Pourquoi une meilleure sécurité Mac commence par l'identité cloud

L'évolution de la main-d'œuvre crée de nouvelles opportunités

For years, employees drove to an office, opened their computer, logged onto a corporate network with their username and password and got on with their workday.

Pendant des années, la journée de travail se résumait ainsi : partir au bureau, ouvrir son ordinateur, puis se connecter à un réseau d'entreprise avec un nom d'utilisateur et un mot de passe.

Mais travailler selon des horaires fixes depuis un même lieu est une pratique qui tend à se raréfier. En effet, un rapport établi par l'institut Gallup révèle que 43 % des employés américains travaillent à distance.[1] Cette main-d'œuvre mobile en pleine croissance a besoin du même accès sécurisé aux ressources que ses collègues au bureau — mais les employés sur site et à distance ont besoin de moyens sécurisés pour accéder au nombre croissant d'applications et de ressources hébergées dans le cloud. Les entreprises doivent donc adapter leurs pratiques informatiques à ce nouvel environnement.

La première étape pour fournir aux employés les outils modernes dont ils ont besoin dans leur nouvelle vie professionnelle consiste à leur offrir un programme choix. Ce programme permet à chacun de choisir un ordinateur PC ou Mac pour son usage professionnel. Étant donné que de plus en plus d'employés choisissent le Mac, le service informatique a besoin d'une solution simple pour protéger l'appareil et l'utilisateur, où qu'ils se trouvent.

Dans ce livre blanc, nous présentons des méthodes inédites et efficaces pour tirer parti de l'identité cloud afin de sécuriser le Mac, l'utilisateur et les données stockées sur le Mac, mais aussi l'entreprise pour laquelle l'utilisateur Mac travaille.

L'authentification sur Mac aujourd'hui

Même si Active Directory (AD) et Lightweight Directory Access Protocol (LDAP) se sont imposées comme des technologies d'authentification efficaces sur le Mac au fil des années, elles deviennent de moins en moins efficaces dans les environnements modernes actuels.

Les utilisateurs sont contraints d'adopter l'approche traditionnelle qui consiste à se connecter au réseau local (LAN) d'une organisation ou à utiliser un réseau privé virtuel (VPN) pour accéder aux ressources internes. Avec le plug-in Active Directory, les utilisateurs ne peuvent modifier leur mot de passe que si AD est accessible, ce qui entraîne souvent une certaine confusion et l'envoi de tickets d'assistance onéreux.

Ce processus présente deux inconvénients majeurs :

1. Gaspillage des ressources informatiques
Lorsque les employés travaillent à distance, ils ne sont pas automatiquement connectés au réseau de l'entreprise. Cela crée des problèmes au niveau des mots de passe. Le cabinet Gartner signale que jusqu'à 40 % des problèmes traités par un service informatique sont liés à des réinitialisations de mots de passe.[2] De plus, bon nombre de ces réinitialisations proviennent de travailleurs distants qui ont oublié leur mot de passe.

Chaque ticket d'assistance coûte de l'argent. Toujours selon Gartner, un appel au service d'assistance coûte en moyenne 17,88 $.[2] Si les entreprises sous-traitent leur service informatique, elles se voient probablement facturer un montant forfaitaire important pour chaque ticket soumis, même pour un simple changement de mot de passe.

Les tickets et les dollars s'additionnent rapidement. Les entreprises pourraient donc perdre des milliers de dollars rien qu'en réinitialisant les mots de passe.

2. Menaces croissantes pour la sécurité
Il est très difficile de mettre en œuvre l'authentification multifacteur ou même d'envisager d'augmenter votre sécurité grâce à des méthodes telles que l'approbation des appareils en utilisant AD, LDAP et Kerberos comme principale méthode d'authentification de l'utilisateur.

iPass a rédigé un rapport montrant que la main-d'œuvre mobile constitue la principale menace pour la sécurité des données de l'entreprise. En effet, 57 % des directeurs financiers et décideurs informatiques mondiaux estiment que leurs employés mobiles ont été victimes ou responsables d'un problème de sécurité mobile au cours l'année écoulée.[3]

Les outils sur site ne sont pas adéquats

Microsoft Active Directory s'est imposé comme la référence en matière de gestion des identités et des comptes sur site. Active Directory garantit la protection des données et des applications de l'entreprise contre tout accès d'une personne extérieure qui ne figure pas dans l'annuaire des employés.

