Microsoft

LA TECHAUCARRÉ

Comprendre la stratégie identité de Microsoft

Novembre 2020

Philippe Beraud, Microsoft France

Table des matières

Introduction 03

Un constat : Le monde a évolué 04

Le cloud est en train de recâbler le monde qui change à un rythme rapide 04

Les services d'identité Microsoft aujourd'hui 05

La stratégie Identité de Microsoft 07

Commencer par un état d'esprit de co-ingénierie 07

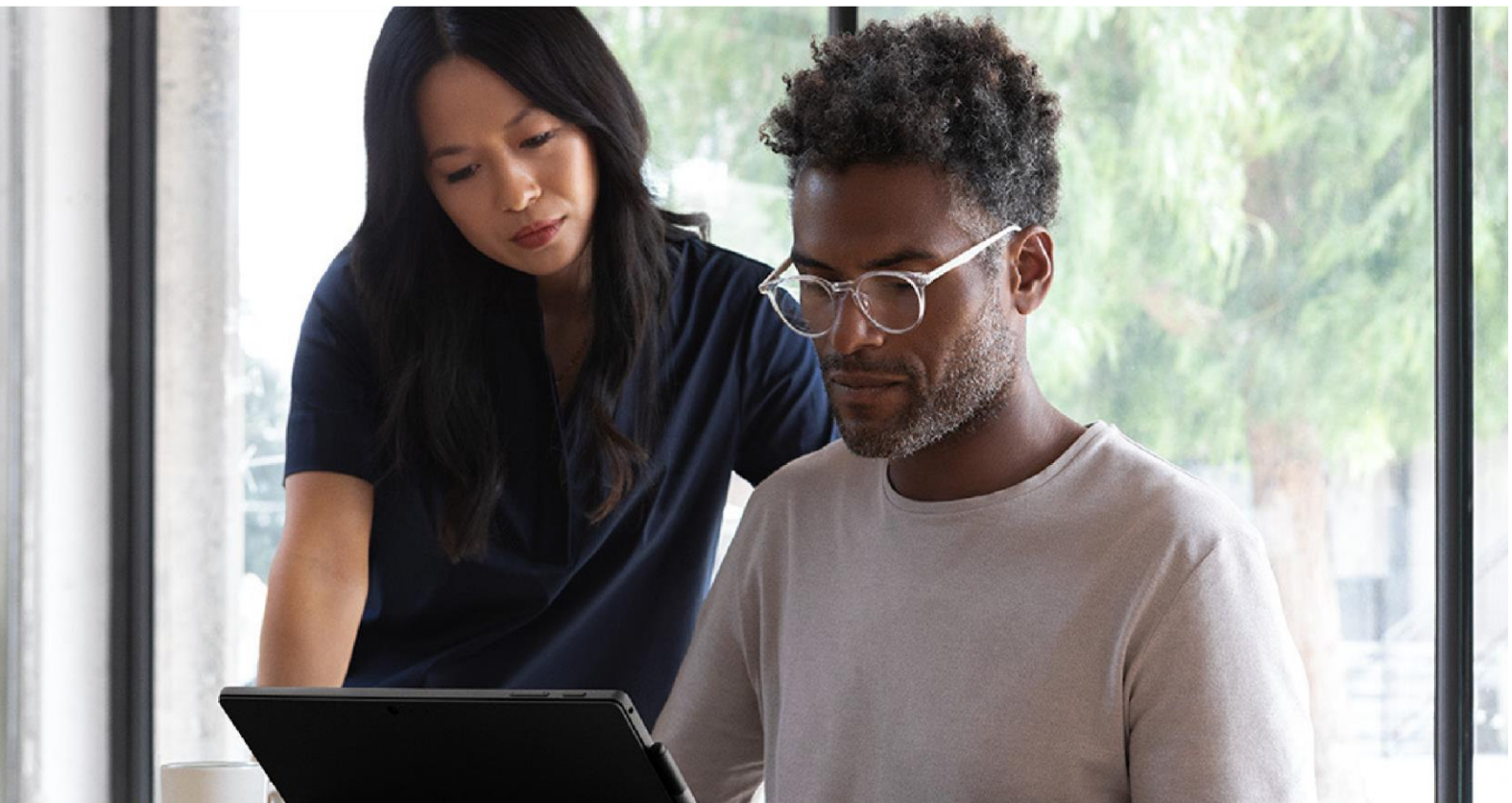
Développer et favoriser un écosystème partenaire solide 08

Être guider par des principes directeurs 09

Les 5 priorités de l'identité pour 2020 - 2021 14

Le paysage de l'identité au-delà de 2020 24

Conclusion 27



Introduction

La technologie numérique est omniprésente dans nos vies et le monde change effectivement très vite. Le rythme tend même à s'accélérer.

Dans un monde où l'actualité ne cesse de parler d'« Ubérisation », nous trouvons intéressant de citer ici Bertolt Brecht (1898-1956), un poète allemand avec une pensée politique et sociale :

Parce que les choses sont comme elles sont, les choses ne resteront pas telles qu'elles sont.

Un bel aphorisme sur l'évolution sociale, l'évolution technologique, et leur moteur.

Facteur de croissance, d'innovation et de différentiation sur un marché à la concurrence exacerbée, la transformation numérique est en marche.

Cette transformation impose de considérer de nouvelles technologies, de nouveaux usages et de nouveaux modèles d'affaire.

A ce titre, nous vivons aujourd'hui certainement une des périodes les plus intéressantes et importantes en termes de transformations technologiques. Le cloud constitue un élément tellement transformationnel, qu'il définit de facto dans la pratique l'ère dans laquelle il se trouve. Le cloud est en effet tellement disruptif que l'on peut parler de l'ère du Cloud.

Nous avons avec l'avènement de cette nouvelle ère nombre de défis à relever. Mais dans le même temps, le cloud apporte d'innombrables ressources pour s'atteler à ces défis. Si le cloud rebat toutes les cartes, les opportunités de transformation (numérique) sont nombreuses en particulier pour embrasser des scénarios de collaboration B2B, B2C, B2B2C, G2C pour de nouveaux usages, de nouveaux d'affaires - nous n'avons pas le temps de toutes les considérer – les interrelations, les interpénétrations tout autant.

Ceci étant, nous retrouvons en fait une constante dans ces opportunités : il n'est pas possible de concevoir une économie numérique sans identité.

Dans ce contexte, quels sont les propositions de Microsoft en la matière ? Quelle est sa stratégie ? Quels en sont les principes structurants ? les priorités d'investissement du moment ? pour la décennie à venir ?

C'est ce que nous vous proposons de découvrir dans ce livre blanc.

Un constat : Le monde a évolué

(1) 2018 Thales Data Threat Report: 94% of organizations using cloud, IoT and other transformative technologies, data breaches at all-time high
(2) Syntonic 2016 Employer Report: BYOD Usage in the Enterprise
(3) State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time

Le cloud est en train de recâbler le monde qui change à un rythme rapide

Des vagues de changements multiples se sont succédées avec la rationalisation de l'informatique, le passage au numérique grâce à l'économie des API, la consumérisation de l'IT, l'entrée dans le monde de l'internet des objets ou IoT (industriel) et la périphérie du cloud (Edge), la généralisation de l'analytique avancées et de l'Intelligence Artificielle (IA) avec une utilisation croissante de modèles partout, etc.

Dans ce (nouveau) monde, il n'est pas possible de concevoir une économie numérique sans identité. Ceci propulse l'identité au premier rang d'importance en connaissant et en reconnaissant les personnes, les applications, les appareils, etc. afin qu'ils puissent être autorisés le cas échant (de façon adaptive en fonction du contexte et des risques afférents) à accéder à/utiliser l'information de l'organisation n'importe où, à celles d'autres organisations dans le cadre des dynamiques de collaboration et de partenariat en place, etc.

A un moment où toutes les frontières s'estompent, et pas uniquement le périmètre de sécurité, il est nécessaire de connaître les noms et les caractéristiques des entités numériques et physiques avec lesquelles nous interagissons :

- Il faut être en mesure d'authentifier les entités lors d'une interaction avec elles,
- De disposer d'un moyen de stocker de l'information sur elles,
- De pouvoir découvrir cette information,
- De faire tout cela au-delà des limites organisationnelles, tout en empêchant l'accès non autorisé, en limitant l'accès de façon adaptative le cas échéant en fonction du contexte et du risque associé

Toutes les hypothèses sur lesquelles nous avons construit nos anciens modèles ont changé. Il est remarquable de voir à quel point la transformation numérique a remodelé la façon dont les personnes travaillent et la façon dont les entreprises font des affaires. Prenons un exemple : vos utilisateurs.

À une certaine époque, vos « utilisateurs » désignaient uniquement les employés. Vos utilisateurs incluent désormais vos partenaires, vos clients, voire des robots logiciels (*bots*) et des appareils connectés de toute sorte. Ce qui a commencé comme identité pour la « main-d'œuvre » est maintenant l'identité pour tout le monde et tout. Le périmètre du réseau d'entreprise a disparu, faisant de l'identité le plan de contrôle de la sécurité qui offre désormais un contrôle d'accès efficace à tous les utilisateurs et ressources numériques.

Cela rend l'identité absolument essentielle au succès commercial de nos clients. Il n'est pas seulement essentiel à la sécurité, mais également à la transformation de votre organisation.

