EBOOK

5 étapes pour une gouvernance efficace des accès tiers

Évaluez votre degré d'exposition et sécurisez votre entreprise avec Saviynt

Saviynt

Sommaire

Saviynt

Introduction

Il est devenu plus difficile ces dernières années d'attirer des talents et de les fidéliser. Pour pallier ce phénomène, les dirigeants font le choix de confier certaines fonctions à des tiers (sous-traitants, agences, consultants, fournisseurs, etc.) afin d'accélérer leur croissance et/ou de réduire leurs coûts. Cependant, cette précipitation à intégrer une main-d'œuvre externe a révélé des risques importants pour la sécurité. Ces risques proviennent non seulement des utilisateurs tiers eux-mêmes, mais aussi de la possibilité que leurs accès soient détournés pour accéder aux données sensibles de l'entreprise.

Et le problème ne touche pas seulement les utilisateurs humains. Les appareils IoT (Internet des objets), les bots et les comptes de service se sont sensiblement multipliés, et toutes ces entités doivent pouvoir accéder à des applications et des données, de la même manière que des utilisateurs humains.

« 66 % des entreprises interrogées reconnaissent ignorer le nombre de relations qu'elles entretiennent avec des tiers ou la manière dont sont gérées ces relations, bien que 61 % de ces entreprises aient signalé une violation imputable à un tiers. »

- Data Risk in the Third-Party Ecosystem: Third Annual Study, Ponemon Institute

Bien que les entreprises tierces soient largement sollicitées dans de nombreux secteurs d'activité (santé, fabrication, énergie, etc.), il n'en reste pas moins que la plupart des organisations ne savent pas estimer avec précision le nombre de relations qu'elles entretiennent avec des tiers. Selon une étude du Ponemon Institute, 66 % des entreprises interrogées reconnaissent ignorer le nombre de relations qu'elles entretiennent avec des tiers ou la manière dont sont gérées ces relations, bien que 61 % de ces entreprises aient signalé une violation imputable à un tiers.

Secteur		Cas d'utilisation		
SANTÉ	Médecins et personnel infirmier contractuels	Facturation de services médicaux	Fournisseurs	Cliniques, services de soins ambulatoires
FABRICATION	Fabricants en sous-traitance	Fournisseurs	Distribution	Clients
VENTE AU DÉTAIL	Travailleurs saisonniers	Franchisés	Fournisseurs	e-commerce
ADMINISTRATIONS PUBLIQUES	Prestataires de santé en sous-traitance	Services postaux en sous-traitance	Services IT	Fournisseurs

Tandis que le recours à des ressources tierces s'est considérablement répandu à travers de nombreux secteurs, nombreuses sont les organisations qui ignorent le nombre de relations qu'elles entretiennent à cet égard.

L'enjeu est de taille. Exemple marquant d'une violation due à un tiers, l'attaque menée contre l'appliance de transfert de fichiers (FTA) d'Accellion en 2021 a été la plus destructrice de l'année, touchant 31 entreprises et plus de 5,6 millions d'utilisateurs. Des acteurs malveillants avaient alors exploité une vulnérabilité zero-day pour dérober des fichiers stockés sur un serveur en place depuis plusieurs dizaines d'années. Les utilisateurs de l'appliance FTA ont établi un parallèle entre cette attaque et la cyberattaque de SolarWinds survenue en 2020. Les hackers avaient alors employé des techniques sophistiquées pour se frayer un chemin dans de grandes organisations, en passant par leurs prestataires tiers moins bien protégés. L'attaque n'est qu'un exemple parmi les 81 incidents signalés et les 200 violations dévoilées publiquement en 2021, en lien avec des tiers.

Et le nombre d'attaques liées à des tiers ne fait que croître. Entre 2019 et 2020, le nombre de violations de données imputables à des tiers n'a fait qu'augmenter à un rythme régulier, avant d'enregistrer un fort rebond de 17 % en 2021.

