Microsoft

Gérez et sécurisez l’accès à vos applications avec Azure Active Directory

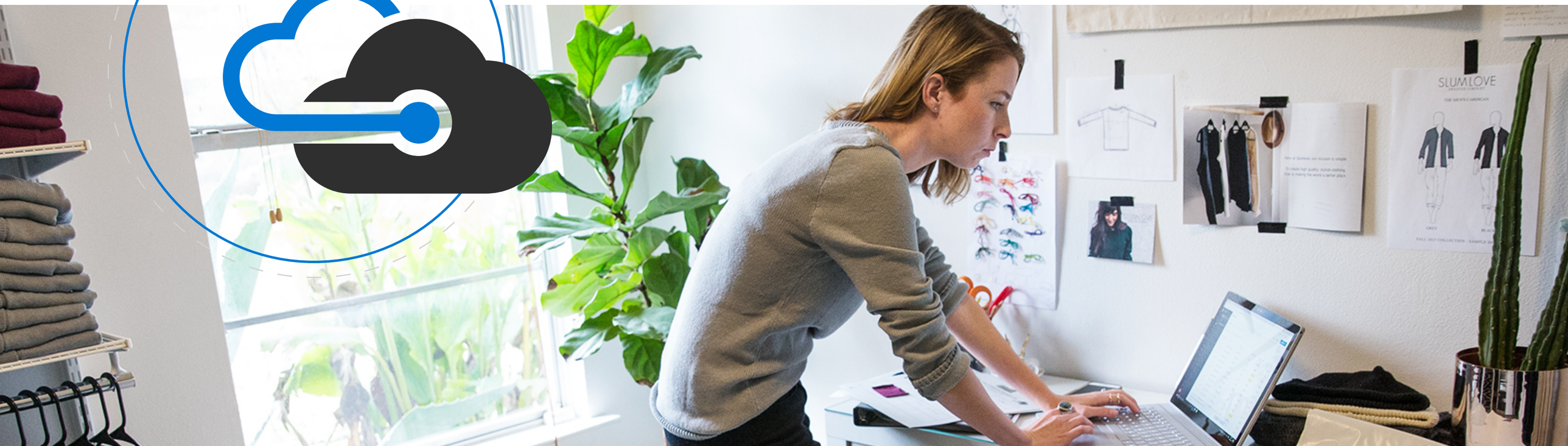
Section 1

Qu’est-ce que la gestion des identités et des accès ?

Qu’est-ce que la gestion des identités et des accès ?

Transition numérique

Le cloud computing et les appareils mobiles ont transformé le lieu de travail moderne. Une main-d’œuvre de plus en plus mondiale dispose de la flexibilité nécessaire pour travailler en tout lieu à l’aide de logiciels en tant que service (SaaS, Software-as-a-Service) gratuits ou bon marché pour résoudre des problèmes de productivité et de collaboration. Les grandes entreprises migrent des applications et leur informatique vers le cloud afin de moderniser leur architecture, et les différents secteurs d’activité profitent des nouveaux services cloud pour créer des applications personnalisées répondant à leurs besoins spécifiques. Les entreprises ont profité de l’essor des nouvelles technologies pour gagner en productivité, mais la transformation numérique a également introduit trois nouveaux défis.



Qu’est-ce que la gestion des identités et des accès ?

Nouveaux défis

Risque en matière de sécurité : Avant la révolution du cloud, l’informatique faisait office de portier technologique. Les applications et plateformes que vous gériez et sécurisiez étaient contenues dans le périmètre réseau, et toute personne qui se connectait à vos ressources d’entreprise était d’abord validée par le pare-feu. Ces jours sont révolus. Vos employés contrôle davantage la technologie qu’ils utilisent, dont une grande partie est accessible via Internet. Les cyber-attaquants ont appris à exploiter ces vulnérabilités. Même quand un utilisateur connaît le mot de passe d’un compte, vous ne pouvez pas toujours être certain qu’il est bien celui qu’il prétend être.

Fardeau administratif : L’explosion des points de terminaison offre aux utilisateurs davantage de moyens de se connecter, mais cela crée également un cauchemar administratif. De nombreuses entreprises ne connaissent pas tous les outils que les employés utilisent, et même quand elles disposent d’un bon inventaire, le nombre considérable d’applications cloud signifie que vous devez gérer plusieurs systèmes d’identité, augmenter les coûts et composer avec les risques de sécurité existants.

Expérience utilisateur médiocre : Les utilisateurs en pâtissent également. Ils apprécient la flexibilité mais sont contrariés par le nombre d’informations d’identification qu’ils doivent mémoriser.

Défis liés à la transition numérique

Risque en matière de sécurité

Fardeau administratif

Expérience utilisateur médiocre

Qu’est-ce que la gestion des identités et des accès ?

