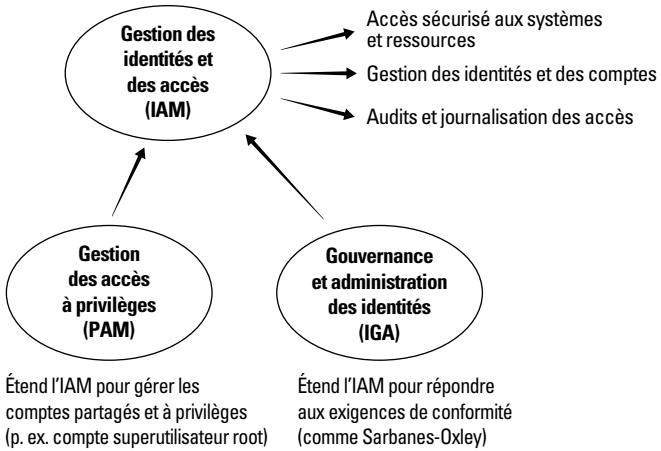

FIGURE 1-2 : Les trois domaines de l'identité (IAM, PAM et IGA) et leurs modes d'interaction.

RAPPEL

La technologie IAM, sur laquelle repose l'identité, exécute les fonctions importantes suivantes :

- Elle stocke les données utilisateurs, les politiques et les configurations.
- Elle gère les comptes utilisateurs et les identifiants.
- Elle affecte et retire aux utilisateurs des applications et des ressources (selon un processus appelé provisioning/déprovisioning).
- Elle authentifie les utilisateurs.
- Elle contrôle l'accès aux applications.
- Elle vérifie les identités pour savoir qui a fait quoi et quand.

Gestion des accès à privilèges (PAM)

Il arrive souvent que plusieurs utilisateurs soient amenés à partager un compte unique doté d'accès à privilèges pour l'exécution de tâches administratives. Par exemple, Linux dispose d'un compte superutilisateur (root) qui dispose d'un accès à privilèges et peut réaliser n'importe quelle tâche sur un serveur. Parmi d'autres exemples de comptes superutilisateur figurent le compte Windows « Administrateur » et l'utilisateur « SYS » d'Oracle Database.

Ces comptes n'étant pas individualisés, de nombreuses entreprises en communiquent les identifiants à plusieurs utilisateurs (en d'autres mots, tous les administrateurs de l'équipe IT connaissent le mot de passe du compte root), ce qui constitue une pratique dangereuse en soi.

De plus, il devient difficile de savoir qui a fait quoi et quand. Imaginons qu'un dossier système critique ait été supprimé : même si les journaux du serveur indiquent que le superutilisateur est l'auteur de la suppression, comment savoir qui utilisait le compte root à ce moment précis ? Ainsi, chaque administrateur IT devient suspect.

La gestion des accès à privilèges (PAM, Privileged Acess Management) complète l'IAM par un « coffre-fort numérique » servant d'intermédiaire. Ce coffre sécurise les comptes partagés dotés de droits superutilisateurs au moyen d'un mot de passe secret/aléatoire que personne ne connaît. Chaque fois qu'un utilisateur a besoin d'utiliser un compte à privilèges, il se connecte au système PAM ; ce dernier analyse la demande, valide la durée d'utilisation autorisée et le niveau de privilèges, consigne la transaction à des fins d'audit, modifie le mot de passe du compte superutilisateur et le révèle à l'utilisateur ayant émis la demande. Une fois le délai d'autorisation expiré, le système PAM reprend le contrôle sur le compte (en modifiant le mot de passe par une autre valeur secrète).

CONSEIL

Outre les droits individuels, le PAM permet de gérer des types de comptes spéciaux tels que les comptes de service (utilisés par exemple pour interagir avec un système d'exploitation), des comptes applicatifs (utilisés par exemple pour exécuter un travail par lots ou un script) et des comptes de base de données (utilisés par exemple pour modifier un schéma de base de données).

Gouvernance et administration des identités (IGA)

Au début des années 2000, des sociétés comme Tyco, MCI WorldCom et Enron ont manipulé leurs systèmes IT pour gonfler frauduleusement leurs résultats financiers et faire monter le prix de leurs actions. Après la révélation de ces scandales, de nombreux actionnaires ont perdu gros.

Pour éviter qu'une telle situation ne se reproduise, le gouvernement américain a exigé des sociétés cotées en bourse qu'elles contrôlent et auditent plus rigoureusement les comptes utilisés dans les systèmes IT liés à leurs finances. Ces contrôles comprenaient un examen régulier de qui a accès à quoi (un processus appelé *attestation*), ainsi que la mise en œuvre d'approbations de demandes et l'élimination des conflits d'intérêts (un processus appelé *séparation des obligations*).

Pour faciliter la satisfaction de certaines de ces exigences, les entreprises peuvent booster leur IAM à l'aide de la gouvernance et de l'administration des identités (IGA, Identity Governance and Administration).

RAPPEL

L'IGA s'est avéré nécessaire à l'apparition d'exigences de conformité réglementaire telles que les lois SOX (Sarbanes-Oxley) et HIPAA (Health Insurance Portability and Accountability Act) aux États-Unis. L'IGA

applique les principes d'attestation et de séparation des obligations, en plus de fournir des rapports de conformité.

Tandis que l'IAM et le PAM sont des composantes technologiques de la gestion des identités, l'IGA peut être considéré comme la composante relevant des politiques et des processus. Une solution IGA englobe les politiques qui définissent :

- à qui il convient d'accorder l'accès à quelles ressources réseau en fonction de ses rôles et responsabilités au sein de l'entreprise ;
- les processus de gestion du cycle de vie des identités de l'entreprise (tels que les demandes et les approbations d'accès, ou le provisioning/déprovisioning des comptes) ;
- la vérification continue de la conformité à la gouvernance des identités, notamment la journalisation, la surveillance et l'audit des identités et des accès.

CONSEIL

De nombreux systèmes IGA gèrent également le provisioning – c'est-à-dire l'allocation automatique de ressources à des comptes. Toutefois, les solutions avancées de gestion des identités intègrent déjà ces fonctions de façon native. (Reportez-vous au chapitre 2 pour en savoir plus.)

Évolution de la gestion des identités

Comme toute autre technologie, la gestion des identités a évolué dans le temps pour s'adapter aux nouveaux défis et exigences (voir la figure 1-3).

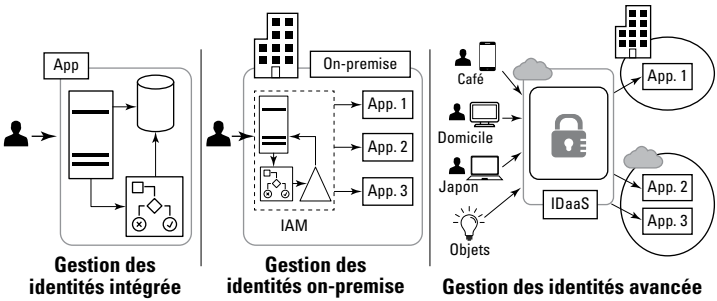

FIGURE 1-3 : Évolution de l'identité pour répondre aux nouveaux défis en matière d'IT et de sécurité.

Gestion des identités intégrée

Au début, la gestion des identités consistait en une authentification locale auprès d'un serveur central ou d'une application de bureau. À cette époque, relativement peu d'ordinateurs étaient connectés entre eux, de sorte qu'il s'agissait essentiellement de limiter l'accès local à un

poste de travail ou à une application, et de protéger le système d'exploitation. Un grand nombre de systèmes d'exploitation pour postes de travail et d'applications installées en local disposaient donc de fonctionnalités d'authentification de base intégrées, ne nécessitant qu'un nom d'utilisateur et un mot de passe simples.

Gestion des identités on-premise

Au milieu et jusqu'à la fin des années 1990, les entreprises ont commencé à interconnecter des postes de travail et des serveurs au sein de réseaux locaux ou LAN (Local Area Network) afin de partager des informations. Avec l'adoption d'Internet et d'applications Web (e-mail, portails intranet, Oracle, SAP, etc.), le besoin d'une gestion des identités plus robuste s'est lui aussi accentué. Les réseaux prennent de l'ampleur, s'étendant à plusieurs milliers d'ordinateurs régulièrement connectés à des millions de services sur Internet, exposant les entreprises à une multitude d'intrusions et d'actes de piratage commis à distance. Dans le même temps, la gestion des comptes utilisateurs devenait un vrai casse-tête pour l'IT, car les utilisateurs devaient établir de multiples connexions, notamment à leur ordinateur de bureau, à des dizaines d'applications et à leur logiciels de messagerie. Les nombreux points d'accès à l'environnement d'entreprise devaient tous faire l'objet d'un contrôle par l'équipe IT, à qui il revenait également de réinitialiser les mots de passe oubliés.

Pour surmonter ces difficultés, les entreprises ont adopté une gestion des identités assurée par des systèmes dédiés. Microsoft Active Directory (AD), introduit pour la première fois avec Windows 2000 Server, a permis de centraliser la gestion des comptes et d'implémenter des services d'annuaire liés à l'identité au niveau des réseaux et applications Windows. De même, Novell eDirectory (maintenant NetIQ eDirectory) et le protocole LDAP (Lightweight Directory Access Protocol) fournissaient des services d'annuaire à la fois aux réseaux Windows et non Windows. Et pour sécuriser l'accès aux applications Web et à la messagerie électronique, les entreprises ont adopté des solutions Web à authentification unique – également appelées SSO (Single Sign-On) ou WAM (Web Access Management) – telles qu'Oracle Access Manager, CA SiteMinder, PingAccess, Tivoli Access et Microsoft Active Directory Federation Services (ADFS).

Gestion des identités avancée ou IDaaS (Identity-as-a-Service)

De nos jours, il est plus que jamais nécessaire d'assurer une gestion robuste des identités. Le risque d'une compromission ou d'une cyber-attaque est constant et réel, et les adversaires malveillants de tous bords – utilisateurs internes , cybercriminels, hacktivistes, cyberterroristes –

sont extrêmement motivés, que ce soit par l'appât du gain ou par une idéologie.

Dans le même temps, le nombre d'applications disponibles explose. Ajoutons à cela qu'elles sont de plus en plus souvent proposées en mode SaaS, sous la forme de service cloud (par exemple Microsoft 365, Slack et Zoom). Selon le rapport Okta 2020 « Businesses @ Work », le nombre moyen d'applications par entreprise est actuellement de 88, avec un taux de croissance de 21 % ces trois dernières années. La multiplication et la diversification des terminaux aggravent encore le problème. En plus de l'ordinateur portable fourni par l'entreprise, presque chaque utilisateur dispose d'un autre terminal mobile et d'un ordinateur ou d'un iPad à la maison. Nombre d'entreprises ne contrôlent pas nécessairement ces environnements ; par exemple, Microsoft Active Directory ne peut pas contrôler les applications sur les terminaux Android, Mac et autres équipements non Windows. Enfin, les utilisateurs accèdent aux applications et aux données quasiment partout, y compris sur des réseaux Wi-Fi publics (c'est-à-dire non sécurisés).

CONSEIL

Pour en savoir plus sur la manière dont les entreprises utilisent aujourd'hui les applications, consultez le rapport « Businesses @ Work » sur `www.okta.com/businesses-at-work/2020` et le tableau de bord Businesses @ Work sur `www.okta.com/businesses-at-work`. Ces données sont compilées en temps réel et annuellement par Okta à partir de données anonymisées provenant de milliers d'organisations clientes, d'applications, d'intégrations IT et de l'activité quotidienne des utilisateurs.

