# Créer ou acheter

## Guide pour la gestion des identités

Auth0

# Table des matières



# Qu'est-ce que la gestion des identités ?

La gestion des identités et des accès (GIA), ou tout simplement la gestion des identités, se réfère à un service ou une plate-forme qui identifie les individus et contrôle leur accès aux ressources du système par le biais de droits et de restrictions d'utilisateur. La gestion des identités est importante pour la sécurité et accroît la productivité des utilisateurs par la mise en place d'un répertoire central : les utilisateurs n'ont pas besoin de mémoriser et de conserver plusieurs noms d'utilisateurs et mots de passe. La GIA contribue également à protéger les entreprises et leurs utilisateurs contre les violations des données. En 2015, le coût total moyen d'une violation de données s'élevait à 3,8 millions de dollars[1]. La gestion de l'identité peut offrir une protection contre ces types de menaces avec des fonctionnalités de sécurité telles que l'authentification à facteurs multiples, la protection contre la violation de mot de passe, la détection d'anomalie, et plus encore.

Les solutions de gestion des identités offrent des avantages pour les entreprises de tout type. La GIA peut également offrir des fonctionnalités distinctes et spécialisées pour les cas d'utilisation B2B, B2C et B2E.

- **B2B:** Une entreprise fournit une gestion des identités fédérée à une autre entreprise, par exemple Trello qui permet à une autre entreprise de se connecter à Trello avec ses identifiants d'entreprise.
- **B2C:** Une entreprise fournit une authentification sur les réseaux sociaux aux consommateurs par l'intermédiaire de Facebook, Google, ou d'autres fournisseurs d'identité de réseaux sociaux.
- **B2E:** Une entreprise fournit une authentification unique SSO à ses propres employés.

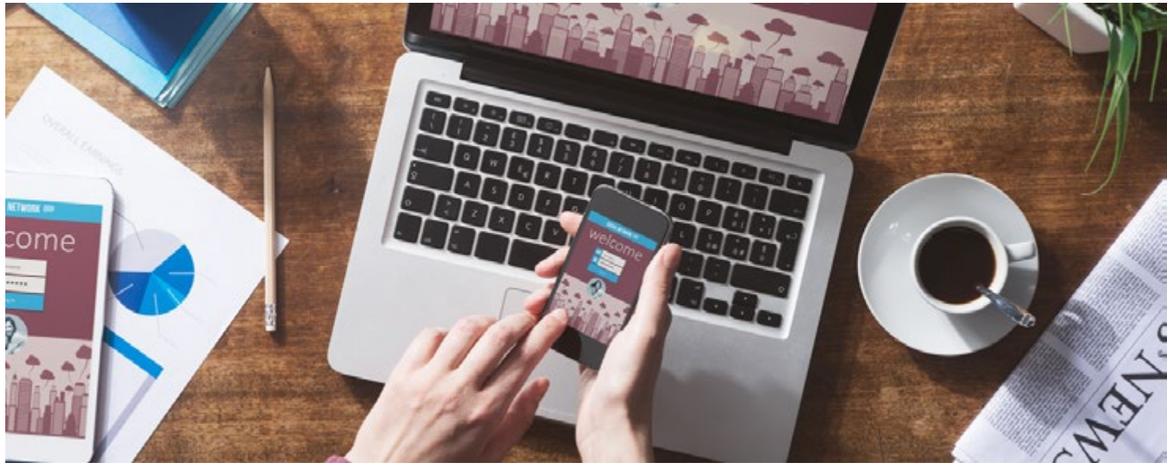
[1] http://www.prnewswire.com/news-releases/ponemon-institutes-2015-global-cost-of-data-breach-study-reveals-average-cost-of-data-breach-reaches-record-levels-300089057.html Retrieved Mar 9, 2017.

Nous allons aborder les avantages de la GIA concernant ces trois types d'activités dans ce document.