Les principaux problèmes qui compromettent la sécurité des accès tiers

Les efforts autour de la sécurité des accès tiers connaissent un certain retard par rapport aux efforts déployés pour protéger les employés. Nombre d'entreprises en sont désormais à leur deuxième, voire troisième génération de solutions de gestion des identités et des accès (IAM, Identity and Access Management) pour leurs employés, alors que les problématiques associées à la gestion des accès tiers commencent tout juste à susciter une attention plus généralisée. Car force est de constater que l'importance des accès tiers est désormais reconnue comme primordiale. Auditeurs et législateurs s'accordent à dire que les accès tiers constituent une vulnérabilité majeure.

LA CONFUSION AUTOUR DE LA NOTION DE PROPRIÉTÉ

La situation se complique dès lors qu'il s'agit d'attribuer à un membre d'une entreprise la responsabilité des accès tiers. Les dirigeants à la tête d'une division n'hésitent généralement pas à recourir à des tiers pour résoudre un problème métier. Le RSSI a pour mission de concentrer ses efforts sur la cybersécurité globale de l'entreprise. L'équipe des achats, quant à elle, veille à ce que l'entreprise honore ses obligations contractuelles, tandis que l'équipe de gestion des risques et de la conformité intervient pour faire appliquer des mesures de contrôle internes. En fin de compte, ce sont les équipes IAM ou de sécurité IT qui finissent par devoir gérer le problème.

UNE PÉNURIE D'OUTILS DÉDIÉS À LA GOUVERNANCE DES TIERS

Traditionnellement, ces équipes ont eu pour habitude de déployer des applications et processus développés en interne, à la portée assez limitée. Certaines ont peut-être tenté d'utiliser le module d'un système RH proposé par un fournisseur, mais qui n'était malheureusement pas conçu pour contrôler, intégrer, surveiller, certifier les accès tiers et en évaluer les risques. Dans tous les cas, il leur manque généralement une solution adaptée pour résoudre le problème.

LE NOMBRE ÉLEVÉ D'EMPLOYÉS TIERS

Mais le problème ne se résume pas à la pénurie d'outils. La charge de travail associée à la gestion des tiers ne fait qu'aggraver la situation. Dans certains secteurs, le nombre d'utilisateurs tiers dépasse celui des employés. Le flux d'arrivées, de mutations et de départs observé dans une organisation tierce est donc également appelé à dépasser les mouvements du personnel interne d'une entreprise. La charge de travail associée à l'ajout et à la gestion sécurisés d'employés tiers impose de s'accorder avec le prestataire sur une responsabilité partagée. Mais les entreprises manquent de visibilité sur les changements de statut d'un travailleur d'une société tierce.

LE PROBLÈME DE L'APPROBATION ET DE LA COPIE DE RÔLES

Les responsables de divisions se plaignent beaucoup du temps que cela implique d'intégrer une organisation tierce et d'ajouter leurs utilisateurs pour les aider à devenir productifs le plus rapidement possible. Pour soulager les tensions, les employés peuvent parfois se contenter d'approuver une intégration ou de copier simplement des rôles, ce qui va à l'encontre du but même de s'équiper d'une solution IAM dédiée aux tiers.

LE RISQUE LIÉ AUX « N^{ièmes} PARTIES »

Outre le risque associé aux utilisateurs tiers, les sociétés tierces, elles-mêmes, multiplient les relations avec d'autres tiers (les « n^{ièmes} parties ») car les accès B2B se poursuivent tout au long de la chaîne de valeur.
Ces relations complexes mettent en péril la sécurité. Bon nombre d'utilisateurs tiers ont toujours accès au système plusieurs mois, voire plusieurs années, après que leurs droits d'accès auraient normalement dû être révoqués. Ces comptes orphelins sont une terre fertile pour les hackers qui cherchent à faire intrusion dans une entreprise.

Une autre technique consiste à injecter des logiciels malveillants dans les systèmes de l'organisation en exploitant les mises à jour de sécurité des outils couramment utilisés. Ces attaques peuvent créer une véritable onde de choc susceptible d'avoir des répercussions sur des centaines d'organisations lorsque des hackers parviennent à contourner les plus faibles défenses d'une n^{ième} partie. La cyberattaque de SolarWinds commise en 2020 est un excellent exemple de ce type d'attaque.