Les services d'identité Microsoft aujourd'hui

Microsoft est aujourd'hui l'un des plus grands fournisseurs d'identité avec le service de comptes pour tous vos produits Microsoft (Microsoft Accounts) pour les comptes personnels et le service d'identité d'entreprise Azure Active Directory (Azure AD) pour les comptes professionnels ou scolaires.

Comme solution d'identité sous forme de service (Identity-as-a-Service ou IDaaS), Azure AD est une plateforme d'identité universelle qui vous permet de gérer et de sécuriser tous vos utilisateurs quels qu'ils soient et d'accéder à toutes vos applications quelles qu'elles soient où qu'elles soient.

Cette plateforme propose pour cela un ensemble de capacités pour assoir les **4 « A » de l'identité**, à savoir :

- **Administration** dans un monde hybride et multicloud avec une synchronisation entre les différents « domaines de sécurité » et une gestion des identités privilégiées.
- **Authentification** unique pour simplifier l'accès à toutes vos applications en tout lieu, avec l'authentification multifacteur pour vous aider à protéger vos utilisateurs contre 99,9 % des attaques de cybersécurité.
- **Autorisation** (ou contrôle d'accès) conditionnelle intégrant différentes dimensions dont les risques relatifs à l'utilisateur et à la session.
- **Audit** avec la revue régulière des accès, des privilèges accordées, etc.

Et qui couvrent les utilisateurs internes ET externes, les appareils, les données et les applications, Cf. Qu'est-ce qu'Azure AD ?

Microsoft est aujourd'hui l'un des plus grands fournisseurs d'identité

Azure AD un service d'identité véritablement mondial qui opère à très grande échelle avec :

- Plus de 21 millions d'organisation dont 200 000 avec des abonnements premium.
- Plus de 345 millions d'utilisateurs actifs par mois, avec une moyenne de 35 milliards de demandes d'authentification quotidiennes ; beaucoup plus que ce que certains de nos compétiteurs peuvent renvidiquer en une année complète

Le cloud, son niveau d'adoption (avec l'effet de réseau), sa portée, son degré d'automatisation, la généralisation des politiques ou stratégies, l'intelligence et l'analytique sur la masse des signaux générés ou captées, les capacités qui en découle influent sur le monde de l'identité, et conduisent à l'image d'Azure AD à de meilleures solutions IDaaS plus simples et plus naturelles pour les personnes et utilisateurs que nous sommes (employées, partenaires, consommateurs, usagers, etc.), les appareils, les machines, et autres objets connectés, c.à.d. les choses – *the things* – de l'IoT (industriel), les robots logiciels, etc.

La stratégie Identité de Microsoft

En juin dernier, Joy Chick, Corporate Vice President, Microsoft Identity, a partagé les 5 principes à la base d'une stratégie d'identité chez Microsoft « obsédée par le client ».

Vis-à-vis de ce « nouveau » monde, si beaucoup d'organisations avaient admis/adopté l'idée d'un environnement désormais sans frontières, mais relativement peu l'avaient mise en œuvre dans la pratique. La pandémie mondiale que nous connaissons encore a rendu l'accès à distance essentiel et a contraint nombre d'entre elles à accélérer leurs plans de transformation numérique.

La nouvelle réalité nécessite non seulement de prendre en charge la productivité et la collaboration sécurisées à distance, mais également d'autres opérations à distance, telles que l'intégration, la formation, ou encore la sortie des employés. Et cette réalité se poursuivra dans un proche avenir. Selon notre indice de vie professionnelle le plus récent, 71% des employés et des responsables managériaux (*Information Workers*) ont déclaré vouloir continuer à travailler à domicile au moins à temps partiel après la pandémie. Le monde physique sera vraisemblablement hybride comme le monde numérique mais dans d'autres dimensions.

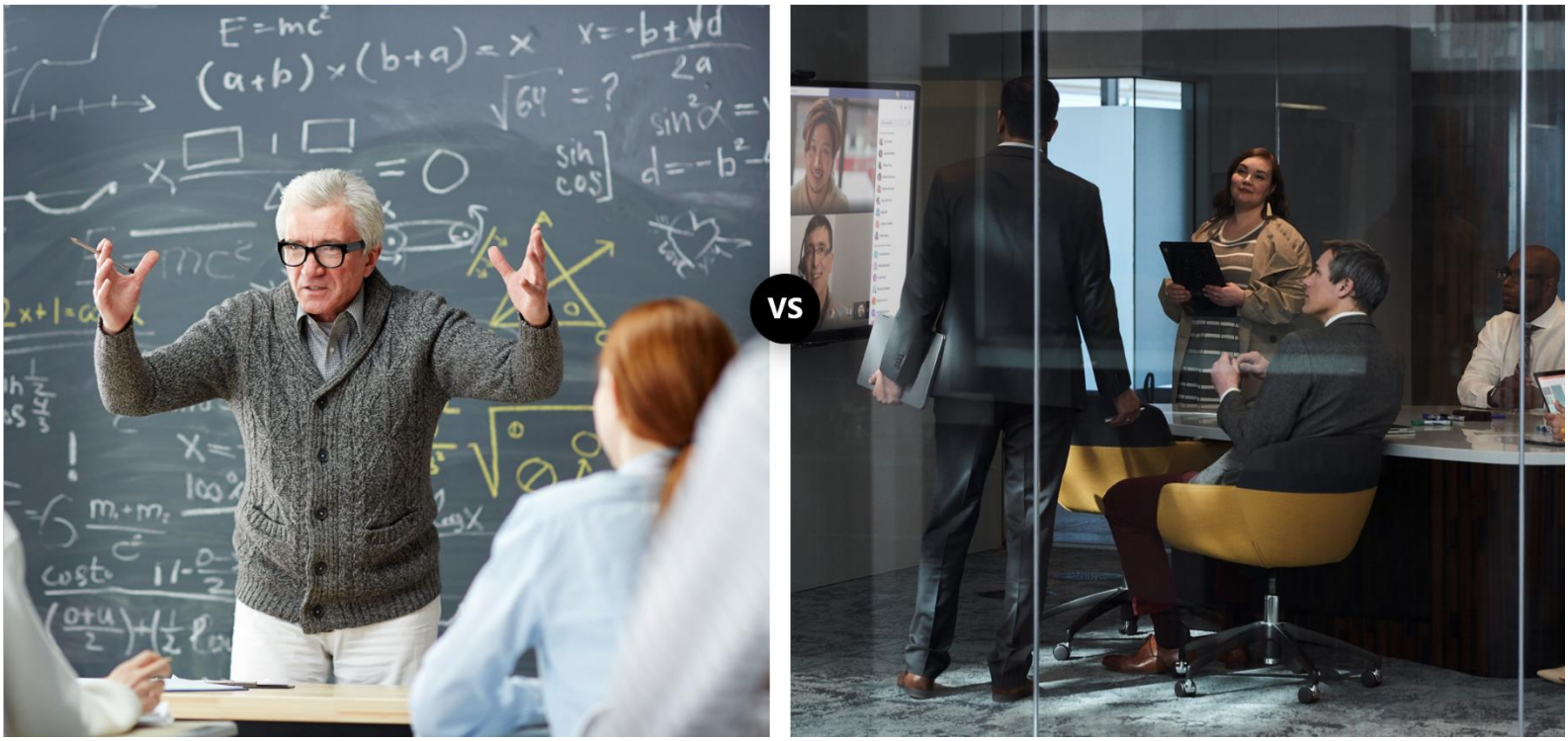
Vos expériences et vos connaissances ont contribué et continuent à façonner les investissements que nous faisons dans nos services d'identité pour cette fin d'année, l'année à venir et au-delà.

Avec une obsession pour nos clients et partenaires, nous suivons 5 principes directeurs pour proposer une solution d'identité sécurisée et évolutive, transparente pour vos utilisateurs finaux. Cf. 5 principles driving a customer-obsessed identity strategy at Microsoft et Guiding principles of our identity strategy: staying ahead of evolving customer needs.

Commencer par un état d'esprit de co-ingénierie

L'ère du cloud a radicalement changé la façon dont les organisations doivent penser la sécurité. Pendant longtemps, nous avons construit la sécurité autour du périmètre. Mais aujourd'hui, le paysage sans frontières exige que nous commencions par l'individu.

Il n'est pas question aujourd'hui du professeur dans sa tour d'ivoire mais d'un nuage collaboratif de clients et partenaires pour coconcevoir nos produits et services.



Au cours de notre parcours avec les clients en co-conception, nous avons appris que nos solutions d'identité doivent faire plus que simplement soutenir la productivité de vos employés. Nous devons aller plus loin pour nous assurer que nos solutions vous permettent de travailler plus étroitement avec vos partenaires de toute sorte et de toute taille et d'entretenir des relations plus étroites avec vos clients, qui attentent des garanties quant à la sécurité de leurs informations personnelles et la protection de leur vie privée. Les problèmes que vous devez résoudre et les scénarios que vous souhaitez voir se concrétiser pour votre résilience dans la situation courante, votre avenir et votre expansion future ont façonné et façonne les principes de conception qui guident notre stratégie en matière d'identité. La résolution de vos problèmes nous anime. Cf. Solving real problems for real customers.