Gestion des identités et des accès en tant que plan de contrôle central

Le dénominateur commun à ces soucis est l’inefficacité des systèmes de vérification des identités. L’identité a remplacé le périmètre réseau en tant que nouveau plan de contrôle. Vous avez besoin de solutions qui connectent des outils, architectures, appareils et services disparates au sein de l’entreprise pour mieux protéger celle-ci et gérer l’accès tant des employés que des partenaires externes. Les systèmes de gestion des identités et des accès (IAM) unifient les accès sous un seul système, vous offrant ainsi plus de contrôle. Ils permettent une collaboration transparente au-delà des limites de l’organisation, tout en améliorant la sécurité de ses ressources. Une bonne solution IAM vous permet de connecter vos utilisateurs à toutes leurs applications professionnelles, tant dans le cloud que localement, via un ensemble d’informations d’identification. Les solutions IAM sont conçues pour donner aux utilisateurs l’accès uniquement aux ressources dont ils ont besoin et empêcher des utilisateurs non autorisés d’accéder à des données dont l’accès devrait leur être interdit. Vous gérez les droits d’accès et les autorisations des utilisateurs à partir d’un portail centralisé, réduisant ainsi une grande partie des processus manuels impliqués dans l’approvisionnement et le déprovisionnement des comptes d’utilisateur. Les solutions IAM fournissent également des outils pour gérer les stratégies de sécurité en lien avec les identités et les applications. Les meilleures solutions IAM protègent mieux les identités, améliorent l’expérience utilisateur et renforcent l’efficacité administrative.

Les solutions IAM relèvent ces défis

Mieux protéger les identités

Améliorer l’expérience utilisateur

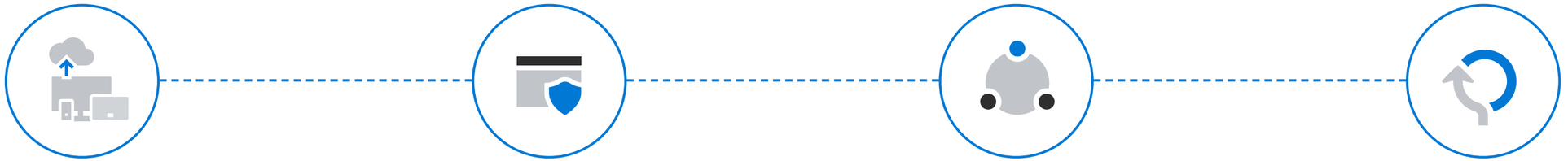
Renforcer l’efficacité administrative

Section 2

Vue d’ensemble d’Azure AD

Une solution complète

Microsoft Azure Active Directory (Azure AD) est une solution IAM complète dans le cloud à la pointe du secteur en matière de gestion des annuaires, d’accès aux applications et de protection des identités avancée. Azure AD permet aux organisations de gérer et sécuriser les identités des employés, partenaires et clients dans le cadre de l’accès aux applications et services dont ils ont besoin. Azure AD aide des millions d’organisations à gérer et à sécuriser plus d’un milliard d’identités.



Modernisez l’accès

Gérez et sécurisez l’accès aux données et ressources de votre organisation localement et dans le cloud. Connectez l’ensemble de vos utilisateurs, applications et appareils au cloud pour permettre un accès transparent et sécurisé ainsi qu’une visibilité et un contrôle accrus. L’automatisation les workflows et l’activation d’options en libre-service contribuent à réduire les coûts et à renforcer la productivité des utilisateurs.

Sécurisez et gouvernez

Compte tenu du volume élevé d’attaques quotidiennes visant les informations d’identification des utilisateurs, le moyen de prévenir des compromissions consiste à suivre continuellement les comportements normaux et anormaux sur la base de l’ensemble le plus large possible de signaux, à recourir à l’intelligence artificielle et à automatiser les réponses. Équilibrez la productivité et la sécurité en permettant un accès en temps opportun aux bonnes ressources et en mettant en place des révisions d’accès régulières et des stratégies.

Connectez et collaborez

Développez votre entreprise avec un service cloud fiable pouvant adapter son échelle à des millions d’utilisateurs tout en offrant une sécurité et une flexibilité de pointe. Connectez-vous avec vos utilisateurs externes et permettez-leur d’être productifs au travers d’expériences conviviales en libre-service et de contrôles de sécurité intégrés.

Développez et intégrez

Créez des applications qui permettent aux utilisateurs de se connecter facilement avec leur compte Microsoft personnel, professionnel ou scolaire, ou avec leurs comptes sociaux. Commencez à vous connecter à Microsoft Graph, la passerelle d’accès aux données et au renseignement dans Microsoft 365, et créez des applications riches. Activez l’authentification unique et automatisez l’approvisionnement des utilisateurs pour atteindre les plus grandes organisations du monde.

