

# Veza, société de sécurité des données bâtie sur la puissance de l'autorisation, sort de sa phase confidentielle de développement et annonce un financement de 110 millions USD

Veza, plateforme de sécurité des données, fondée sur la puissance de l'autorisation, annonce aujourd'hui sortir de sa phase confidentielle de développement. Fondée en 2020, Veza annonce également un financement total de plus de 110 millions USD, auprès de sociétés de capital-risque de premier plan, parmi lesquelles Accel, Bain Capital, Ballistic Ventures, GV, Norwest Venture Partners, et True Ventures, ainsi que plusieurs investissements providentiels de la part de dirigeants reconnus dans le secteur, parmi lesquels Kevin Mandia, fondateur et PDG de Mandiant ; Enrique Salem, ancien PDG de Symantec, et associé chez Bain Capital ; Lane Bess, ancien PDG de Palo Alto Networks ; Manoj Apte, ancien directeur stratégique de ZScaler ; Joe Montana de chez Liquid2 Ventures ; ainsi que les dirigeants du secteur de la sécurité Niels Provos, Karthik Rangarajan, et bien d'autres.

Ce communiqué de presse contient des éléments multimédias. Voir le communiqué complet ici : <https://www.businesswire.com/news/home/20220427005386/fr/>

Veza's co-founders (left to right) - Tarun Thakur, CEO; Maohua Lu, CTO; Robert Whitcher, Chief Architect (Photo credit: Eric Millette)



Tandis que les données sont rapidement et irréversiblement transférées vers le cloud, les organisations du monde entier manquent encore d'un élément central de la sécurité des données : l'autorisation. Les solutions préexistantes et de première génération en matière de sécurité des données ne fonctionnent pas dans les environnements hybrides multi-cloud, les dirigeants du secteur des données et de la sécurité sont confrontés à

d'importantes difficultés liées aux logiciels rançonneurs, à la transformation numérique, à l'adoption du cloud, à la perte de confiance des clients en conséquence de violations de données, ainsi qu'à des manquements en matière d'audit et de conformité. La quantité de données étant vouée à [tripler entre 2020 et 2025](#), et le nombre d'incidents de cybercriminalité étant [multiplié par deux chaque année](#), les organisations ont besoin d'une solution de sécurité des données qui leur confère la possibilité de comprendre, de gérer et de contrôler qui est en capacité et qui doit prendre des mesures concernant quelles données.

« Lorsque nous avons créé notre entreprise il y a deux ans, nous étions animés par la volonté de contribuer à faire progresser la sécurité des données dans les décennies à venir », a déclaré Tarun Thakur, PDG et cofondateur de Veza. « Les équipes en charge des données et de la sécurité sont inondées d'outils, sans pour autant parvenir à répondre à une question fondamentale : qui peut et qui doit prendre quelles mesures concernant quelles données ? Grâce à l'implication de notre équipe, ainsi qu'aux précieux retours d'expérience de nos clients, Veza a démontré que la puissance des métadonnées d'autorisation constituait la source de vérité permettant aux organisations de moderniser la sécurité des données à l'ère du multi-cloud hybride. Nous sommes déterminés à permettre aux entreprises d'opérer en toute confiance, afin qu'elles puissent libérer la valeur de leurs données. »

Veza est la première et la seule plateforme de sécurité des données à reposer sur la puissance de l'autorisation. La plateforme soutient les systèmes à la fois sur site et dans le cloud, et confère aux équipes de sécurité des données la possibilité de comprendre la nature sensible des données, de gérer les identités humaines, ainsi que d'administrer les comptes sur plusieurs centaines voire milliers de systèmes de données, applications, et services cloud distincts. La différenciation clé de

Veza réside dans son graphique de métadonnées d'autorisation (Authorization Metadata Graph). Ceci inclut :

- Un moteur de diffusion haute performance, qui intègre le hors bande et le sans agent avec de multiples systèmes informatiques et infrastructurels d'identités, de données et d'applications, dans le cloud et sur site
- Un modèle objet canonique, qui organise les identités, les relations et les objets de données granulaires
- Une couche de traduction qui traite de multiples permissions spécifiques aux systèmes, et qui les convertit en un langage naturel pour les professionnels des données et de la sécurité, le tout dans un unique panneau de contrôle
- Des applications de sécurité des données incluant : recherche en temps réel de qui accède à quoi, flux de travail avec autorisation pour la gouvernance de l'accès et la gestion des privilèges, alertes préconçues de violation du moindre privilège et solutions associées pour y remédier, règles et requêtes automatisées pour la résolution, recommandations, et bien plus encore.