5 étapes essentielles pour sécuriser les accès tiers

La bonne nouvelle, c'est que les entreprises et leurs prestataires tiers collaborent aujourd'hui activement pour améliorer la posture de sécurité liée aux tiers et assurer un meilleur contrôle d'accès.

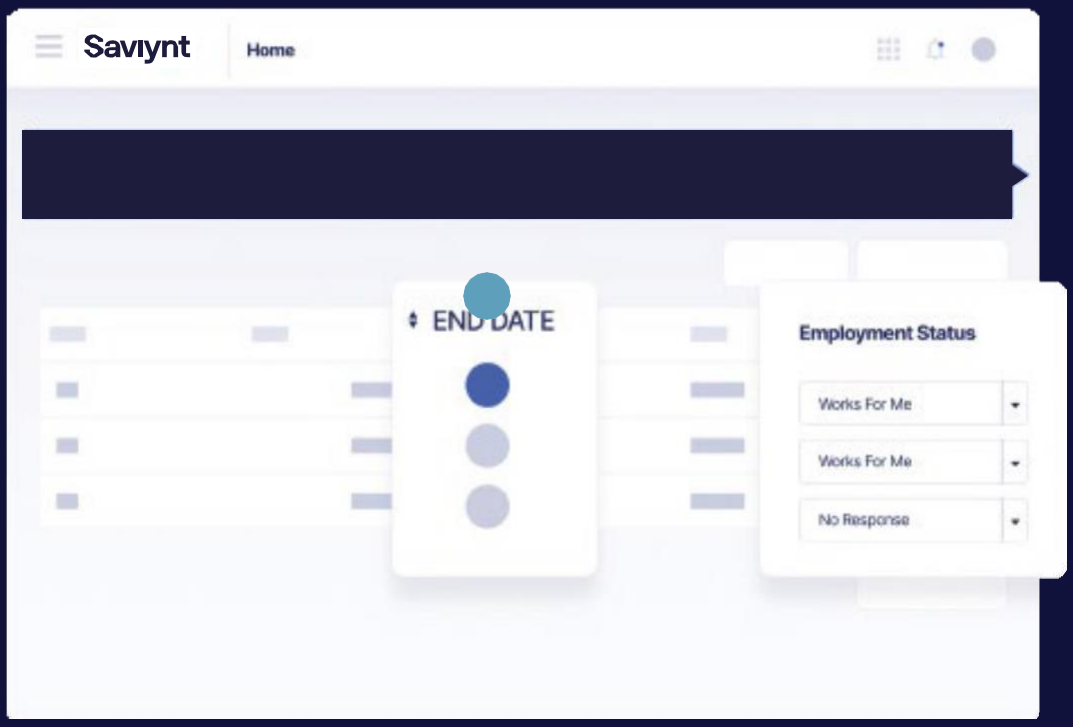
Si votre entreprise cherche à agir, nous vous recommandons de mettre en œuvre les cinq stratégies suivantes pour réduire le risque d'exposition à des risques liés aux tiers.

ÉTAPE 1

Consolider les organisations tierces

Les finances et les achats peuvent constituer un bon point de départ pour la consolidation de l'ensemble des organisations tierces. Toute entité ayant souscrit un contrat de prestation de services auprès d'un quelconque service de votre entreprise doit être identifiée et cataloguée dans un système d'enregistrement (SoR, System of Record) faisant autorité, qui recense tous les privilèges d'accès permanents attribués aux utilisateurs actuels. Saviynt propose plusieurs passerelles d'intégration (intégration déléguée ou intégration fédérée, notamment).

Si votre entreprise en est aux premières phases de son parcours, il convient qu'elle réalise un test initial afin d'identifier la dernière fois que des organisations tierces ont utilisé des informations d'identification. Cette étape vous permettra de repérer les comptes inactifs et de prendre des mesures pour atténuer les risques associés. Les informations d'identification inutilisées pendant une certaine durée doivent être signalées afin de faire l'objet d'un suivi et d'être désactivées en cas de départ ou de changement de poste de l'utilisateur.



