Le Zero Trust : la sécurisation de tous vos accès, d'où qu'ils proviennent

Comment mettre en place un nouveau périmètre de sécurité avec une approche Zero Trust

Okta France
paris@okta.com

Okta et le Zero Trust : la sécurisation de tous vos accès, d'où qu'ils proviennent

Le nouveau périmètre, c'est l'individu

À une époque où la gestion des identités dans le Cloud est devenue commune, tant au sein de l'entreprise qu'en dehors, le périmètre de sécurisation de l'entreprise a été entièrement redéfini pour se centrer autour de l'utilisateur. Jusqu'à présent, la plupart des sociétés avaient adopté une approche conventionnelle de la sécurité, consistant à dépendre totalement de l'infrastructure sur site pour créer la couche de sécurité couvrant l'ensemble des ressources. Progressivement, le nombre et le type de terminaux se sont multipliés, incitant les personnes à travailler de n'importe où. Tout lieu doté d'une connexion Internet devient alors un lieu de travail potentiel. Les départements informatiques sont par conséquent confrontés à de nouveaux défis. Il est en effet devenu plus difficile de contrôler les terminaux et les réseaux depuis lesquels les utilisateurs se connectent. Les solutions de sécurité traditionnelles sont adaptées uniquement lorsque le terminal et le réseau appartiennent au service informatique. L'approche classique basée sur le périmètre est donc naturellement en train de disparaître. Se reposer sur des serveurs, des VPN et des pares-feux pour renforcer la sécurité n'est plus une approche suffisamment sûre et s'avère trop restrictive pour les utilisateurs. Ces derniers ont besoin de pouvoir être productifs à tout moment et en tout lieu, et depuis des terminaux qui ne sont pas nécessairement contrôlés par leur service informatique.

C'est là qu'entre en jeu l'identité, et son importance vitale en tant que point de contrôle centralisé. À mesure que les entreprises évoluent et reconnaissent la valeur apportée par les technologies Cloud et le BYOD (Bring Your Own Device, utilisation des terminaux personnels dans la sphère professionnelle), il devient plus qu'indispensable de redéfinir le périmètre et de se concentrer sur une approche axée autour des utilisateurs connectés. Il n'est désormais plus possible d'établir une confiance uniquement basée sur les terminaux et les réseaux utilisés. Avec la notion d'entreprise étendue, la sécurité doit en plus prendre en considération les partenaires, les contractants et les clients qui ont besoin de pouvoir se connecter tout aussi facilement que s'ils étaient au sein de l'entreprise. Les solutions basiques ne suffisent plus. Lorsque les utilisateurs accèdent à une large gamme d'applications à partir de systèmes d'exploitation et de navigateurs très variés, une solution permettant les interconnexions avec toutes les applications et garantissant une interopérabilité exceptionnelle, une expérience utilisateur optimale et une faible complexité s'avère nécessaire.

La sécurité sans limite

La sécurité d'entreprise repose désormais sur quelques approches communément acceptées, dont deux des plus connues : le modèle Zero Trust, introduit par Forrester, et BeyondCorp de Google.

