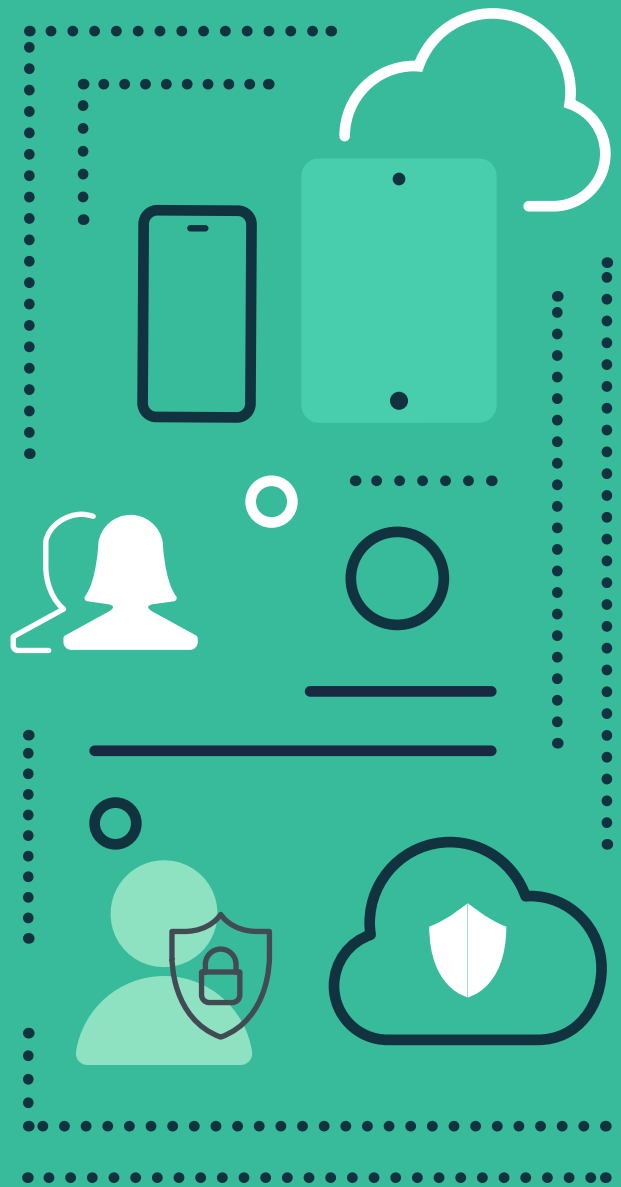

jamf

Gestion des identités

une introduction

CHAQUE EMPLOYÉ A SA PROPRE IDENTITÉ.

Traditionnellement, les employés se rendaient dans les locaux de leur entreprise. Ils avaient un ordinateur de bureau à leur poste et le matériel ne quittait jamais cet endroit. Si l'on multiplie ce chiffre par le nombre d'employés d'une entreprise, on peut se faire une idée du nombre d'appareils et d'accès que le service informatique devait gérer. L'environnement de travail d'aujourd'hui est très différent. Le travailleur moderne est mobile. Il passe de façon transparente de l'ordinateur portable à la tablette ou au téléphone tout au long de sa journée, et il a besoin d'accéder aux informations et aux données de l'entreprise partout où il va.

L'empreinte numérique des travailleurs s'est considérablement élargie, tant en termes de temps passé sur les appareils que de volume de données consultées. Pour protéger ces informations, l'une des principales tactiques des entreprises consiste à contrôler qui a accès à certains fichiers, logiciels et données. Cette méthode simple a des avantages sur le plan l'expérience de l'utilisateur final : celui-ci accède uniquement aux données utiles, en temps utile, ni plus ni moins.

C'est aujourd'hui un sujet courant dans l'informatique. Mais avec l'évolution de la technologie et des besoins des employés, il devient essentiel pour les entreprises de mettre en place des workflows modernes et à l'épreuve du temps. L'un d'eux est la gestion des identités et des accès, et c'est une priorité absolue.