Ainsi, le concept d'identité n'a pas seulement évolué : il s'est transformé en une réalité hybride où les applications auxquelles on accède, le terminal utilisé et le périmètre réseau changent constamment. Et ces technologies et générations différentes coexistent dans nos environnements – un peu comme si nos ancêtres primates, les hommes préhistoriques et nos contemporains essayaient de travailler ensemble en combinant silex et ordinateurs portables…

Les solutions traditionnelles de gestion des identités telles qu'Active Directory et l'authentification unique (SSO) sur site sont incapables de gérer les comptes et de sécuriser l'accès efficacement face à ces nombreux défis. Et même si elles le pouvaient techniquement, il faudrait des centaines de serveurs et des milliers d'heures de travail pour seulement gérer la charge et les exigences particulières, ce qui rend la tâche pratiquemment insurmontable avec des solutions traditionnelles on-premise.

La solution se trouve dans l'IDaaS (Identity-as-a-Service), c'est-à-dire une gestion des identités avancée qui permet de répondre à tous ces besoins. Nous allons l'évoquer plus en détail dans le reste de ce livre.

ADOBE UTILISE OKTA POUR CONNECTER DES MILLIERS DE CRÉATIFS ET DE COLLABORATEURS AU CLOUD

En 2012, Adobe lançait Creative Cloud et révolutionnait le monde de la création en migrant les célèbres produits Creative Suite dans le cloud. Un abonnement Creative Cloud permettait ainsi aux utilisateurs de télécharger et d'installer toutes les applications Adobe Creative Suite.

Suite à la migration de l'ensemble du processus de création dans le cloud, le cycle commercial d'Adobe a radicalement changé. Du jour au lendemain, l'entreprise est passée d'un modèle de licences permanentes et de cycles de lancement de 18 mois à des formules d'abonnement mensuelles et annuelles et à des mises à jour régulières.

Cette mutation a également modifié ses besoins en gestion des identités et des accès. La première version de Creative Cloud ne permettait pas de se connecter aux systèmes de gestion des identités d'entreprises déjà utilisés par la plupart des clients professionnels d'Adobe. Les administrateurs IT devaient donc configurer et gérer des identifiants utilisateurs entièrement nouveaux au sein d'Adobe Creative Cloud. Impossible alors d'échapper aux redondances et inefficacités en tous genres liées aux oublis de mot de passe et aux modifications d'identifiants par les utilisateurs.

Adobe ne voyait pas l'intérêt de développer une solution interne évolutive pour établir des connexions fédérées entre Creative Cloud et les systèmes de gestion des identités des clients. L'entreprise préférait mobiliser les équipes d'ingénieurs sur des projets tels que le développement de fonctionnalités Photoshop ou le lancement de nouvelles applications de création mobiles connectées. « Je n'ai pas l'intention de réinventer la roue en ce qui concerne la gestion des identités. Je veux simplement utiliser ce qui se fait de mieux sur le marché pour répondre aux exigences spécifiques d'Adobe en la matière et proposer très rapidement une solution efficace à nos clients », explique Scott Castle, chef de produit Creative Cloud.

Le double défi du cloud

L'équipe produits d'Adobe n'était pas la seule à faire face à des problèmes d'authentification. Fin 2014, la petite équipe informatique interne d'Adobe assurait la prise en charge de quelque 300 applications cloud avec une solution d'authentification unique open source qu'elle avait elle-même développée. Cette année-là, l'entreprise avait décidé de déployer Microsoft Office 365 auprès de ses 13 500 collaborateurs, transférant donc la messagerie, le calendrier et les outils SharePoint dans le cloud. L'ancienne plateforme de gestion des identités, avec ses pannes et son comportement capricieux, ne serait pas à la hauteur de la tâche.

Par chance, se souvient Den Jones, Senior Manager of IT Services, c'est à peu près à cette époque que l'équipe a découvert Okta. Il était logique de faire appel à un fournisseur externe spécialisé dans la sécurisation et

(suite)

(suite)

l'authentification des applications cloud – et de laisser Adobe se concentrer sur les outils de création.

Après avoir étudié les options proposées par Okta et constaté son expérience sur le marché, l'équipe IT d'Adobe a décidé d'abandonner son système d'authentification SSO interne et de déployer Office 365 avec la solution d'authentification d'Okta. Une fois le déploiement terminé, Adobe a commencé à transférer ses autres applications cloud vers la plateforme Okta. Comme le renouvellement de la maintenance de l'ancienne plateforme approchait, les délais étaient relativement serrés : trois mois pour migrer 300 applications.

Le calendrier s'est finalement avéré tout à fait raisonnable, au grand soulagement de Den Jones et de son équipe. Il a fallu environ quatre semaines pour traiter les 200 premières applications, précise-t-il. Aujourd'hui, il ne faut que quelques minutes pour intégrer la plupart des applications, contre plusieurs semaines, voire plusieurs mois auparavant. Depuis, Adobe a déployé plusieurs produits à partir d'Okta Identity Cloud auprès de collaborateurs sans cesse plus nombreux (20 500 personnes), qui sont ainsi parfaitement administrés et protégés.

L'identité pour tous

Après cette première collaboration fructueuse pour sécuriser l'accès des collaborateurs aux applications cloud, le choix d'Okta s'est tout naturellement imposé lorsque l'équipe produits d'Adobe a souhaité intégrer une solution professionnelle de gestion des identités à Creative Cloud abonnement Entreprise.

Aujourd'hui, Adobe utilise Okta pour offrir une couche de gestion des identités complète à tous ses clients professionnels, y compris ceux d'Adobe Marketing Cloud et d'Adobe Document Cloud, sans oublier Creative Cloud. La solution connectée sécurise les applications cloud d'Adobe et permet aux utilisateurs d'accéder à ses outils innovants avec leurs identifiants d'entreprise, rapidement, en toute sécurité et à moindre coût.

Afin de satisfaire les utilisateurs de Creative Cloud (et de rassurer les équipes IT des clients), la plateforme de gestion des identités d'Adobe offre d'importants avantages :

- Elle se connecte aux systèmes de gestion des identités d'entreprise des clients (Active Directory ou LDAP, par exemple), ce qui évite aux administrateurs IT de dupliquer les activités de gestion.
- Elle intègre les fonctionnalités d'Okta dans le code d'Adobe Creative Cloud.
- Elle arbore la marque Adobe.
- Elle fédère les identités des utilisateurs sur la base de comptes individuels, mais aussi de plusieurs comptes d'entreprise et d'agence.

DANS CE CHAPITRE

- Présentation de l'IDaaS (Identity-as-a-Service)
- Relever les défis de la gestion des identités avancée avec l'IDaaS
- Cas d'usage de l'IDaaS, pour les personnes et les objets

Chapitre 2
L'IDaaS (Identity-as-a-Service), ou la gestion des identités avancée

Dans ce chapitre, vous apprendrez en quoi consiste l'IDaaS, comment il permet de relever les défis actuels de la gestion des identités, les avantages qu'il procure et comment il prend en charge différents cas d'usage pour les collaborateurs, les prestataires, les clients et les objets.

Principes de base de l'IDaaS

L'IDaaS (Identity-as-a-Service) désigne la gestion des identités et des accès (IAM) en mode SaaS (Software-as-a-Service), hébergée par un fournisseur de services dans le cloud, à laquelle les entreprises peuvent souscrire par le biais d'un abonnement. L'IDaaS répond aux exigences actuelles de la gestion des identités, sans présenter les limites du modèle IAM on-premise.

RAPPEL

En adoptant des solutions SaaS telles que l'IDaaS, les entreprises et les administrateurs IT bénéficient d'avantages tels que :

- **Rentabilisation plus rapide –** Les solutions SaaS sont opérationnelles dès l'activation de l'abonnement, ce qui élimine des tâches telles que la mise en place de serveurs et l'installation de logiciels.

- **Moins de tâches de maintenance –** Les solutions SaaS sont constamment mises à jour par leurs fournisseurs, par l'ajout de nouvelles fonctions et le renforcement de la sécurité sans temps d'indisponibilité, réduisant ainsi le nombre de tâches de maintenance incombant aux administrateurs IT.
- **Moins d'intégrations manuelles –** Les solutions SaaS intègrent tout ce qu'il vous faut pour travailler, ce qui élimine les coûts d'intégration entre les composants internes tels que les serveurs, les systèmes de sauvegarde et les réseaux.
- **Coûts flexibles –** Comme les solutions SaaS sont généralement facturées par utilisateur et par mois, les entreprises peuvent mieux contrôler leurs dépenses et ne payer que pour les services qu'elles utilisent.

Ces avantages ont une telle importance que les entreprises en viennent à transférer la plus grande partie de leur activité de base vers le cloud. Si vous adoptez aujourd'hui une nouvelle solution pour votre entreprise, il est plus difficile de convaincre votre patron d'acheter des serveurs, de déployer des data centers, d'installer des logiciels et de demander à l'équipe IT de se charger de toute la maintenance, que de s'abonner à un service cloud.

RAPPEL

L'objectif de l'IDaaS est le même que celui de l'IAM : s'assurer que les utilisateurs sont bien ceux qu'ils prétendent être et leur octroyer les droits adéquats pour accéder aux ressources au bon moment. La différence majeure, c'est que l'IDaaS vous offre les avantages du cloud, sans les limites et les frais de l'IAM on-premise.

Comparons par exemple la mise en place de l'authentification unique (SSO, Single Sign-On) à l'aide de l'IAM on-premise traditionnel, comme Microsoft Active Directory Federation Services (ADFS) ou Oracle Access Manager, par rapport à une solution IDaaS telle qu'Okta. Dès que vous vous abonnez à l'IDaaS et importez vos utilisateurs, ces derniers peuvent tous bénéficier du service. Il n'est pas nécessaire de consacrer du temps et de l'argent à acheter et installer des serveurs et des systèmes d'exploitation, ni à estimer la charge et la capacité requises pour assurer le service.

En outre, chaque fois qu'une nouvelle fonctionnalité est introduite ou qu'une mise à jour est effectuée (comme une nouvelle application mobile pour sécuriser l'accès sur Apple iOS et Android, ou une amélioration de la sécurité pour empêcher les accès malveillants), vous recevez automatiquement les modifications nécessaires sans avoir à planifier, tester, prévoir une interruption de service pour maintenance et mettre à niveau le système manuellement. Étant donné que l'IDaaS dispose déjà de tous les composants requis pour la gestion des identités, tels que l'authentification multifacteur (MFA) et les solutions de

provisioning, renforcer la sécurité devient un jeu d'enfant et vous n'avez pas besoin d'acheter, d'installer manuellement et d'intégrer des solutions MFA ou de provisioning distinctes provenant d'autres éditeurs. Enfin, vous pouvez contrôler les coûts en fonction de la manière dont le service est utilisé ; ainsi, par exemple, si vous souhaitez déployer l'authentification MFA uniquement pour les cadres, vous n'avez pas besoin de payer pour ce service pour l'ensemble de vos collaborateurs.

Une solution IDaaS peut être utilisée pour sécuriser l'accès et gérer les identités au niveau de ressources diverses – dont les API, les systèmes on-premise, le cloud, les applications mobiles et les serveurs. Elle fournit également de multiples fonctionnalités natives, telles que l'authentification MFA adaptative (présentée au chapitre 3) pour améliorer la sécurité d'authentification, ou encore l'authentification unique (SSO), qui permet à l'utilisateur de ne s'authentifier qu'une seule fois sur le réseau pour avoir accès à toutes les applications et ressources qu'il est autorisé à consulter.

