

24 novembre 2020

Microsoft Azure Active Directory une nouvelle fois nommé « Leader » dans le Magic Quadrant de Gartner pour la Gestion des accès

Alex Simons, Vice-Président Corporate, Microsoft Identity Program Management



Bonjour à tous,

J'ai le plaisir de vous annoncer que pour la quatrième année consécutive, [Microsoft Azure Active Directory \(Azure AD\)](#) a été classé en tant que Leader Mondial dans le [Gartner Magic Quadrant pour la Gestion des accès](#).

Figure 1: Magic Quadrant for Access Management



Source: Gartner (November 2020)

Figure 1 : Magic Quadrant pour la Gestion des accès

En début d'année, Joy Chik, Vice-Présidente Corporate Identity Engineering, a présenté les [principes directeurs](#) de la stratégie de gestion des identités et des accès (IAM) de Microsoft, en insistant sur la volonté d'apporter une [solution de gestion des identités sûre et évolutive](#). Azure AD protège l'accès à vos applications, à travers des politiques d'authentification forte et des règles d'accès adaptables en fonction du risque qui se traduisent par un accès utilisateur plus fluide grâce à l'authentification unique (SSO) et par une réduction des coûts informatiques. Pour nous, Azure AD est LA solution capable de mener vers un [modèle de sécurité « Zero Trust »](#), qui garantira un [accès sécurisé aux applications](#) et une productivité renforcée pour l'ensemble des utilisateurs, des applications et des appareils.

La place que nous occupons de manière constante depuis quatre ans dans le Magic Quadrant de Gartner témoigne du travail accompli dans la réalisation de notre vision et de la valeur ajoutée apportée à nos clients.

Votre capacité à vous adapter au télétravail tout au long de l'année passée nous a servi de modèle, et vos commentaires ont abouti à des avancées dans plusieurs domaines :

- **Sécurité adaptable** : Azure AD propose en natif des fonctions complètes de connexion, de tableau de bord et de reporting, sans oublier l'analyse des identités avec [Azure AD Identity Protection](#).
- **Accès sécurisé aux applications** : Azure AD prend en charge l'[authentification unique \(SSO\) prédéfinie](#) et le provisionnement de connecteurs pour des milliers d'applications en mode SaaS, ainsi que l'authentification d'applications locales historiques à travers notre Proxy d'application et nos différents partenariats pour un accès hybride sécurisé.
- **Mode Audit** : Le mode Audit permet aux administrateurs d'évaluer l'impact des stratégies d'[accès conditionnel](#) avant de les rendre accessibles aux utilisateurs.
- **Règles pour l'accessibilité des contenus Web** Nous sommes fiers de [notre engagement à créer des systèmes conçus pour favoriser l'inclusion et l'accessibilité](#), qui va au-delà de la simple conformité aux Règles pour l'accessibilité des contenus Web (WCAG) et garantit une expérience positive à l'ensemble des utilisateurs.
- **Contrôle d'accès aux API** : Nous proposons une gestion intégrée et centralisée des stratégies, des services de gestion des jetons de sécurité et de traduction des jetons, et un support en libre-service pour les développeurs. Par ailleurs, en vue d'améliorer la sécurité des API, Azure AD offre une intégration native avec le service [Azure API Management](#) ou avec des produits tiers de passerelle API.
- **Standards ouverts** : Azure AD [prend en charge les principales normes de gestion des identités](#), notamment SAML 2.0, WS-Fed, OIDC ou OAuth 2.0, ainsi que l'utilisation de coffres pour les mots de passe, avec remplissage de formulaires de connexion en JavaScript.

Nous sommes honorés de l'excellente place obtenue pour la quatrième année et nous sommes convaincus que ce classement rend compte de l'énergie et de l'enthousiasme déployés pour aider nos partenaires clients à mener à bien leur transformation numérique. Il reste toutefois énormément à accomplir, et nous avons hâte de poursuivre cette collaboration avec vous, nos clients, pour continuer de créer des produits qui garantissent la sécurité et la productivité de vos entreprises. Nous vous remercions pour votre confiance, et nous attendons avec impatience de découvrir ce que nous pourrions réaliser ensemble au cours de l'année à venir.



Pour en savoir plus sur les solutions de gestion des identités de Microsoft, rendez-vous sur notre [site Web](#). Ajoutez le [blog Sécurité](#) à vos favoris pour accéder aux derniers articles de nos experts sur les questions de sécurité. Vous pouvez également suivre nos comptes Twitter [@AzureAD](#) et [@MSFTSecurity](#) pour obtenir les dernières informations et mises à jour concernant les identités et la cybersécurité.

Ce diagramme a été publié par Gartner, Inc. dans le cadre d'un document de recherche et devrait être évalué en tenant compte de l'intégralité de ce document. Le document de Gartner peut être obtenu sur demande auprès de Microsoft.

Gartner ne fait la promotion d'aucun fournisseur, produit ou service présenté dans ses publications de recherche et n'incite pas les utilisateurs de technologies à se limiter dans leurs choix aux fournisseurs les mieux notés ou autrement désignés. Les publications de recherche de Gartner reprennent les avis du cabinet d'études de Gartner et ne doivent en aucun cas être interprétées comme un exposé des faits. Gartner exclut toute garantie expresse ou tacite concernant cette recherche, y compris toute garantie de qualité marchande et d'adéquation à un usage particulier.

Mots clés :

Sécurité Azure, Cybersécurité, Gestion des identités et des accès

"Gartner has positioned Microsoft in the Leaders Quadrant in the 2020 Magic Quadrant for Access Management, Worldwide, based on its completeness of vision and ability to execute in the access management market. According to Gartner, Leaders show evidence of strong vision and execution for anticipated requirements related to technology, methodology, or means of delivery."

Gartner does not endorse any vendor, product, or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