La gestion des identités englobe de nombreuses solutions d'authentification, notamment :

- **Identités fédérées:** La gestion des identités fédérées est une méthode de transfert des données d'authentification sans violation de la politique d'origine, généralement en utilisant un serveur d'autorisation externe.
- **Authentification unique SSO:** L'authentification unique SSO est un type de gestion des identités fédérée. L'authentification unique SSO est utilisée lorsqu'un utilisateur se connecte à un client et qu'il se connecte ensuite à d'autres clients automatiquement, indépendamment des différences au niveau de la plate-forme, de la technologie ou du domaine. Un jeton ou cookie est généré pour authentifier l'utilisateur sur plusieurs domaines.
- **Fédération d'entreprises:** Une Fédération d'entreprises est une gestion des identités fédérées avec des connexions d'entreprise telles que Active Directory, LDAP, ADFS, SAML, Google Apps, etc.





La gestion des identités est en constante évolution. Le paysage numérique se développe et change très rapidement. Les smartphones et les tablettes sont partout, et les entreprises sont passées au numérique. Pour réussir, les entreprises doivent pouvoir protéger et sécuriser les identités sur une large gamme de périphériques et de plates-formes. Au cours des dernières années, les concepts de gestion des identités tels que l'authentification à facteurs multiples (AFM), l'authentification sans mot de passe et l'authentification unique (SSO) sont passées au premier plan pour ce qui est de la gestion des identités pour des systèmes modernes distribués.

*L'Authentification à facteurs multiples* utilise des méthodes d'authentification distinctes pour fournir au moins deux étapes de connexion. Sans mot de passe, il existe des méthodes (SMS, liens magiques ou même des caractéristiques biométriques telles que l'authentification par empreinte digitale) pour authentifier les utilisateurs.

Les applications basées sur le cloud sont l'un des principaux facteurs conduisant à l'adoption d'une gestion des identités. Les applications et les services cloud, tels que Google Apps et Amazon Web Services

(AWS), utilisent un réseau de serveurs distants pour stocker, gérer et traiter des données. La GIA est une composante vitale des applications qui utilisent des services hébergés sur le cloud. La gestion des identités offre des méthodes permettant de surveiller et de fournir un accès utilisateur sécurisé aux ressources nécessaires. Une autre tendance conduisant à l'adoption de la GIA est la nécessité pour les utilisateurs de pouvoir accéder aux applications de n'importe où et sur n'importe quel appareil. Avec le développement de l'informatique personnelle, les entreprises doivent pouvoir fournir un accès sécurisé à leurs utilisateurs quel que soit l'endroit où ils se trouvent ou l'appareil qu'ils utilisent. La gestion des identités centralise l'authentification afin que l'identité de l'utilisateur puisse être confirmée dans toutes les circonstances de connexion.

Pour les entreprises B2C, l'authentification via les réseaux sociaux est une autre tendance conduisant à l'adoption de solutions GIA. Les clients potentiels utilisent différents réseaux sociaux quotidiennement. Les solutions GIA permettent l'authentification sur les réseaux sociaux avec différents fournisseurs d'identité sociale, et permettent aux clients de s'authentifier avec des informations de connexion qu'ils utilisent déjà régulièrement sans devoir créer et retenir de nouveaux identifiants.



# Les signes indiquant vous devez passer d'une solution artisanale à une solution de gestion des identités

## Tous les cas d'utilisation

- Vous avez besoin d'une solution basée sur des normes, telles que OpenID Connect, SAML, WS-Federation, et/ou OAuth.
- Vous avez des utilisateurs qui s'authentifient auprès de divers fournisseurs d'identité, mais vous ne disposez d'aucun moyen pour lier leurs comptes.
- Vous avez des applications sur des domaines différents et demandez aux utilisateurs de se connecter séparément pour chacun de ces domaines.

- Vos meilleurs développeurs consacrent leur temps à créer et maintenir la gestion des identités et l'authentification au lieu de créer des applications essentielles à l'activité.
- Votre entreprise a subi tout type de violation de données, ou vous vous inquiétez d'une possible violation des données.
- On vous demande des certifications industrielles auxquelles vous n'avez pas réfléchi ou que vous n'avez pas prises en compte.

## B2B

- Vos clients demandent à utiliser leurs identifiants d'entreprise pour se connecter à votre produit. Vous devez prendre en charge une Fédération d'entreprises avec de nombreux types de fournisseurs d'identité, comme Active Directory, en plus d'une option de nom d'utilisateur/mot de passe.
- Vous ne pouvez pas déléguer la gestion des utilisateurs au service d'assistance de votre client.