DANS CE GUIDE, NOUS ALLONS :

- Les éléments de base de la gestion des identités
- Les workflows d'une gestion moderne des identités et des accès
- Pourquoi le cloud est indispensable pour réussir aujourd'hui
- Comment Jamf combine tous ces aspects

LES ÉLÉMENTS DE BASE DE LA GESTION DES IDENTITÉS

La gestion des identités et des accès (IAM) est la discipline générale permettant de vérifier l'identité d'un utilisateur et son niveau d'accès à un système donné. **Pour ce faire, les utilisateurs doivent être authentifiés et autorisés.**

L'**authentification** est généralement liée à l'acte de « connexion ». C'est à ce stade que l'authenticité de votre identification est établie. Cela se fait le plus souvent à l'aide d'un nom d'utilisateur et d'un mot de passe.

Toutefois, dans le cadre de la gestion des identités, l'authentification ne donne pas directement accès à quoi que ce soit. Elle confirme simplement l'identité d'un utilisateur. Pour accéder aux données, aux logiciels et aux fichiers, il faut une autorisation. L'**autorisation** concerne les ressources, les logiciels, les données, etc., auxquels vous avez accès, une fois que vous êtes authentifié.

Authentification = qui vous êtes
Autorisation = ce que vous pouvez faire

LES ÉLÉMENTS DE BASE DE LA GESTION DES IDENTITÉS

Pour donner corps à ces concepts d'authentification et d'autorisation, les entreprises ont créé un annuaire – en substance, un fichier technologique des employés. Cet annuaire contient généralement le nom, le type d'appareil, le poste, le service, les noms d'utilisateur, les mots de passe, ainsi que les logiciels et fichiers dont l'employé a besoin. Cette approche a jeté les bases de la gestion des identités. C'est ce qu'on appelle parfois l'informatique héritée.

Il y a 15 ans, la gestion des identités était assez cohérente. Le protocole LDAP (Lightweight Directory Access Protocol) permettait de cataloguer l'identification et les informations de vos utilisateurs. Kerberos se chargeait de leur authentification. Et en combinant les deux, vous obteniez Active Directory (AD), qui était au cœur de la gestion des identités. Mais cette approche a évolué au cours de la dernière décennie.

L'informatique traditionnelle considère les services d'annuaire comme une « source de vérité ». Mais avec l'évolution des besoins en matière de sécurité et de déploiement, les entreprises doivent intégrer une nouvelle approche de l'identité à leur stratégie. En s'appuyant sur une pile complète de gestion des identités, les entreprises unifient toutes les identités – matérielles et logicielles. Cette unification débloque des fonctionnalités et des workflows avancés qui ont un véritable pouvoir de transformation sur l'entreprise.

LES ÉLÉMENTS DE BASE DE LA GESTION DES IDENTITÉS

La gestion d'identité ne s'arrête pas à l'authentification et à l'autorisation des utilisateurs. Elle détermine également la manière dont les utilisateurs accèdent aux ressources de l'organisation.

Pour les employés qui travaillent à distance, l'accès aux ressources se fait traditionnellement via un réseau privé virtuel (VPN). Lorsqu'on utilise un VPN, l'utilisateur reçoit un accès global à l'ensemble des ressources du réseau – et cela représente un risque de sécurité important. Si des acteurs malveillants obtiennent un accès complet au réseau via le VPN, des déplacements mettent potentiellement tous les contenus à leur portée.

D'autre part, les VPN n'ont jamais été conviviaux ni adaptés à la mobilité. Dans les entreprises modernes, les utilisateurs doivent pouvoir accéder à l'information à tout moment, où qu'ils se trouvent.

GESTION MODERNE DES IDENTITÉS ET DES ACCÈS

Le passage de l'informatique héritée à l'informatique moderne n'est pas qu'une question de technologie : ces nouvelles pratiques ont pour but de libérer la productivité de l'utilisateur final et de permettre la transformation de l'entreprise.