Dans l'univers on-premise, la configuration de toutes ces fonctionnalités (MFA adaptative, SSO, services d'annuaire et provisioning, entre autres) impose de travailler avec différents serveurs, diffférents fournisseurs (tels qu'Oracle, RSA, Microsoft et Symantec) et différentes intégrations manuelles. Avec l'IDaaS, tout est disponible en une seule offre, dimensionnée en fonction des besoins et rapidement rentabilisée (voir figure 2-1).

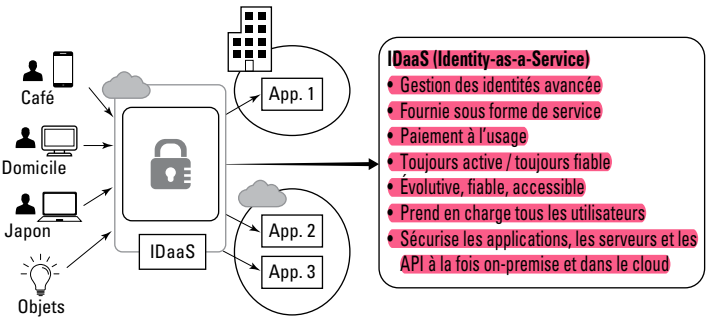

FIGURE 2-1 : Fonctionnement de l'IDaaS dans le cadre d'un environnement IT moderne et avantages de son utilisation.

Relever les défis liés à l'identité

L'IDaaS permet de relever de nombreux défis en matière d'identité caractéristiques de nos environnements actuels. Ainsi, il permet l'intégration rapide aux applications cloud et on-premise en tirant parti de normes ouvertes, telles que SAML (Security Assertion Markup Language) et OIDC (OpenID Connect), ainsi que des catalogues

d'applications. L'IDaaS consolide également le contrôle d'accès quel que soit le lieu dans lequel une application est hébergée – une caractéristique précieuse pour les entreprises qui disposent d'un environnement IT hybride, alliant systèmes on-premise, cloud public et cloud privé.

L'IDaaS procure l'évolutivité, la fiabilité et l'accessibilité dont ont besoin les entreprises actuelles dans un monde hyperconnecté où, potentiellement, des centaines de milliers, voire des millions d'utilisateurs – notamment les collaborateurs et les clients – nécessitent un accès à leurs applications mobiles, sites Web, API à tout moment depuis n'importe quel terminal.


RAPPEL

Une solution IDaaS offre de nombreux avantages aux entreprises, notamment :

- Elle améliore le niveau de cybersécurité d'une entreprise grâce à des fonctionnalités telles que l'authentification MFA adaptative (voir chapitre 3) et l'IAM centralisé.
- Elle optimise la productivité des utilisateurs et de l'IT. Les utilisateurs peuvent se connecter plus rapidement à toutes leurs applications via l'authentification SSO et le centre d'assistance passe moins de temps à réinitialiser les mots de passe. Que l'utilisateur s'authentifie sur un réseau Wi-Fi public dans un aéroport ou depuis son poste au bureau, le processus est toujours fluide et sécurisé.
- Elle contribue à réduire fortement les coûts de l'IT. La fourniture de services d'identité on-premise (par exemple, sur Active Directory ou Oracle Identity Manager), peut générer de nombreux coûts, parmi lesquels :
  - l'achat, l'installation, la mise à niveau et la maintenance de matériel serveur (ou de licences logicielles en cas de virtualisation) et de logiciels ;
  - le paiement de frais d'hébergement pour l'espace dans un data center, un cloud privé ou un cloud public ;
  - la configuration, la maintenance et la surveillance de connexions VPN.


RAPPEL

Avec l'IDaaS, vos seuls coûts sont ceux liés à l'abonnement et au travail d'administration IT nécessaire pour gérer vos comptes utilisateurs. Vos licences utilisateurs peuvent être rapidement et facilement augmentées ou réduites pour répondre aux besoins de votre entreprise. L'IDaaS diminue considérablement le coût d'exécution des services d'identité : des demandes de support IT manuel pour le provisioning et la réinitialisation des comptes utilisateurs, jusqu'aux services professionnels de déploiement, correction et mise à niveau des différentes solutions. Selon Forrester, « le plus grand avantage de

l'IDaaS par rapport aux solutions IAM on-premise est un taux de maintenance inférieur de 30 à 35 % ».

Cas d'usage

L'IDaaS prend en charge de nombreux cas d'usage courants en matière de gestion des identités (voir la figure 2-2) impliquant les collaborateurs, les prestataires, les partenaires, les clients et les objets.

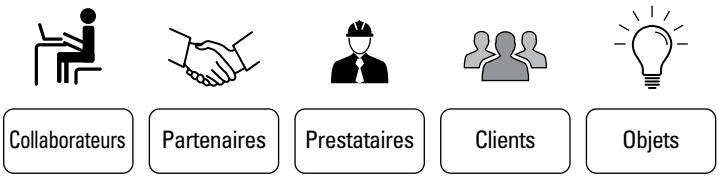

FIGURE 2-2 : Les cas d'usage (et les utilisateurs) qui nécessitent des services d'identité.

Pour les collaborateurs

Les collaborateurs sont la ressource la plus importante de toute entreprise. Il est essentiel de leur donner accès en toute sécurité aux technologies dont ils ont besoin. À l'heure actuelle, les collaborateurs se connectent aux systèmes d'entreprise en tous lieux, et travaillent et collaborent à distance. En même temps, ils font la cible d'attaques spécifiquement destinées à exploiter abusivement leurs accès.

L'IDaaS aide les collaborateurs :

- en effectuant l'onboarding et la modification des droits d'accès de façon dynamique en fonction des données utilisateurs communiquées par les systèmes RH tels que Workday et SuccessFactors ;
- en stockant de manière sécurisée les identités et droits des collaborateurs ;
- en sécurisant l'accès des collaborateurs à toutes les ressources, notamment les applications, les serveurs et les API, à la fois sur site et dans le cloud, avec un seul jeu de d'identifiants à authentification forte ;
- en permettant un accès sécurisé quel que soit le contexte, le terminal et l'emplacement réseau de l'utilisateur ;
- en augmentant l'efficacité des collaborateurs par un accès plus convivial et mobile aux ressources de l'entreprise ;
- en modifiant les exigences d'accès en fonction du risque, par exemple en refusant ou exigeant dynamiquement l'authentification MFA en cas d'accès à haut risque ;

- en accordant aux utilisateurs à faible risque un accès sans mot de passe ;
- en auditant et en fournissant des informations d'évènement pour l'équipe de sécurité.

Pour les prestataires et partenaires

Les partenariats sont une composante essentielle de l'activité d'une entreprise, mais des processus et systèmes rigides peuvent faire obstacle à une collaboration efficace. Les partenaires et prestataires introduisent dans l'environnement de nouveaux types d'utilisateurs dynamiques, ce qui complique la tâche des équipes IT. Parallèlement, accorder un accès excessif aux partenaires expose les systèmes critiques à des risques inutiles en matière de sécurité.

Traditionnellement, les entreprises octroyaient un accès aux prestataires et partenaires soit en gérant leurs identités à l'aide de la même solution IAM que pour leurs collaborateurs, dans le cas de relations à court terme ou relativement mineures, soit en intégrant la pile IAM de leur partenaire et en créant une intégration business-to-business (B2B) pour les partenariats à long terme et de grande envergure.

Créer des intégrations B2B est une opération coûteuse et chronophage. Par exemple, le coût total de propriété moyen pour la création et la maintenance d'une intégration B2B SAML est de 20 000 $ par intégration en interne.

CONSEIL

L'IDaaS aide à optimiser l'intégration des partenaires dans le cadre de relations B2B à court et à long terme. Ses principaux avantages :

- **Création d'une expérience fluide –** Vous effectuez une intégration native à la solution IAM de votre partenaire pour lui permettre d'accéder à vos ressources à l'aide de ses identifiants existants.
- **Promotion de la collaboration –** Vous optimisez l'expérience de votre partenaire en lui assurant un accès immédiat aux bonnes ressources via un portail personnalisé et sécurisé.
- **Automatisation du cycle de vie des comptes partenaires –** Vous centralisez la gestion des utilisateurs et vous automatisez le provisioning des identités de vos partenaires pour décharger les équipes IT de leurs tâches administratives.
- **Renforcement de la sécurité –** Vous conservez un contrôle total sur l'authentification, les services d'identité, les applications et les ressources et vous automatisez le déprovisioning pour éviter les accès persistants.

Pour les clients et consommateurs

Aujourd'hui, toute entreprise possède une activité numérique par le biais de sites Web, d'API et d'applications. Pour attirer des clients et les fidéliser le plus longtemps possible, il est devenu nécessaire de répondre à leurs attentes en leur fournissant une expérience numérique fluide, en phase avec les nouvelles technologies, multicanale et personnalisée.

Supposons que vous fassiez vos achats en ligne ou consultiez vos photos sur Instagram. Dans ces deux exemples, la sécurité est essentielle car vous voulez être sûr que personne n'utilise votre carte de crédit à votre insu, et que vos photos et commentaires sont sécurisés. Cela étant, si votre expérience utilisateur est fastidieuse, il est peu probable que vous reveniez sur ces sites. Vous escomptez également utiliser les mêmes identifiants et bénéficier du même niveau de sécurité et d'expérience utilisateur sur différents terminaux. Par exemple, il est probable que vous utiliserez Instagram à la fois sur votre ordinateur et votre smartphone, et que vous fassiez du shopping à la fois sur le site Web amazon.com et via Alexa. Fournir une sécurité irréprochable, mais sans friction est primordial en matière de gestion des identités des consommateurs.

CONSEIL

L'IDaaS peut aider les entreprises à sécuriser et à fournir une expérience client optimale, grâce aux avantages suivants :

- **Meilleure expérience client pendant l'enregistrement et la connexion –** Offrez des expériences attrayantes, à l'image de votre marque et personnalisées sur tous les canaux. De même, vous pouvez personnaliser facilement le processus d'enregistrement et de connexion sur de multiples applications sans codage ni travail de développement coûteux.
- **Vue à 360° du client –** Éliminez le cloisonnement que créent des comptes disparates. Avec une seule identité par client, vous pouvez mieux comprendre les intérêts et préférences de ce client, pour mieux le fidéliser.
- **Engagement –** Simplifiez l'onboarding grâce au progressive profiling et à l'authentification sans mot de passe. L'IDaaS intègre de façon transparente les applications dans le portail clients pour une expérience de connexion unique.
- **Gestion du consentement –** Donnez aux clients le contrôle de leurs données et répondez aux exigences de conformité réglementaires telles que celles du Règlement général sur la protection des données (RGPD) de l'Union européenne, par example. Pour en savoir plus sur la gestion du consentement, reportez-vous au chapitre 4.

Pour les objets

L'Internet des objets (IoT, Internet of Things) et les milliards d'appareils intelligents connectés (déjà plus de 30 milliards en 2020) présentent de nouveaux défis pour les entreprises modernes. La sécurité IoT est d'une importance capitale, car ses failles représentent des menaces encore plus critiques pour la vie humaine et la sécurité publique que tous les autres aspects de la cybersécurité.

Les objets intelligents, tels que l'application Amazon Alexa, les ampoules et les télévisions intelligentes, ont besoin de services d'identité pour s'authentifier et contrôler ce à quoi ils peuvent avoir accès – tout comme les êtres humains ! Toutefois, ces objets sont beaucoup plus nombreux que les humains et ils communiquent différemment : à l'aide d'API au lieu de navigateurs et d'applications.