## B2C

- Votre principale source de données utilisateur consiste à demander directement aux utilisateurs de remplir des formulaires ou des sondages. Pouvoir extraire facilement les données tierces sur vos utilisateurs vous aidera à mieux comprendre vos clients et à générer plus de revenus grâce à des ventes additionnelles et à un marketing ciblé.
- Si vous vendez aux consommateurs, vous ne proposez pas d'option d'inscription facile en un clic par le biais de fournisseurs d'identité de réseaux sociaux.
- Vous êtes confronté à des problèmes de performance en raison de l'augmentation de votre base d'utilisateurs.

## B2E

- Vous devez gérer les différents niveaux d'autorisation et d'accès pour vos employés.
- Vous devez être en mesure de provisionner et déprovisionner des utilisateurs facilement lorsque des employés rejoignent ou quittent votre entreprise.

# Arguments économiques justifiant l'achat d'une solution de gestion des identités

Il y a beaucoup de bonnes raisons justifiant l'achat d'une gestion des identités pour tous les cas d'utilisation, notamment le B2B, le B2C et le B2E. Voici quelques exemples:

## Tous les cas d'utilisation

**Réduction des coûts d'ingénierie:** L'implémentation d'une solution tierce de gestion des identités est simple et l'activation de fonctionnalités peut se faire très facilement en appuyant sur un commutateur. Des centaines, si ce n'est des milliers d'heures de développement précieuses peuvent de nouveau être consacrées à l'écriture de la logique d'entreprise plutôt qu'à la création de l'authentification. Beaucoup de temps consacré aux tests et à la sécurité de l'authentification peut également revenir au travail d'application de base. L'intégration et le mappage des fournisseurs d'identité peuvent prendre du temps et être pénible. Avec une solution GIA, ces intégrations sont déjà construites et fournies. Une GIA devrait également offrir des SDK pour des infrastructures de développement populaires, réduisant encore plus le codage supplémentaire nécessaire pour intégrer le système d'authentification. L'équipe d'ingénierie d'une entreprise peut se consacrer à la configuration plutôt qu'au codage et la personnalisation.

**Sécurité accrue:** Le stockage des données avec une solution de gestion des identités de tiers renforce la sécurité. Les solutions GIA respectent les politiques de conformité et les certifications en matière de sécurité. Une solution assure le stockage et le transport des données en toute sécurité. De plus, une solution GIA fournit une identité fédérée afin que les utilisateurs ne se livrent pas à de mauvaises pratiques,



comme par exemple réutiliser le même mot de passe pour éviter d'avoir à se souvenir de plusieurs identifiants de connexion.having to remember multiple login credentials.

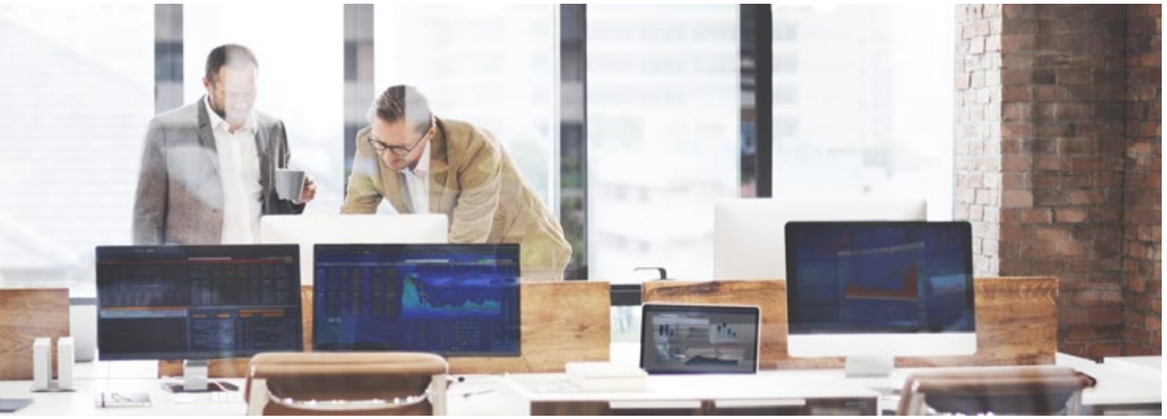
## B2B

**Adoption accrue de l'entreprise:** Une solution de gestion des identités offre une fédération d'entreprises solide, permettant des connexions d'entreprise, comme par exemple Microsoft Active Directory, LDAP, ADFS, SAML, Google Apps, et plus encore. La fédération d'entreprises augmente l'adoption par les entreprises qui utilisent déjà ces technologies en permettant aux utilisateurs de se connecter avec leurs identifiants d'entreprise existants. Avec l'authentification unique SSO, les utilisateurs n'ont pas besoin de mémoriser des noms d'utilisateur ou de mots de passe supplémentaires. Cela améliore la facilité d'accès et réduit le taux de désabonnement.

