Top 8
des challenges liés à la gestion des identités et des accès (IAM)

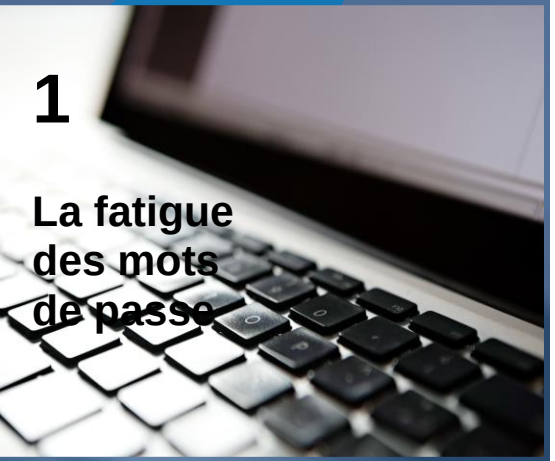
okta

L'importance de l'identité pour les applications cloud (SaaS)

La révolution cloud pour les entreprises est en cours depuis quelques années. Les organisations IT du monde entier, qu'il s'agisse de petites et moyennes entreprises ou de sociétés figurant dans le Fortune 500, passent d'un système basé sur des logiciels on-premises (stockés sur site) à des services cloud à la demande. À mesure que l'IT opère cette transition vers une nouvelle configuration, hybride ou 100% cloud, il devient crucial de savoir gérer l'identité des individus qui ont accès à toutes ces applications et le type d'accès que l'on souhaite leur accorder. À cet égard, les responsables de l'information et leurs équipes sont confrontés à un nouvel ensemble de défis relatifs à la gestion des identités. En outre, il faut parvenir à aider les utilisateurs à gérer la multitude d'URL, de noms d'utilisateurs et de mots de passe... Le rôle de l'IT change donc en profondeur. En tant que coordinateur de ces nouveaux services, l'IT doit être en mesure d'apporter des conseils en matière de Software-as-a-Service (SaaS) pour s'assurer que la société tire tout le potentiel de la valeur commerciale de ses investissements.

Il existe huit principaux défis dans le domaine de la gestion des identités et des accès (IAM) associés à l'adoption et au déploiement d'applications SaaS / Cloud, ainsi que des bonnes pratiques pour faire face à chacun d'entre eux.

Crédit image : fuyu liu / Shutterstock Inc.



1

La fatigue des mots de passe

Crédit image : MJTH / Shutterstock Inc.

Bien que le modèle SaaS facilite en soi l'accès aux applications, en permettant une connexion en tout lieu, la complexité augmente rapidement avec le nombre d'applications. Chaque application a des exigences en termes de mots de passe et des cycles de vie bien différents. La variété des règles associées aux mots de passe mène à une réduction de productivité chez l'utilisateur, et à une plus grande frustration causée par la perte de temps à réinitialiser, essayer de se souvenir et gérer sans arrêt les mots de passe et les URL, qui changent tout le temps sur toutes leurs applications.

Un sujet qui devrait inquiéter encore davantage l'IT, c'est celui des risques sur la sécurité, causés par ces mêmes utilisateurs, qui réagissent à cette « fatigue de mots de passe » en utilisant des mots de passe trop évidents ou en utilisant le même sur plusieurs plateformes, en les écrivant sur un post-it ou en les enregistrant sur un fichier Excel sur leur ordinateur.

Les services IT gérant l'IAM peuvent éliminer ces risques en mettant en place une authentification unique (ou SSO, pour Single Sign-On) sur l'ensemble des applications. Ils mettent ainsi à disposition de leurs utilisateurs une plateforme unique depuis laquelle ils peuvent accéder à toutes leurs applications grâce un seul identifiant et un seul mot de passe.

Et dans le meilleur des cas, le système de gestion des identités choisi par l'IT peut permettre à plusieurs départements de l'entreprise de de gérer les identités et les accès aux applications, qu'elles soient sur site ou cloud.