« Une startup s'attaque enfin à la plus grande difficulté en matière de cybersécurité : notre ignorance collective concernant nos propres environnements de données », a déclaré Nicole Perlroth, conseillère spéciale de Veza, ancienne journaliste spécialisée dans la cybersécurité au New York Times et conseillère au sein de l'Agence américaine de la cybersécurité et de la sécurité des infrastructures. « Jusqu'à présent, aucun cadre dirigeant ne pouvait affirmer avec certitude savoir où se situaient ses données, et qui pouvait y avoir accès. Veza ne permet plus aucune excuse. Cette plateforme marque une avancée majeure en matière de cyberdéfense. »

De nombreuses sociétés du Fortune 500 et organisations émergentes dans de multiples secteurs, tels que la finance, la santé, l'hôtellerie, les médias, les technologies et hautes technologies, font confiance à Veza. Parmi les clients de Veza figurent : ASAPP, ATN International, Barracuda Networks, Choice Hotels, InComm, Nozomi Networks, The Translational Genomics Research Institute (TGen), et bien d'autres.

« L'élaboration et l'exécution de politiques de sécurité des données ne sont pas une tâche facile, car il existe une multitude de produits de sécurité des données, qui fournissent des contrôles de sécurité spécifiques, sur la base de registres ou d'étapes de traitement tout aussi spécifiques. Ceci souligne la nécessité et l'opportunité d'une convergence de marché, ainsi que de l'émergence de nouveaux marchés de la sécurité des données, qui permettent des privilèges d'accès d'entreprise appropriés, pour l'utilisation et le partage des données avec les partenaires tout au long de leur cycle de vie. »

Hype Cycle for Data Security, 2021

Brian Lowans, directeur analyste principal chez Gartner

### **Citations de nos clients**

« L'autorisation constitue une exigence de sécurité fondamentale pour n'importe quelle entreprise qui crée de la valeur à partir des données », a déclaré Craig Rosen, directeur de la sécurité et de la

confiance chez ASAPP. « L'heure est venue d'adopter une approche moderne qui permette aux entreprises de raisonner au-delà de l'authentification, et de maîtriser les complexités inhérentes à l'autorisation dans un univers multi-cloud. Veza résout le problème complexe de l'alignement des identités avec les données, afin de véritablement comprendre qui accède à quoi, et simplifie cette possibilité d'une manière facile à intégrer pour n'importe quelle organisation, quelle que soit sa taille. »

« La mission d'Axon consiste à protéger la vie et la vérité, en promouvant la sécurité publique grâce aux technologies. Cet accent placé sur la sécurité vaut évidemment également pour l'ensemble de l'écosystème Axon », a déclaré Jenner Holden, directeur de la sécurité des systèmes d'information chez Axon. « En utilisant Veza, nos équipes en charge de la sécurité ont obtenu une visibilité précieuse sur nos systèmes — applications, infrastructure et données — afin de mieux comprendre qui peut accéder à quoi, favorisant ainsi de meilleures pratiques de sécurité concernant l'accès privilégié. »

« Si vous utilisez un cloud, quelle que soit sa taille, vous avez probablement effectué par le passé une multitude de choses qui n'étaient pas accompagnées d'une gouvernance appropriée », a déclaré Jason Simpson, vice-président de l'ingénierie chez Choice Hotels. « C'est l'un des avantages de Veza que nous apprécions particulièrement : la possibilité de revenir en arrière, de constater la situation, d'y remédier, puis de mettre en place la gouvernance appropriée afin de veiller à ce que celle-ci ne décline pas à nouveau. »

« Nous avons besoin de comprendre comment les utilisateurs et les comptes de service étaient autorisés à accéder à des données spécifiques. À ma connaissance, Veza est le seul outil capable de vous présenter les deux volets de la situation », a déclaré Steven Guy, vice-président des solutions de sécurité chez InComm Payments. « Le premier volet est celui des personnes ou des comptes supposés avoir accès dans le cadre d'un groupe de sécurité. Le second volet vous permet de regarder du côté des données, et de déterminer qui y a également accès, ainsi que la manière dont cet accès a été octroyé. Veza offre l'aperçu le plus clair que je connaisse sur l'accès aux données. »

### **Ce que disent les investisseurs de Veza**

« La gestion sécurisée de l'autorisation en matière de cloud peut constituer une question épineuse pour les directeurs de la sécurité des systèmes d'information et pour les équipes informatiques, dans la mesure où les environnements multi-cloud sont extrêmement vastes », a déclaré Eric Wolford, associé chez Accel. « Veza permet aux équipes de gérer facilement cette complexité. Résultat, la société constate d'ores et déjà une adoption massive chez plusieurs de ses clients professionnels. »