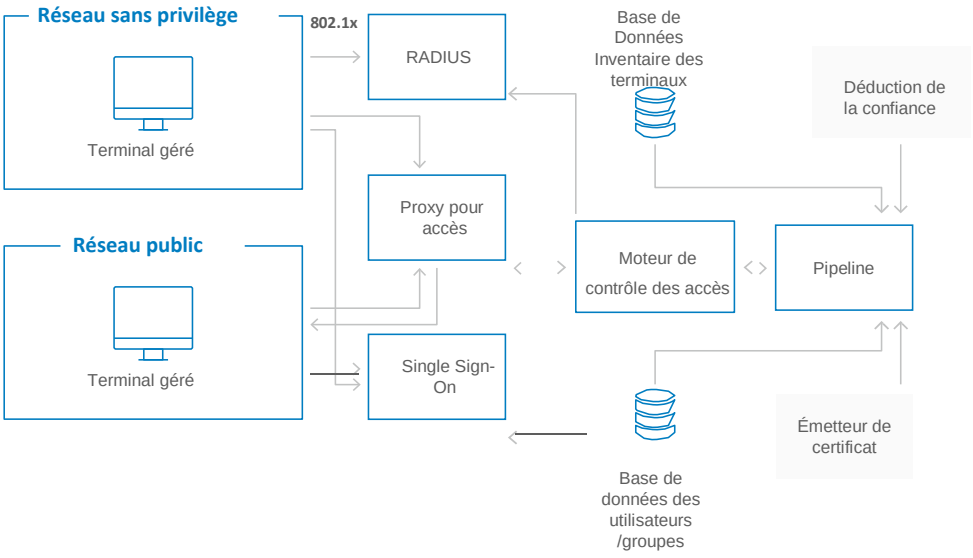
Le modèle Zero Trust de Forrester a été mis au point en 2009, en réponse à des attaques malveillantes ciblées, venues de l'intérieur. Dans ce type de scénario, le modèle basé sur le périmètre est inefficace. A l'image du modèle Zero Trust dont le principe de base consiste à ne faire confiance à personne, l'approche développée par Forrester pour sécuriser l'entreprise consiste à éliminer l'idée même d'un réseau interne plus fiable qu'un réseau externe. En d'autres termes, le réseau interne et le réseau externe doivent être considérés aussi peu sûrs l'un que l'autre[1]. Forrester a d'ailleurs souligné le fait que l'utilisation de plus en plus fréquente de la technologie mobile joue un rôle moteur dans la création d'un nouveau modèle de sécurité informatique. Le modèle Zero Trust repose sur trois concepts principaux[2]:

- Assurer un accès sécurisé à toutes les ressources quel que soit le lieu de connexion ;
- Adopter le principe du moindre privilège et imposer un contrôle strict des accès ;
- Contrôler et consigner l'intégralité du trafic.

En résumé, il est primordial de :

1. partir du principe que tout trafic constitue une menace, à moins d'avoir été vérifié et autorisé ;
2. attribuer aux utilisateurs finaux ainsi qu'aux administrateurs des autorisations minimales d'accès aux ressources de l'entreprise ;
3. investir dans des outils de contrôle du réseau conformes à la méthodologie « vérifier et ne jamais faire confiance ».

Google s'est également rendu compte qu'il fallait renouveler la sécurité d'entreprise et a par conséquent crée BeyondCorp, un modèle de sécurité réaliste et concret qui transfère le périmètre de contrôle des accès du réseau aux terminaux et utilisateurs individuels[3]. L'architecture BeyondCorp est constituée de quatre composants : Data Sources, Access Intelligence, Gateways et Resources. Chacun d'entre eux est associé à divers contrôles qui permettent de déterminer de façon dynamique un niveau d'accès pour un utilisateur et ses terminaux. BeyondCorp met en pratique le concept de niveaux de confiance organisés en différents paliers, et chaque ressource (telle qu'une application ou un service) est dotée d'un palier de confiance minimal requis pour y accéder.



Composants et flux d'accès de BeyondCorp (tel que conçu par Google)

Le modèle Zero Trust et les méthodologies BeyondCorp concernent toutes les organisations. Il convient de noter que ni l'une ni l'autre de ces méthodes n'indique de technologies ou fournisseurs spécifiques. Elles insistent plutôt sur l'importance d'une approche sûre, flexible et évolutive de la sécurité informatique, pour assurer la protection des données et ressources de l'entreprise.

Grâce à son nouvel ensemble de fonctionnalités de gestion des accès contextuels, Okta fait du modèle Zero Trust une réalité pour ses clients. Parallèlement au modèle Zero Trust, Okta suit également les sources de données et les composants de ressources de BeyondCorp pour offrir à votre entreprise une stratégie de sécurité globale axée sur l'identité et les appareils. Nous avons également mis en place un écosystème d'intégrations en pleine expansion, avec les principaux fournisseurs d'analyse de sécurité, dans une optique de visibilité et de réaction. Enfin, nous avons encore amélioré nos politiques de détection contextuelle grâce à l'authentification multi-facteurs contextualisée, ce qui vous permet de consigner toute connexion utilisateur anormale auprès d'Okta. Ces technologies et notre écosystème d'intégrations sécurisées peuvent être associés à l'efficacité et la fiabilité des politiques SSO et MFA adaptative d'Okta mettant ainsi à votre disposition une solution de sécurité exhaustive pour tous vos utilisateurs. Nous nous sommes donnés pour mission de garantir un accès simple et sûr à vos ressources d'entreprise grâce à la gestion des accès selon le contexte, et l'implémentation du modèle Zero Trust aujourd'hui n'en est que la première étape. À mesure que l'ensemble des fonctionnalités de gestion des accès contextualisée se développe, notre solution intègre plus profondément la sécurité des réseaux selon Zero Trust et sleon l'approche de BeyondCorp axée sur les terminaux.