LA PILE D'IDENTITÉ

Services d'annuaire

Sortes de registres centralisant des informations sur les employés (nom, service, etc.). Souvent utilisés en intégration avec des plateformes de gestion comme Jamf Pro, pour déployer des appareils personnalisés auprès des utilisateurs finaux.

Tradition : Active Directory sur site

Modernité : annuaire cloud

SSO cloud

Le SSO cloud exploite les informations des services de répertoire et impose la saisie d'identifiants sécurisés pour autoriser l'accès aux ressources de l'entreprise.

Tradition : les utilisateurs s'authentifient chaque fois qu'ils accèdent à des applications ou des ressources basées sur le cloud.

Modernité : les utilisateurs accèdent aux applications basées sur le cloud, comme Microsoft Outlook et Slack, en s'authentifiant moins souvent.

Jamf Connect

Avec les services d'annnuaire et le SSO cloud, Jamf Connect unifie les identités sur l'ensemble des applications de l'entreprise et sur l'appareil de l'utilisateur pour une confiance sans faille. Grâce à leur identité cloud unique, les utilisateurs finaux accèdent facilement et rapidement aux ressources dont ils ont besoin pour être productifs.

Modernité :

- Rationalisation de l'approvisionnement et de l'authentification pour une prise en charge complète des employés à distance
- Synchronisation automatique des identités des utilisateurs et des identifiants des appareils.
- L'informatique dispose de capacités complètes de gestion des identités.
- Accès sécurisé aux ressources et aux applications de l'entreprise avec un VPN nouvelle génération

Services d'annuaire

Services d'annuaire + SSO cloud

Services d'annuaire + SSO cloud + Jamf Connect

UNE GESTION MODERNE DES IDENTITÉS

La pile d'identité moderne se compose aujourd'hui de trois éléments :

1. **Les services d'annuaire et d'authentification unique (SSO) proviennent d'un fournisseur d'identité cloud (cloud IdP), généralement Azure ou Okta**
2. **Jamf pour la gestion des appareils mobiles**
3. **Jamf Connect pour unifier votre IdP cloud, votre équipement et vos logiciels, et fournir un accès sécurisé aux applications professionnelles**

Ces composants se coordonnent pour améliorer l'expérience des équipes mobiles et renforcer la sécurité de l'ensemble de votre déploiement.

Qu'est-ce qu'un fournisseur d'identité ?
Un fournisseur d'identité (IdP) est un service qui stocke et gère les identités numériques. Les entreprises utilisent ces services pour permettre à leurs employés ou utilisateurs de se connecter aux ressources dont ils ont besoin. Ils permettent de gérer les accès en ajoutant ou en supprimant des autorisations, tout en maintenant un haut niveau de sécurité.

Qu'est-ce que l'authentification unique (SSO) ?
Avec l'authentification unique, un même jeu d'identifiants permet de s'authentifier en toute sécurité sur différents sites web et applications.

GESTION MODERNE DES IDENTITÉS ET DES ACCÈS

Quand les équipes travaillent au même endroit et exploitent uniquement la technologie à leur disposition, leur empreinte numérique est réduite. Dans ce contexte classique, les pratiques de base en matière de gestion des identités suffisent. Mais la technologie a évolué : votre personnel utilise quotidiennement différents appareils pour accéder à un volume accru de données et un large éventail de logiciels. Les risques de sécurité ont augmenté et vos équipes, autrefois statiques, sont bien plus dynamiques.

