Livre blanc

Okta Secure Identity Commitment

Proposer des produits et services d'identité sécurisés de pointe

Renforcer notre infrastructure d'entreprise

Promouvoir les bonnes pratiques auprès des clients pour optimiser leur protection

Encourager notre secteur à renforcer la protection contre les attaques ciblant l'identité

okta

Sommaire

Résumé

L'identité constitue le principal point d'entrée de sécurité en entreprise, tant pour les applications collaborateurs que clients. En parallèle, le volume et la complexité des attaques contre les entreprises, des plus petites aux plus grandes, continuent d'augmenter. La détection et la protection contre ces attaques sont cruciales.

Leader indépendant du secteur de l'identité, Okta est en première ligne face aux attaques. Voilà pourquoi nous avons lancé l'initiative « Okta Secure Identity Commitment » pour :

- Proposer des produits et services d'identité sécurisés de pointe
- Renforcer notre infrastructure d'entreprise
- Promouvoir les bonnes pratiques auprès des clients pour optimiser leur protection
- Encourager notre secteur à renforcer la protection contre les attaques ciblant l'identité

Dans le cadre de cette initiative, nous avons déjà distribué ou annoncé un certain nombre de fonctionnalités et mises à niveau importantes au sein de notre infrastructure d'entreprise et de notre gamme de produits. Un récapitulatif de ces mises à jour est proposé ci-après.

Nous sommes conscients qu'il s'agit d'un travail de longue haleine. Dès lors, nous sommes déterminés à nous donner les moyens nécessaires pour anticiper de manière proactive ou réagir rapidement à l'évolution du paysage des cybermenaces.

Introduction

Lorsque nous avons fondé Okta en 2009, nous nous sommes concentrés principalement sur la gestion IT, et plus particulièrement sur l'identité en tant qu'outil permettant de connecter les personnes et les technologies.

Depuis lors, deux grandes tendances ont radicalement changé la perspective sur l'identité et, par extension, la demande en solution d'identité :

1. **L'identité constitue désormais le principal point d'entrée de sécurité en entreprise**, tant pour les applications axées collaborateurs que pour celles axées clients.
2. **Le volume et la complexité des cyberattaques ne cessent de s'intensifier**. Un large éventail de cybercriminels, dont les groupes spécialisés en ransomware, les acteurs étatiques et les acteurs malveillants internes, développent chaque jour des tactiques, techniques et procédures (TTP) avancées pour contourner les défenses et échapper à la détection.

Ces tendances ont marqué un tournant majeur pour le secteur, mais ont également contraint notre entreprise à se repositionner : axées au départ sur la connectivité entre personnes et technologies, nos solutions sont devenues un point d'entrée critique pour la protection des données essentielles des entreprises.

Cette responsabilité se reflète dans ***notre vision, qui est de permettre à tous d'utiliser n'importe quelle technologie en toute sécurité.***

Okta Secure Identity Commitment

La gestion des identités a évolué pour devenir une infrastructure de sécurité stratégique.

Leader indépendant du secteur de l'identité, Okta est en première ligne de la lutte contre les attaques ciblant l'identité. Nos équipes produits, ingénierie, sécurité et technologies métier apportent constamment des innovations à notre plateforme pour protéger efficacement nos quelque 18 000 clients. Par exemple :

- Okta ThreatInsight ***détecte et bloque plus de 2 milliards de demandes malveillantes*** en l'espace de 30 jours. (Source : source interne d'Okta, janvier 2024)
- Nous avons ***réduit les tentatives de credential stuffing et le trafic des bots malveillants de plus de 90 %*** pour quelques-uns de nos plus gros clients sur une période de 90 jours. (Source : Okta, The State of Secure Identity Report 2023)
- Nous contribuons aux bonnes pratiques du secteur : 100 % des collaborateurs d'Okta utilisent ***Okta FastPass et Adaptive MFA (AMFA) comme facteurs résistants au phishing.*** (Source : source interne d'Okta, février 2024)

Nous sommes déterminés à jouer un rôle de premier plan dans la lutte contre les attaques prenant l'identité pour cible. Voilà pourquoi nous avons lancé l'initiative « Okta Secure Identity Commitment ».