RAPPEL

L'IDaaS fournit les services d'identité et l'évolutivité nécessaires pour répondre aux demandes de trafic de l'Internet des objets (IoT). En outre, l'IDaaS prend en charge les protocoles attendus par les appareils IoT intelligents, tels qu'Open Authorization (OAuth), pour sécuriser l'accès aux API.

CE QUE N'EST PAS L'IDAAS

Ce chapitre décrit ce qu'est l'IDaaS. En bref, il s'agit d'une solution IAM hébergée dans le cloud qui sécurise l'accès aux applications et systèmes pour les utilisateurs d'une entreprise – notamment ses collaborateurs, prestataires, partenaires, clients et objets.

Mais à l'inverse, que *n'est pas* l'IDaaS ? Tout d'abord, il ne s'agit pas d'une solution de gestion des identités on-premise qui a été migrée vers le cloud dans le cadre d'une offre IaaS (Infrastructure-as-a-Service) ou PaaS (Platform-as-a-Service). Le passage de vos serveurs Active Directory on-premise à une solution PaaS, ou même l'adoption d'une technologie de container moderne telle que Docker, par exemple, impose toujours d'installer et de corriger manuellement les systèmes, de planifier la capacité requise et d'effectuer manuellement l'intégration avec d'autres modules ou fournisseurs. Et ce, sans tirer parti du modèle de paiement à l'usage d'une vraie solution IDaaS. Ce type d'architecture n'est donc pas de l'IDaaS. Bien que les containers soient très pratiques (particulièrement pour créer vos propres applications), vous n'avez fait que déplacer vers le cloud les obstacles que vous rencontriez sur site.

L'IDaaS n'est pas non plus une solution de fournisseur de services gérés (ou MSP, pour Managed Service provider). Ceux-ci exécutent en général une IAM d'ancienne génération en votre nom, tout en vous facturant des frais d'abonnement. Même si ces solutions réduisent les tâches de maintenance fastidieuses, elles n'éliminent pas les limites fondamentales de l'IAM traditionnel, puisque contrairement à l'IDaaS, elles n'offrent pas des mises à niveau en temps réel sans périodes d'indisponibilité planifiées, ou des milliers d'intégrations prêtes à l'emploi avec les applications mobiles, applications cloud et API.

DANS CE CHAPITRE

- Éléments constitutifs de l'IDaaS
- Contrôle de l'accès aux ressources
- Autres facteurs pertinents tels que les intégrations, la sécurité, la confidentialité ou la conformité

Chapitre 3
Les éléments constitutifs de l'IDaaS

Dans ce chapitre, vous découvrirez les principaux composants de l'IDaaS (Identity-as-a-Service), les ressources qu'il permet de sécuriser et les principaux facteurs à prendre en compte lorsque vous adoptez une solution IDaaS.

Éléments constitutifs

Les solutions IDaaS reposent généralement sur quatre éléments constitutifs :

- Annuaire
- Authentification unique (SSO)
- Authentification multifacteur (MFA)
- Provisioning et workflows

Annuaire

L'annuaire est un composant essentiel de toute solution de gestion des identités et des accès (IAM). Il s'agit d'une base de données d'entités (utilisateurs, groupes et ressources), de métadonnées (configurations et règles) et de données d'audit nécessaires à l'IAM pour exécuter ses tâches.

Par exemple, Microsoft Active Directory (AD) est un annuaire traditionnel installé dans un environnement on-premise. On pourrait

également citer ApacheDS, NetIQ eDirectory, OpenLDAP et Oracle Internet Directory (OID).

Les annuaires on-premise traditionnels ont été créés avant le cloud, le télétravail, le foisonnement des fusions et acquisitions, l'activité business-to-business (B2B) et la révolution des smartphones/applications. Ces annuaires ne sont donc pas entièrement optimisés pour répondre aux exigences modernes. Lorsqu'une entreprise essaie de forcer l'implémentation d'annuaires on-premise afin de répondre aux exigences modernes, par exemple pour prendre en charge des applications cloud ou gérer des terminaux mobiles, elle se retrouve à déployer une multitude de forêts d'annuaires, domaines approuvés, serveurs, intégrations personnalisées et scripts PowerShell/bash, ce qui crée des environnements extrêmement complexes qui ne répondent finalement pas à ses besoins.

RAPPEL

Une solution avancée et efficace doit répondre aux exigences de son époque et s'intégrer de façon transparente aux systèmes qui utiliseront l'annuaire, sans exiger des intégrations manuelles et sans accroître la complexité de l'environnement.

Les solutions IDaaS fournissent un annuaire intégré qui stocke de façon sécurisée les données nécessaires pour traiter tous les cas d'usage modernes – du mobile aux fusions-acquisitions et au cloud – sans exiger d'infrastructure, de configurations personnalisées et de scripts bash ou PowerShell. Cet annuaire s'intègre de façon native à tous les services qui vont l'utiliser, tels que le SSO pour l'authentification des utilisateurs, ce qui élimine les tâches d'intégration manuelles.

CONSEIL

Lorsqu'elles adoptent une pile IDaaS moderne, de nombreuses entreprises cherchent à décommissionner leurs annuaires on-premise. Cette mise hors service est facile à réaliser lorsque l'annuaire est utilisé uniquement pour l'IAM, mais nécessite une planification minutieuse dans des environnements complexes. Par exemple, dans de nombreuses entreprises, non seulement Active Directory stocke les données d'identité, mais il est également utilisé pour des services tels que le DNS et les certificats de clés privées. En outre, certaines sociétés développent des intégrations PowerShell personnalisées ou combinent tant bien que mal plusieurs centaines de contrôleurs de domaine pour stocker leurs données. En cas de déploiement complexe, les bonnes pratiques préconisent de réduire l'utilisation d'annuaires d'ancienne génération en migrant les services vers des solutions modernes et en réduisant dans le même temps la complexité.

Par exemple, en utilisant une solution IDaaS avec annuaire et provisioning intégrés, vous pouvez éliminer les scripts PowerShell personnalisés destinés aux activités liées à l'identité, telles que

l'onboarding de nouveaux collaborateurs lors d'une fusion-acquisition, ou la synchronisation des adresses e-mail de systèmes disparates. Décharger ces tâches vers l'IDaaS réduit considérablement le nombre de serveurs et la complexité de vos annuaires on-premise.

Authentification unique (SSO)

Les données d'authentification ont pour but d'assurer la sécurité des comptes, mais sont également source de difficultés dès lors que les utilisateurs disposent de comptes différents pour des centaines d'applications. Pour continuer à utiliser ces nombreuses applications tout en évitant la prolifération des mots de passe et la perte de productivité, les utilisateurs adoptent des raccourcis dangereux, tels que réutiliser les identifiants d'une application à l'autre, ou écrire les mots de passe sur des bouts de papier ou dans des fichiers enregistrés sur leurs terminaux. Selon Verizon, le vol de données d'identification est la source la plus courante de compromissions de données, et l'on peut dire à juste titre que ce phénomène est largement dû à la difficulté qu'éprouvent les utilisateurs à gérer leurs nombreux identifiants.

L'authentification unique (SSO, Single Sign-On) résout ce problème en autorisant l'accès à toutes les applications avec un seul identifiant. Pour ce faire, elle repose sur des normes ouvertes telles que SAML (Security Assertion Markup Language) et OIDC (OpenID Connect) pour fédérer les utilisateurs sur les systèmes et applications tiers.

CONSEIL

Les solutions SSO sont parfois critiquées parce qu'elles introduisent un point de défaillance unique dans le processus d'authentification – les fameuses « clés du royaume » que certains leur reprochent d'accorder. Toutefois, il existe certaines fonctions importantes et bonnes pratiques qui non seulement résolvent ce problème, mais améliorent également la sécurité et la productivité. En voici quelques exemples :

- **Authentification multifacteur (MFA) –** L'authentification MFA est la meilleure alliée de la SSO. Elle renforce la sécurité de la SSO par des facteurs d'authentification supplémentaires, comme les données biométriques de l'utilisateur, qui sont plus sûres que les mots de passe traditionnels.
- **Accès adaptatif –** Une bonne pratique consiste à utiliser des solutions qui réévaluent l'accès des utilisateurs en fonction de leur contexte, réseau, terminal et emplacement, tout en tirant parti de flux d'informations sur les menaces. Ainsi, l'authentification SSO modifie automatiquement les exigences de connexion, bloque les accès et déclenche les alertes de sécurité quand des évènements suspects se produisent.

L'authentification SSO est une excellente méthode pour imposer à vos utilisateurs des pratiques de mot de passe à authentification forte. Avec seulement un mot de passe à contrôler, l'équipe IT peut définir des politiques pertinentes pour s'assurer que ce mot de passe est aussi sécurisé que possible, et notamment exiger que les mots de passe :

- expirent après une certaine durée ;
- soient différents des mots de passe précédents pour empêcher la réutilisation ;
- ne correspondent pas à une liste existante d'identifiants piratés ;
- se verrouillent après un certain nombre de tentatives infructueuses afin de protéger contre les attaques par force brute.

CONSEIL

Les gestionnaires de mots de passe peuvent également simplifier les accès pour les utilisateurs finals, mais leur principe de fonctionnement est de protéger les identifiants en les stockant dans un coffre virtuel, pas d'éliminer les mots de passe. En outre, ils ne comportent pas des fonctions de sécurité essentielles telles que l'examen du contexte de l'utilisateur ou le blocage de l'accès aux réseaux malveillants.

Grâce à ces fonctionnalités, même si un utilisateur saisit les identifiants corrects, selon la configuration, il se peut que sa session soit limitée dans le temps (avec une validité de quelques minutes et non de plusieurs heures), qu'il doive effectuer une authentification supplémentaire ou qu'il se voie refuser complètement l'accès. Par exemple, si un utilisateur utilise un anonymiseur Tor pour se connecter à un système sensible, cet accès peut lui être entièrement refusé. L'authentification unique offre aux administrateurs un contrôle plus étendu et granulaire sur la façon dont les utilisateurs peuvent accéder aux ressources de l'entreprise.

CONSEIL

Pour en savoir plus sur l'authentification SSO, lisez la série d'articles d'Okta qui dissipe tous les mythes à son sujet, sur le blog d'Okta (`okta.com/blog`).

Authentification multifacteur adaptative (MFA)

Authentifier un utilisateur implique généralement de valider une déclaration d'identité (telle qu'un nom d'utilisateur) au moyen de ce qu'on appelle communément un *facteur*. Les facteurs d'authentification correspondent en général à l'un des trois types suivants :

- Une chose que vous savez – par exemple, un numéro d'identification personnel (PIN), un mot de passe ou le nom de jeune fille de votre mère
- Une chose que vous possédez – comme un smartphone, votre badge de collaborateur ou une clé USB de type FIDO U2F

» Une caractéristique de votre personne – un identificateur biométrique unique comme l'empreinte digitale, la rétine ou l'iris de l'œil

La plupart des applications authentifient les utilisateurs à l'aide d'un seul facteur, généralement un mot de passe. Bien que ce soit une méthode simple et directe, utiliser des mots de passe présente beaucoup de désavantages. Les mots de passe sont le moyen le plus facile de compromettre vos systèmes et les cyberpirates peuvent en tirer parti de nombreuses manières.


CONSEIL

Les cinq principales attaques exploitant les mots de passe sont : le phishing à large diffusion, le phishing ciblé, le vol d'identifiants, l'usage en masse de mots de passe piratés et les interceptions de communications. Pour savoir comment sont menées ces attaques, consultez la page `www.okta.com/resources/whitepaper/5-identity-attacks-that-exploit-your-broken-authentication`.