Dans de nombreux aspects de la technologie et de l'infrastructure informatique, il a fallu changer les pratiques lorsque la main-d'œuvre est devenue mobile. La gestion des identités ne fait pas exception. Pour utiliser AD et LDAP, un utilisateur lie son appareil à un annuaire AD sur site. Mais comme nous l'avons mentionné, les équipes ne sont plus systématiquement dans les locaux, ce qui pose plusieurs problèmes :

- Les utilisateurs ne peuvent modifier leurs mots de passe que sur place, quand AD est accessible. Si un utilisateur oublie son mot de passe ou doit en changer, il est ralenti dans son travail et mobilise inutilement l'assistance.
- Comme AD est conçu pour Windows, utiliser AD comme fournisseur d'identité principal réduit les capacités de gestion pour Mac. Il faut en effet recourir à des extensions tierces, ce qui rend la gestion des utilisateurs à la fois plus complexe et plus coûteuse.
- Les utilisateurs à distance doivent se trouver sur le réseau local (LAN) ou utiliser un réseau privé virtuel (VPN) pour accéder aux ressources internes. Pour l'utilisateur final, cette expérience est souvent source de frustrations.

Ces raisons, et d'autres, conduisent à l'adoption d'IdP cloud, un élément essentiel de la gestion moderne des identités et des accès.

POURQUOI LE CLOUD EST INDISPENSABLE POUR RÉUSSIR AUJOURD'HUI

L'identité cloud permet aux services informatiques de gérer les utilisateurs, groupes et mots de passe à distance et de manière centralisée, mais aussi l'accès aux applications d'entreprise et aux ressources cloud. Les IdP cloud, comme Microsoft, Google et Okta, offrent à tous les utilisateurs – sur site et à distance – un accès sécurisé aux ressources nécessaires à leur travail.

Identités traditionnelles	Identités modernes
• Active Directory	• Azure
• Open Directory	• Okta
• LDAP	• Google Suite

En s'appuyant sur un fournisseur d'identité cloud, les organisations peuvent dépasser le périmètre de leurs bureaux. Elles leur offrent ainsi une expérience transparente, tout en assurant la sécurité de leurs données et de leurs appareils.

POURQUOI LE CLOUD EST INDISPENSABLE POUR RÉUSSIR AUJOURD'HUI

Votre IdP – Okta, Azure, G Suite, etc. – va faire office de service d'annuaire des employés. Il rassemble toutes leurs informations personnelles : leur service, leur fonction et, surtout, les applications et ressources qui leur sont destinées. Lorsqu'un utilisateur se connecte à l'IdP cloud et valide son identité, il a alors accès à tout ce qui lui est attribué dans l'annuaire. **L'authentification et l'autorisation en action !**

Cet IdP cloud vous permet également d'exploiter la puissance du SSO : en plus de renforcer la sécurité des appareils mobiles de votre organisation, cette approche améliore nettement l'expérience des utilisateurs. Plutôt que de s'authentifier à chaque fois qu'ils se connectent à une plateforme, un application ou un service, la SSO les identifie une fois pour toute en toute sécurité. Ils ont ensuite accès à tout ce dont ils ont besoin.

POURQUOI LE CLOUD EST INDISPENSABLE POUR RÉUSSIR AUJOURD'HUI

Les entreprises désireuses de renforcer cette sécurité peuvent se tourner vers l'authentification multifacteur (AMF). L'AMF ajoute une étape supplémentaire qui demande à votre utilisateur final de confirmer son identité, en plus du nom d'utilisateur et du mot de passe, vulnérables par nature. Il accède ensuite à toutes les ressources dont il a besoin.

C'est là qu'intervient Jamf Connect : cette solution donne corps à ce concept en unifiant votre IdP cloud et vos appareils.

Qu'est-ce que l'authentification multifacteur ?

L'authentification multifacteur oblige l'utilisateur à fournir plusieurs preuves d'identité pour accéder à une ressource. Un code PIN sur son téléphone, la fonctionnalité Face ID ou la vérification de l'empreinte digitale peuvent servir à cette fin.

JAMF CONNECT RÉUNIT CES PRATIQUES DE MANIÈRE TRANSPARENTE.