Les mécanismes de vérification de poste et d'accès ponctuel développés par Saviynt réduisent les comptes orphelins.

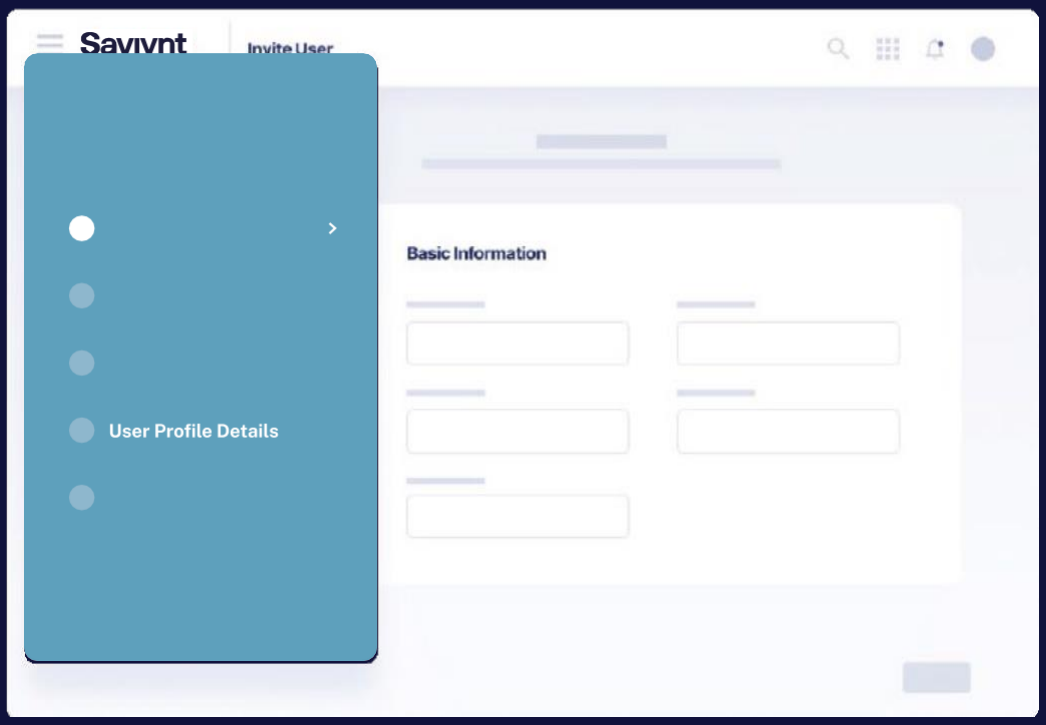
Cette étape est le moment idéal d'obtenir le soutien des administrateurs tiers et de solliciter une responsabilité commune. Ces administrateurs disposent d'une meilleure visibilité sur le flux d'arrivées, de mutations et de départs observé au sein de leur organisation. Il est donc important qu'ils agissent comme principaux interlocuteurs pour procéder aux examens et certifications des accès récurrents. Au moment de la reconduction de contrats, il est essentiel de se référer aux accords de niveau de service qui stipulent les responsabilités de l'organisation tierce et son engagement à apporter un soutien administratif.

ÉTAPE 2

Instaurer des processus de contrôle et d'intégration fondés sur une connaissance des risques

Votre entreprise et son organisation tierce doivent mettre en place un workflow de contrôle et d'intégration des utilisateurs tiers afin de vérifier leur identité et que leur processus d'intégration respecte le concept du « moindre privilège ». Il convient de ne leur accorder que les droits d'accès strictement nécessaires aux rôles qui leur sont attribués. Les définitions de rôles doivent se rapporter spécifiquement aux tâches réellement confiées, en évitant de simplement les dupliquer au prétexte que les rôles présentent des similitudes.