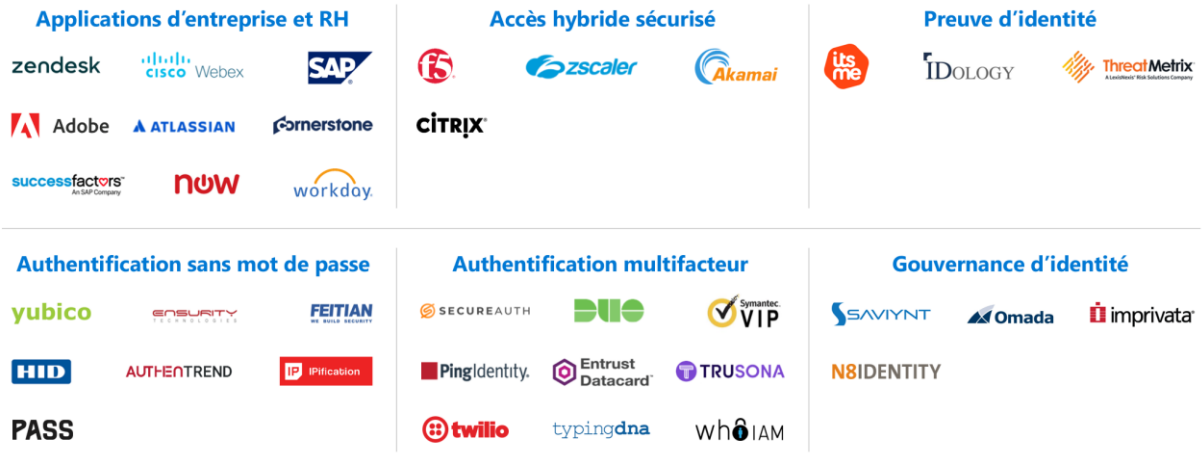
À cette fin, et à titre d'illustration, l'invitation à participer à une série d'aperçus technologiques – ce que nous appelons préversion privée (*private preview*), préversion publique (*public preview*) avant tout disponibilité générale (*general availability*) - est au cœur de cet effort, où vos commentaires aident à façonner la façon dont les services d'identité nous rapprocheront d'un monde sans mot de passe, où les organisations peuvent facilement gérer et sécuriser les environnements complexes et les personnes individuelles peuvent moins s'inquiéter et cesser de faire des compromis entre la facilité d'utilisation, la protection de la vie privée, et la sécurité…

Développer et favoriser un écosystème partenaire solide

Nous travaillons en partenariat avec nombre des principaux éditeurs de logiciels indépendants (ISV) pour intégrer leurs solutions qui font sens à notre plateforme.

Nous croyons en effet en un écosystème riche et ouvert pour aider les organisations comme la vôtre à faire plus, plus facilement et plus simplement.

Nous nous intégrons à une grande variété de partenaires dans les applications d'entreprise, la gestion des ressources humaines, les scénarios hybrides, la vérification des preuves d'identités, l'authentification sans mot de passe, l'authentification multifacteur et la gouvernance des identités.



Quelques annonces sur le blog Azure AD (aka.ms/identityblog) :

- SAP SuccessFactors : Ring in the New Year with automated user provisioning from SAP SuccessFactors to Azure AD.
- F5 : Azure AD + F5—helping you secure all your applications.
- Clés de sécurité sans mot de passe : Replace passwords with a biometric security key.

Être guider par des principes directeurs

01 Adopter des standards ouverts

Le monde du cloud, celui de sa périphérie (*Edge*) et des appareils est intrinsèquement hétérogène.

Nos clients, leurs partenaires et leurs clients utilisent d'ores et déjà ou utiliseront de nombreux appareils, applications et services de nombreux fournisseurs différents. La complexité de la gestion et de la sécurisation d'un environnement aussi varié pourrait être écrasante s'il n'y avait pas de standards ouverts.

Par exemple, les protocoles de l'industrie OAuth 2.0, Open ID Connect (OIDC) et SAML 2.0 permettent une authentification unique (*single sign-on* ou SSO) entre les applications et les clouds de plusieurs fournisseurs, SCIM (*System for Cross-domain Identity Management*) le provisionnement automatisé des utilisateurs et les nouveaux standards de l'Alliance FIDO (*Fast IDentity Online*) rendent la connexion plus sécurisée. C'est pourquoi chaque API REST et protocole pris en charge par Azure AD est basé sur des standards ouverts et pourquoi Microsoft est activement engagé dans tous les principaux organismes de normalisation et de standardisation d'identité, ainsi que des fondations qui s'investissent dans l'émergence de nouveaux schémas et modèles d'identité à l'image de la fondation DIF (*Decentralized Identity Foundation*).

En adoptant des standards ouverts, en y contribuant de façon active - Microsoft est co-éditeur de la spécification Open ID Connect par exemple -, nous pouvons vous aider non seulement à gérer et à sécuriser plus facilement votre environnement hybride et potentiellement multicloud mais également à accélérer dans votre innovation. Cf. The role of standards in accelerating innovation.

02 Offrir une sécurité de pointe

Selon nos propres recherches, nous avons constaté une augmentation de 300 % des attaques d'identité au cours de l'année écoulée et la pandémie actuelle ne fait que confirme tout cela. Quelques chiffres que bous souhaitons vous partager quant à notre plateforme d'identité :

- 27 millions de comptes utilisateurs compromis (détectés) en 2019
- 30 milliards de tentatives de connexion malveillantes bloquées en temps réel en 2019
- 900 000 tentatives de connexion à haut risque détectées en octobre 2019

Ces capacités de détection sont ici le résultat de la fonctionnalité de la protection d'identité d'Azure AD, et des classifieurs et les modèles de Machine Learning (apprentissage automatique) mis en œuvre au sein de nos systèmes tirent parti des quelques 8000 milliards de signaux corrélés par jour au niveau du graphe de sécurité Microsoft intelligent qui synthétise l'ensemble des renseignements sur les menaces et de signaux de sécurité provenant de tous les produits, services et partenaires Microsoft à l'aide d'analyses avancées pour identifier et atténuer les cybermenaces. Cf. We collect 8 trn threat signals daily, says Microsoft's Ann Johnson.

Notre objectif est de créer un système d'identité digne de confiance, et donc sécurisé, ancré dans le respect et la protection de la vie privée. Cela signifie bloquer toutes les voies d'attaque que nous pouvons.

Dans une enquête récente menée auprès de plus de 500 responsables de la sécurité, atteindre un niveau de protection élevé sans entraver la productivité des utilisateurs a été considéré comme le défi numéro un.

Nous mettons toute la puissance du cloud derrière chaque demande d'authentification. À l'aide de stratégies d'accès conditionnel basées sur les risques dans Azure AD, vous pouvez protéger les données sensibles avec un minimum de friction pour vos utilisateurs finaux.

Désormais gérées comme du code via des APIs, les stratégies vous permettent de définir les conditions d'authentification des utilisateurs et d'accéder aux applications et aux données, afin d'examiner non seulement l'identité de l'utilisateur, mais également le type et la santé de leur appareil, les propriétés et la réputation du réseau auquel/à partir duquel ils se connectent, l'application qu'ils utilisent et la sensibilité des données auxquelles ils essaient d'accéder. Cela renforce non seulement la sécurité, mais améliore également l'expérience utilisateur.

Cela se combine également avec la puissance de la protection d'identité pour avertir les utilisateurs uniquement lorsque la connexion est considérée comme risquée. Comme souligné ci-dessus, nous utilisons ici des algorithmes de Machine Learning qui traitent les milliards de signaux du graphe de sécurité Microsoft intelligent pour apprendre les modèles de comportement courants de chaque utilisateur et signaler les tentatives d'authentification qui sont anormales ou à haut risque. De cette façon, les stratégies invoquent l'authentification multifacteur (MFA) ou d'autres mesures supplémentaires uniquement lorsque cela est nécessaire, ce qui rend l'expérience moins perturbatrice pour les utilisateurs.

Alors que l'accès conditionnel protège les ressources des demandes suspectes, la protection de l'identité va plus loin en fournissant une détection continue des risques et une remédiation des comptes d'utilisateurs suspects. La protection de l'identité vous tient informé 24h/24 et 7j/7 des utilisateurs suspects et des comportements de connexion dans votre environnement. Sa réponse automatique empêche de manière proactive les identités compromises d'être abusées.

Il s'agit de vous offrir les capacités suivantes :

- **Une détection continue en temps réel** pour i) surveiller les alertes de sécurité qui affectent les identités de votre organisation avec un risque de connexion et un risque utilisateur continus et agrégés en temps réel et recevoir des alertes lorsque le risque d'un utilisateur atteint un seuil spécifié.
- **Une protection proactive** pour i) définir des stratégies pour bloquer automatiquement les connexions au-dessus d'un certain seuil de risque (élevé, moyen), ii) examiner les alertes et iii) automatiser les réponses pour les scénarios courants.
- **Une intelligence connectée** afin i) d'examiner les utilisateurs et les connexions à risque pour résoudre les vulnérabilités potentielles et ii) aller plus loin si vous constatez un incident suspect et mettre en corrélation les alertes avec d'autres solutions Microsoft à l'image d'Azure Sentinel, notre solution de SIEM réinventée (*Security Information and Event Management*) et SOAR (*Security Orchestration and Automated Response*) pour orchestrer des opérations de sécurité de nouvelle génération avec le cloud et l'intelligence artificielle afin d'augmenter l'intelligence et la rapidité de la détection des menaces et de la réponse à celles-ci. Cf. Changement SIEM : comment le Cloud transforme les opérations de sécurité.