Un compte a été compromis : réagir avec Okta

À l'heure actuelle, la visibilité et la réactivité sont confrontées aux défis suivants :

- la disparition des périmètres, qui entraîne de nouvelles contraintes au niveau de la réaction au risque : quelle est la meilleure manière de gérer le contrôle des accès aux terminaux, aux services et aux individus ?
- la difficulté à établir la cause profonde de l'incident ;
- l'utilisation conjointe de systèmes de sécurité disparates visant à fournir une vraie visibilité de la sécurité, qui restreint de façon significative la réduction des risques.

Le moteur de politiques de sécurité d'Okta impose l'utilisation d'une authentification solide pour accéder à vos applications, ce qui permet de réduire les risques de violation.

Nos technologies partenaires, intégrées à notre plateforme, se connectent à nos API ou utilisent notre journal de systèmes, vous apportant ainsi des informations supplémentaires relatives à la gestion de la sécurité de votre organisation. Grâce à ces technologies, Okta est en mesure d'obtenir des données extrêmement précises sur les utilisateurs, les applications et les appareils. Vous disposez ainsi d'une vue holistique de la sécurité à l'échelle de votre entreprise.

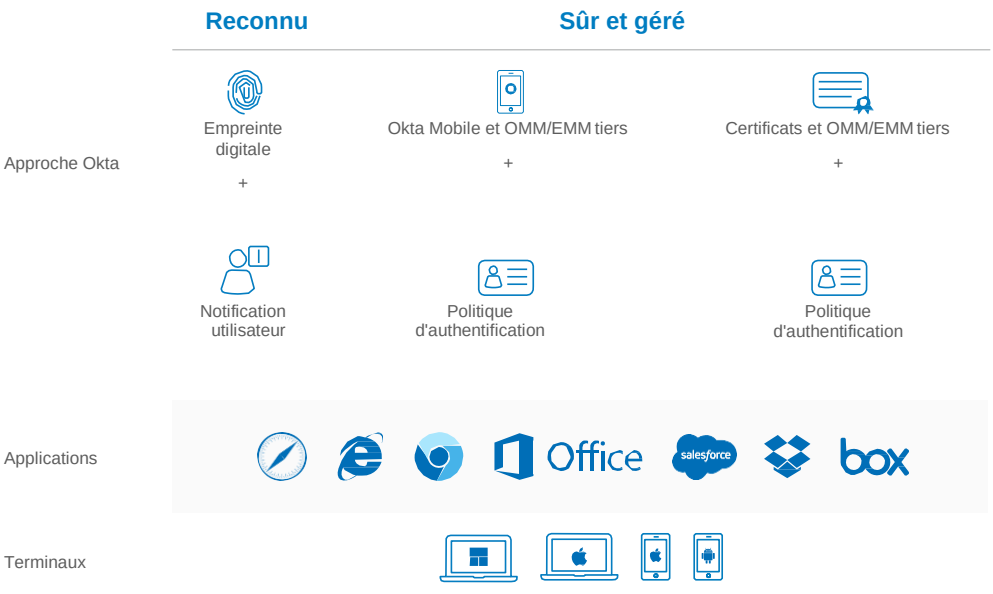
La sécurisation du périmètre moderne

Les informations de contexte les plus fiables sont celles fournies par les terminaux utilisés lors de l'accès à vos ressources d'entreprise. Le modèle Zero Trust prend en compte diverses informations contextuelles relatives à un utilisateur : ses identifiants, son terminaux, son emplacement géographique, son réseau et l'application ou le navigateur utilisé pour accéder à une ressource. Moteur de conditions et d'autorisations, le cadre de politiques de sécurité devient alors la première ligne de défense pour assurer la protection de votre entreprise. Il se base sur les conditions que vous avez définies pour réagir, par exemple en autorisant l'accès ou en le refusant, ou encore en invitant à utiliser l'authentification multi-facteurs (MFA). Ce cadre permet de repérer une activité inhabituelle telle qu'un emplacement nouveau, une adresse IP ou des terminaux inconnus.