**Augmentation des revenus de l'entreprise:** Une solution de gestion des identités garantit qu'une application peut prendre en charge tous les types de Fédération d'entreprises que les clients peuvent demander. Elle garantit également que les exigences en terme de sécurité sont satisfaites, réduisant ainsi les coûts.

Les clients potentiels de l'entreprise disposant d'identifiants existants peuvent s'authentifier avec le même identifiant. Cela permet de générer des revenus par les entreprises clientes tout en réduisant les frictions avec les utilisateurs.

**Réduction du cycle de vente/de l'intégration:** L'identité fédérée permet aux entreprises d'utiliser leurs propres identifiants avec un produit ou un service tout en garantissant le respect des exigences de sécurité. Cela favorise des cycles de vente plus rapides et l'intégration client. Les clients n'ont pas besoin de procéder à une nouvelle ouverture de session peu familière, ni de mémoriser un autre mot de passe. Elles peuvent utiliser leurs identifiants d'entreprise pour avoir une authentification unique sur toutes les propriétés.



## B2C

**Adoption accrue des consommateurs:** En fournissant un espace de connexion unifié et convivial pour les clients, la gestion des identités offre une expérience d'inscription et de connexion cohérente et sans heurts à toutes les applications, quel que soit le navigateur ou l'appareil. Une solution de gestion des identités peut recueillir plus de données sur les utilisateurs. À leur tour, les entreprises peuvent utiliser les données pour favoriser l'adoption et générer efficacement des opportunités de ventes additionnelles.



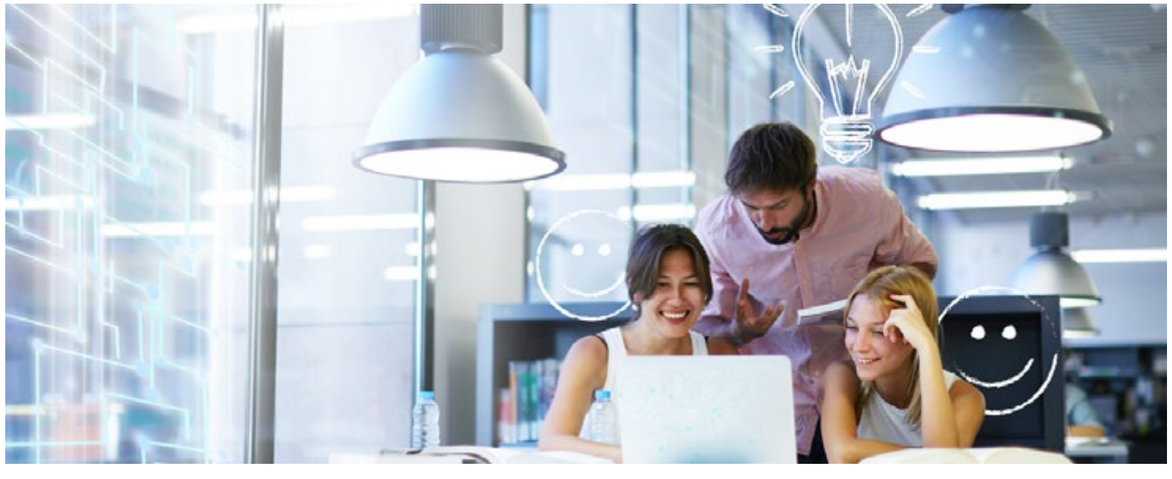
Une solution qui offre un espace de connexion intuitif pour optimiser les taux d'inscription et de connexion permet également de réduire les ressources nécessaires pour la conception et le marketing. Une solution tierce est construite à l'échelle pour s'adapter à autant de demandes d'authentification que nécessaire, afin de maintenir des performances et une disponibilité élevées.