Pour faciliter la collecte d'informations dans le cadre des procédures de contrôle et de vérification d'identité, les utilisateurs tiers peuvent utiliser un portail en libre-service pour demander l'accès et fournir la documentation demandée. En accélérant les étapes de contrôle et de mise en service, les portails en libre-service aident les utilisateurs à devenir rapidement productifs. Établir un workflow clair entre le sponsor de votre entreprise et l'administrateur tiers permet de réduire le volume d'appels téléphoniques et d'e-mails qui tendent à ralentir le processus.



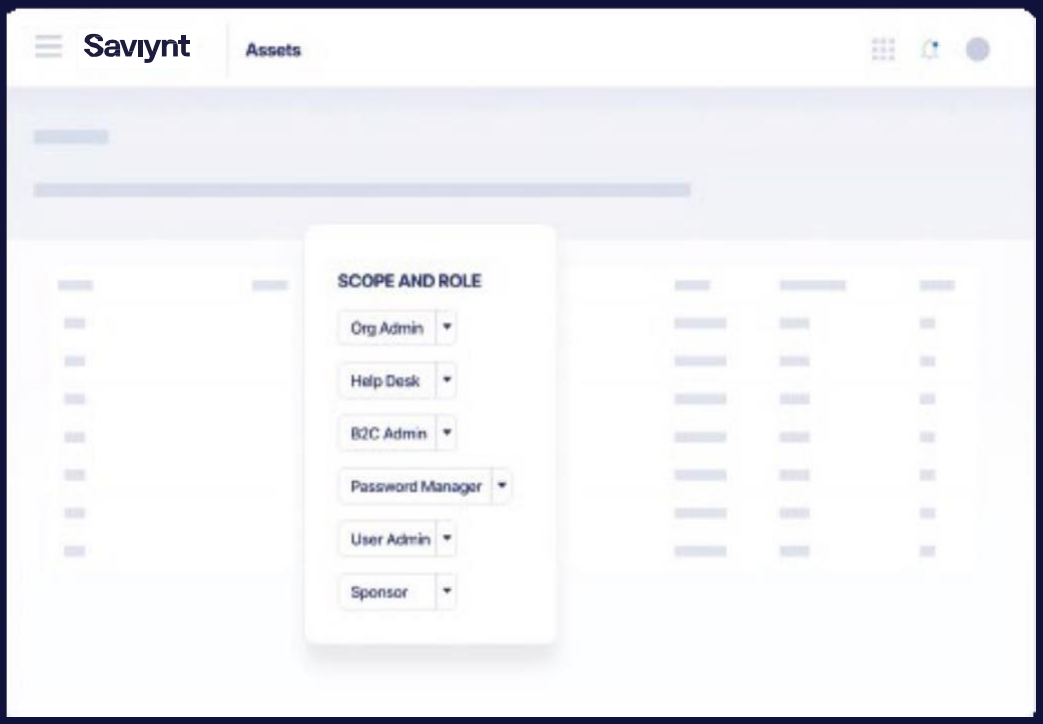
Saviynt assure une intégration simple et cohérente des utilisateurs tiers.

ÉTAPE 3

Définir et affiner les politiques et moyens de contrôle

Votre entreprise, en collaboration avec les organisations tierces, doit définir des politiques et des moyens de contrôle, et les optimiser en permanence afin d'identifier d'éventuelles violations et de réduire les faux positifs, de manière à réduire la charge de travail administrative. Au fil du temps, vous pouvez encore gagner en efficacité en adoptant des mécanismes d'auto-remédiation.

Testez vos politiques et moyens de contrôle à intervalles réguliers (chaque mois ou chaque trimestre) avec les administrateurs de votre entreprise et de votre prestataire tiers. Les vérifications régulières des accès et les certifications en continu offrent un excellent moyen d'empêcher le surprovisionnement des utilisateurs et d'éviter que des comptes orphelins ne permettent d'accéder à des données sensibles.



Saviynt offre un système d'enregistrement complet qui recense tous les privilèges permanents octroyés à des utilisateurs tiers.