« Il est temps d'adopter une approche extensible en matière d'autorisation, afin d'appréhender la nature dynamique des environnements d'entreprise multi-cloud hybrides d'aujourd'hui », a déclaré Enrique Salem, ancien PDG de Symantec et associé chez Bain Capital. « Le fait de combiner les relations entre n'importe quel système de données, identité d'entreprise, et application, ainsi que de visualiser et de gérer ces relations en un seul et même lieu, peut apparaître comme une idée simpliste, mais il s'agit d'une problématique extrêmement complexe à résoudre. Veza simplifie la démarche de compréhension de qui peut accéder à quelles données, tout en rendant cette démarche extensible même pour les plus grandes organisations. »

« Un haut niveau de confiance est en réalité nécessaire pour mettre en place le Zero Trust », a déclaré Jake Seid, cofondateur et associé gérant chez Ballistic Ventures. « Explication à cela, ce que les grandes sociétés de sécurité ont bâti par le passé, en créant des espaces sûrs définis par la simple sécurisation des réseaux et de leurs extrémités, ne revêt plus aucune logique dans un univers multi-cloud hybride. Dans ce nouvel univers, Veza considère que c'est l'autorisation qui permet d'apporter de la confiance au Zero Trust. »

« Les organisations ont besoin d'un produit de sécurité des données bâti à la fois sur l'environnement sur site et l'environnement multi-cloud. L'approche complète de Veza rassemble les métadonnées d'autorisation de systèmes distincts, et les présente dans un schéma unique : le graphique de métadonnées d'autorisation », a déclaré Karim Faris, associé général chez GV. « C'est la seule entreprise capable de vous exposer la réalité des permissions — ou autorisation — relatives à vos données dans l'ensemble de l'écosystème cloud de votre organisation. Nous sommes heureux de travailler avec Tarun Thakur et l'équipe Veza sur cette voie d'avenir. »

« L'équipe Veza est un parfait exemple de ce que nous appelons « l'adéquation fondateur-marché » », a déclaré Rama Sekhar, associé chez Norwest Venture Partners. « L'équipe de direction, forte de sa profonde expérience dans le domaine des données, a directement constaté une tendance universelle : le volume de données nées dans le cloud explose actuellement, et la tâche consistant à gérer qui peut et qui doit avoir accès à ces données devient un problème insoluble. Veza s'attaque directement à cette difficulté, en traduisant l'immense complexité des identités, permissions et sources de données en un panneau de contrôle unique. Son approche recueille d'ores et déjà la confiance d'une liste impressionnante de clients, et nous sommes impatients de voir Veza continuer de venir en aide aux entreprises du monde entier pour sécuriser leurs données. »

« Nous avons sauté sur l'occasion de financer Tarun et son équipe pour la deuxième fois », a déclaré Puneet Agarwal, associé chez True Ventures. « Veza comble une importante lacune en matière de sécurité des données, pour les environnements à la fois sur site et dans le cloud, et nous sommes persuadés que son équipe dispose des compétences uniques nécessaires pour façonner et conduire une nouvelle catégorie majeure. »

## **À PROPOS DE VEZA**

Veza est une plateforme de sécurité des données bâtie sur la puissance de l'autorisation. Notre plateforme est conçue spécifiquement pour les environnements multi-cloud hybrides, afin de vous permettre d'utiliser et de partager vos données en toute sécurité. Veza vous permet de comprendre, gérer et contrôler facilement qui peut et qui doit prendre quelles mesures concernant quelles données. Nous organisons les métadonnées d'autorisation concernant les fournisseurs d'identité, les systèmes de données, les fournisseurs de services cloud et les applications — le tout afin de répondre aux plus grands défis de sécurité des données de l'ère moderne. Fondée en 2020, la société est financée par des sociétés de capital-risque de premier plan, qui incluent Accel, Bain Capital, Ballistic Ventures, GV, Norwest Venture Partners, et True Ventures. Pour en savoir plus, rendez-vous sur [veza.com](https://veza.com).

**Débutez par un [essai gratuit](#)**

Inscrivez-vous à notre [webdiffusion de lancement](#)

Explorez [Veza Open Authorization API \(OAA\) sur GitHub](#)

Le texte du communiqué issu d'une traduction ne doit d'aucune manière être considéré comme officiel. La seule version du communiqué qui fasse foi est celle du communiqué dans sa langue d'origine. La traduction devra toujours être confrontée au texte source, qui fera jurisprudence.



Consultez la version source sur [businesswire.com](https://www.businesswire.com) :  
<https://www.businesswire.com/news/home/20220427005386/fr/>