Section 3

Azure AD pour vos applications

Azure AD pour vos applications

Une plateforme universelle

Azure AD vous permet de gérer une identité commune à tous les utilisateurs de votre infrastructure hybride, grâce à laquelle ceux-ci peuvent accéder à toutes les applications dont ils ont besoin, dont des applications métier locales et dans le cloud. Gérez toutes vos identités à partir d'une plateforme universelle augmentant l'efficacité administrative et vous donnant plus de contrôle. Appliquez des stratégies de sécurité précises à chacune des applications utilisées au sein de votre organisation.

Azure AD pour vos applications

Économisez du temps et de l'argent

Azure AD est pré-intégré avec des milliers d'applications, dont des solutions populaires telles que Workday, ServiceNow, SuccessFactors, Adobe et Concur, ce qui simplifie la mise de ces applications à la disposition de vos utilisateurs. Déployez des stratégies cohérentes et surveillez les droits d'accès à partir d'une seule console. Vous pouvez automatiser les workflows pour l'approvisionnement des utilisateurs et la gestion du cycle de vie, ainsi qu'économiser du temps et des ressources grâce à la gestion des comptes en libre-service. Vous pouvez également gérer des informations utilisateur entrantes à l'aide d'outils de RH en tant que source de vérité éliminant la nécessité de recourir à des scripts personnalisés ou à des processus manuels pour gérer les attributs d'utilisateur.

Les applications configurées via Azure AD permettent une authentification unique (SSO) pour un accès transparent, ce qui signifie que les utilisateurs n'ont pas à mémoriser des informations d'identification pour chaque compte d'application ou à réutiliser des mots de passe faibles au risque de violer des données. Les comptes configurés pour l'approvisionnement automatique permettent aux utilisateurs d'accéder à de nouvelles ressources dès qu'elles sont disponibles. Pour l'approvisionnement entrant, Azure AD garantit que les nouveaux employés ont accès à toutes les ressources dont ils ont besoin dès le premier jour.

Économies de temps et d'argent

Intégration de SaaS

Authentification unique

Accès des utilisateurs dès le premier jour

Azure AD pour vos applications

Fournissez un accès plus sécurisé à toutes vos applications

Azure AD offre une protection complète des identités sur toutes les applications, qu'il s'agisse d'applications SaaS ou d'applications métier locales. Que l'utilisateur demande l'accès à Microsoft Word ou à Box, Azure AD s'assure que son identité est confirmée avant de lui accorder l'accès. Vous pouvez également mettre en place des stratégies de gouvernance des accès pour garantir que les utilisateurs n'ont accès qu'à ce dont ils ont besoin, quand ils en ont besoin. Vous pouvez exiger des utilisateurs qu'ils demandent l'autorisation d'accès, ainsi que définir une période pendant laquelle ils peuvent accéder à l'application et qu'examiner régulièrement la conformité de l'accès.

Azure AD tire également parti de la puissance de Microsoft Intelligent Security Graph et du Machine Learning pour analyser des billions de signaux sur tous nos produits et services afin de détecter des comportements atypiques et d'évaluer le risque associé à chaque session. Azure AD examine l'appareil, l'emplacement et d'autres informations contextuelles pour évaluer le risque de la connexion. Vous pouvez mettre en place des stratégies d'accès conditionnel Azure AD qui appliquent automatiquement des mesures de sécurité telles que le blocage d'une demande d'accès, ou exigent la réinitialisation d'un mot de passe quand une connexion est jugée risquée ou certaines conditions sont réunies.

Mesures de sécurité de l'application

Protection des identités

Gouvernance des accès

Stratégies d'accès conditionnel

Section 4

Comment gérer et sécuriser des applications avec Azure AD

Azure AD aide à garder le contrôle et à réduire les coûts grâce à l’automatisation, au libre-service et à l’application de stratégies.

Comment gérer et sécuriser des applications avec Azure AD

Intégrations d'applications Azure AD

La galerie d'applications Azure AD facilite la configuration et la connexion de n'importe laquelle des milliers d'applications pré-intégrées à votre locataire. Toutes ces applications prennent en charge l'authentification unique, et il est facile de les configurer pour l'accès conditionnel Azure AD que ce soit individuellement ou par le biais de stratégies à l'échelle de l'entreprise. Après que vous avez ajouté et configuré l'application conformément à vos besoins, les utilisateurs disposant d'un accès autorisé peuvent facilement la trouver dans le portail Mes applications d'Azure AD qui centralise la découverte et le lancement d'applications pour les utilisateurs finaux.

Si vous avez créé une application ou si vous en avez besoin d'une application intégrée pour votre organisation, vous pouvez également demander qu'elle soit répertoriée dans la galerie d'applications Azure AD.