Le contrôle intelligent des accès aux ressources d'entreprise constitue l'outil de base de la surveillance des comportements. Il est en général difficile de découvrir la cause profonde d'une intrusion, en particulier lorsque le problème porte sur « qui » et non sur « quoi ». Grâce à notre large gamme d'API, vous êtes en mesure de recueillir les données Okta dans votre SI afin d'évaluer les activités anormales. Le rapport d'Okta sur les comptes malveillants compare par exemple les attributions de droits enregistrés dans Okta avec les comptes utilisateurs existant dans une application spécifiée et liste les différences. Cela vous permet d'identifier les comptes directement créés dans l'application sans passer par Okta, puis de les corriger pour vous assurer que la gestion des accès à l'application est correctement sécurisée. Enfin, Okta s'intègre déjà avec des CASB (Cloud Access Security Broker) tels que Netskope et Skyhigh Networks pour vous procurer une visibilité détaillée et vous alerter en cas d'accès non désiré aux ressources d'entreprise.

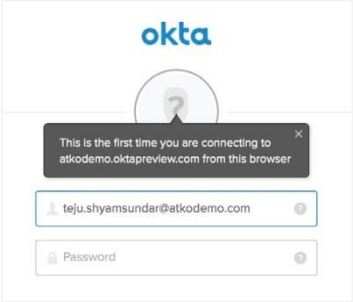
Un accès sécurisé pour tous les terminaux et en tout lieu

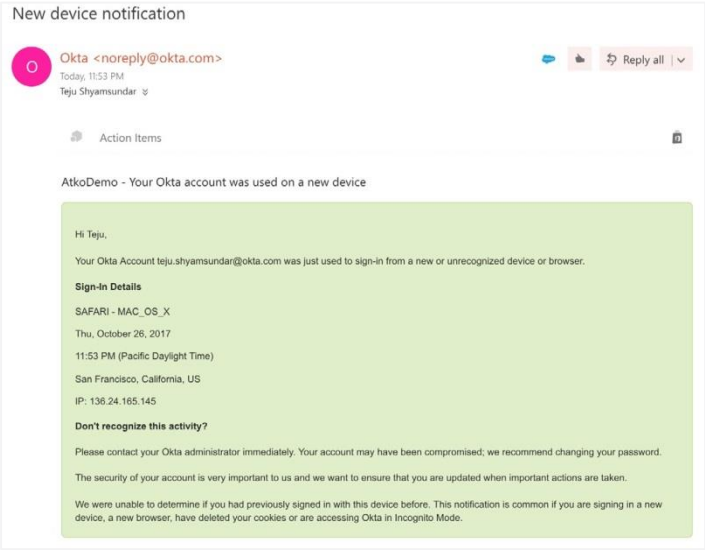
Le Zero Trust joue un rôle essentiel dans votre volonté d'autoriser vos utilisateurs à accéder aux applications et aux ressources uniquement sur des terminaux fiables. Plusieurs étapes sont nécessaires à la confirmation de l'identité d'un utilisateur et du niveau de sécurité de son appareil. En premier lieu, il faut établir que l'accès provient bien du bon utilisateur et que le terminal est reconnu. Ensuite, la plateforme et le client utilisés pour cette tentative d'accès doivent être conformes à la politique de sécurité de votre entreprise. Les paramètres de la politique d'authentification multi-facteurs contextualisée constituent la première étape vers la prise d'une décision d'accès spécifique à un utilisateur. Une fois qu'il est prouvé que l'accès à l'application a bien été effectué par le bon utilisateur, il est temps de procéder aux vérifications spécifiques au terminal. Dans l'approche Zero Trust d'Okta, les entreprises disposent de deux méthodes différentes pour définir ce qu'est, pour elles, un terminal de confiance.