Cet engagement s'articule autour de 4 piliers :

- Proposer des produits et services d'identité sécurisés de pointe
- Renforcer notre infrastructure d'entreprise
- Promouvoir les bonnes pratiques auprès des clients pour optimiser leur protection
- Encourager notre secteur à renforcer la protection contre les attaques ciblant l'identité

Proposer des produits et services d'identité sécurisés de pointe

Nous sommes conscients que votre posture de sécurité est liée à la nôtre, d'où notre volonté d'optimiser et de prioriser les fonctions de sécurité au sein de nos produits et services d'identité.

De cette manière, nous faisons en sorte que la confiance que nous témoignent les marques les plus réputées soit récompensée par les mesures de protection les plus robustes et innovantes.

Renforcer notre infrastructure d'entreprise

Tous nos collaborateurs, processus et technologies internes doivent respecter les mêmes standards de sécurité que nos produits orientés client, en mettant l'accent sur une approche globale, capitalisant sur nos atouts en matière de sécurité.

Par ailleurs, nous intensifions nos investissements pour renforcer nos systèmes d'entreprise et auxiliaires (attachés à l'environnement de production).

Promouvoir les bonnes pratiques auprès des clients pour optimiser leur protection

Si elle est mal configurée, l'identité devient un point d'entrée supplémentaire pour les acteurs malveillants ou les collaborateurs internes malintentionnés. Forts d'une expérience de 15 ans et d'une large clientèle de plus de 18 000 entreprises, nous possédons une expertise unique et les compétences spécialisées nécessaires pour aider nos clients à optimiser la configuration de leurs identités.

Pour que nos clients profitent de notre longue expérience, nous renforçons encore nos politiques clients.

Par ailleurs, nous mettons tout en œuvre pour que nos produits soient déployés selon les bonnes pratiques de sécurité d'Okta afin de renforcer directement les défenses des clients contre les brèches liées à l'identité.

Encourager notre secteur à renforcer la protection contre les attaques ciblant l'identité

Montrer la voie en matière de sécurité de l'identité est un impératif d'Okta. Nous nous sommes fixé pour mission de participer activement à la détection et à la neutralisation des attaques ciblant l'identité dans le cadre de notre secteur. Pour ce faire, nous accélérons le développement de nos capacités et adoptons de nouvelles technologies, telles que l'intelligence artificielle. Nous jouons également un rôle proactif dans l'élaboration d'une approche sectorielle en matière de sécurité de l'identité. Nous soutenons par exemple l'initiative « Okta for Good » afin de participer au financement de la transformation digitale des organisations à but non lucratif et d'encourager les parcours inclusifs dans le secteur des technologies.

Le reste du présent document explique comment nous prévoyons de tenir nos engagements.

Proposer des produits et services d'identité sécurisés de pointe

Lors de l'événement Oktane 2023, nous avions annoncé une série de fonctionnalités visant à renforcer la sécurité des clients, dont un grand nombre intégrant Okta AI.

Pour l'avenir, nous prévoyons quelques améliorations majeures dans nos produits et services, dont les suivantes :

- Restriction de l'accès administrateur dans une organisation Okta
- Renforcement de la sécurité des sessions
- Promotion des bonnes pratiques auprès de notre clientèle