CONSEIL

Vous pouvez utiliser des ressources libres telles que `haveibeenpwned.com` et le module d'extension PassProtect du navigateur Google Chrome pour déterminer si vos mots de passe et vos comptes ont été compromis.


TECHNIQUE

Les mots de passe peuvent être également la cible d'attaques par force brute. Toutefois, la plupart des systèmes peuvent bloquer ces attaques par des mécanismes de verrouillage de compte après un certain nombre de tentatives de connexion infructueuses.

La solution aux faiblesses inhérentes des mots de passe et de l'authentification à facteur unique est l'authentification multifacteur (MFA, Multi-Factor Authentication).

L'authentification MFA impose au moins deux facteurs pour vérifier et valider une identité. Par exemple, il peut être exigé qu'un utilisateur se connecte à un site Web avec un mot de passe, puis qu'il entre un code à usage unique reçu sur son smartphone. Le code n'est valide qu'un temps limité (généralement de trois à cinq minutes) et ne peut être utilisé que pour une seule tentative de connexion. Si le code est incorrect ou si l'utilisateur se déconnecte de la session et tente de se reconnecter à l'aide du même code, la tentative de connexion échoue.

L'inconvénient de l'authentification MFA est la frustration qu'elle peut engendrer si l'utilisateur doit renouveler ces demandes de code chaque fois qu'il se connecte. L'authentification multifacteur constitue un point de friction pour l'utilisateur qui doit se réauthentifier au cours de sa journée de travail, ou utiliser une combinaison de jetons matériels et logiciels pour obtenir un accès. Chaque facteur d'authentification obligatoire supplémentaire renforce le contrôle d'accès, mais au détriment de l'expérience utilisateur. Toutefois, la friction liée à

l'authentification MFA peut être atténuée de différentes façons : en réduisant le nombre de connexions qu'effectue l'utilisateur (grâce à l'authentification SSO), en utilisant des facteurs plus ergonomiques et intuitifs, et en adoptant une MFA adaptative, c'est-à-dire sensible aux différents contextes et profils de risque.

Pour trouver un équilibre entre sécurité, coûts et facilité d'utilisation, l'IDaaS fournit la prise en charge complète de différents facteurs MFA. Ces facteurs vont d'une authentification faible, telle que des questions de sécurité et des codes envoyés par SMS, à une authentification forte, telle que des notifications push, la biométrie ou des jetons physiques.

CONSEIL

De nombreuses entreprises font encore confiance à des facteurs d'authentification à faible assurance tels que les questions de sécurité et des codes envoyés par SMS. Les questions de sécurité sont aujourd'hui le facteur le plus utilisé par les entreprises, et leur usage gagne encore du terrain. Selon Okta, 38 % des utilisateurs de l'authentification MFA emploient aujourd'hui des questions de sécurité comme deuxième facteur, par rapport à 30 % l'année dernière. Or, le problème que posent les questions de sécurité est que les réponses relèvent souvent du domaine public et peuvent être dénichées sur les réseaux sociaux (par exemple, le nom de jeune fille de votre mère ou le nom de votre conjoint). Utiliser des SMS comme seul deuxième facteur n'est pas non plus sans risque. D'ailleurs, certaines entreprises et réglementations (notamment dans le secteur de la défense) interdisent l'emploi des SMS comme deuxième facteur MFA en raison des risques d'interception des codes. Cela ne signifie pas que ces facteurs soient inefficaces dans le cadre d'une authentification multifacteur, mais il convient d'associer les bons facteurs avec les bons niveaux de risque.

Pour renforcer la sécurité sans créer de points de friction, l'IDaaS implémente l'authentification MFA adaptative. Celle-ci examine les demandes de connexion individuelles grâce à des outils d'analyse fonctionnant en arrière-plan afin de déterminer le nombre de facteurs à demander et le niveau d'accès à accorder. À titre d'exemple, si un collaborateur travaille dans les locaux de l'entreprise et doit utiliser un badge intelligent pour passer les contrôles de sécurité avant de s'asseoir à son bureau, l'authentification MFA adaptative pourrait estimer qu'il se trouve dans un endroit sécurisé et ne demander que ses empreintes digitales pour la connexion au système. Toutefois, si ce même collaborateur travaille sur un appareil personnel depuis un café ou tout autre lieu public, l'authentification MFA adaptative l'invitera à entrer un facteur d'authentification supplémentaire.

Provisioning et workflows

Nous avons abordé jusqu'à présent trois éléments constitutifs de l'IDaaS : l'annuaire, qui conserve les données utilisateurs et les

configurations ; l'authentification unique (SSO), qui fluidifie l'accès des utilisateurs à des centaines de systèmes et d'applications ; et l'authentification multifacteur adaptative (MFA), qui renforce la sécurité des utilisateurs en définissant les accès aux applications en fonction du niveau de risque. Mais il reste un défi à relever : comment vous assurer que vos utilisateurs sont correctement ajoutés à votre annuaire IDaaS et provisionnés sur les systèmes dont ils ont besoin pour se connecter ? Le provisioning et les workflows relèvent de cette problématique.

À l'aide du provisioning, les entreprises peuvent utiliser l'IDaaS non seulement pour contrôler l'accès aux systèmes, mais aussi pour créer, mettre à jour et supprimer des comptes et des privilèges en fonction du statut de leurs utilisateurs. Le statut de l'utilisateur peut être défini directement dans l'annuaire IDaaS ou dans des systèmes tiers importants qui sont considérés comme sources fiables par l'entreprise (par exemple, la meilleure source pour les collaborateurs de l'entreprise pourrait être le SIRH).

Le provisioning automatise la gestion des comptes et des droits, en interne et en externe, ce qui permet de gagner du temps et d'argent. En moyenne, les entreprises gagnent 30 minutes sur chaque demande de provisioning d'applications, 30 minutes dans la détermination et la configuration des groupes et droits, et 20 $ par utilisateur pour préparer les audits annuels. Multiplié par les milliers de demandes de provisioning et les différents audits que doit traiter une entreprise chaque année, cela représente des économies et des gains de temps substantiels.

Toutefois, au-delà de l'aspect de gestion des comptes, les changements au niveau de l'identité doivent également déclencher certains processus dans les systèmes tiers. Voici deux scénarios à titre d'exemple :

- Martin intègre l'équipe de sécurité. En plus d'obtenir l'accès aux systèmes de sécurité, Martin doit suivre une formation de sécurité (par exemple, dans Udemy) et signer un document (peut-être dans Adobe Sign ou DocuSign) qui confirme qu'il a suivi et réussi cette formation.
- Yara, une cliente vivant en Allemagne, accède à votre application d'e-commerce et demande un document répertoriant toutes les données à caractère personnel collectées par votre marque à son sujet. Le Règlement général sur la protection des données (RGPD) de l'Union européenne exige que votre entreprise fournisse à Yara une copie de ses données dans les 30 jours.

Les workflows sont une fonctionnalité d'automatisation IDaaS qui va au-delà du provisioning des comptes et vous permet d'automatiser et d'orchestrer ces types de processus sans nécessiter l'écriture de code supplémentaire.

RAPPEL

L'IDaaS fournit tous les éléments constitutifs de l'IAM (annuaire ; SSO ; MFA adaptative ; provisioning et workflows) en un seul package cohérent pleinement opérationnel dès l'activation de votre abonnement. Cela vous permet de rentabiliser le service au plus vite et de privilégier les tâches importantes comme la configuration de la sécurité et l'amélioration de l'expérience utilisateur. Vous économisez aussi du temps et de l'argent plutôt que de les consacrer à l'installation, à la correction et à l'intégration de solutions disparates.

Ressources

Dans cette section, nous allons décrire certaines des principales ressources dont vous pouvez sécuriser l'accès et gérer l'identité à l'aide de l'IDaaS et de ses divers composants (annuaire ; SSO ; MFA adaptative ; provisioning et workflows).

Applications cloud

Il existe de nombreuses applications cloud, comme Microsoft 365, Salesforce, Amazon Web Services et Slack. En fait, le cloud devient le modèle prédominant de fourniture d'applications et supplante peu à peu les logiciels on-premise. Les solutions IDaaS modernes vous fournissent un catalogue d'intégrations préconfigurées, grâce auquel vous pouvez effectuer l'intégration de vos applications cloud en quelques minutes.

CONSEIL

Les intégrations entre solutions IDaaS et applications cloud suivent les prescriptions de normes ouvertes telles que SAML pour la fédération et SCIM (System for Cross-domain Identity Management) pour le provisioning.

CONSEIL

Okta dispose actuellement de plus de 6 000 intégrations d'applications préconfigurées.

Applications on-premise

Bien que les entreprises adoptent un nombre croissant d'applications et services cloud, la plupart conservent au moins certains systèmes sur site. Les solutions IDaaS modernes offrent des fonctionnalités permettant de sécuriser l'accès aux applications Web on-premise, à l'aide de modèles et de normes d'intégration sur site traditionnels tels que LDAP (Lightweight Directory Access Protocol), RADIUS (Remote Authentication Dial-In User Service), Kerberos et l'authentification header-based, sans nécessiter de changements au code source de l'application.

CONSEIL

Vous pouvez utiliser une seule solution IDaaS pour protéger tous vos systèmes, qu'ils soient on-premise ou dans le cloud, à l'aide des mêmes politiques de sécurité, ce qui vous assure un gain de temps et d'argent

tout en vous garantissant de disposer des dernières fonctions de sécurité.

Applications personnalisées

Comme l'a si bien écrit Mark Andreessen, fondateur de Netscape, il y a près de dix ans, « les logiciels dévorent le monde ». Chacune à son échelle, chaque entreprise repose sur les technologies et crée sa propre présence numérique, par le biais d'une application d'e-commerce par exemple. L'innovation logicielle est une mise de départ dans laquelle les entreprises investissent pour survivre dans l'économie mondiale hypercompétitive actuelle.

Il suffit d'observer votre propre entreprise. Combien de développeurs comptez-vous aujourd'hui, comparé à il y a seulement cinq ans ? Si votre entreprise est vraiment innovante, il est probable que le nombre, mais aussi le type de développeurs a augmenté (développeurs d'applications mobiles, experts en données, ingénieurs machine learning, etc.). Ils créent des applications personnalisées qui doivent être sécurisées, mais ils ne sont pas (et ne seront sans doute jamais) des experts en sécurité. Produire et publier une application non sécurisée, vulnérable aux prises de contrôle de compte ou aux compromissions d'identifiants peut coûter une fortune à une entreprise, voire l'amener à la faillite en raison des litiges, amendes et pénalités, mauvaise publicité, atteinte à l'image de marque, perte de confiance des clients et perte de chiffre d'affaires.

L'IDaaS fournit l'authentification unique (SSO) et l'authentification multifacteur (MFA) intégrées sous la forme de kits de développement de logiciels et d'API que les développeurs peuvent ajouter à leurs applications rapidement et facilement afin de pouvoir se consacrer à ce qu'ils font de mieux – créer des applications – tout en bénéficiant d'une sécurité aux performances irréprochables au niveau des composants que sont l'annuaire, la SSO, la MFA, le provisioning et les workflows.