La majorité des entreprises utilisent Microsoft Active Directory (AD) comme annuaire des utilisateurs de référence, qui régit l'accès aux services IT de base comme les boites e-mail et le partage de fichiers. AD est également souvent utilisé pour contrôler l'accès à une plus large gamme d'applications et de systèmes IT. Sachant cela, il est préconisé de choisir une solution IAM qui est mesure de se connecter à Active Directory, et ainsi de permettre aux utilisateurs de continuer à utiliser leurs identifiants AD pour accéder à leurs applications SaaS quotidiennes. La mise en place de cette connexion est aussi un pari d'avenir : elle augmente la probabilité que les utilisateurs puissent bénéficier au fur et à mesure des dernières et des meilleures applications SaaS que leur entreprise pourrait leur fournir.

2 Les processus de provisioning et de déprovisioning manuels, complexes et peu fiables

Crédit image : javarman / Shutterstock Inc.

Lorsqu'un nouvel employé débute dans une entreprise, l'IT lui fournit souvent un accès au réseau d'entreprise, aux serveurs de fichiers, à une boîte e-mails et aux imprimantes. De nombreuses applications cloud sont gérées directement par les métiers (par exemple, les Sales Operations gèrent salesforce.com, la comptabilité gère Concur, le marketing gère Marketo, etc.), et l'accès à ces applications est souvent déterminé séparément par l'administrateur de l'application, plutôt que par l'IT.

En raison de leur nature même (« As-a-Service », soit « à la demande »), les apps SaaS devraient être synonymes de provisioning simple. Le service de gestion des identités et des accès devrait pouvoir automatiser le provisioning de nouvelles applications SaaS, comme extension directe du processus d'accueil existant. Lorsqu'un utilisateur est ajouté au répertoire central (comme Active Directory), son appartenance à certains groupes devrait suffire à lui garantir un provisioning automatique pour toutes les applications inhérentes à son métier, et lui fournir les permissions et le niveau de sécurité nécessaires.

Il va sans dire que le sujet devient encore plus complexe lorsqu'il s'agit du départ d'un collaborateur. L'IT peut bien sûr résilier de manière centralisée l'accès aux e-mails et aux réseaux, mais il dépend d'administrateurs divers pour ce qui est de résilier l'accès aux application métiers SaaS. Cela rend l'entreprise vulnérable, car les applications et les données commerciales critiques sont alors amenées à rester entre les mains d'anciens collaborateurs, potentiellement mal intentionnés. C'est le genre de failles typiques que recherchent les responsables d'audit au sein des process de déprovisioning.

Une solution d'IAM ne doit pas seulement permettre à l'IT d'ajouter automatiquement de nouvelles applications, elle doit également fournir à minima les éléments suivants :

- Un provisioning automatisé des utilisateurs sur toutes les applications, qu'elles soient on-premises ou cloud,
- Une intégration complète et en profondeur avec Active Directory.
- Des traces claires pour tout besoin d'audit.

Il s'agit de garantir aux organisations une tranquillité d'esprit en leur apportant la certitude qu'une fois que le collaborateur ne fait plus partie de l'entreprise, les données de l'entreprise ne partent pas avec lui.

3 La conformité et la visibilité

Il est important de comprendre qui a accès aux applications et aux données, d'où ils y accèdent et ce qu'ils en font. Cela est particulièrement vrai lorsqu'il s'agit de services cloud.
Cependant, seules les offres les plus avancées comme Salesforce.com offrent un reporting portant sur la conformité, et lorsque ce reporting existe comme dans le cas de Salesforce.com, il est cloisonné à une seule application.

Pour répondre aux auditeurs qui vous demandent quels sont les collaborateurs qui ont accès à vos applications et à vos données, vous avez besoin d'une visibilité centralisée et d'un contrôle sur tous vos systèmes. Votre solution de gestion des identités et des accès doit par conséquent vous assurer une vue unifiée sur l’ensemble des droits d'accès aux services, et vous fournir des rapports de conformité regroupant les droits d'accès, le provisioning et le déprovisioning, ainsi que les activités utilisateurs et administrateurs.

4 Le cloisonnement des répertoires utilisateurs

Crédit image : nd3000 / Shutterstock Inc.