Disponibles depuis peu	Fonctionnalités prévues en février 2024	Fonctionnalités prévues en juillet 2024
• Okta Privileged Access • Entitlement Management • Passkeys • Highly Regulated Identity • Okta Expert Assist • Acquisition de Spera • Changement de l'accès aux dossiers dans l'Okta Help Center • Authentification des sessions administrateurs • Gestion des API – Session administrateur obligatoire pour les appels d'API Okta • Etc.	• MFA obligatoire pour accéder à la console d'administration Okta • MFA obligatoire pour les actions protégées dans la console d'administration • Possibilité pour les administrateurs de détecter et de bloquer les demandes émanant d'un anonymiseur • Liaison de l'adresse IP avec la console d'administration Okta, et liaison IP/ASN avec la console d'administration • Zone réseau autorisée pour les API • Élimination des privilèges permanents pour les rôles administrateurs Okta • Liaison de tokens pour les intégrations avec les services d'application M2M • Prévention du verrouillage de comptes pour les utilisateurs Okta • Liaison de l'adresse IP à la solution PAM (Privileged Access Management) • Etc.	• Cookies de session liés aux terminaux pour les applications Okta • Amélioration de la fonction Bot Detection • Code CAPTCHA par défaut renforcé • Extension du contrôle de gestion des sessions et renforcement de la sécurité des tokens • Accélération des comptes de service des solutions SaaS et des hyperscalers en tant que ressources protégées dans Okta Privileged Access • Inscription de FastPass limitée aux terminaux gérés • Ajout de nouveaux guides de bonnes pratiques intégrés aux produits • Etc.

Annonces et distributions récentes

Nous avons récemment lancé plusieurs produits et fonctionnalités destinés à renforcer la sécurité client :

- **Okta Privileged Access** pour aider les clients à éliminer les privilèges permanents et à réduire les risques
- **Entitlement Management** pour limiter les menaces potentielles résultant d'erreurs de configuration grâce à la détection et à l'ajustement automatiques des attributions de droits
- **Passkeys** pour offrir un accès sécurisé sans mot de passe aux applications grand public
- **Highly Regulated Identity** pour fournir une sécurité adaptée aux services financiers dans les workflows d'identité
- **Okta Expert Assist** pour aider les clients à renforcer leur sécurité et à optimiser leur configuration grâce à l'assistance d'un expert en sécurité d'Okta
- **Acquisition de Spera Security** pour faire progresser la sécurité basée sur l'identité et aider les entreprises à atténuer les risques, à réduire les coûts et à limiter la fragmentation de l'IT
- **Identity Threat Protection avec Okta AI** *bientôt disponible en Early Access* : la solution inclut des fonctionnalités puissantes telles que Universal Logout (p. ex. en réponse aux menaces dans l'écosystème des clients)

Okta Expert Assist

Les clients peuvent collaborer avec Okta afin de prendre des mesures supplémentaires pour renforcer leur sécurité et optimiser leurs configurations globales.

Voici comment fonctionne le service Okta Expert Assist :

1. **Découverte : bénéficiez de l'assistance d'un expert en sécurité de l'identité**. Votre architecte Okta procède à une évaluation complète de la sécurité de vos tenants Okta (via des ateliers) pendant une période de 2 semaines.
2. **Analyse : votre expert en sécurité identifie les mesures applicables**. Votre architecte Okta réalise une évaluation globale de vos paramètres par rapport aux bonnes pratiques qui tiennent compte des fonctionnalités produits les plus récentes d'Okta, ainsi que de l'évolution permanente du paysage des menaces.
3. **Planification : renforcez votre posture de sécurité actuelle et future**. Votre architecte Okta vous propose des recommandations prescriptives, pratiques et priorisées pour améliorer votre posture de sécurité et garder une longueur d'avance sur des menaces de sécurité toujours plus nombreuses.

→ Pour en savoir plus, consultez la page : www.okta.com/expert-assist/

Parmi les autres nouveautés disponibles, citons :

- **Changement de l'accès aux dossiers dans l'Okta Help Center —** Les dossiers de support dans l'Okta Help Center sont uniquement accessibles à l'administrateur qui a ouvert le dossier.
- **Authentification des sessions administrateurs —** Les délais d'expiration de la console d'administration seront limités par défaut à une durée de vie de session de 12 heures et à une durée d'inactivité avant fermeture de 15 minutes. Les clients ont la possibilité de modifier ces paramètres.
- **Gestion des API – Session administrateur obligatoire pour les appels d'API Okta —** Les bonnes pratiques d'Okta prévoient l'utilisation des tokens d'API lorsque les clients exécutent des appels d'API avec l'automatisation ou Terraform. Cette exigence sera implémentée dans le produit pour améliorer la sécurité de l'administrateur du client.