Explorez les milliers d'applications pré-intégrées >

Accès hybride sécurisé

Utilisez le proxy d'application Azure AD pour fournir un accès distant sécurisé à une application web locale basée sur des revendications sans nécessité de disposer d'un VPN. Le proxy d'application nécessite l'installation d'un connecteur léger et offre la même expérience informatique et d'utilisateur final que les applications SaaS connectées via la galerie d'applications Azure AD.

Ou bien, si vous souhaitez tirer parti d'une infrastructure existante de partenaires tels que F5 ZScaler, SAP, Oracle ou Ping Identity, pour connecter d'autres types d'applications, par exemple, de celles qui utilisent des protocoles d'authentification basés sur l'en-tête ou Kerberos, vous le pouvez en continuant de bénéficier des avantages de centralisation et de sécurité d'Azure AD.

Découvrez comment ajouter une application locale via un proxy d'application >

Connectez d'autres réseaux d'application et clouds partenaires >

Comment gérer et sécuriser des applications avec Azure AD

Approvisionnement automatisé

Azure AD vous permet d'automatiser la création, la maintenance et la suppression d'identités d'utilisateur dans des applications SaaS populaires. Vous pouvez créer automatiquement des comptes dans les systèmes appropriés pour de nouvelles personnes rejoignant votre équipe ou votre organisation. Vous pouvez définir des stratégies qui désactivent automatiquement dans certains systèmes les comptes de personnes quittant une équipe ou une organisation. En automatisant ces tâches, vous pouvez vous assurer que les identités dans vos applications et systèmes sont tenues à jour en fonction des modifications apportées à l'annuaire ou à votre système de ressources humaines, ce qui permet de limiter les erreurs et de gagner du temps.

Apprenez-en davantage sur la configuration de la fourniture et de la désaffectation automatisées d'applications SaaS >

Gestion des groupes

Azure AD vous aide à donner accès aux ressources de votre organisation en octroyant des droits d'accès à un utilisateur ou à un groupe d'utilisateurs. L'utilisation de groupes permet au propriétaire d'une ressource de définir des autorisations d'accès pour tous les membres du groupe, au lieu de devoir accorder les droits individuellement. Cette méthode est plus sécurisée car vous êtes moins susceptible d'accorder accidentellement un accès individuel inapproprié, et elle peut vous faire gagner du temps. Vous pouvez également mettre à l'échelle de façon dynamique la gestion de votre groupe en automatisant l'inscription via des stratégies basées sur des attributs d'identité.

Découvrez comment créer un groupe dans le portail Azure >

Comment gérer et sécuriser des applications avec Azure AD

Libre-service pour les utilisateurs

Azure AD vous permet de déléguer certaines tâches ne nécessitant pas l'intervention d'un professionnel de l'informatique à d'autres personnes au sein de l'organisation. Vous pouvez autoriser des utilisateurs à créer et à gérer leurs propres groupes de sécurité dans Azure AD. Un propriétaire de groupe peut approuver ou refuser des demandes d'adhésion, ou déléguer le contrôle de l'appartenance au groupe.

Configurez des groupes autogérés >

Le libre-service s'étend également aux utilisateurs. Le portail en libre-service permet aux utilisateurs titulaires d'un e-mail vérifié de créer un compte, ainsi que de réinitialiser leur mot de passe. Cela permet à votre service d'assistance d'économiser du temps et de l'argent.

Configurez la réinitialisation du mot de passe en libre-service >

Modernisez l'authentification

Si vous utilisez actuellement un mode d'authentification locale tel que les services de fédération Active Directory (AD FS), vous pouvez envisager de migrer vos applications vers Azure AD. Vous conservez des avantages tels que l'authentification unique pour les utilisateurs, et bénéficiez en outre des avantages d'évolutivité et de sécurité qu'offre le cloud, tels que l'application de contrôles d'accès granulaires par application à l'aide de l'accès conditionnel Azure AD ou l'octroi à des partenaires d'un accès aux ressources grâce à Azure AD B2B Collaboration. Vous pouvez migrer toutes les applications qui utilisent les normes SAML 2.0, WS-Federation, OAuth ou OpenID Connect pour la connexion fédérée.

Élaborez des stratégies d'accès conditionnel Azure AD pour sécuriser l'accès à vos applications >

Utilisez Azure AD B2B pour collaborer en toute transparence avec vos partenaires externes >

Connectez en toute sécurité à Azure AD toute application sur n’importe quel cloud ou serveur.

1 million d’applications uniques actives connectées.

Microsoft

Commencez dès aujourd'hui.

Commencez à utiliser la version d'évaluation gratuite d'un mois d'Azure AD pour découvrir à quel point il est simple de gérer l'accès des utilisateurs à toutes vos applications et de sécuriser votre entreprise.