Serveurs

Les logiciels doivent s'exécuter à un emplacement donné, généralement sur des serveurs qui peuvent être hébergés dans des lieux divers, par exemple un data center sur site, un cloud privé ou un cloud public tel qu'Amazon Web Services (AWS), Google Cloud Platform (GCP) ou Microsoft Azure. À l'aide d'architectures modernes et d'outils de développement d'applications tels que les microservices, les containers, l'informatique sans serveurs, Kubernetes et DevOps, le nombre des instances qui exécutent votre application peut varier dynamiquement en fonction de la charge. Par exemple, une nouvelle application pourrait être lancée sur seulement dix serveurs s'exécutant dans un cloud public et lorsqu'elle devient virale, s'exécuter sur plus de 1 000 serveurs d'une

infrastructure cloud pour traiter la charge. Imaginez si vous deviez vous-même sécuriser tous ces serveurs à mesure que leur nombre augmente ou diminue. Les solutions IDaaS modernes vous fournissent une méthode pour sécuriser automatiquement l'accès à tous vos serveurs et instances d'application.

API (Application Programming Interface)

Les API sont le carburant de tous ces logiciels qui dévorent le monde. On peut comparer une API à une application pouvant être consommée elle-même par d'autres applications ou par des terminaux intelligents de l'Internet des objets (IoT). Les API font gagner du temps aux développeurs en leur permettant d'utiliser des fonctions que d'autres ont déjà créées. Par exemple :

- utiliser Twilio pour envoyer des messages SMS sur un smartphone ;
- utiliser Stripe pour traiter des paiements par carte de crédit ;
- utiliser Google Analytics pour suivre les visites sur votre site Web.

En tant qu'entreprise, vous pouvez également participer à l'écosystème des API : créer vos propres API, les proposer à d'autres entreprises qui pourront les intégrer à leurs applications et gagner de l'argent grâce aux demandes. Par exemple, si vous êtes une société de transport, vous pouvez proposer une API qui sert à calculer le temps de livraison ou les frais d'expédition ou à demander des étiquettes d'expédition.

Les solutions IDaaS modernes sécurisent et autorisent l'accès aux API, en tirant parti de normes de sécurité d'API telles qu'OAuth (Open Authorization).

Et bien d'autres choses encore…

Il arrive parfois que des ressources informatiques nécessitent une authentification d'identité, mais ne soient pas classées comme une application cloud, une application on-premise, un serveur, une application personnalisée, ni même une API. Dans ce cas, vous pouvez tout de même bénéficier de la sécurité d'identité de l'IDaaS par le biais de normes ouvertes. Les modèles et normes ouverts sont utilisés dans de nombreux secteurs (notamment IT) pour fournir une intégration fluide entre systèmes.

Sans normes, tout serait beaucoup plus compliqué. Imaginez le casse-tête si chaque fabricant avait ses propres ampoules exclusives ne fonctionnant qu'avec ses lampes, ou si chacun de vos contacts avait un numéro d'une longueur différente.

Comme pour tout autre secteur, les services d'identité ont leurs normes. Il existe des normes d'identité pour tout : des annuaires (par exemple, LDAP) à l'authentification et la SSO (par exemple, SAML, RADIUS et

OIDC), en passant par le provisioning et les workflows (par exemple, SCIM, REST et Webhooks). L'IDaaS tire parti de ces normes pour prendre en charge une large gamme de systèmes.

RAPPEL

Les normes vous permettent d'implémenter les meilleures solutions de leur catégorie et d'éviter la dépendance à un fournisseur particulier et à ses solutions propriétaires. La dépendance vis-à-vis d'un éditeur limite la flexibilité de votre entreprise. Vous êtes obligé d'accepter le prix imposé pour la maintenance et le support, tout comme vous êtes limité aux fonctionnalités qu'il ajoute (pour autant qu'il en ajoute). Et si vous en avez assez, le coût de l'adoption d'une autre solution peut s'avérer prohibitif ou problématique, notamment lorsqu'il s'agit de migrer toutes les données de l'ancien système vers le nouveau.

CONSEIL

Pour en savoir plus sur les normes et l'intégration, téléchargez l'eBook d'Okta sur l'intégration aux applications d'ancienne génération, à la page `okta.com/resources/whitepaper-integration-patterns-for-legacy-applications`, et consultez le blog d'Okta à la page `okta.com/blog`.

Autres facteurs à prendre en compte

La gestion des identités est un composant essentiel à la bonne marche de votre IT. Sans elle, vos collaborateurs perdent l'accès à de multiples ressources. Et si votre solution de gestion des identités n'est pas sécurisée, votre entreprise tout entière est exposée à des risques importants. Pour choisir une solution IDaaS fiable, qui vous préserve de la dépendance vis-à-vis des fournisseurs, vous devez prendre en compte des facteurs supplémentaires. Parmi eux, on peut citer les intégrations, la neutralité, la sécurité et la confidentialité, la conformité et la disponibilité.

Intégrations

Les intégrations de logiciels tiers sont un élément clé à prendre en compte pour les entreprises qui recherchent une solution IDaaS. Un large écosystème d'intégrations vous aide à activer l'authentification unique (SSO) de manière fluide, à éviter les relations de dépendance et à mieux tirer parti des applications et systèmes informatiques en place. Une solution IDaaS doit prendre en charge les applications que vous utilisez, mais aussi celles que vous envisagez d'adopter, par le biais d'un catalogue d'intégrations. Elle doit aussi proposer une riche panoplie d'intégrations au-delà de l'authentification SSO, notamment :

- **Connexion et provisioning –** La solution IDaaS doit vous permettre de contrôler le provisioning et l'accès des applications, telles que Box, Microsoft 365, Salesforce, ServiceNow, Slack et Zoom,

en quelques minutes. Il est recommandé que l'intégration aille au-delà de l'authentification SSO et prenne en charge le provisioning, l'offboarding, les intégrations avancées via les workflows, la gestion des terminaux et la gestion des licences.

- **Systèmes de gestion des ressources humaines (SIRH) –** Connectez-vous aux systèmes RH tels que Workday et SuccessFactors pour automatiser l'onboarding/offboarding des collaborateurs.
- **Contrôleurs de mise à disposition d'applications (ADC) –** Connectez les utilisateurs externes aux ADC on-premise tels que Citrix, F5 et Akamai.
- **Sécurité réseau –** Étendez la SSO et la MFA aux solutions de sécurité réseau telles que Cisco, Check Point, Palo Alto Networks et ZScaler.
- **Analyse de la sécurité –** Bénéficiez d'une visibilité complète pour l'étendre au cloud, aux mobiles et aux systèmes on-premise pour plus de corrélation et une mise en application plus homogène des politiques d'entreprise. Citons par exemple LogRhythm, Rapid7, QRadar et Splunk.

CONSEIL

Okta publie son catalogue d'applications sur son site, à la page `www.okta.com/okta-integration-network`.

Neutralité

Dans une solution IDaaS moderne, utiliser des normes ouvertes et fournir des intégrations est important, mais pas suffisant. Un fournisseur de services IDaaS doit être neutre. En d'autres termes, votre fournisseur de services doit fournir la preuve irréfutable qu'il ne privilégie pas les solutions d'un certain fournisseur, ce qui vous rendrait indirectement dépendant de ce dernier. Par exemple, Microsoft, NetSuite, Salesforce et Zoho (que nous classons dans l'ordre alphabétique dans un souci de neutralité, nous aussi) fournissent tous un excellent logiciel de gestion de la relation client et sont tous concurrents. Une solution IDaaS moderne doit prendre en charge le plus grand nombre d'options logicielles possibles dans une catégorie donnée.

CONSEIL

Recherchez chez un fournisseur IDaaS de pointe les signes de neutralité suivants :

- Un vaste écosystème d'intégrations natives de systèmes informatiques et logiciels (au moins 5 000)
- Des intégrations avancées, même avec des produits concurrents de fournisseurs offrant une solution particulière
- Une prise en charge étendue des normes ouvertes du secteur

CONSEIL

Okta prend en charge un vaste éventail de fournisseurs et de solutions, répertoriés à la page `www.okta.com/oin`.

Sécurité et confidentialité

Aujourd'hui, la sécurité et la confidentialité sont des priorités pour toute entreprise et votre fournisseur IDaaS n'y fait pas exception. Recherchez chez votre fournisseur IDaaS les garanties de sécurité et de confidentialité suivantes :

- Documentation sur ses contrôles de sécurité (c'est-à-dire, confidentialité, intégrité et disponibilité).
- Prise en charge d'un modèle de responsabilité partagée au niveau du cloud, définissant clairement ses responsabilités et les vôtres.
- Documentation, bonnes pratiques et fonctionnalités produits qui vous aident à sécuriser votre instance du service.
- Références bien établies en matière de sécurité et de confidentialité. Il convient que votre fournisseur IDaaS fournisse des outils et éléments de preuve tels que des portails d'approbation, programmes publics de Bug Bounty (chasse aux bugs) et tests de sécurité automatisés.
- Possibilité de mettre à l'épreuve la sécurité de sa plateforme et sa solution IDaaS.
- Certifications telles que CSA (Cloud Security Alliance), STAR (Security Trust Assurance and Risk), FedRAMP (Federal Risk and Authorization Management Program), ISO 27001, et SOC 2 Type 2.

CONSEIL

Pour plus d'informations sur le service de sécurité d'Okta, consultez le livre blanc à la page `www.okta.com/resources/whitepaper-okta-security-technical-white-paper`.

Conformité

Selon les secteurs, les entreprises sont soumises à des contraintes de conformité différentes. Vérifiez que votre solution IDaaS répond aux exigences réglementaires ou normes industrielles qui peuvent être en vigueur pour votre entreprise. Citons par exemple le RGPD (règlement général sur la protection des données) de l'Union européenne, les législations américaines telles que les lois SOX (Sarbanes-Oxley) ou HIPAA (Health Insurance Portability and Accountability Act), la norme de sécurité des transactions de paiement PCI DSS ou la norme ISO 27001.

CONSEIL

Pour en savoir plus sur l'approche de la conformité et les certifications d'Okta, consultez la page `trust.okta.com/compliance`.

EXEMPLE D'IDAAS : OKTA

Okta Identity Cloud est la plateforme IDaaS créée et gérée par Okta. En tant que service cloud natif, c'est-à-dire conçu pour le cloud et hébergé à 100 % dans le cloud, le service d'Okta fournit notamment les avantages essentiels suivants :

- Il est disponible partout dans le monde, totalement multitenant, sans état et redondant.
- Il est régulièrement mis à jour par l'ajout de nouvelles fonctions et des améliorations des mesures de sécurité.
- Il assure une indisponibilité planifiée de zéro ; Okta met à jour sa plateforme à la volée et ne planifie pas d'indisponibilité pour la maintenance.
- Il réduit drastiquement les activités opérationnelles et les coûts de configuration et de maintenance.
- Il est disponible sur abonnement et offre une tarification flexible.

Ces avantages sont rarement présents dans les logiciels on-premise, les services cloud gérés ou chez les fournisseurs qui transfèrent sur le cloud des logiciels on-premise existants.

La plateforme Okta Identity Cloud comprend à la fois les produits de *gestion de l'identité des collaborateurs* et des produits de *gestion de l'identité des clients*.

Identité des collaborateurs

Les produits de gestion de l'identité des collaborateurs sont conçus à l'intention des dirigeants des équipes IT et sécurité. À un très haut niveau, ils simplifient le mode de connexion aux technologies de l'entreprise tout en augmentant l'efficacité et en renforçant la sécurité des environnements IT. Parmi ces solutions :

- **Universal Directory –** Personnalisez, organisez et gérez n'importe quel ensemble d'attributs utilisateurs provenant de sources d'identités multiples grâce à un référentiel d'utilisateurs cloud flexible.
- **Single Sign-On –** Libérez vos collaborateurs des mots de passe multiples. Un jeu d'identifiants unique leur donne accès aux applications d'entreprise dans le cloud, on-premise et sur mobiles.
- **Lifecycle Management –** Automatisez les processus d'onboarding/offboarding des utilisateurs grâce à une communication fluide entre les annuaires tels qu'Active Directory et LDAP et les applications cloud telles que Workday, SuccessFactors, Microsoft 365 et RingCentral.