## B2E

**Authentification SSO tiers:** Une solution GIA fournit une authentification unique SSO, ce qui permet aux utilisateurs de se connecter à plusieurs tiers avec une seule ouverture de session. Que ce soit pour les applications sur site ou sur le cloud, l'authentification unique SSO permet aux utilisateurs de se connecter une fois et d'accéder à n'importe quelle application sans être invité une deuxième fois à saisir leurs identifiants. L'authentification unique SSO peut être utilisée pour authentifier des applications telles que ERP, Salesforce, Workday, Office 365, et plus encore.

**Gestion des niveaux d'autorisation:** Une solution de gestion des identités permet de contrôler facilement différents niveaux d'accès pour les utilisateurs. Des privilèges peuvent être assignés et modifiés

lorsque des employés rejoignent une entreprise ou sont promus. Les utilisateurs peuvent également être déprovisionnés, et tous les accès et autorisations peuvent être révoqués.



## Principaux facteurs à prendre en compte pour l'évaluation d'une solution GIA

Plusieurs Critères doivent être pris en compte lors de la sélection d'une solution de gestion des identités pour votre entreprise.

**Options de déploiement:** Recherchez l'option permettant d'héberger n'importe où. Votre solution de gestion des identités doit avoir l'option pour être déployée sur le cloud de la solution, sur votre cloud, ou sur votre propre Data Center.



**Facilité d'intégration:** L'un des nombreux avantages de l'utilisation d'une solution GIA est que cela permet de réduire le temps de développement. Recherchez une solution qui propose des SDK, une documentation approfondie, des API puissantes et des fonctionnalités simples et faciles à configurer et à activer.

**Prise en charge de tous les fournisseurs d'identité:** Une solution de gestion des identités efficace doit prendre en charge pratiquement toutes les sources d'identification populaires. Pour les employés, cela comprend Microsoft Active Directory, ADFS, Office 365, Google Apps et les solutions SAML. Pour les consommateurs, cela inclut la prise en charge de toutes les bases de données personnalisées, les fournisseurs d'identité de réseaux sociaux (comme Google, Twitter, Facebook, etc.) et les solutions sans mot de passe telles que SMS, email, et Touch ID.

**Extensibilité:** Votre entreprise ne reste pas statique, par conséquent votre gestion des identités ne doit pas l'être non plus. Votre GIA doit vous permettre de personnaliser facilement le canal d'authentification et d'autorisation. Idéalement, vous devriez pouvoir personnaliser le produit selon vos besoins dans le tableau de bord, sans avoir besoin de contacter l'assistance ou d'acheter un forfait d'assistance specifique. Votre solution GIA doit également vous permettre d'étendre ses fonctionnalités, par exemple l'importation/exportation de données utilisateur, l'intégration facile avec d'autres applications, l'autorisation ou l'exécution de scripts personnalisés pour étendre les fonctionnalités standard du produit.

**Fonctionnalités de sécurité de pointe:** Votre choix de GIA doit être étudié par des experts internationaux de la sécurité et se conformer à des normes telles que SAML, OAuth, WS-Federation, et des certifications comme OpenID Connect, SOC2, HIPAA, etc. Vérifiez qu'elle offre des fonctionnalités de protection importantes contre les menaces d'attaque et la violation des données, comme par exemple la détection de violation de mot de passe et la protection contre la force brute.

**Facilité de migration:** La migration vers et depuis votre solution de gestion des identités doit être prise en charge sans restriction. Assurez-vous qu'il n'y a pas de verrouillage du fournisseur susceptible d'empêcher les utilisateurs de migrer, dans le futur, hors du système actuel. La solution doit également se connecter à n'importe quelle boutique utilisateur que vous utilisez déjà, et ne doit pas obliger les utilisateurs à réinitialiser leur mot de passe manuellement lors de la migration vers la nouvelle solution.

**Assistance rapide des experts en sécurité / du service clients:** L'équipe d'assistance de votre GIA doit disposer d'une équipe d'experts prêts à régler tous les problèmes 24 heures sur 24. L'équipe doit également inclure 15 ingénieurs experimentés dans l'implémentation de solutions GIA.