ÉTAPE 4

Instaurer des contrôles de conformité pour l'ensemble du personnel

Un certain nombre de cadres réglementaires met en évidence l'importance croissante des accès tiers, qui sont aujourd'hui au centre de l'attention des auditeurs. Par exemple, la loi Sarbanes-Oxley (SOX) prévoit plusieurs mesures de contrôle pour gérer le risque lié aux tiers :

- APO10.01/APO10.02 : la sélection des fournisseurs doit être conforme aux politiques et processus de l'organisation en matière de gestion des risques liés aux fournisseurs tiers ;
- APO10.03 : une personne désignée doit s'assurer, par une surveillance régulière et par la production de rapports, que les tiers répondent aux critères de performances de niveau de service de l'organisation ;
- APO10.04 : les contrats de services conclus avec des tiers doivent couvrir les différents risques, contrôles de sécurité et procédures associés à la protection des systèmes d'information et des réseaux.

L'objectif ultime est de soumettre tous les accès tiers aux mêmes exigences de conformité que celles imposées aux employés, pour assurer une cohérence dans l'ensemble du personnel et être en mesure de limiter rapidement les conséquences de toute violation. Vous pouvez relier des contrôles de conformité à un type d'utilisateur donné et faire appliquer des politiques d'auto-remédiation pour agir rapidement en cas d'identités non conformes.

Pour faciliter la mise en application des contrôles de conformité et être en mesure de présenter plus efficacement les documents d'audit exigés, l'idéal est d'opter pour des rapports de conformité réglementaire prêts à l'emploi qui couvrent la loi Sarbanes-Oxley, l'HIPAA, le RGPD, le PCI-DSS et d'autres réglementations.

ÉTAPE 5

Mettre en œuvre une gouvernance convergée

Au terme des quatre premières étapes, vous pouvez relever le niveau de maturité de votre approche de cybersécurité en combinant les solutions de Gouvernance et d'Administratioin des Identités (IGA), Privileged Access Governance et Third-Party Access Governance pour faire converger la gouvernance de l'ensemble de votre personnel.

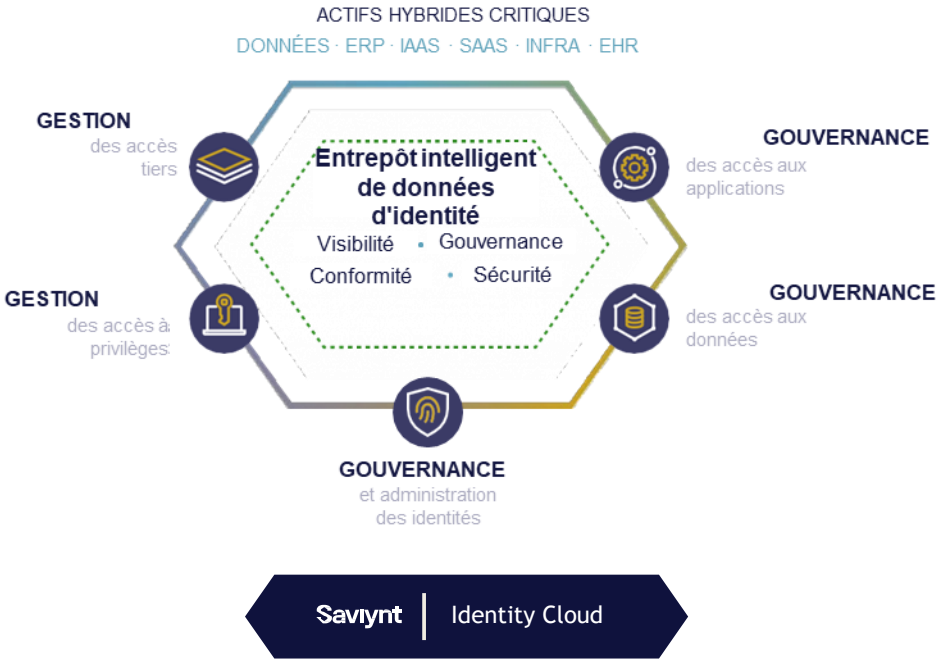
Cette vue convergée offre une interface unique qui vous permet d'obtenir une visibilité complète sur vos équipes. Elle apporte également un niveau de sécurité supplémentaire, en révoquant immédiatement l'accès aux systèmes en aval, si les conditions l'exigent et en accordant un accès ponctuel, révocable au terme d'un contrat. Et en ajoutant à votre suite la solution Application Access Governance, vous pouvez identifier les cas potentiels et réels de violation du principe de séparation des tâches sur l'ensemble de vos applications SaaS et de vos applications sur site.