Une majorité d'entreprises ont utilisé Active Directory pour résoudre des problèmes d'authentification dans le passé, mais cette solution ne répond plus aux défis actuels.

Pourquoi ?

À mesure que le monde de l'entreprise passe de Windows à Apple, les professionnels de l'informatique s'interrogent sur les meilleures pratiques pour intégrer Mac à Active Directory.

À l'heure actuelle, de nombreux problèmes se posent en ce qui concerne les moyens sûrs et conviviaux permettant aux travailleurs à distance de s'authentifier via Active Directory :

1. Lorsqu'ils s'authentifient avec Active Directory, les employés doivent être sur le domaine de l'entreprise. Cela n'est pas possible pour les travailleurs à distance.

2. Historiquement, les entreprises se sont appuyées sur Active Directory comme principal fournisseur d'identité, mais de nombreux employeurs se tournent vers les appareils Mac. Cela entraîne une baisse du niveau de contrôle pour les utilisateurs

Apple distants, ainsi qu'une limitation des capacités de gestion des utilisateurs. Des add-ons tiers sont également nécessaires, ce qui ajoute de la complexité à la gestion des utilisateurs et augmente les coûts.

3. Les administrateurs informatiques ne peuvent pas déployer des commandes et des scripts sous la forme de stratégies ou de règles qui appliquent leurs réglages aux ordinateurs et aux utilisateurs sous leur contrôle.

Pendant 20 ans, la liaison à un domaine Active Directory était une excellente solution pour résoudre les problèmes d'authentification. Mais dans un monde de plus en plus mobile, les mots de passe et les horloges ne sont plus synchronisés, les enregistrements Domain Name System (DNS) ne sont pas toujours disponibles en externe, et la solution Active Directory n'est pas toujours la solution la plus adaptée.

De nos jours, les employés veulent travailler n'importe où, en toute sécurité et le plus facilement possible.

Alors comment ne plus avoir à lier un ordinateur à Active Directory tout en garantissant la sécurité des comptes ? Grâce aux solutions d'identification cloud !

Présentation de l'identité cloud

Sans les bons outils, la sécurité des appareils distants est menacée. L'approche de l'identité et de la sécurité doit donc évoluer. Les fournisseurs d'identité cloud, par exemple Microsoft, Google, Okta, IBM et OneLogin, Security Assertion Markup Language (SAML) et Open Authorization (OAuth) ouvrent la voie pour faire de cette évolution une réalité.

Qu'est-ce que l'identité cloud ?

L'identité cloud permet aux services informatiques de gérer de manière centralisée et à distance des utilisateurs, groupes, mots de passe ainsi que l'accès aux applications d'entreprise et au ressources cloud.

> **Avec 81 % des entreprises exploitant des environnements multi-cloud et 26 % dépensant plus de 6 millions de dollars par an en infrastructure cloud publique, il n'a jamais été aussi difficile de garantir l'identité et la sécurité des ressources.**

À ce titre, Microsoft encourage les entreprises à s'éloigner d'une infrastructure Active Directory sur site au profit d'une solution Microsoft Azure Active Directory de type cloud.

Microsoft Azure regroupe des services cloud permettant aux entreprises de créer, gérer et déployer des applications sur un vaste réseau mondial en utilisant des outils et des infrastructures spécifiques. Pour preuve, 95 % des entreprises Fortune 500 utilisent Microsoft Azure.4

Mais Microsoft Azure n'est pas le seul fournisseur d'identité cloud ; de nombreuses options sont disponibles. Alors, vers qui les organisations devraient-elles se tourner ?