- **Adaptive Multi-Factor Authentication –** Sécurisez vos applications et réseaux VPN en tirant parti d'un solide framework de politiques robustes, d'une série complète de facteurs d'authentification avancés et d'une authentification adaptative basée sur les risques qui s'intègre à toutes vos applications et à votre infrastructure.

Grâce aux solutions de gestion de l'identité des collaborateurs, l'équipe IT peut centraliser la gestion reposant sur les politiques qui régit quels utilisateurs ont accès aux applications critiques et aux données qui alimentent les processus métier fondamentaux.

Les collaborateurs tirent parti d'une page d'accueil à authentification unique qui leur simplifie la vie et réduit les risques de sécurité dus à la mauvaise gestion des mots de passe. Grâce à Okta, ils n'ont plus à recourir à des pratiques risquées de mémorisation de mots de passe – par exemple, en choisissant des mots de passe évidents ou réutilisés, en les notant sur des Post-it ou en les sauvegardant dans des fichiers Excel sur leurs ordinateurs portables.

Identité des clients

Les produits de gestion de l'identité des clients vous permettent d'intégrer Okta en tant que couche d'identité sur vos applications ou de personnaliser Okta pour :

- **Fournir une expérience utilisateur personnalisable –** Tirez parti des API et des widgets d'Okta pour créer des flux de connexion propres à votre marque et des portails à l'intention des utilisateurs. Vous pouvez même utiliser les API d'Okta pour créer une expérience d'administration personnalisée, en vertu de laquelle les clients ou chefs de service peuvent gérer leurs utilisateurs.
- **Étendre Okta à n'importe quel cas d'usage –** Relevez tout défi d'intégration complexe d'identités, de données ou d'automatisation en tirant parti de la large gamme d'API d'Okta. Exécutez des scripts pour modifier les données utilisateurs, intégrer automatiquement les applications ou effectuer l'intégration aux workflows.
- **Tirer parti de solutions IAM client (CIAM) de pointe –** Libérez vos développeurs pour qu'ils se focalisent sur l'expérience client et confient à Okta les tâches liées à l'identité. Tirez parti d'Okta comme d'une « API d'identité » pour tous vos projets de développement d'applications, Okta s'occupant de l'authentification, de l'autorisation et de la gestion des utilisateurs.

Les produits de gestion de l'identité des clients fournissent un accès par programmation à Okta Identity Cloud, ce qui permet à vos développeurs

(suite)

(suite)

de créer des expériences utilisateurs de haut niveau et d'étendre Okta en laissant libre cours à leur imagination. En renforçant la gestion des identités côté clients de votre entreprise numérique, Okta peut relever vos défis d'architecture d'entreprise les plus complexes.

Les entreprises qui adoptent le service Okta améliorent considérablement la sécurité et l'expérience des utilisateurs qui interagissent avec leurs applications, qu'il s'agisse de collaborateurs, de prestataires ou de clients, qu'ils utilisent un service cloud, une application on-premise, un VPN, un pare-feu ou une application personnalisée.

Disponibilité

Un fournisseur IDaaS doit garantir que le service est toujours disponible pour que les collaborateurs et clients de votre entreprise puissent se connecter à tout moment, où qu'ils se trouvent et depuis n'importe quel terminal.

Privilégiez un fournisseur IDaaS qui dispose d'une architecture cloud robuste, d'accords sur les niveaux de service (SLA) qui répondent à vos exigences métier et d'un tableau de bord public avec une surveillance en temps réel et des informations d'état sur le service.

CONSEIL

Okta publie la disponibilité de ses services en temps réel à la page `trust.okta.com`.

DANS CE CHAPITRE

- Adoption du Zero Trust
- Identité décentralisée et auto-souveraine
- Internet des objets (IoT)
- Contraintes et obligations liées à la confidentialité
- Liberté dans le choix des applications de pointe

Chapitre 4
L'avenir proche de l'identité

Dans ce chapitre, nous aborderons l'évolution de l'identité dans un avenir plus ou moins proche et nous verrons comment une solution de gestion des identités avancée vous aide à rester à la pointe de l'innovation.

Zero Trust

L'omniprésence du mobile et du cloud a rendu pratiquement obsolète la notion traditionnelle de périmètre réseau, en vertu de laquelle le réseau interne est considéré « digne de confiance », contrairement au réseau externe qui ne l'est pas. Dans cette nouvelle réalité, les entreprises doivent permettre un accès sécurisé à leurs utilisateurs indépendamment de l'emplacement, du terminal ou du réseau.

Pour relever ces défis, l'analyste du bureau d'études Forrester Research John Kindervag a introduit pour la première fois en 2010 le cadre de sécurité Zero Trust. Ce modèle se fonde sur le principe « ne jamais faire confiance, toujours vérifier », imposant d'une part que les bonnes personnes aient le bon niveau d'accès aux bonnes ressources dans le bon contexte, et d'autre part, que l'accès soit constamment évalué. La gestion des identités et des accès (IAM) est donc une technologie fondamentale dans le modèle Zero Trust et doit constituer un point de départ pour les entreprises souhaitant implémenter celui-ci.

CONSEIL

Forrester Research a nommé Okta au rang de « leader » dans son rapport *The Forrester Wave: Zero Trust eXtended Ecosystem Platform Providers* (4e trimestre 2019) et lui a décerné la note maximale dans la moitié des catégories d'évaluation.

Identité décentralisée et auto-souveraine

Dans un modèle d'identité décentralisée et auto-souveraine, les individus gèrent eux-mêmes leur identité numérique et exercent un plus grand contrôle sur leurs comptes et données. Une identité auto-souveraine comporte trois éléments : une *déclaration d'identité*, que la personne utilise pour définir son identité ; des *preuves* (tel qu'un bloc dans une blockchain) qui permettent de confirmer la validité de la déclaration ; et une *attestation*, dans laquelle un système valide la déclaration en fonction de la preuve présentée.

Un exemple courant d'identité auto-souveraine est aujourd'hui Apple FaceID, qui est utilisé sur les iPhones pour accéder au téléphone, effectuer des achats en ligne et se connecter aux applications. La déclaration d'identité est enregistrée localement sur le téléphone lors de la configuration initiale de FaceID par le propriétaire de l'iPhone. La preuve est constituée par l'ensemble des caractéristiques faciales propres à l'utilisateur, qui ont été enregistrées précédemment avec la déclaration d'identité dans le cadre du processus de configuration, et l'attestation est la vérification automatisée du logiciel de FaceID de la déclaration d'identité et de la preuve.

Internet des objets (IoT)

L'Internet des objets (IoT, Internet of Things) désigne le réseau de terminaux intelligents qui sont intégrés aux composants électroniques, aux logiciels, aux capteurs et à la connectivité réseau pour activer des fonctionnalités avancées. Bien que l'Internet des objets fournisse de nombreuses innovations, il présente également un risque énorme pour le contrôle d'accès et les données.

Quelles sont donc les conséquences de l'Internet des objets pour l'IAM ? Il est clair que les objets connectés doivent être correctement identifiés et authentifiés, et le cloud est la seule plateforme qui fournit l'évolutivité robuste nécessaire pour prendre en charge les services d'annuaire et le contrôle d'accès de dizaines de milliards de terminaux dans le monde.

CONSEIL

Il s'avère également que l'Internet des objets peut faire partie de la solution. Les solutions IDaaS peuvent tirer parti d'objets connectés personnels tels que l'Apple Watch en tant que facteur d'authentification

multifacteur adaptative (MFA), en fournissant des notifications push pour authentifier les demandes d'accès.

Obligations de confidentialité à l'échelle mondiale

Les réglementations sur la confidentialité comme le Règlement général sur la protection des données (RGPD) de l'Union européenne, le California Consumer Privacy Act (CCPA) et l'Australian Privacy Principles (APP) ont renforcé les droits des citoyens et les obligations des entreprises, avec les problèmes de conformité que cela entraîne pour ces dernières.

Une modalité de nombreuses réglementations sur la protection des données est l'exigence en matière de données de consentement (accords juridiques, informations marketing, etc.) qui doivent être collectées, revues périodiquement, reconfirmées par les consommateurs et fournies dans un but de traitement spécifique. De plus, quand le consentement est donné, les entreprises doivent s'assurer que seules les données minimales requises sont collectées et qu'elles ne sont utilisées qu'à des fins de traitement autorisées et légitimes. Et pour compliquer encore les choses, certains consentements (comme les demandes marketing) peuvent être révoqués par l'utilisateur tandis que d'autres, comme les accords juridiques, ne le peuvent pas.

La gestion du consentement exige que les entreprises effectuent le suivi de multiples réglementations et données client enregistrées dans de multiples systèmes et bases de données. Des solutions comme les plateformes de données clients et l'IDaaS aident à agréger les données des clients et simplifient la gestion du consentement sur de multiples systèmes de traitement.

CONSEIL

De plus en plus de pays renforcent leurs exigences en matière de consentement, dont la gestion nécessite des solutions assurant la confidentialité des données à l'échelle mondiale.

Identité et liberté dans le choix des applications

À mesure que l'écosystème des logiciels d'entreprise s'agrandit et se diversifie, les entreprises explorent les possibilités qui s'offrent à elles, à la recherche d'applications répondant aux besoins de leurs collaborateurs et susceptibles d'en améliorer l'efficacité, tout en préservant le contrôle et la sécurité. Elles déploient de plus en plus d'applications spécialisées telles que Slack et Zoom, mais aussi des suites complètes comme Microsoft 365, et ce, même si leurs fonctionnalités font double emploi.

CONSEIL

En juin 2019, plus de 77 % des clients d'Okta disposant d'Office 365 avaient également adopté des applications spécialisées de pointe comme Slack, Zoom, Box, AWS, Salesforce et G Suite, et ce nombre est en croissance constante. Entre octobre 2018 et juin 2019, l'adoption de Zoom a augmenté de 25 % auprès des utilisateurs d'Office 365, la plus importante progression enregistrée pour une application individuelle au sein de la clientèle d'Okta. Slack a également connu une croissance à deux chiffres chez les clients d'Office 365, passant de 11 à 31 %, révélant une concurrence féroce entre les applications de collaboration en entreprise.

Mais si les applications leader du marché font souvent l'objet d'une adoption rapide, l'aspect de l'identité et de l'accès peut s'avérer un obstacle majeur. Pour promouvoir les applications novatrices et éviter l'exclusivité d'un fournisseur, les utilisateurs ont besoin d'une solution IDaaS qui sécurise l'accès à toutes les applications, quels que soient leurs éditeurs.

L'IDaaS, une solution d'avenir

Le monde est en mutation constante, mais une chose est sûre : les innovations de l'IT, les cybermenaces et les méthodes de sécurisation des identités vont continuer à se développer. L'IDaaS est parfaitement conçu pour gérer les changements actuels et à venir. Contrairement aux solutions de gestion des identités et des accès d'ancienne génération, l'IDaaS :

- prend en charge le modèle Zero Trust, en sécurisant l'accès des utilisateurs indépendamment de l'emplacement, du terminal ou du réseau ;
- prend en charge des normes ouvertes et peut se connecter aux systèmes qui fournissent une identité auto-souveraine ;
- sécurise et autorise l'accès aux API utilisées par des terminaux intelligents et s'adapte aux besoins de l'Internet des objets ;
- agrège les données clients et simplifie la gestion du consentement sur de multiples systèmes ;
- offre une grande liberté au niveau des identités pour que les entreprises puissent adopter les meilleures technologies du marché et éviter de s'enfermer dans une relation exclusive avec un fournisseur.