Pour améliorer la sécurité de l'identité, nous investissons par ailleurs dans des technologies de prévention des compromissions telles que les valeurs par défaut de sécurité, le blocage des attaques et la protection par mot de passe, ainsi que des systèmes de réputation et anti-abus. Les mécanismes de sécurité tels que les notifications des utilisateurs finaux et les interruptions en ligne peuvent aider tout le monde à se défendre contre les acteurs malveillants.

Chaque jour, nos data scientists et nos analystes évaluent la menace, traitent des données pour recueillir des informations concrètes, afin de pouvoir ajuster nos algorithmes de Machine Learning pour reconnaître et protéger nos clients contre les dernières menaces.

03 Fournir une solution complète, pas des blocs de construction

Pour une gestion unifiée des identités

L'une des principales choses que nous avons apprises de nos clients professionnels est qu'ils en ont assez de concocter des solutions d'identité basées sur des ensembles « *mix and match* » de blocs de construction d'identité acquis auprès d'une myriade de fournisseurs - Il est difficile de faire évoluer et de gérer la sécurité lorsque vous avez des produits qui se chevauchent de plusieurs fournisseurs qui doivent travailler ensemble sans avoir forcément été conçu pour ; ce qui n'arrange rien -.

De plus en plus nombreux sont celles et ceux qui veulent une solution holistique qui prenne en charge toutes leurs applications et toutes leurs identités différentes tout en leur donnant sécurité et contrôle sans les lacunes et « les trous dans la raquette » qui se produisent inévitablement lorsque de multiples solutions disparates bien que potentiellement à l'état de l'art sont intégrées ensemble, sans parler de l'effort à consacrer pour cela.

C'est l'objectif que nous poursuivons en fournissant une suite de gestion des identités et des accès complètement intégrée vous confère un seul lieu où aller pour gérer - et protéger - toutes vos identités, qu'elles appartiennent à vos employés, vos partenaires commerciaux ou vos clients et toutes les ressources auxquelles ils besoin d'accéder.

Azure AD fournit une solution IAM (*Identity & Access Management*) / CIAM (*Customer Identity & Access Management*) complète avec des capacités vous permettant de gérer et de sécuriser les identités de votre organisation et au-delà.

Azure AD est votre plateforme universelle pour gérer et sécuriser les identités et accéder à toutes les applications depuis n'importe quel emplacement ou appareil avec un seul jeu de crédentités.

Avec l'identité comme plan de contrôle et Azure AD, vous débloquez une sécurité de classe mondiale.

Azure AD peut vous aider à connecter vos employés (distants) à n'importe quelle application avec une authentification unique (SSO) transparente et un accès sécurisé depuis n'importe quel lieu. Vous augmentez la productivité et réduisez les coûts grâce à des processus d'identité automatisés, tels que la gestion du cycle de vie de l'utilisateur, en ajoutant de nouveaux droits d'accès lorsqu'un employé ou un partenaire rejoint une équipe ou en change et en les révoquant lorsque la personne quitte l'organisation. Le portail en libre-service facilite dans le même temps la réinitialisation des mots de passe et la configuration de l'authentification multifacteur pour vos utilisateurs.

Azure AD propose des intégrations approfondies avec notamment Microsoft 365, Microsoft Intune, Microsoft Cloud App Security (*Cloud Access Security Broker*) afin de constituer une solution complète, intelligente et sécurisée pour aider vos employés à être encore plus productifs. (Azure AD sous-tend chaque service cloud Microsoft et vous l'utilisez donc très probablement déjà aujourd'hui si vous utilisez ces services.)

04 Rendre la gouvernance plus simple et plus automatique

Pour une gouvernance d'identité simplifiée

Si la mise en œuvre d'une gouvernance solide renforce les barrières de sécurité, la plupart des clients trouvent la tâche ardue. Accorder un accès est facile. S'en souvenir des mois plus tard pour supprimer cer accès pour chaque personne qui peut avoir changé de rôle ne l'est pas.

Les systèmes d'identité devraient faciliter l'attribution du bon accès aux bonnes personnes, par exemple, en automatisant le provisionnement et l'annulation de l'accès des utilisateurs en fonction d'un rôle d'utilisateur, d'un emplacement et d'une entité métier. Il devrait être plus facile pour les employés et les partenaires de demander un accès lorsqu'ils en ont besoin.

S'il est essentiel de pouvoir contrôler les demandes d'accès, les approbations et les privilèges de manière rapide et efficace, les solutions traditionnelles de gouvernance des identités et de gestion des accès privilégiés peuvent s'avérer lourdes et rigides. Cela est particulièrement vrai aujourd'hui alors que ces workflows sont désormais plus souvent effectués à distance qu'en personne.

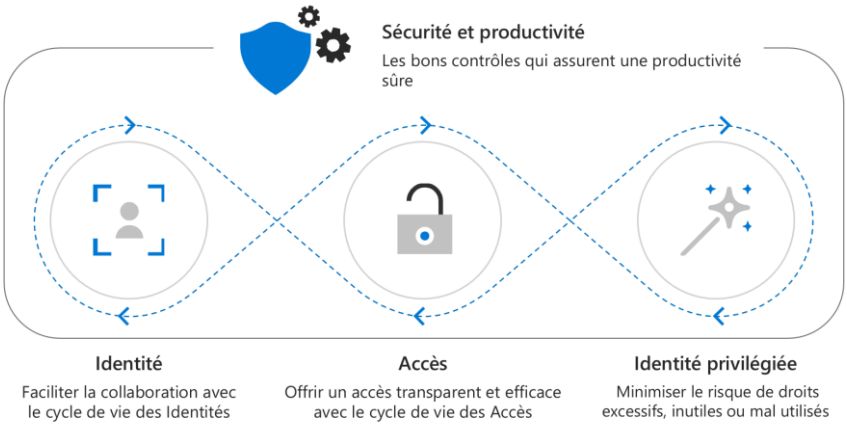
Fournir à chaque utilisateur l'accès aux applications et aux fichiers dont il a besoin devrait être aussi simple que de définir des packages d'accès et des attributions de groupe à l'avance. Il s'agit de permettre aux employés et aux partenaires commerciaux d'accéder aux ressources à l'échelle de l'entreprise et d'améliorer ainsi la productivité. L'intégration et le retrait des employés deviennent alors aisés avec une solution automatisée connectée à votre système RH.

Et surtout, pour contrôler constamment l'accès à toutes les applications en fonction des politiques organisationnelles et réglementaires, le système doit également inviter les administrateurs à notamment revoir les autorisations d'accès à une cadence régulière ou lorsque les personnes changent de rôle. Afin de simplifier le processus de mise en conformité, tous ces processus doivent être pilotés et éclairés par du Machine Learning à l'état de l'art et donc d'une IA qui surveillent en permanence les patterns ou modèles inhabituels et les risques non reconnus.

Nous souhaitons aider davantage d'entreprises à adopter ces scénarios et à intégrer notre technologie de Machine Learning dans Azure AD pour réduire les risques liés aux abus d'accès, prendre des décisions d'accès intelligentes, ou encore de fournir de meilleures recommandations et alertes en réponse à un comportement inhabituel ou à un trop grand nombre de privilèges inutiles.

Notre objectif est que ces capacités construites dans le cloud pour un bénéfice maximal compte tenu de la couverture et de la globalité des signaux disponibles couvrent à la fois les scénarios des identités des employés et celles des personnes externes. Cela aidera à renforcer votre sécurité globale, votre efficacité et votre conformité.

La gouvernance d'identité d'Azure AD vous permet d'accorder à chaque personne le niveau d'accès approprié aux ressources dont elle a besoin.



Il s'agit de protéger, surveiller et auditer l'accès à vos actifs (critiques) et plus précisément à date :

1. De vous assurer que **seuls les utilisateurs autorisés ont accès** en fonction des stratégies d'accès conditionnel appliquées.
2. De fournir à vos utilisateurs externes des **workflows pour demander l'accès**, d'approuver ces demandes au travers de **workflows d'approbation**.
3. De procéder à des **revues régulières des accès invité** afin de valider si l'accès est toujours nécessaire.
4. Et enfin d'établir des contrôles efficaces avec un accès limité dans le temps pour les **attributions de rôles privilégiés**.

Cf. Best practices to simplify governing employee access across your applications, groups and teams.

Les 5 priorités de l'identité pour 2020 - 2021

A présent que nous avons couvert les principes directeurs qui soutiennent notre stratégie d'identité, nous souhaitons partager avec vous cinq domaines à prioriser pour cette année fin d'année 2020 et l'année prochaine 2021, avant de conclure sur une nouvelle approche technologie à surveiller lorsque vous vous préparez pour la suite. Cf. 5 identity priorities for 2020 - preparing for what's next.

Ces priorités sont basées sur de nombreuses conversations que nous avons eues tout en travaillant en étroite collaboration avec nos clients pour les accompagner et les aider à réorganiser et moderniser leurs environnements dans le cadre de leur transformation.

Nos priorités

01 Connecter toutes les applications et les ressources cloud pour améliorer les contrôles d'accès et les expériences utilisateur

À mesure que les employés s'adaptent au travail à distance, ils ont besoin d'un accès sécurisé et transparent à tous les types d'applications, des applications cloud aux applications sur site. Les organisations visent à simplifier (et sécuriser) l'accès à leurs applications pour continuer à collaborer de n'importe où avec leur portefeuille d'applications sur site et basées sur le cloud qu'elles gèrent.

Nous simplifions ces expériences dans Azure AD, ce qui facilite la gestion de toutes vos applications pour tous vos utilisateurs en un seul endroit : **Azure AD en tant que plan de contrôle unique pour toutes vos applications**.