# Études de cas de différentes industries

## Pilotez la croissance avec une gestion des identités unifiée

Avec plus de 170 000 employés dans plus de 100 pays, Schneider Electric, leader mondial dans la gestion de l'énergie et l'automatisation, avait besoin d'une stratégie de gestion des identités capable d'évoluer avec la croissance de l'entreprise, tout en optimisant l'utilisation efficace des ressources. Le principal besoin de Schneider Electric lors du choix de la GIA était un système d'authentification unique pour créer un processus d'authentification unifiée. Cela permettrait à l'entreprise d'utiliser les mêmes identifiants et autorisations pour tous les différents systèmes et applications de la société.



Une analyse coûts-bénéfices a rapidement montré que Schneider Electric pourrait tirer un meilleur profit de ses ressources pour atteindre les buts et objectifs principaux de l'entreprise. L'utilisation d'Auth0 pour la gestion des identités pourrait éliminer les obstacles au sein de l'entreprise et résoudre des problèmes complexes en matière d'intégration des identités. Auth0 fournissait également une solution solide et flexible axée sur les développeurs et facile à intégrer. La plate-forme était optimisée pour le Web et les appareils mobiles, prenait en charge des normes standardisées, offrait des fonctionnalités puissantes, une pérennité, la prise en charge d'un grand nombre de fournisseurs d'identité et une migration facile.

Une fois Auth0 sélectionné et implémenté, de nombreux avantages ont été constatés. L'utilisation de la solution de gestion des identités Auth0 a éliminé tout travail de développement supplémentaire. Cela a libéré davantage de ressources pour l'innovation informatique. Le temps de mise sur le marché a été réduit et le système a bénéficié d'une sécurité accrue et de meilleures pratiques. Auth0 offrait également des réactions rapides et complètes aux vulnérabilités.

*"Avant que les sites d'information ne rendent compte de la vulnérabilité zero-day Heartbleed l'an dernier, Auth0 nous a envoyé un e-mail pour nous alerter de la situation. Il existait déjà un correctif pour éliminer la menace Heartbleed des systèmes Auth0, et Auth0 nous a envoyé un e-mail de confirmation indiquant que ce correctif avait déjà été installé sur l'instance du service Auth0 de Schneider Electric », explique Berard. « Auth0 permet à notre équipe de plate-forme de faire très bonne impression. Dans ce scénario, le problème de sécurité a été corrigé et notre équipe informatique a pu gagner un temps précieux en exploitant les étapes détaillées sur la façon dont les problèmes ont été atténués pour faire rapport directement à notre équipe interne. De plus, Auth0 offrait un suivi cyclique des certificats, ce qui aurait là aussi demandé un travail intensif à l'équipe si elle avait dû le faire toute seule."*

*"Avec la plate-forme Auth0, nous pouvons très tôt planifier et intégrer l'architecture d'identité pour gagner un temps précieux et être assuré qu'un système sécurisé est mis en place lorsque le projet démarre"*

## Unification de l'identité entre les applications sur site et les applications cloud

Bluetooth, leader mondial dans la technologie sans fil, disposait d'un écosystème en plein développement qui posait plusieurs problèmes. L'entreprise, qui a démarré sous la forme d'une application unique, a rapidement développé plusieurs applications différentes. Les applications développées en interne ainsi que les applications SaaS tierces (Sharepoint, ServiceNow, SiteCore) nécessitaient toutes des identifiants différents. La solution existante développée en interne de Bluetooth était basée sur des formulaires et utilisait des identifiants avec nom d'utilisateur et de mot de passe. Cette plate-forme n'était pas adaptée à l'identité fédérée. L'entreprise avait donc besoin d'une solution de gestion des identités moderne avec une authentification unique pour prendre en charge toutes leurs applications SaaS développées en interne et tierces. La solution devait être implémentée tout en maintenant la plate-forme existante en fonctionnement avec la capacité future d'offrir une migration complète. Les rôles et accès utilisateur étaient également essentiels pour assurer des niveaux d'accès adéquats aux documents confidentiels.