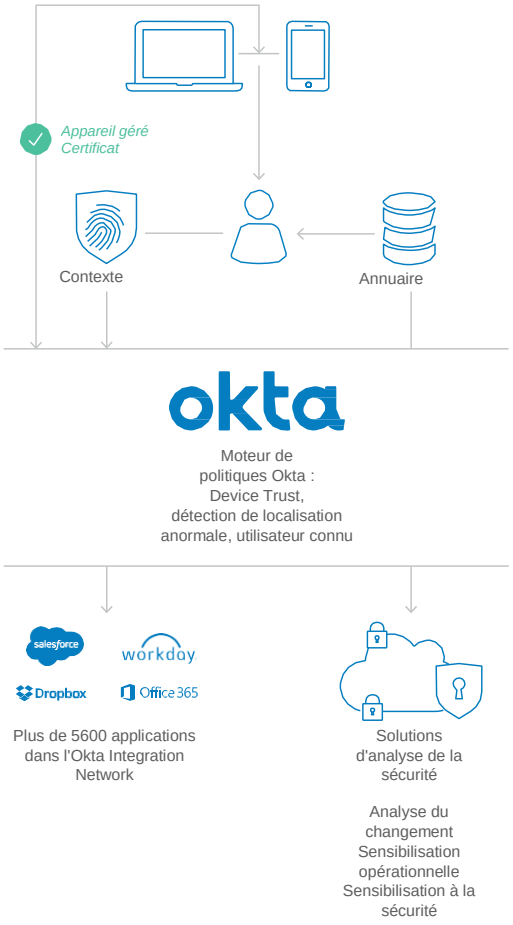
Le Device Trust en détails

Puisque la plupart des entreprises utilisent désormais les certificats pour identifier un terminal connu, Okta a développé une autorité de délivrance de certificats, l'Okta Certification Authority. Dès le déploiement du certificat, la gestion des certificats par l'Okta Certification Authority est réalisée de manière indépendante. Ainsi, les entreprises peuvent faire appel à une solution tierce de gestion des terminaux pour établir et gérer la confiance liée à ces derniers.
Bien que les certificats soient un indicateur de confiance extrêmement fiable, leur utilisation est soumise à certaines limites techniques. Okta a identifié des scénarios dans lesquels l'approche basée sur les certificats doit être modifiée afin d'évaluer avec certitude la confiance à l'échelle de toutes les applications mobiles natives. Afin de relever ce défi technique, Okta a également créé une application permettant de couvrir un périmètre plus grand et d'intégrer les solutions tierces de gestion des appareils mobiles utilisées par les entreprises. Une fois la gestion de l'appareil confirmée par Okta, la dernière étape consiste à décider d'autoriser ou non le client (navigateur Web ou application native) depuis lequel l'utilisateur accède à une ressource. Pour les cas où le terminal n'est pas géré mais où Okta a estimé que l'accès pouvait être accordé après sécurisation du terminal, l'utilisateur est invité à suivre une procédure d'enregistrement qui lui permettra finalement d'accéder à la ressource d'entreprise. Enfin, si un utilisateur accède aux applications protégées par Okta depuis un nouveau terminal, un e-mail lui est envoyé sous quelques secondes, détaillant la localisation de la tentative d'accès.





Le cadre de politiques de sécurité joue un rôle majeur dans ces trois étapes (identification de l'utilisateur, évaluation de la sécurité du terminal et de la plateforme, et évaluation de l'accès client).



La sécurité des accès mobiles revêt une importance capitale pour de nombreuses entreprises, en particulier lors de l'évaluation d'une stratégie globale de gestion des accès selon le contexte. La solution Device Trust d'Okta évolue en permanence pour couvrir toujours plus de scénarios et de plateformes.

À l'heure actuelle, de nombreuses entreprises évoluent encore dans un environnement hybride, jusqu’à ce que leur transition vers le Cloud s'effectue. Okta s'intègre facilement à votre infrastructure existante et fonctionne avec des annuaires tels qu'Active Directory, des outils de gestion des ressources comme LANDESK ou System Center Configuration Manager, ainsi que des outils de gestion des terminaux mobiles comme Airwatch et MobileIron. Vous n'aurez pas besoin d'abandonner vos outils de gestion des ressources existants pour les paramètres tels que le chiffrement de disque, les niveaux de patch ou les versions d'applications, ni de mettre en place un code PIN ou de déployer des applications gérées sur les terminaux mobiles. Il vous suffira d’utiliser Okta pour vérifier que le terminal est géré et fiable.

Le rôle d'Okta dans l'évaluation du niveau de sécurité d'un terminal

Le Device Trust d'Okta est conçu pour s'intégrer aux technologies que vous utilisez déjà.

L'approche que nous avons adoptée pour vérifier si un terminal est fiable est optimisée pour les plateformes les plus courantes, ce qui permet aux utilisateurs d'exploiter leurs outils de gestion des terminaux existants. En termes de postes de travail, vous pouvez continuer à utiliser vos systèmes de gestion des appareils tels que System Center Configuration Manager, IBM BigFix ou LANDESK. Dans le cas des terminaux mobiles, nos clients utilisent des solutions telles qu'Airwatch et MobileIron, en parallèle desquelles Okta Device Trust peut fonctionner.