Notre principale promesse :

Azure AD est une solution d'identité de Microsoft, pas seulement pour Microsoft. Nous voulons nous assurer que vous pouvez connecter et sécuriser TOUTE application à Azure AD, afin que vous puissiez protéger l'intégralité de votre environnement.

Connecter toutes les applications - des applications Software-as-a-Service (SaaS) populaires aux applications locales en passant par les ressources cloud ou en périphérie - à un service d'identité cloud unique comme Azure AD donnera non seulement à vos utilisateurs une authentification unique (SSO) pour une meilleure expérience, mais améliorer également la sécurité.

Nous avons commencé comme un service d'identité pour Office 365 (désormais Microsoft 365), mais aujourd'hui Microsoft 365 ne représente qu'une fraction des applications que nous connectons.

Nous avons aujourd'hui plus de 2 millions d'applications tierces qui utilisent les identités Microsoft. La grande majorité de ces applications sont des applications métier (ou *Line-Of-Business*) propres à chaque organisation.

Bien sûr, ces applications s'ajoutent à nos applications de premier plan telles que Microsoft 365. Bien qu'elles soient petites dans le nombre d'applications, elles ont un très grand nombre d'utilisateurs.

Les applications que vous créez aujourd'hui gèrent leur authentification avec la même plateforme que Microsoft utilise pour sécuriser certaines des applications qui ont plus de 345 millions d'utilisateurs commerciaux actifs par mois.

De plus, des centaines de partenaires ont construit des intégrations qui prennent en charge l'authentification unique et le provisionnement des utilisateurs et notre galerie d'applications Azure AD est passée à plus de 3400 applications pré-intégrées, et plus à venir, afin que vous puissiez fournir aux utilisateurs un jeu de crédentités pour un accès sécurisé à n'importe quelle application. Nous continuons d'étendre les fonctionnalités d'Azure AD afin que vous puissiez migrer l'accès de toutes vos applications à gérer dans le cloud.

Alors que l'utilisation des applications cloud continue de croître, de nombreuses entreprises s'appuient toujours sur des applications basées sur l'authentification héritée. Grâce à nos partenaires d'accès hybride sécurisé - Akamai, Citrix, F5 networks et Zscaler - nous avons pu aider les clients à accéder à des applications basées sur l'authentification héritée qui utilisent des protocoles tels que l'authentification basée sur l'en-tête et Kerberos.

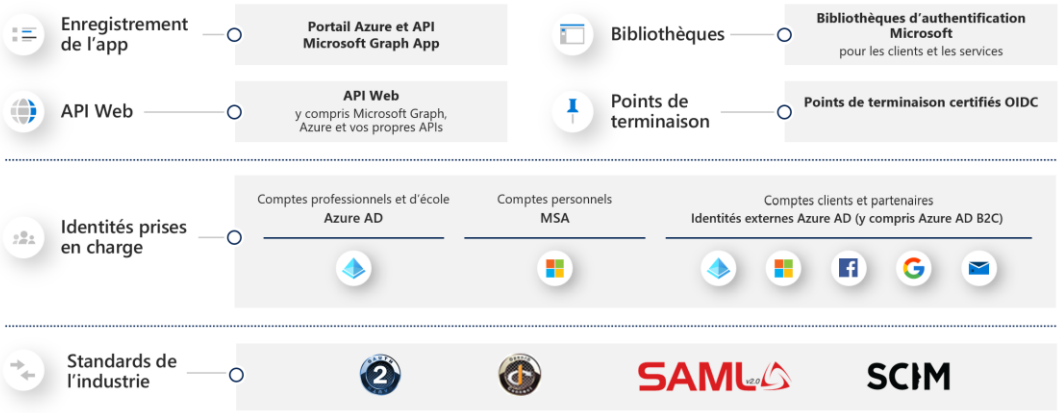
Avec Azure AD comme plan de contrôle unique pour toutes vos applications, vous bénéficiez d'une visibilité et de contrôles d'accès granulaires adaptatifs sur l'ensemble de votre parc numérique. Vous bénéficiez également des 171 téraoctets de données que nos algorithmes de Machine Learning à l'échelle du cloud traitent chaque jour pour apprendre les modèles de comportement de chaque utilisateur et application, signaler les attaques potentielles et les corriger. Par exemple, pour protéger les utilisateurs susceptibles d'être à risque, vous pouvez appliquer des stratégies simples telles que la réinitialisation forcée du mot de passe qui empêchent la compromission d'identité avec une perturbation minimale de l'utilisateur. Cf. Advancing Password Spray Attack Detection.

02 Permettre aux développeurs d'intégrer l'identité dans leurs applications et d'améliorer la sécurité

La plupart des organisations sont confrontées à une explosion d'applications, qui introduisent des exigences de sécurité et de confidentialité de plus en plus complexes. L'intégration à Azure AD améliore la sécurité et la confidentialité des applications. Mais suivre le flot de nouvelles applications tout en continuant à gérer un portefeuille déjà écrasant est un gros travail pour les administrateurs d'identité. Une aide serait la bienvenue.

Pour réussir, les administrateurs d'identité doivent déléguer davantage à leurs équipes de développement d'applications. Ainsi, nous permettons aux développeurs d'intégrer facilement l'authentification dans leurs

applications avec la plateforme d'identité Microsoft et de créer des applications et une automatisation basées sur les données avec Microsoft Graph.



Celle plateforme vous propose pour cela :

- Un portail pour enregistrer toutes vos applications connectées
- Un ensemble de bibliothèques d'authentification (*Microsoft Authentication Library* ou MSAL) pour créer des applications Web, mobiles et de bureau avec votre langage de programmation préféré
- Des points de terminaison, conformes aux standards ouverts de l'industrie, et certifiés lorsqu'un cadre de certification existe ; ce qui permet la compatibilité avec des bibliothèques tierces.
- Un accès sécurisé aux APIs REST de Microsoft Graph aux ressources Azure en passant par vos propres API protégées.

Cela vous donne la possibilité d'authentifier toute identité Microsoft, et y compris des comptes professionnels ou scolaires ou des comptes personnels. Votre application peut signer n'importe quel utilisateur externe tel que les identités sociales des clients, des identités d'entreprise de partenaires ou encore des comptes locaux créés pour la circonstance.

Comme bénéfice supplémentaire, les développeurs peuvent configurer des autorisations granulaires qui spécifient les privilèges minimums nécessaires pour chaque application, de sorte qu'elle ne puisse accéder qu'aux données Microsoft Graph nécessaires pour effectuer ses tâches.

Et notre plateforme prend en charge les standards ouverts de l'industrie. Donc, si vous avez une application existante basée sur ces standards, il est simple de connecter votre application.

Lors de la conférence Microsoft Build, nous avons annoncé plusieurs améliorations pour permettre aux développeurs de créer plus facilement des applications sécurisées et fiables. Nous avons déjà vu des centaines de développeurs faire vérifier l'éditeur, ce qui aide les administrateurs et les utilisateurs finaux à comprendre l'authenticité des développeurs d'applications qui s'intègrent à la plateforme d'identité Microsoft.

Lorsqu'une application est accompagnée de la mention « éditeur vérifié », cela signifie que l'éditeur a validé son identité à l'aide d'un compte Microsoft Partner Network auquel le processus de vérification a été appliqué jusqu'à son terme et qu'il a associé ce compte MPN à son inscription d'application. Plus de 660

demandes de 390 éditeurs ont été vérifiées à ce jour. Cf. Build 2020: Fostering a secure and trustworthy app ecosystem for all users et Publisher verification and app consent policies are now generally available.

Nous avons également ajouté plus de fonctionnalités Azure AD dans Microsoft Graph pour permettre à nos partenaires de créer des applications et des workflows axés sur l'identité et la sécurité. Par exemple, Lumagate a créé un chatbot alimenté par l'IA qui simplifie la gestion des identités et des points de terminaison avec Microsoft Graph. RSA a exploité les données utilisateur à risque d'Azure AD et d'autres signaux de sécurité Microsoft pour enrichir son moteur de score de risque. Et F5 networks utilise l'API de galerie d'applications Azure AD pour simplifier la configuration de certaines applications SAP et Oracle entre Azure AD et F5 BIG-IP APM.

Nous avons également étendu les capacités d'Azure AD B2C avec plusieurs partenaires éditeur qui permettent aux développeurs de mieux protéger leurs applications destinées aux clients.

Outre la vérification d'identité qui devient aujourd'hui clé dans les relations numériques, nous avons également divers autres partenaires qui fournissent diverses solutions pour répondre aux besoins des identités externes avec la capacité :

1. De se connecter avec un fournisseur de messagerie personnalisé pour fournir une personnalisation de bout en bout des modèles de courrier électronique
2. D'ajouter la capacité de vérifier et de confirmer l'identité d'un utilisateur grâce à la vérification de titres ou d'autres pièces d'identité et pouvoir détection les fraudes.
3. D'apporter la gouvernance à Azure AD B2C et en particulier appliquer un contrôle d'accès en fonction du rôle.
4. D'élargir les méthodes pour l'authentification aux premier et deuxième facteurs - en utilisant la biométrie, l'authentification forte pour la conformité notamment avec la directive PSD2 qui va bouleverser le paysage bancaire et technologique européen.
5. D'améliorer la fonctionnalité de sécurité pour les clients en ajoutant une protection supplémentaire contre les attaques de robots logiciels et la prise de contrôle de compte

Ainsi, vos développeurs peuvent s'intégrer à des partenaires tels que LexisNexis et Experian pour l'analyse des risques et la détection des fraudes et s'intégrer avec des partenaires tels que IDology, Jumio et Onfido pour effectuer la vérification des titres et des preuves d'identité.