Auth0 a offert une solution à la hauteur de la situation. L'implémentation d'Auth0 s'est faite facilement et a permis à l'équipe d'ajouter l'authentification unique moderne SSO. Le système hérité a été conservé intact pendant l'implémentation et l'exécution du plan de migration. Il n'a fallu que quelques jours pour implémenter Auth0 contrairement à l'implémentation d'une plate-forme interne qui nécessite plusieurs mois. La documentation de grande qualité, avec des exemples de code détaillés couvrant des sujets similaires et des questions pointues, a permis aux ingénieurs de Bluetooth SIG de comprendre et d'implémenter rapidement leur solution de gestion des identités moderne. Bluetooth a travaillé avec les ingénieurs chevronnés d'Auth0 pour élaborer une démonstration de faisabilité, afin de présenter conjointement les capacités de la plate-forme. Les temps de réponse du support étaient courts et un traitement rapide. Globalement, l'ensemble de la technologie, la documentation et l'assistance d'Auth0 était tout à fait adapté pour fournir la solution idéale à Bluetooth.

# Conclusion

La gestion moderne des identités est une tâche difficile. Suivre l'évolution des normes et des bonnes pratiques, corriger les bugs de sécurité vous coûtent du temps et de l'argent que vous ne pouvez pas consacrer pour votre activité principale. Si vous prenez en compte les fonctionnalités qui se développent selon les besoins de votre organisation et la façon dont d'autres entreprises ont évalué et implémenté avec succès leurs propres solutions, vous pouvez rapidement mesurer les bénéfices d'une solution de gestion des identités.

En résumé, votre organisation peut transformer sa GIA: au lieu d'être un point de risque critique et un bloquer ainsi le developpement de votre société, cela peut devenir un système qui permet à votre entreprise de générer des revenus et de les faire augmenter. Avec Auth0, vous pouvez implémenter une GIA en quelques jours seulement et pérenniser de votre organisation en utilisant la solution GIA la plus facile, la plus complète et la plus extensible disponible.

# Nous pouvons vous aider

Auth0 peut vous aider à gérer les identités pour vos utilisateurs. En tant qu'experts en sécurité, nous avons élaboré une plate-forme de gestion des identités en tant que service (IDaaS) conçue dans l'optique de sécurité avancée. Plus de 80 000 développeurs dans 167 pays font confiance à Auth0 pour leur solution de gestion des identités.

La plate-forme de gestion des identités d'entreprise Auth0 offre de nombreuses fonctionnalités et avantages à ses clients, notamment:

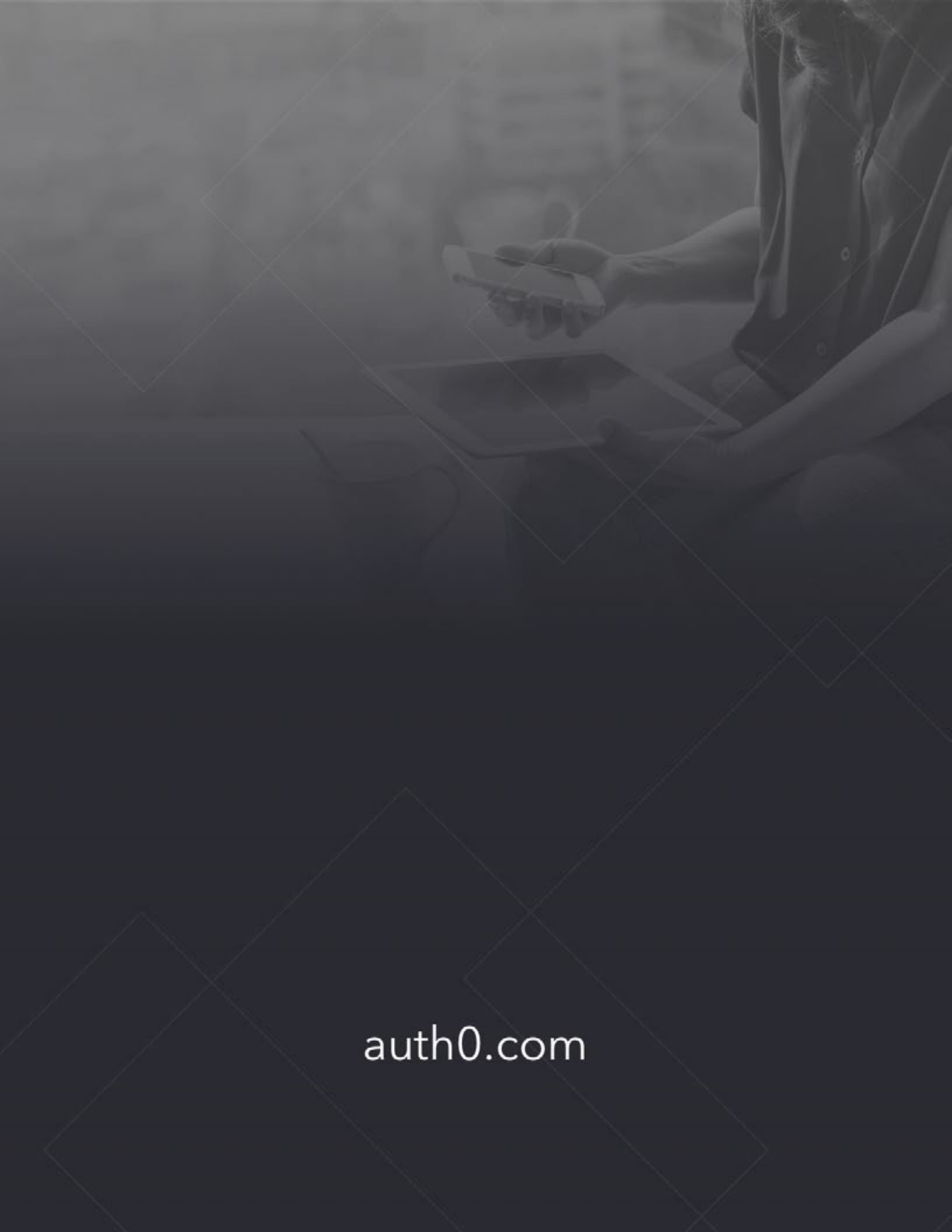
- La possibilité de configurer et d'implémenter une fédération d'entreprises et une authentification unique SSO qui ne nécessitent qu'une configuration de base et aucun developpement.
- Les connexions d'entreprise prises en charge par Auth0 incluent Active Directory, LDAP, ADFS, SAML, Google Apps, et plus encore.
- Auth0 prend en charge les connexions vers des réseaux sociaux avec tous les principaux fournisseurs, notamment LinkedIn, Facebook, Twitter, Google, et bien d'autres.
- Auth0 fournit une authentification traditionnelle avec nom d'utilisateur et mot de passe, à partir de la base de données Auth0 ou toute base de données. Des fonctionnalités de sécurité renforcées telles que l'authentification à facteurs multiples, la détection de violation de mots de passe, la protection contre les attaques par force brute et la détection des anomalies sont inclues dans la solution.
- Les utilisateurs peuvent migrer sans difficulté de systèmes existants sans réinitialisation forcée des mots de passe.
- Auth0 fournit des méthodes de contrôle, d'analyse et d'affichage basées sur l'identité pour garantir la conformité organisationnelle et faire ressortir les opportunités de ventes additionnelles.
- Les entreprises peuvent gérer facilement l'accès utilisateur avec des autorisations affinées et des règles personnalisées et puissantes.
- L'administration déléguée d'Auth0 permet aux entreprises de gérer des accès granulaires, la visibilité et la gestion des utilisateurs pour les clients.
- Avec Auth0, il faut, généralement, moins de trente minutes à un développeur pour configurer une gestion des identités solide et personnalisable sur n'importe quelle infrastructure technologique.

# Ressources

Pour plus d'exemples sur la façon dont d'autres entreprises ont évalué Auth0, veuillez consulter la page **auth0.com/customers** ou nous contacter à l'adresse **sales@auth0.com**.

Vous pouvez essayer Auth0 gratuitement; la configuration ne prend que quelques minutes. Vous pouvez également consulter la page de tarification Auth0 ici: **auth0.com/pricing**.

Vous pouvez consulter les études de cas Auth0 ou en savoir plus sur la solution d'entreprise Auth0. Auth0 fournit également une documentation approfondie pour les API, SDK, démarrages rapides et plus encore. Le blog à l'adresse **auth0.com/blog** est une source d'information importante pour obtenir toutes les dernières actualités ainsi que des tutoriels sur les technologies émergentes populaires et les sujets liés à sécurité.



auth0.com