Jamf Connect pour l'intégration de l'identité cloud

Avec Jamf Connect, peu importe le fournisseur d'identité cloud que vous sélectionnez. Jamf Connect permet un provisionnement simple des utilisateurs à partir d'un service d'identité cloud, dans le cadre d'un workflow de provisionnement Apple et avec une authentification multifacteur.

Il offre la flexibilité nécessaire pour gérer des utilisateurs locaux contrôlés par les mêmes règles et contrôles que ceux proposés par un service d'annuaire ou un fournisseur d'identité.

Avec Jamf Connect, un utilisateur peut déballer son Mac, l'allumer et accéder à toutes les applications

approuvées, après s'être authentifié avec un ensemble d'identifiants cloud.

Voici les avantages :

1. **SÉCURISER LE PROCESSUS D'ENRÔLEMENT :** Tirez parti de l'authentification moderne pour vérifier que le bon utilisateur est configuré sur l'appareil avant d'y déployer des informations sensibles.

2. **CRÉATION DE COMPTE JUSTE-À-TEMPS :** Créez des comptes locaux basés sur les identités Okta, Azure, Google Cloud, IBM Cloud et OneLogin.

3. **CLOUD MULTIFACTEUR :** Utilisez les méthodes multifacteur Okta, Azure, Google Cloud, IBM Cloud ou OneLogin prises en charge dans la fenêtre d'ouverture de session.

Vous disposez d'une infrastructure sur site ?

La solution NoMAD est faite pour vous. Libérez vos Mac en exploitant la puissance de NoMAD, une méthode rapide pour synchroniser les comptes dans des environnements qui utilisent Active Directory.

Gestion des appareils mobiles (MDM) et accès conditionnel

À mesure que les entreprises abandonnent une solution Active Directory sur site et constatent une augmentation du nombre d'appareils Mac sur le lieu de travail, elles doivent absolument sécuriser les informations d'entreprise tout en offrant l'expérience utilisateur qui a fait la renommée mondiale d'Apple.

Les fournisseurs d'identités dans le cloud intégrés à Jamf Connect permettent aux administrateurs informatiques de gérer à distance les mots de passe des utilisateurs et l'accès aux applications de l'entreprise, garantissant la sécurité des informations dans un monde plus mobile.

Grâce à un système d'enrôlement MDM automatisé, le processus est très simple.

1. Un utilisateur est invité à s'inscrire via l'enrôlement MDM automatisé.

2. Pendant ce processus d'enrôlement, le package Jamf Connect est téléchargé et installé depuis le serveur MDM.

3. L'utilisateur est directement dirigé vers la fenêtre d'ouverture de session Jamf Connect, sans avoir à créer ses propres nom d'utilisateur et mot de passe.

Il se voit attribuer les mêmes nom d'utilisateur et mot de passe pour tout, et profite ainsi d'une formidable expérience et d'un compte parfaitement sécurisé.

Une solution MDM dédiée Apple garantit donc une expérience d'installation automatisée et prête à l'emploi, peu importe si un employé se trouve au bureau ou à l'autre bout du monde.

Nous sommes là pour vous aider

Si vous êtes prêt à renforcer la sécurité de votre environnement et à réduire le nombre de tickets d'assistance liés aux mots de passe, contactez-nous dès aujourd'hui : nous vous aiderons à franchir une nouvelle étape en matière de sécurité des appareils Apple.

Laissez Jamf résoudre vos problèmes d'authentification.

Contactez-nous dès aujourd'hui pour vous lancer, ou testez gratuitement Jamf Connect grâce à nos intégrations d'identité cloud.

Nous contacter **Demander un essai**

Ou contactez votre revendeur d'appareils Apple agréé pour tester Jamf Connect.

SOURCES:
1: http://news.gallup.com/reports/199961/7.aspx#aspnetForm
2: Gartner Document #G00258742
3: https://www.ipass.com/mobile-security-report/
4: https://www.rightscale.com/lp/state-of-the-cloud

jamf

www.jamf.com

To see how Jamf Connect can help you transition to more modern workflows, visit **www.jamf.com.**