03 Permettre une collaboration sans limites et un cycle de vie automatisé pour tous les utilisateurs

Pour des expériences utilisateur fluides

La collaboration numérique, à la fois à l'intérieur et à l'extérieur des frontières organisationnelles, a augmenté de façon exponentielle.

Lorsque vos employés ont besoin de faire avancer les choses, il est essentiel d'offrir une excellente expérience utilisateur. Les employés qui interagissent directement avec les clients, les patients et les citoyens ont besoin d'outils simples à apprendre et à utiliser parce qu'une expérience de connexion simple et rapide peut faire toute la différence pour vos utilisateurs - et votre service d'assistance -. Vos clients, partenaires commerciaux

et fournisseurs méritent également une excellente expérience de connexion et de collaboration de qualité grand public.

A ce propos, nos clients et experts du secteur nous disent que les responsables informatiques ont plus que jamais du mal à gérer les utilisateurs en dehors de l'entreprise.

Les organisations s'engagent avec un nombre croissant d'utilisateurs externes, avec des technologies fragmentées avec différents niveaux de sécurité.

Les défis communs auxquels nos clients sont confrontés comprennent :

- **Des relations toujours plus numériques** : toute personne qui interagit avec votre organisation, du fournisseur au consommateur, a besoin et espère se connecter et collaborer numériquement. Alors que les attentes des consommateurs / clients pour s'engager où et quand ils le souhaitent ont augmenté au fil du temps, les attentes des partenaires commerciaux sont également plus élevées que jamais.
- **Des relations utilisateur en évolution constante au fil du temps** : les relations évoluent, donc la manière dont les utilisateurs sont gouvernés doit également changer. Un candidat à une université aujourd'hui, peut être un étudiant demain, puis un ancien - ayant besoin de niveaux d'accès et de capacités très différents à différentes étapes, tout en s'attendant à l'expérience la plus fluide possible.
- **Un risque accru en matière de sécurité pour les clients** : les organisations sont depuis longtemps conscientes du risque posé par les utilisateurs externes dans leur système, mais les clients en sont également de plus en plus conscients en raison des violations de sécurité et de confidentialité de haut niveau qui compromettent la confiance de la marque.
- **Des structures organisationnelles complexes et une main-d'œuvre diversifiée** : les organisations ne sont plus uniquement constituées d'employés traditionnels à plein temps avec une adresse e-mail professionnelle et un badge. De plus en plus d'organisations créent des effectifs flexibles et mixtes qui incluent des fournisseurs, des travailleurs à temps partiel ou à la demande et d'autres partenaires qui contribuent à accroître leur productivité.
- **Une appétence pour la donnée et des aperçus sur les relations** : les chefs d'entreprise et les décideurs recherchent une vue à 360 degrés de leurs clients ainsi que des partenaires commerciaux, afin de transformer ces données et connaissances en action. Les responsables informatiques sont sous pression pour offrir ce point de vue holistique.
- **Une demande de consolidation IT avec une recherche de maitrise des couts** : Enfin, les responsables informatiques font face à des pressions continues pour consolider leur pile informatique et réduire le coût total des opérations, notamment en évaluant s'ils ont besoin de plusieurs systèmes IAM et CIAM et si leurs solutions passeront à l'échelle le cas échéant.

Avec la fonctionnalité Identités externes d'Azure AD, nous investissons pour permettre aux organisations et aux développeurs de sécuriser, gérer et créer plus facilement des applications qui se connectent avec différents utilisateurs extérieurs à votre organisation.

(Les identités externes couvrent les capacités précédemment offertes par Azure B2B Collaboration et Azure AD B2C et nous sommes engagés dans une convergence complète à terme de ces capacités. A ce propos, nous leur permettons de capitaliser sur toutes les APIs partenaires disponibles pour Azure AD B2C et d'utiliser ces mêmes APIs avec l'ajout d'un connecteur d'API dans les flux d'utilisateurs à destination des identités externes de vos partenaires. Il s'agit d'une traduction concrète de ce travail conséquent désormais engagé pour intégrer cette désormais perméabilités des différents types d'utilisateurs.)

Aujourd'hui, nous poursuivons nos investissements pour accompagner l'ensemble de vos relations numériques, et au-delà de vos clients et partenaires par exemple, avec plus de deux milliards de travailleurs dits « en première ligne » (Firstline Workers) qui étaient auparavant exclus des bénéfices de la transformation numérique afin de relever les défis auxquels ils sont confrontés, pour exemple, en fournissant des transferts transparents d'appareils mobiles partagés et en améliorant les outils et les workflows pour les responsables.

À l'avenir, une telle dynamique et les investissements afférents favoriseront également la collaboration entre les personnes et les robots logiciels, les micro-services et les appareils intelligents.

De plus, une collaboration efficace nécessite plus que la simple connexion de tous les utilisateurs. Cela nécessite de donner aux bons utilisateurs le bon accès aux bonnes ressources au bon moment. Avec la croissance du nombre d'utilisateurs et d'applications, il est impossible pour un service informatique de connaître les besoins d'accès de chacun. C'est là que la gouvernance des identités peut aider.

La gouvernance des identités basée sur le cloud automatise le cycle de vie des accès grâce à l'intégration avec des systèmes RH tels que SAP Success Factors ou Workday et simplifie les décisions d'accès pour les réviseurs grâce à la puissance de l'analyse avancée et du Machine Learning. Ainsi, vis-à-vis des systèmes RH précédents, plus tôt cette année, nous avons annoncé la préversion publique du provisionnement des utilisateurs de SAP SuccessFactors vers Azure AD, vous permettant d'orchestrer facilement les données utilisateur de SAP SuccessFactors dans Azure AD. Nous avons également ajouté d'autres améliorations à nos intégrations Workday existantes, telles que la prise en charge de plus de champs de réécriture et la possibilité de spécifier la version de l'API Workday à utiliser.

La gouvernance des identités permet également aux utilisateurs professionnels de gérer l'accès via des demandes d'accès et des workflows ou une gestion déléguée des utilisateurs pour les responsables de première ligne.

Enfin, une collaboration efficace entre les employés, les partenaires et les clients nécessite plus que de simplement les connecter aux bonnes ressources, mais de s'assurer qu'ils ont le bon accès. Nos intégrations avec des partenaires de gouvernance des identités tels que Saviynt et Omada permettent des scénarios de gouvernance avancés tels que la séparation des tâches, des workflows complexes et des rapports granulaires entre les domaines d'applications hybrides, ou encore la gouvernance pour Microsoft Teams. De plus, nos partenaires axés sur l'industrie, tels qu'Imprivata, fournissent une gouvernance d'accès clinique pour le cloud et les applications de santé héritées (c'est-à-dire les Dossiers de santé électroniques ou DSEs).

04 Passer au « sans mot de passe » pour rendre la sécurité sans effort pour les utilisateurs finaux

L'authentification sans mot de passe présente de nombreux avantages. L'un d'eux, comme nous l'avons vu dans le parcours de Microsoft, est une réduction de 87 % des coûts matériels et accessoires.

Notre objectif d'éliminer les dépendances aux mots de passe et de les remplacer par une authentification plus sécurisée ne peut être atteint qu'avec nos partenaires. Remplacer une solution à ce point universelle par une solution propriétaire serait pour le moins incongru...

Nous savons tous que les mots de passe ne sont pas sécurisés, coûteux à gérer et frustrants pour les utilisateurs. Selon le rapport de violation de données de Verizon, 81% des violations utilisent des mots de passe volés ou faibles. Une grande partie de l'hyperbole sur les mots de passe - « ne jamais utiliser un mot de passe qui a déjà été vu dans une violation », « utiliser des mots de passe très longs », « des passphrases-nous sauveront », etc. - est incohérente et inconsistante avec nos recherches et avec la réalité de ce que nos équipes voient alors que nous nous défendons contre des centaines de millions d'attaques par mot de passe chaque jour.

Se concentrer sur les règles de mot de passe, plutôt que sur les choses qui peuvent vraiment aider n'est qu'une distraction. Par exemple, L'authentification multifacteur peut bloquer plus de 99,9% des attaques de compromission de compte. En introduisant une barrière et une couche de sécurité additionnelle, connaître ou déchiffrer le mot de passe ne suffira pas pour accéder au compte. Cf. Your Pa$$word doesn't matter.

(D'autres attaques de crédentités sont décrites ici : aka.ms/allyourcredsarebelongtous)

Plus de 150 millions de personnes - à travers nos comptes grand public et Azure AD - se connectent chaque mois à l'aide de méthodes sans mot de passe.

Azure AD prend en charge les options d'authentification de plateforme, de logiciel et de matériel qui sont résistantes à l'hameçonnage (*phishing*) et conviviales pour répondre aux besoins de votre entreprise.

Nos partenaires ont créé une variété de clés de sécurité matérielles parmi lesquelles choisir, qui répondent aux standards FIDO2 de l'Alliance FIDO et s'intègrent à Azure AD.