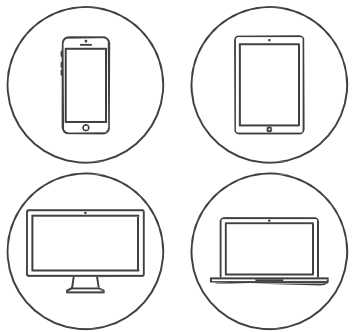
La plupart des entreprises ont investis des sommes considérables dans leur répertoire utilisateur (de type Microsoft Active Directory) pour gérer les accès aux ressources et réseaux sur site. Alors que les organisations adoptent de plus en plus de services cloud, elles ont besoin d'amortir leur investissement et de faire en sorte que leur solution d'IAM s'étende bien au-delà du cloud, afin de ne pas tomber dans la configuration où elles doivent créer un répertoire parallèle et une infrastructure de gestion d'accès uniquement pour ces nouvelles applications SaaS.

Une solution d'IAM idéale doit donc permettre une intégration centralisée et prête à l'emploi avec le répertoire central Active Directory ou LDAP, pour que vous puissiez vraiment en tirer profit et prolonger l'utilité de cet investissement avec les nouvelles applications, sans modifications de pare-feu ou autre lourde modification. Ainsi, à mesure que vous ajoutez ou supprimez des utilisateurs dans votre répertoire, l'accès aux applications cloud sera modifié automatiquement, dans le respect des standards de l'industrie comme SSL, et sans changements de réseau ou de configuration de sécurité.

5 La prolifération des navigateurs et des terminaux

Crédit image : Valeri Potapova / Shutterstock Inc.

L'un des grands avantages des applications cloud est que l'on peut y accéder depuis n'importe quel terminal connecté à internet. Mais plus d'apps veut aussi dire plus d'URL et de mots de passe, et la multiplication des terminaux mobile représente des points d'accès supplémentaire à gérer et à maintenir.



Les services d'IT se doivent de faciliter l'accès depuis plusieurs des terminaux et plateformes variés, sans pour autant faire de compromis sur la sécurité. Cela peut représenter un vrai challenge avec certaines solutions d’IAM existantes.

Une solution d’IAM idéale doit en effet aider les utilisateurs et les administrateurs à résoudre le défi d'un accès « partout, tout le temps, depuis n'importe quel terminal ». Elle ne doit pas seulement fournir un SSO basé sur le navigateur, mais elle doit également permettre un accéder à ces mêmes services depuis tout autre terminal au choix de l'utilisateur, avec autant de facilité et surtout de sécurité.

Crédit image : GaudiLab / Shutterstock Inc.

6

Le maintien à jour des intégrations

Une centralisation totale du SSO et de la gestion des accès implique un grand nombre d'intégrations avec tout type d'applications, et surtout le maintien à jour des intégrations à chaque nouvelle version de chacune de ces applications. Pour la vaste majorité des organisations, demander à leur service IT d'entretenir une collection de « connecteurs » dans un environnement en constante évolution n'est ni réaliste ni productif.

Les applications cloud d'aujourd'hui ont toutes des architectures de pointe et sont optimisées pour le modèle SaaS. Ces technologies offrent un vaste choix aux développeurs, qui peuvent designer leur service et ses interfaces en suivant leur propre méthode.

Malheureusement pour les professionnels de l'IT, cela signifie également que chaque nouvelle application représente potentiellement une nouvelle approche d'intégration, en particulier en ce qui concerne l'authentification et la gestion des accès utilisateurs.

De plus, comme les applications hébergées, les applications SaaS évoluent avec le temps. La solution d'IAM que vous choisirez doit être capable de suivre ces évolutions et de garantir que les intégration mises en place seront toujours à jour et fonctionnelles. Votre solution d'IAM doit même servir de véritable médiateur entre toutes les technologies et approches d'intégration différentes, pour que les questions de compatibilité et d'évolutivité soient transparentes aux yeux de l'IT. Ainsi, même lorsque les API d'une application changent, votre solution de gestion des identités et des accès gère elle-même l'interfaçage des programmes selon les différentes versions, débarrassant votre service IT de ces problématiques.

Ceci simplifie du coup l'ajout de toute nouvelle application au sein de votre réseau, au point que ce soit aussi facile que d'ajouter une application sur votre smartphone. Après une configuration minimale et propre aux caractéristiques de l'entreprise, vous pourrez intégrer de nouvelles applications SaaS avec votre SSO en quelques minutes.