Sécurisez votre entreprise avec une plateforme de gestion d'identités cloud-native, de bout en bout

Plutôt que d'avoir à gérer plusieurs relations et intégrations pour fournir une solution de gestion d'identités de bout en bout, vous pouvez utiliser la plateforme Identity Cloud de Saviynt pour bénéficier rapidement des avantages d'une solution d'identité de première classe.

Saviynt Identity Cloud

La première plateforme cloud d'identité et de gouvernance, conçue pour allier simplicité et évolutivité.



Saviynt Identity Cloud intègre dans une même plateforme plusieurs fonctionnalités de gestion d'identités afin d'unifier les moyens de contrôle et la gestion des risques pour chaque identité, chaque application et chaque solution cloud dans l'ensemble de votre entreprise. Identity Cloud vous permet d'intégrer des personnes, des applications et des machines en seulement quelques minutes, et d'activer de manière sélective les fonctionnalités d'accès et de gouvernance.

Intégré à la solution Identity Cloud, le module Saviynt Third-Party Access Governance aide un grand nombre d'organisations à simplifier le processus d'accès tiers et à réduire les risques en adoptant une approche de l'accès tiers fondée sur l'appui de sponsors. Saviynt offre des fonctions d'automatisation, de demande d'accès, de visualisation des risques et de contrôle d'accès, tout au long du processus d'intégration des tiers et gère ces identités tout au long de leur cycle de vie.

Notre produit Third-Party Access Governance vous permet :

- de collaborer en toute confiance avec des tiers ;
- de réduire les risques liés au personnel travaillant à distance ;
- de gérer le cycle de vie des organisations, des personnes et des identités tierces ;
- de consolider sur une même plateforme la visibilité et les contrôles sur les accès.

Les sponsors internes et externes surveillent le compte au fil de ses différentes étapes : création, gestion des accès, examens périodiques, mise hors service finale. Choisir Saviynt, c'est la garantie :

- d'une intégration rapide à moindres coûts ;
- d'une visibilité totale sur les risques liés aux fournisseurs ;
- d'une solide gestion du cycle de vie des comptes fournisseurs ;
- de politiques de demandes d'accès configurables ;
- d'une auto-remédiation en cas de compte non conforme.

Il va devenir de plus en plus impératif de renforcer la gouvernance des accès tiers. En traitant ce problème dès maintenant, avec la solution cloud-native de bout en bout de Saviynt qui a fait ses preuves, vous serez en mesure de combler vos lacunes en matière de sécurité des tiers et d'assurer à votre entreprise une sécurité complète, dès maintenant et pour les années à venir.

À PROPOS DE SAVIYNT

Saviynt est la principale plateforme de gouvernance d'identités conçue pour le cloud. Nous aidons les entreprises à accélérer les initiatives de cloud et à relever en un temps record les défis les plus complexes en matière de sécurité et de conformité. Saviynt Identity Cloud regroupe des fonctions de gouvernance et d'administration d'identités (IGA), d'accès granulaire aux applications, de sécurité cloud et d'accès à privilèges dans la seule solution SaaS d'entreprise disponible sur le marché. Pour en savoir plus, rendez-vous sur saviynt.com/fr.

Envie de parler à un expert de l'identité et de la sécurité ?

Contactez-nous dès maintenant sur
saviynt.com/fr/contact-us

Saviynt

Headquarters, 1301 E
El Segundo Bl, Suite D, El Segundo,
CA 90245, États-Unis

310. 641. 1664 | info@saviynt.com
www.saviynt.com/fr