L'Alliance FIDO est l'un de nos partenariats les plus importants aujourd'hui. Plus de 250 organisations sont membres de l'alliance. Les membres de FIDO Alliance travaillent ensemble pour améliorer les standards d'authentification et contribuer à réduire la dépendance mondiale à l'égard des mots de passe. Nous voulons nous assurer que toute personne qui utilise des services sur le Web ou sur site dispose d'une expérience de connexion sécurisée et pratique avec des crédentités qui éliminent l'hameçonnage de l'équation. Cf. Inside Identity: Moving to a passwordless world with the FIDO Alliance.

Par exemple : je me connecte à mon Microsoft Surface Book 3 ou à un autre appareil compatible avec la biométrie Windows 10 à l'aide de la reconnaissance faciale au lieu d'un mot de passe. Je dispose ensuite d'une authentification sécurisée sur mon appareil et sur chaque service et application que j'utilise tout au long de la journée avec cette connexion sécurisée. Le système d'exploitation, le navigateur, les applications et les informations d'identification que j'utilise prennent en charge les standards FIDO pour y parvenir.

Le nombre d'appareils et de services compatibles FIDO continue d'augmenter. Edge, Firefox et Chrome prennent tous en charge FIDO et plusieurs options de clé de sécurité qui utilisent USB, Bluetooth ou NFC pour se connecter répondent à différents besoins commerciaux en fonction du coût et du facteur de forme préféré. Windows Hello, inclus dans la dernière version de Windows 10, est également compatible FIDO.

Des partenaires comme Yubico et Feitian ont récemment publié de nouvelles clés de sécurité telles que iePass FIDO Security Key and YubiKey 5Ci conçues pour être faciles à utiliser avec les appareils mobiles.

Pour aider chaque organisation à se préparer à passer sans mot de passe, nous proposons donc une variété de méthodes - de Windows Hello à Microsoft Authenticator et aux clés de sécurité FIDO2 - qui fonctionneront dans les environnements cloud et hybrides.

Windows Hello


Microsoft Authenticator

Clés de sécurité FIDO2

Et pour vous faciliter la tâche, nous avons identifié quatre étapes pour commencer à planifier votre déploiement en fonction de l'expérience de nos clients et de notre propre équipe informatique.

05 Initier votre parcours « Zero Trust » pour protéger votre organisation lors de votre transformation numérique

Les clients du monde entier réagissant à la COVID-19 en invitant leurs employés de bureau à un travail à distance, des solutions de sécurité basées sur l'identité sont nécessaires pour aider à protéger les ressources de l'entreprise.

Les clients avec lesquels nous parlons sont absolument clairs sur un point : sans périmètre de réseau, sans frontières autour de la collaboration et avec une explosion d'appareils et d'applications, l'ancien paradigme de sécurité ne s'applique plus.

Nous vivons dans une nouvelle réalité. Ces anciennes hypothèses ne nous garderont pas en sécurité dans le nouveau monde.

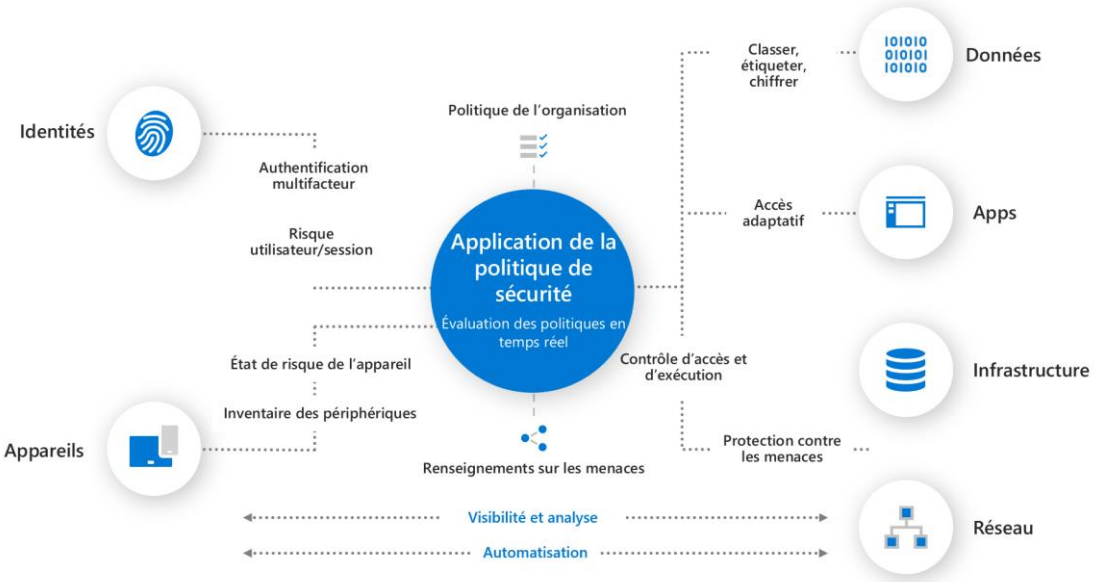
Dans ce monde, « Zero Trust » est à la fois une vision du monde et une stratégie de sécurité. Il remplace l'hypothèse selon laquelle tout ce qui se trouve derrière le pare-feu d'entreprise est sûr par trois nouveaux principes simples :

1. **Vérifier explicitement**. Authentifier et autoriser toujours en fonction de tous les points de données disponibles, y compris l'identité de l'utilisateur, l'emplacement, l'état de l'appareil, le service ou la charge de travail, la classification des données et les anomalies.

2. **Utiliser l'accès le moins privilégié**. Limiter l'accès des utilisateurs avec un accès de type « Just In Time » et « Just Enoug » (JIT / JEA), pour protéger à la fois les données et la productivité.
3. **Supposer une violation** (Assume Breach). Minimiser le rayon de souffle pour les brèches et utiliser une stratégie de sécurité pour empêcher les mouvements latéraux.

Zero Trust commence par une base d'identité solide. Cf. Securing a remote workforce with Zero Trust.

Nos investissements dans nos produits et notre écosystème sont guidés par l'adoption de la stratégie de sécurité Zero Trust comme notre vision du monde. Une approche holistique de l'approche Zero Trust doit s'étendre à l'ensemble du domaine numérique - elle sert de philosophie de sécurité intégrée et de stratégie de bout en bout.



Nous construisons Azure AD sur les principes de Zero Trust pour rendre la mise en œuvre de ce modèle dans l'ensemble de votre parc numérique réalisable à grande échelle. Cf. Implementing a Zero Trust approach with Azure Active Directory.

Cela dit, comme Microsoft l'a appris de notre propre expérience, chaque parcours Zero Trust sera unique en fonction de vos priorités commerciales, des technologies que vous possédez déjà et des actifs que vous souhaitez protéger. Au fur et à mesure que vous tirez parti de vos investissements existants, vous pouvez évaluer votre maturité Zero Trust et prendre des mesures pratiques vers une posture de sécurité encore plus forte.

Se lancer dans votre aventure Zero Trust peut être intimidant, mais nous sommes là pour vous aider. Nous avons créé l'outil d'évaluation Microsoft Zero Trust pour vous aider à déterminer où vous en êtes dans votre parcours Zero Trust. Cf. Zero Trust framework to enable remote work.

Par ailleurs, bon nombre de nos partenaires de service aident les clients à mettre en œuvre une stratégie de sécurité Zero Trust qui place l'identité au centre. Par exemple, des partenaires comme Concurrency, Edgile et Optiv ont aidé les clients à faire la transition vers le travail à distance grâce à nos solutions de sécurité basées sur l'identité, ce qui facilite et sécurise le travail des employés à domicile.

Selon une nouvelle étude du Forrester, The Total Economic Impact ™ of Securing Apps with Microsoft Azure Active Directory, investir dans l'identité peut non seulement vous aider à accélérer votre parcours Zero Trust, mais également vous faire économiser de l'argent et offrir plus de valeur. Cf. New Forrester study shows customers who deploy Microsoft Azure AD benefit from 123% ROI.

Le paysage de l'identité au-delà de 2020

2020 est une année dont nous nous souviendrons tous pour son intensité et son rythme accéléré de changement. La sécurité de vos utilisateurs, où qu'ils soient, a été notre priorité collective. Quelle que soit l'évolution de la « nouvelle normalité » après cette pandémie, l'identité restera le cœur de tous les services sur lesquels vos utilisateurs comptent.

Au-delà de 2020, de nombreuses technologies passionnantes sont sur le point de changer le paysage de l'identité. Nous voudrions en souligner une en particulier : l'identité décentralisée.

Une plus grande vérifiabilité et une meilleure protection de la vie privée grâce à une identité décentralisée et des revendications vérifiables

À mesure que de plus en plus de transactions et d'échanges d'informations se déroulent numériquement, il est essentiel de vérifier que les personnes sont bien celles qu'elles prétendent êtres et que les informations qu'elles présentent sont exactes et non falsifiées. Cela met une pression énorme sur les organisations pour valider les données qu'elles collectent tout en les gardant privées et sécurisées dans le respect du RGPD. Cela exige également que tout un chacun accorde une énorme confiance aux organisations qui gèrent leur identité et collectent des informations personnelles autour d'eux. Comme chacun sait, la confiance ne se décrète mais se mérite…

L'identité décentralisée a la capacité de transformer nos interactions numériques, rendant chaque réclamation en ligne facilement vérifiable tout en redonnant aux personnes le contrôle de leur(s) identité(s) et de leurs données. Et ce n'est pas seulement un concept - c'est réel.

Alliance ID2020

Microsoft estime que chacun a le droit de posséder et de contrôler son ou ses identités numériques, une identité qui stocke toutes les données personnelles de manière sécurisée et privée.

