jamf

LIVRE BLANC

Authentification et authentification unique pour les débutants

Sécuriser les accès quand plane l'insécurité

Il est indispensable à la réussite des entreprises de protéger leur sécurité à tous les niveaux. Des réseaux aux appareils en passant par les utilisateurs, tout doit être protégé, en toutes circonstances. Sans cela, la situation pourrait se révéler catastrophique. En effet, une fuite de données peut mettre un frein à l'activité et ébranler la confiance des clients.

De nos jours, de plus en plus d'employés travaillent à distance et en dehors des horaires habituels et ont besoin de pouvoir accéder aux mêmes ressources que leurs collaborateurs sur site. Cependant, protéger l'ensemble des appareils et utilisateurs contre les menaces et logiciels malveillants ne s'improvise pas. Cette protection nécessite une part de planification et la mise en place de ressources et de flux de travail adaptés.

Aussi, comment les entreprises peuvent-elles combattre ces menaces sans pour autant nuire à la productivité des utilisateurs ? Tout simplement en adoptant des mesures de sécurité comme l'authentification unique et l'authentification des appareils et utilisateurs.

DANS CE LIVRE BLANC, NOUS VOULONS :

- Définir l'authentification et l'authentification unique
- Identifier le rôle des fournisseurs d'identité dans le cloud dans les flux d'authentification et d'authentification unique
- Fournir un aperçu pour mettre en place de meilleures pratiques de sécurité

QU'EST-CE QUE L'AUTHENTIFICATION UNIQUE ?

L'authentification unique (SSO) permet d'accéder à plusieurs applications au moyen d'un même jeu d'informations de connexion. Selon **TechTarget**, SSO est une entente de gestion fédérée des identités qui s'appuie sur le cadre OAuth afin que toutes les données de compte des utilisateurs puissent être utilisées sur des services tiers, sans pour autant révéler d'informations sensibles comme les mots de passe.

OAuth agit en tant qu'intermédiaire au nom de l'utilisateur en fournissant un jeton d'accès qui autorise le partage de certaines informations de compte. Quand un utilisateur tente d'accéder à une application auprès du fournisseur de services, ce dernier envoie une demande au fournisseur d'identité pour authentification. Le fournisseur de services valide ensuite l'authentification et permet à l'utilisateur de se connecter ou au contraire l'en empêche en cas d'échec.

Types de configurations SSO :

- Security Assertion Markup Language (SAML) aide à échanger l'authentification et les autorisations de l'utilisateur sur des domaines sécurisés. Ce processus nécessite une communication entre l'utilisateur, un fournisseur d'identité qui gère l'annuaire des utilisateurs et le fournisseur de services.

- SSO via Kerberos délivre un ticket TGT (ticket-granting ticket) une fois les informations d'identification de l'utilisateur fournies. Ce ticket récupère les tickets de service des applications auxquelles l'utilisateur souhaite accéder, sans l'obliger à saisir de nouveau à chaque fois ses informations d'identification.

- Les cartes à puce SSO exigent de l'utilisateur qu'il utilise une carte avec ses informations de connexion. Après une première utilisation, inutile pour lui de saisir à nouveau son nom ou son mot de passe dans la mesure où la carte à puce stocke ces informations.

Les avantages de l'authentification unique sont multiples. D'une part, les utilisateurs ne multiplient pas les identifiants et mots de passe. Ils sont donc moins susceptibles de les oublier et d'ouvrir un ticket d'aide et d'autre part, le processus de connexion aux applications est simplifié.

QU'EST-CE QUE L'AUTHENTIFICATION ?

Selon **The Next Web**, l'authentification est le processus sécurisé d'identification et de validation de l'identité d'un système ou d'une personne. Par exemple, vous utilisez un nom d'utilisateur et un mot de passe pour vous connecter à un appareil. Le processus d'authentification valide que vous êtes bien la personne que vous prétendez être avant de vous accorder l'accès.

Active Directory (AD) et Lightweight Directory Access Protocol (LDAP) sont tous deux des exemples de services d'authentification pour la gestion des comptes et des identités sur site. Toutefois de nos jours, dans les environnements modernes dans lesquels de plus en plus d'utilisateurs accèdent à des ressources dans le cloud, ces services deviennent rapidement obsolètes.

Limites des services AD et LDAP :

- Les utilisateurs à distance doivent se trouver sur le réseau local (LAN) ou utiliser un réseau privé virtuel (VPN) pour accéder aux ressources internes, autant dire une expérience tout sauf optimale.

- Les utilisateurs qui utilisent un plug-in AD peuvent uniquement modifier leurs mots de passe lorsque AD est joignable. Cela est source de confusion et a un coût compte tenu des nombreux tickets qu'il est nécessaire d'ouvrir auprès du centre d'assistance en cas d'oubli du mot passe.

- Il est extrêmement difficile de mettre en œuvre une authentification multifacteur pour accroître les protocoles de sécurité avec AD ou LDAP.

- De plus en plus d'entreprises délaissant les PC sous Windows au profit des Mac, l'utilisation d'AD comme identité principale limite les capacités de gestion. Cela exige sur Mac l'utilisation d'extensions tierces, autant dire une gestion des utilisateurs plus complexe et des coûts plus élevés.