Il vous suffit simplement d'indiquer dans Okta les applications à associer à votre politique Device Trust. Cette dernière fonctionnera de manière cohérente avec les autres politiques d'Okta afin d'assurer la sécurité des accès sur toutes les plates-formes et tous les appareils clients.

Le Zero Trust et l'avenir

L’approche basée sur les politiques de sécurité et incorporant les données provenant des terminaux, des identifiants, des réseaux, de l'adresse IP et des sessions n’est qu’un début. Nous continuerons à faire évoluer notre moteur de politiques de sécurité de manière à ce qu'il prenne davantage en compte les comportements.

Il est impossible d'anticiper toutes les tentatives d'accès malveillants, tout comme il n'est pas réaliste de chercher à définir une règle correspondant à chaque combinaison d'accès, mais il est essentiel de faire évoluer ses solutions de sécurité pour couvrir le plus de scénarios possibles.

À mesure que nos solutions Zero Trust et BeyondCorp évoluent, des améliorations de sécurité sont apportées à l'intégralité de notre offre. L'application Okta Mobile s’est par exemple adaptée en prenant en charge TouchID sur iOs et l'utilisation des empreintes digitales sur Android lors de leur arrivée sur le marché.

La transition vers un environnement basé sur le Cloud peut s'avérer difficile. Heureusement, le déploiement d'une solution de gestion des accès peut se faire progressivement, et de façon optimisée pour les environnements hybrides. Lorsque vous commencerez à redéfinir votre périmètre et à adopter une approche non plus basée sur le site, nous pourrons vous aider à répondre à des questions courantes :

- Quelles sont les applications les plus importantes pour mon entreprise ?
- Qui sera en premier soumis aux politiques de gestion des accès selon le contexte ?
- Comment un utilisateur final résoudra-t-il la non-conformité d'un terminal ?
- Que comprend une solution idéale ?
    - Authentification multi-facteurs pour vos applications gérées ;
    - MFA pour les ressources sur site ;
    - Device Trust ;
    - Analyses de la sécurité.

Produire une solution de gestion des accès de bout en bout qui prend en compte le contexte et qui intègre des fonctionnalités de surveillance, de réponse aux événements et de gestion des terminaux sur toutes les plateformes et applications : telle est la vision Zero Trust d'Okta. Cette vision est non seulement sécurisée, mais également intégrée : elle fonctionne parallèlement à vos outils de gestion des annuaires, de la sécurité et des terminaux. Vous pouvez ainsi conserver vos fournisseurs existants, puisque nous nous intégrons à des milliers d'applications et en ajoutons chaque jour de nouvelles.

[1] No More Chewy Centers: The Zero Trust Model of Information Security—
ht tps: //w w w.forres ter.com /repor t /No+More+ Chew y + Centers+The+Zero+Trus t+Model+ O f+Information+Securit y/- /E - RES56682
[2] BeyondCorp A New Approach to Security— ht
tps: //cloud.google.com /beyondcorp/
[3] Developing a Framework to Improve Critical Infrastricutre Cybersecurity—
ht tps: //w w w.nis t .gov/sites/default /files/document s/2017/06/05/040813_forres ter_research.pdf
[4] Security Analytics Partner Integration Guide—
ht tps: //w w w.ok ta.com /sites/default_files/Ok ta_Securit y- Analy tic s_Partner- Integration - Guide.pdf

À propos d'Okta

Okta est le leader indépendant des services d'identification et de gestion d'accès pour les entreprises. Okta Identity Cloud permet aux entreprises de sécuriser et gérer leur entreprise étendu (employés, partenaires, fournisseurs, clients) et d'améliorer l'expérience de leurs clients. Avec plus de 5.500 intégrations préexistantes avec des applications et des fournisseurs de services logiciels, les clients d'Okta peuvent intégrer facilement et de manière sécurisée les technologies dont elles ont besoin pour mener à bien leurs activités. Plus de 5.000 organisations à travers le monde font confiance à Okta pour connecter les gens et tout type de technologie, comme par exemple : Engie, 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America ou Twilio.

Pour en savoir plus, rendez-vous sur : www.okta.com/fr


okta