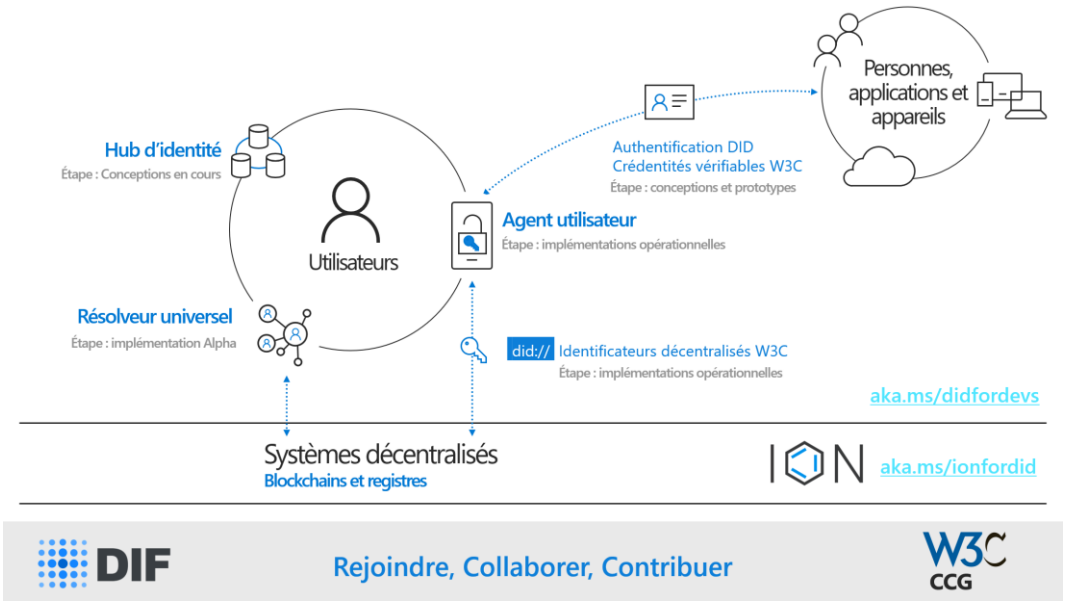
Microsoft est membre fondateur de l'Alliance ID2020, un partenariat public-privé mondial dédié à aider les 1,1 milliard de personnes à travers le monde qui n'ont aucune forme légale d'identité, Cf. Partnering for a path to digital identity.

Pour réaliser cette vision, nous devons augmenter les systèmes d'identité cloud existants avec un système que les personnes individuelles, les organisations et les appareils peuvent posséder afin qu'ils puissent contrôler leur identité numérique et leurs données. Nous pensons qu'un système d'identité décentralisé basé sur des normes et standards peut débloquer un nouvel ensemble d'expériences qui permet aux utilisateurs et aux organisations d'avoir un meilleur contrôle sur leurs données et d'offrir un plus haut degré de confiance et de sécurité.

Photo gracieusement mise à disposition par Mercy Corps

Une solution holistique qui accepte les identités que les personnes apportent avec elles est une condition préalable nécessaire à la vision d'une identité décentralisée.

Grâce à un effort communautaire avec la fondation DIF (Decentralized Identity Foundation), nous sommes sur la voie d'un nouveau standard web W3C pour les crédentités vérifiables.



L'aperçu des crédentités vérifiables par Azure AD disponible en open source est basé sur cela et exploite le protocole Open ID Connect : vous pourrez donc les incorporer dans vos systèmes existants.

Lors de la conférence Microsoft Build 2020, nous avons montré comment les applications peuvent échanger de telles crédentités avec des sources qu'elles jugent faisant autorité et illustré comment tirer parti de ce protocole afin de permettre aux développeurs de réutiliser plus facilement leurs compétences et les bibliothèques avec lesquelles ils sont familiers

Pour accélérer l'adoption des crédentités vérifiables et des identifiants décentralisés (DID), nous avons également mis en open source le code que nous utilisons dans l'application Microsoft Authenticator qui gère les clés cryptographiques pour les DID et facilite l'échange des crédentités à l'aide d'OpenID Connect. Cf. Building trust into digital experiences with decentralized identities (DID).

Au-delà de faciliter le développement de solutions et de disposer de standards ouverts sur lesquels reposer dans ce contexte, il est également clé que de telles solutions passent à l'échelle.

Les membres du DIF ont collaboré sur des implémentations évolutives de DIDs, en utilisant les blockchains publiques existantes pour garantir l'accès ouvert et la résistance à la censure. Dans cette dynamique, ION est un réseau de DIDs public, sans autorisation, qui implémente le protocole Sidetree indépendant de la blockchain au-dessus du mainnet Bitcoin (en tant que superposition de « couche 2 ») pour prendre en charge les DIDs / DPKI (infrastructure à clé publique décentralisée) à grande échelle . Le stade de la Beta est désormais atteint. Cf. ION – Booting up the network.

Et nous testons une identité décentralisée en partenariat avec le National Health Service du Royaume-Uni, les hôpitaux d'enseignement de Blackpool et Truu. Grâce à ce projet pilote, nous avons pu réduire le temps nécessaire aux médecins pour valider leurs informations d'identification de cinq mois à cinq minutes, ce qui les a aidés à passer plus de temps avec leurs patients.

Conclusion

Microsoft s'engage avec passion à garantir que les systèmes que nous construisons permettent aux personnes de faire de leur mieux et de vivre leur meilleure vie.

Que dit l'industrie à notre sujet ?

Microsoft est reconnu comme un « leader » dans le Magic Quadrant (MQ) 2020 de Gartner pour la gestion de l'accès, dans le monde entier. Cf. Gartner Magic Quadrant for Access Management, Worldwide.

Figure 1: Magic Quadrant for Access Management

Source: Gartner (November 2020)

Le Gartner MQ est un guide décisionnel important pour les services informatiques des entreprises. Par exemple, certaines organisations ne peuvent acheter que des produits du quadrant Leader. Vous pouvez obtenir le rapport Gartner ici : https://www.gartner.com/doc/reprints?id=1-24F36V24&ct=201021

Pour reprendre le verbatim d'Alex Simons, CVP of Program Management, Microsoft Identity :

Nous sommes honorés de ce positionnement pour la quatrième fois et nous pensons qu'il reflète l'énergie et la passion que nous avons déployées dans nos partenariats avec nos clients pour les aider à transformer avec succès leurs activités numériques.

Cela dit, il reste encore beaucoup de travail à faire et nous sommes impatients de continuer à collaborer avec vous, nos clients, pour garantir que les produits que nous construisons assurent la sécurité et la productivité de vos organisations. Nous vous sommes reconnaissants de votre confiance et j'ai hâte de voir ce que nous pouvons accomplir ensemble au cours de l'année à venir.

D’autres analystes s’expriment sur Azure AD.

- Azure AD selon KuppingerCole : Selon KuppingerCole, Microsoft se classe en tête du marché, des produits et de l’innovation.
- Azure AD selon IDC

Notre engagement pour la prochaine décennie

Si une chose est claire, cependant, et comme souligné par Alex Simons ci-dessus, c’est que toutes ces initiatives en matière sont un voyage à l’instar de la sécurité. En travaillant tous ensemble en tant qu'industrie, nous construisons une meilleure voie vers la sécurité et la protection de la vie privée, ancrée autour de la seule constante de ce monde hétérogène en évolution rapide : vous.

Dans cette nouvelle décennie, comme dans la dernière, les priorités commerciales que nos clients partagent avec nous guideront nos investissements en ingénierie dans l'identité. Notre priorité absolue est la fiabilité et la sécurité du service proposé.

Nos principes d'innovation fondamentaux demeurent les mêmes :

- Commencer par une sécurité de pointe.
- Construire une solution d'identité simple, intégrée et complète.
- Soutenir un écosystème ouvert et interopérable.

Même si chacune de vos priorités d'identité pour cette fin d'année et l'année prochaine 2021 sera unique aux objectifs de votre organisation, l'identité sera un élément essentiel de votre parcours de transformation d'entreprise. Microsoft s'engage à travailler en étroite collaboration avec vous pour innover dans nos produits, vous aider à concevoir une architecture d'identité optimale et à la déployer rapidement dans vos organisations.

Nos plans commencent toujours par vos commentaires et retours, alors dites-nous ce dont vous avez besoin pour rester en avance sur la suite.

Nous nous engageons à vous accompagner dans votre parcours de transformation numérique. Quoi qu'il arrive, vous pouvez être sûr que nous continuerons à écouter vos commentaires et vos contributions, afin que nous puissions faire évoluer nos priorités et principes d'ingénierie pour vous aider à garder une longueur d'avance et à vous préparer à ce qui va suivre.

Pour aller plus loin

Nous espérons que ce document vous a apporté une vue d’ensemble sur la stratégie Identité de Microsoft, les principes qui la structure, les priorités qui en découle ainsi que nos engagements pour les années à venir.

Dans l'intervalle, pour aller plus loin, nous vous conseillons les ressources suivantes pour rester au courant de notre actualité sur l'identité :

→ Blog Azure AD : aka.ms/azureadblog, avec notamment les billets de blog.

- Identity at Microsoft Ignite: Rising to the challenges of secure remote access and employee productivity
- What's new in Azure Active Directory at Microsoft Ignite 2020

→ Série de vidéos : aka.ms/identityyoutube.

Microsoft

LA TECHAUCARRÉ

Restons en contact :

aka.ms/LaTechAuCarre