Active Directory a été pensé pour Windows. Les utilisateurs d'Apple n'avaient donc pas d'autre choix que de se lier à AD, avant que Jamf Connect ne change la donne. Le modèle AD perd de sa popularité dans les entreprises qui intègrent à leur parc davantage d'appareils Mac pour répondre aux demandes des utilisateurs. Elles doivent donc mettre en place des workflows à même de sécuriser leurs informations, tout en préservant une excellente expérience pour les utilisateurs.

Les IdP cloud intégrés à Jamf Connect permettent au service informatique de gérer les mots de passe des utilisateurs et leur accès aux applications de l'entreprise, à distance. Avec une inscription MDM automatisée, ce processus se veut simple et sécurisé :

1. **L'utilisateur est invité à suivre le processus d'enrôlement MDM automatisé.**
2. **Pendant l'enrôlement, Jamf Connect est téléchargé et installé depuis le serveur MDM.**
3. **Les utilisateurs sont dirigés directement vers la fenêtre de connexion Jamf Connect. Ils y saisissent leurs identifiants cloud au lieu de créer un nom d'utilisateur et un mot de passe.**

JAMF CONNECT RÉUNIT CES PRATIQUES DE MANIÈRE TRANSPARENTE.

Ce jeu d'identifiants donne accès à tout : l'utilisateur bénéficie d'une expérience exceptionnelle qui ne nuit nullement à la sécurité du compte.

Les avantages sont nombreux :

Création de comptes : vous créez des comptes Mac locaux en vous appuyant sur les identités Okta, Microsoft Azure ou Google Cloud. L'objectif : améliorer l'expérience de connexion des utilisateurs tout en organisant la flotte de Mac placée sous la supervision du service informatique.

Inscription sécurisée : une méthode moderne d'authentification suit et surveille qui accède à quels appareils et depuis où. Elle garantit que le bon utilisateur est bien connecté au bon appareil avant de déployer des informations sensibles.

Abandon des comptes d'administration partagés : créez plusieurs comptes d'administration à l'aide des autorisations accordées par l'IdP cloud, sans pour autant avoir besoin de comptes de service partagé.

Application des règles de mots de passe : les administrateurs peuvent mettre en œuvre des règles de mots de passe via l'IdP, pour un maximum de cohérence et de sécurité sur l'ensemble des utilisateurs.

Synchronisation des mots de passe : synchronisez les noms d'utilisateur et mots de passe Mac avec les identifiants cloud afin d'utiliser une seule et même identité pour toutes les ressources de productivité.*

*La synchronisation des mots de passe n'est pas disponible avec Google Cloud pour le moment

JAMF CONNECT RÉUNIT CES PRATIQUES DE MANIÈRE TRANSPARENTE.

Une gestion moderne des identités et des accès combinée à une solution d'accès réseau zero-trust (ZTNA).

Quand une organisation adopte l'approche ZTNA, chaque utilisateur qui souhaite accéder à des données et des ressources est authentifié et autorisé, et son appareil est contrôlé – à chaque fois. Grâce à la mise en œuvre du principe du moindre privilège et aux contrôles en temps réel de l'état des appareils, l'accès à chaque application n'est accordé qu'à des utilisateurs spécifiques et autorisés, munis d'appareils fiables.

Côté authentification, le ZTNA est compatible avec le SSO via votre IdP cloud habituel. De plus, l'intégration aux IdP cloud existants permet de déployer rapidement des règles et facilite leur gestion. Pour établir une connexion, l'utilisateur doit disposer des autorisations appropriées pour l'application spécifiée.

Lisez notre e-book pour tout savoir sur le ZTNA.

LA GESTION DES IDENTITÉS ET DES ACCÈS EST INCONTOURNABLE.

Avec la normalisation du télétravail, la mobilité des équipes et la nécessité d'accéder à tout moment aux outils professionnels, cette approche est devenue une nécessité. Jamf unifie toute votre infrastructure en une seule expérience transparente pour les utilisateurs et l'informatique.

Demander une version d'essai

Ou contactez votre distributeur habituel pour commencer.