- Les administrateurs informatiques ne peuvent pas déployer de commandes ni de scripts sous forme de politiques lesquelles appliquent ces paramètres aux ordinateurs et utilisateurs sous leur responsabilité.

Toutes ces limites ont donc conduit à la nécessité de faire appel à des fournisseurs d'identité dans le cloud.

QU'EST-CE QUE L'IDENTITÉ DANS LE CLOUD ?

L'identité dans le cloud permet aux services informatiques de gérer des utilisateurs, groupes et mots de passe à distance et de manière centralisée, mais aussi d'accéder aux applications et ressources dans le cloud de l'entreprise. Les fournisseurs d'identité dans le cloud (par exemple, Microsoft, Google, Okta, IBM, OneLogin et Ping) utilisent les standards SAML et OAuth pour offrir à tous les utilisateurs (sur site et à distance) un accès sécurisé aux ressources dans le cloud dont ils ont besoin pour rester productifs.

Grâce à la puissance de l'identité dans le cloud, Microsoft encourage les entreprises à délaisser un système Active Directory sur site au profit de Microsoft Azure Active Directory dans le cloud.

Microsoft Azure est un ensemble de services dans le cloud qui permet aux entreprises de créer, gérer et déployer des applications sur un réseau international de grande taille. Microsoft Azure est utilisé par **95 % des entreprises du classement Fortune 500**, mais comme nous l'avons dit précédemment, il ne s'agit pas du seul fournisseur disponible.

INTÉGRATION DE L'IDENTITÉ DANS LE CLOUD

Avec autant de fournisseurs d'identité dans le cloud parmi lesquels choisir, les entreprises voudront une solution qui s'intègre au plus grand nombre, si ce n'est à tous. Jamf Connect propose un approvisionnement simple des utilisateurs à partir d'un service d'identité dans le cloud avec flux d'approvisionnement Apple et authentification multifacteur.

Un utilisateur peut ainsi tout simplement déballer son Mac, l'allumer et accéder à toutes les applications approuvées par le système après s'être connecté au moyen d'un jeu unique d'informations d'identification dans le cloud.

Les avantages sont nombreux :

- **Création de comptes :** Vous créez des comptes Mac en local en vous appuyant sur les identités Okta, Microsoft Azure, Google Cloud, IBM Cloud, PingFederate et OneLogin, l'objectif étant d'améliorer l'expérience de connexion des utilisateurs et d'organiser la flotte de Mac que le service informatique doit gérer.

- **Sécurisation des inscriptions :** Vous utilisez une authentification moderne pour suivre et surveiller les appareils auxquels un accès est demandé, mais aussi savoir qui en demande l'accès et d'où, soit la garantie que l'utilisateur est bien celui connecté à l'appareil avant de déployer des informations sensibles.

- **Suppression des comptes administrateur partagés :** Vous créez plusieurs comptes administrateur informatique en utilisant les autorisations accordées par le fournisseur d'identité dans le cloud, sans pour autant avoir besoin de comptes de service partagé.

- **Mise en œuvre de politiques de mots de passe :** Les administrateurs peuvent mettre en œuvre des politiques de mots de passe via le fournisseur d'identité et ainsi préserver la cohérence et la sécurité auprès de tous les utilisateurs.

- **Synchronisation des mots de passe :** Vous synchronisez le nom d'utilisateur et le mot de passe Mac avec les informations d'identification Azure, Okta et PingFederate afin d'utiliser une seule et même identité pour tout ce qui vous permet de rester productif.

LE RÔLE DE LA GESTION DES APPAREILS MOBILES (MDM)

Les entreprises s'éloignent désormais du modèle AD et intègrent davantage d'appareils Mac pour répondre à l'augmentation de la demande. Pour y parvenir, elles doivent mettre en place des flux de travail à même de sécuriser leurs informations, sans oublier d'offrir aux utilisateurs une expérience optimale.

Les fournisseurs d'identité dans le cloud intégrés à Jamf Connect permettent au service informatique de gérer les mots de passe des utilisateurs et d'accéder aux applications de l'entreprise, le tout à distance. Avec une inscription MDM automatisée, ce processus se veut simple et sécurisé :

1. Un utilisateur est invité à s'inscrire dans le système MDM automatisé.

2. Pendant l'inscription, Jamf Connect est téléchargé et installé depuis le serveur MDM.

3. L'utilisateur accède alors directement à la fenêtre de connexion de Jamf Connect et n'a plus à créer d'identifiant ni de mot de passe.

L'utilisateur possède un identifiant et un mot de passe pour tous les accès, autant dire une expérience unique qui ne nuit nullement à la sécurité du compte.

Pour un environnement plus sûr

L'authentification unique et les fournisseurs d'identité dans le cloud sont le futur de la gestion de la sécurité et des identités. Vous protégez votre environnement et dites adieu aux tickets d'assistance désormais inutiles. Vous êtes donc gagnant sur tous les fronts.

Contactez-vous sans plus attendre pour vous lancer ou demandez à essayer Jamf Connect et à tester ces flux de travail.

Je me lance

Demander un essai

Vous pouvez aussi contacter votre revendeur d'appareils Apple agréé habituel pour tester Jamf Connect.

jamf

www.jamf.com