7

Les modèles d'administration pour différentes applications

Alors que les applications cloud deviennent plus simples et moins chères à mettre en œuvre, leur multiplication n’en simplifie pas la gestion. Ces solutions sont souvent gérées par les métiers directement, par exemple les Sales Operations pour Salesforce.com. Si cela peut présenter un avantage pour l'IT (parce que les métiers sont alors responsables de l'administration du système et que cela leur libère donc du temps), cela ouvre cependant la porte à de nouveaux problèmes, car les utilisateurs se retrouvent décentralisés, rendant impossible la gestion et l’émission de rapports et analyses.

C’est ici que le choix de la bonne solution d’IAM peut faire une nouvelle fois la différence. En centralisant les identités, elle fournit à l'IT une administration, un reporting et une gestion des utilisateurs et des accès complets. Une solution d’IAM optimale doit inclure un modèle de sécurité global, qui permet de fournir le bon niveau d'accès à chaque administrateur d'application métier, pour qu'ils puissent gérer leurs utilisateurs et droits spécifique, sans nuire à la sécurité du système dans son ensemble.

Crédit image : Sergey Molchenko / Shutterstock Inc.

8

L’utilisation non optimale et le manque de bonnes pratiques

Une des raisons pour lesquelles les applications cloud se répandent est que le modèle de prix, à savoir les abonnements mensuels, ont remplacé les paiements annuels ou pluriannuels qui prévalaient auparavant, lorsqu'il fallait acheter la licence d’un logiciel on-premises. Les directeurs financiers préfèrent évidemment payer pour des services que les employés utilisent lorsqu'ils en ont besoin. Toutefois, sans vue claire et centrale des usages, les responsables IT et financiers ne peuvent gérer les dépenses liées aux abonnements, et ils ne savent en définitive pas vraiment s'ils paient le juste prix par rapport à ce qui est utilisé.

Votre solution de gestion des identités et des accès peut vous accompagner en vous fournissant un aperçu précis de l'utilisation par collaborateur et en aidant de ce fait l'IT à optimiser les dépenses associées aux applications.

Les administrateurs doivent avoir accès en temps réel aux rapports d'utilisation des différents services. De plus, en mettant en corrélation les tendances d’usage avec la performance des collaborateurs, il devient possible d’en tirer des bonnes pratiques, applicables aux autres départements.

Faire face à ces défis avec Okta

Okta est une solution de gestion des identités et des accès conçue pour les entreprises, 100% développée dans le cloud. La solution Okta inclus un répertoire universel, du single sign-on, une authentification forte, des fonctionnalités de provisioning, une capacité de gestion des flux de travail et du reporting intégré.

Partout dans le monde, les entreprises utilisent la solution de gestion des accès Okta pour tous les terminaux, individus et applications de l'organisation, afin de renforcer la sécurité et la productivité de cette dernière, tout en se conformant aux normes de son secteur.

Utilisateurs : une personnalisation avancée

Avec la plateforme Okta, il est aussi facile d'ajouter de nouveaux utilisateurs que d'ajouter de nouvelles applications SaaS. Une fois le compte activé, chaque utilisateur se connecte à une page d'accueil personnalisée, sur laquelle il peut accéder à ses applications grâce une authentification unique et sécurisée. Cette page d'accueil, ou « tableau de bord », est accessible depuis tous ses navigateurs et terminaux et est entièrement personnalisée à ses besoins en applications.

Administrateurs : un contrôle sécurisé et intégré pour tout le monde

Okta permet à l'IT de gérer les individus, les applications et les politiques d'accès pour toutes les applications mobiles, cloud et hébergées. Le répertoire universel fournit une vue d'ensemble des membres de l'organisation et des identités auxquelles ils sont associés. Pour ajouter des applications, il suffit de sélectionner une application pré-intégrée à partir du réseau d'applications d'Okta et de régler les configurations spécifiques à votre organisation.

Cadres : un ROI maximisé et des risques minimisés

La solution Okta inclus un journal centralisé qui enregistre l'ensemble des évènements et activités aussi bien sur Okta que sur les applications intégrées. Des fonctionnalités de reporting sont aussi intégrées. Les rapports personnalisés sont des outils précieux pour aider les cadres à monitorer l'activité, à en garantir la conformité et à surveiller l'utilisation des applications.

A propos d’Okta

Pour en savoir plus : www.okta.com/fr

Photo de couverture et de quatrième de couverture : Sofiaworld / Shutterstock Inc.