RAPPEL

Avec l'IDaaS, vous disposez d'un élément charnière au sein de votre environnement grâce auquel votre entreprise peut établir des connexions simples et flexibles à des technologies novatrices, dès aujourd'hui et à l'avenir.

PERSONAL CAPITAL GÈRE SON ENVIRONNEMENT CLOUD

Personal Capital propose une « approche high-tech de l'investissement personnel qui tient compte du capital humain ». Elle apporte de la clarté financière et de la confiance en combinant la puissance des technologies et l'intelligence de ses équipes. En février 2019, la société gérait plus de 9 milliards de dollars d'actifs et plus de 2 millions de comptes clients.

Pour soutenir la croissance et l'ampleur des activités tout en préservant la sécurité des données financières, Personal Capital recourt à une architecture cloud robuste. Au départ, la stratégie de gestion des identités de l'entreprise était beaucoup trop complexe, selon Maxime Rousseau, responsable de la sécurité des systèmes d'information.

Relever les défis pour créer une infrastructure d'accès Zero Trust

Personal Capital exécute à la fois des applications d'interface client et des services d'arrière-plan sur Amazon Web Services (AWS). Après le déploiement d'Okta, l'étape suivante consistait à sécuriser l'accès à son infrastructure cloud.

L'équipe de Personal Capital s'est engagée à appliquer le modèle Zero Trust de Forrester, selon lequel l'accès est accordé en fonction de conditions dynamiques en temps réel pour les utilisateurs et terminaux. « Nous sommes une entreprise moderne sans périmètre traditionnel qui privilégie le cloud et nous sommes convaincus que c'est la bonne méthode pour garantir la sécurité », explique Maxime Rousseau.

Toutefois, assurer ce niveau de surveillance n'a pas été chose facile. « Nous avons dû relever le défi de fournir dynamiquement les bonnes identités, les bons rôles, les bons groupes et les bonnes clés SSH publiques, tout en augmentant ou réduisant les capacités de l'infrastructure selon les besoins », ajoute Maxime Rousseau. Sans une couche unifiée de contrôle d'accès, l'équipe devait créer son propre tissu de connexion ou ajouter des technologies d'accès, ce qui présenterait des problèmes d'adoption, de compatibilité et d'adaptation aux besoins.

Une acquisition propice et opportune

Pour tirer parti de la pile d'authentification d'Okta, l'équipe de Personal Capital a choisi ScaleFT et son produit Zero Trust Server Access, qui a été intégré à Okta pour fournir des fonctionnalités de provisioning dynamique. ScaleFT a permis aux équipes des opérations, de sécurité, de traitement des données et d'ingénierie de Personal Capital de bénéficier d'une méthode transparente et sécurisée pour accéder à l'infrastructure critique d'AWS.

(suite)

(suite)

À l'époque, ScaleFT s'engageait dans le processus officiel de vérification de son intégration à Okta et la société avait besoin d'un client disposant à la fois des solutions Okta et ScaleFT pour confirmer que l'intégration fonctionnait conformément à la documentation. Personal Capital s'est portée volontaire au rôle de ce client des deux sociétés et a contribué à finaliser la vérification menée par Okta sur ScaleFT. « Nous avons été l'un des premiers clients à établir le lien entre ces deux parties », a déclaré Maxime Rousseau.

Après la vérification, Okta a encore renforcé ce partenariat et annoncé en juillet 2018 que l'entreprise allait acquérir ScaleFT pour étendre les services d'identité aux ressources d'infrastructure et accélérer la transition vers le Zero Trust.

Cette annonce a été accueillie avec enthousiasme par l'équipe de Personal Capital. Aujourd'hui, le produit ScaleFT Server Access a pris le nom d'Okta Advanced Server Access. Il optimise les workflows d'authentification Okta pour les serveurs Linux et Windows via SSH et RDP (Remote Desktop Protocol) de Microsoft.

Zero Trust, en toute simplicité et sécurité

« Okta Advanced Server Access a été le bon choix pour Personal Capital, car il simplifie l'accès sécurisé aux serveurs tout en évitant le recours à des technologies supplémentaires, à une intégration manuelle et à des clés statiques », ajoute Maxime Rousseau. En répondant à toutes les exigences en matière de politiques à l'aide d'une seule technologie, Personal Capital évite les intégrations manuelles peu fiables.

Advanced Server Access fournit une architecture Zero Trust qui protège l'infrastructure critique de l'entreprise. « Comme Personal Capital, Okta considère que tout est une question d'identité, affirme Maxime Rousseau. Advanced Server Access lie les terminaux utilisateurs à des sessions authentifiées, et nous avons donc la garantie supplémentaire que chaque terminal et chaque collaborateur sont systématiquement dignes de confiance ».

Advanced Server Access supprime la plupart des tâches opérationnelles associées à l'infrastructure. « Nous n'avons plus à nous soucier de la synchronisation des comptes, ni du vol et/ou du détournement de données d'identification statiques, explique Maxime Rousseau. Nous pouvons voir qui a accédé à quoi, depuis quel poste et quand ».

Alors que Personal Capital conforte sa place de leader dans le segment de la gestion numérique des biens, Maxime Rousseau est confiant que les infrastructures de la société sont prêtes. « Avec l'aide d'Okta qui s'occupe de la gestion des identités et des accès, nous disposons d'un socle sécurisé et évolutif qui soutient notre croissance, dit-il. Okta s'est avéré le bon choix ».

DANS CE CHAPITRE

- **Préserver la simplicité de l'identité et la neutralité vis-à-vis du fournisseur**
- **Aller au-delà du contrôle d'accès pour tous les utilisateurs**
- **Tirer parti des avantages des services cloud**
- **Remplacer les produits d'ancienne génération par une solution évolutive, sécurisée et conviviale**
- **Préparer l'avenir**

Chapitre 5
Dix atouts de l'IDaaS

Voici les dix principaux avantages et caractéristiques d'une solution IDaaS (Identity-as-a-Service) de pointe.

- **Elle est simple à déployer et utiliser.** Une solution IDaaS hébergée dans le cloud permet de déployer une solution de gestion des identités et des accès (IAM) en quelques heures et de l'intégrer à des applications en quelques minutes, plutôt qu'en plusieurs semaines. Lorsque vous souscrivez votre abonnement, elle est déjà pleinement opérationnelle. Aucune installation sur serveur n'est nécessaire.
- **Elle ne privilégie aucun fournisseur.** L'IDaaS s'intègre universellement à toutes les applications. Elle prend en charge les applications cloud et on-premise, les applications personnalisées, les applications mobiles, les serveurs et les API par le biais d'un catalogue comptant plus de 6 000 intégrations préconfigurées, ce qui vous protège de toute dépendance vis-à-vis d'un seul fournisseur.
- **Elle dépasse largement le cadre du contrôle d'accès.** L'IDaaS fournit de multiples services en une seule solution. Parmi eux, on peut citer le stockage des données utilisateurs, les demandes d'accès et la récupération de comptes en libre-service, l'automatisation du provisioning et des clôtures de comptes, l'implémentation de workflow et la simplification des audits de

sécurité. Ces fonctionnalités éliminent les tâches manuelles effectuées par les équipes IT, ce qui réduit globalement les coûts.

- **Elle prend en charge tous les utilisateurs.** L'IDaaS peut gérer tous les utilisateurs sur une seule plateforme. Elle réduit le nombre de systèmes et fournisseurs nécessaires pour sécuriser les identités ainsi que le nombre d'intégrations dont une application a besoin pour supporter tous les utilisateurs.
- **Elle permet le paiement à l'usage.** L'IDaaS fonctionne sur abonnement. Vous payez selon vos besoins. Vous pouvez adapter rapidement le nombre de licences en fonction de l'évolution de votre entreprise, ce qui offre une grande flexibilité en termes de coûts.
- **Elle est toujours active et à jour.** Le prestataire met régulièrement l'IDaaS à jour en appliquant les améliorations de sécurité et en ajoutant les nouvelles fonctions, sans indisponibilité. De plus, le service est accessible en temps réel sur un tableau de bord en ligne, ce qui vous permet de vous consacrer à des projets stratégiques au lieu de corriger manuellement les systèmes.
- **Elle permet de sortir des solutions existantes.** L'IDaaS remplace de nombreuses solutions de gestion des identités existantes – de LDAP, Microsoft Active Directory et Active Directory Fédération Services (ADFS) jusqu'aux serveurs SSO et MFA on-premise. Le remplacement de ces systèmes par un service unifié vous fait gagner du temps et de l'argent en termes de gestion des fournisseurs, d'achats, d'intégrations manuelles, de correction, de maintenance et de support.
- **Elle est évolutive et flexible.** L'IDaaS s'adapte dynamiquement à la demande ; vous n'aurez donc pas besoin de prévoir, d'installer et de corriger l'infrastructure pour suivre la croissance de votre entreprise dans les années à venir.
- **Elle est conviviale.** Les utilisateurs peuvent accéder aux systèmes à partir d'un seul tableau de bord, via leur navigateur ou une application mobile, le tout sans utiliser de nombreux mots de passe ni des systèmes supplémentaires tels que les VPN.
- **Elle est pérenne.** L'identité est un composant essentiel de nombreuses innovations, notamment le Zero Trust, l'Internet des objets (IoT), la confidentialité et la liberté dans le choix du fournisseur. (Pour en savoir plus, reportez-vous au chapitre 4.) Votre entreprise ne peut lancer aucun de ces projets sans une plateforme IDaaS capable d'évoluer pour pallier les incertitudes de l'avenir.

Le leader de la gestion des identités et des accès

okta

okta.com/fr

Découvrez l'avenir de la gestion des identités

Les solutions IAM (Identity and Access Management) permettent aux entreprises de renforcer leur sécurité et de gérer les identités et les accès rapidement et en toute confiance. Pour tirer parti de leurs avantages à grande échelle, nombre d'entreprises les adoptent sous la forme de services cloud : on parle alors d'IDaaS (Identity-as-a-Service). L'IDaaS constitue une solution IAM robuste et évolutive permettant de sécuriser et de gérer les accès de tout utilisateur, où qu'il se trouve dans le monde et quel que soit le terminal qu'il emploie. Grâce à ce livre, vous découvrirez les principaux aspects de la gestion des identités avancée et ce que peut apporter une solution IDaaS à votre entreprise.

À l'intérieur…

- Relever les défis de la gestion des identités
- Sécuriser l'accès avec l'authentification unique (SSO) ou multifacteur (MFA)
- Automatiser le provisionnement de comptes
- Sécuriser les applications cloud et on-premise, les applications mobiles et personnalisées, les serveurs et les API
- Renforcer la sécurité et la conformité
- Adopter une architecture Zero Trust

okta

Lawrence C. Miller est expert informatique depuis plus de 25 ans et a rédigé près de 200 ouvrages de la collection « Pour les nuls ».

Frederico Hakamine est Technical Product Manager chez Okta. Il se consacre au développement de code et à la promotion de la plateforme et des API Okta.

Allez sur Dummies.com®
pour voir des vidéos, des exemples pas à pas, des articles pratiques, ou pour faire des achats !

ISBN : 978-1-119-77029-9

pour les nuls®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.