Fonctionnalités prévues en Early Access en février 2024 :

- **MFA obligatoire pour accéder à la console d'administration d'Okta —** Okta renforce l'accès sécurisé à la console d'administration Okta en exigeant le MFA pour tous les rôles administrateurs. L'application du MFA pour l'accès à la console d'administration offre un niveau de sécurité supplémentaire qui diminue la probabilité de brèche. Nous adoptons une approche progressive, la phase initiale consistant à interdire la création de nouvelles politiques d'authentification des applications d'administration sans MFA.
- **MFA obligatoire pour les actions protégées dans la console d'administration —** Permet de renforcer le niveau de protection pour les actions critiques dans Okta en exigeant une authentification renforcée des administrateurs qui souhaitent effectuer des actions à fort impact.
- **Possibilité pour les administrateurs de détecter et de bloquer les demandes émanant d'un anonymiseur —** Okta offrira aux administrateurs la possibilité d'autoriser ou de refuser l'accès après évaluation de l'association potentielle d'une adresse IP à un anonymiseur, ce qui renforce le contrôle d'une organisation contre l'accès non autorisé via ce type de sources.
- **Liaison de l'adresse IP avec la console d'administration Okta, et liaison IP/ASN avec la console d'administration —** Pour éviter la prise de contrôle des sessions, Okta révoquera automatiquement une session de console d'administration si le numéro ASN (Autonomous System Number) observé pendant une demande web ou d'API diffère du numéro enregistré lors de l'ouverture de la session. Les administrateurs seront en mesure de révoquer automatiquement une session d'administration si l'adresse IP détectée change pendant une session active dans les produits Okta suivants : Workflows Admin, Okta Access Requests (Inbox), Okta Privileged Access (OPA), console d'administration Okta.

- **Zone réseau autorisée pour les API —** Empêche les cybercriminels et les malwares de voler des tokens SSWS et de les relire en dehors de la plage d'adresses IP spécifiée pour obtenir un accès non autorisé.
- *** Élimination des privilèges permanents pour les rôles administrateurs Okta —** Les rôles administrateurs Okta seront gérés avec Okta Identity Gouvernance (OIG). En exigeant des demandes et des certifications d'accès pour les autorisations administrateur, Okta peut aider les clients à limiter les menaces internes et les accès non autorisés, et à appliquer le principe du moindre privilège.

* Disponible en Early Access (EA) pour les clients OIG en février 2024 et pour d'autres clients à partir du mois de mars

Fonctionnalités prévues en disponibilité globale (GA) en février 2024 :

- **Liaison de tokens pour les intégrations avec les services d'application M2M —** Okta améliorera la sécurité des transactions automatisées en appliquant par défaut la liaison des tokens dans les intégrations M2M à l'aide d'une preuve de possession. De cette façon, seules les applications authentifiées pourront utiliser des tokens pour accéder aux API Okta.
- **Prévention du verrouillage de comptes pour les utilisateurs Okta —** Okta propose une fonctionnalité pour bloquer les tentatives de connexion suspectes à partir de terminaux inconnus. Lorsque la fonctionnalité est activée, elle empêche le verrouillage des comptes des utilisateurs légitimes (y compris des administrateurs) si un autre terminal non connu d'Okta déclenche un verrouillage.
- **Liaison de l'adresse IP à la solution PAM (Privileged Access Management) —** Les administrateurs des clients seront en mesure de révoquer automatiquement une session d'administration PAM si l'adresse IP détectée au cours d'une demande web ou d'API diffère de celle enregistrée lors de l'ouverture de la session. Un ticket de support est nécessaire pour désactiver cette fonctionnalité.

Fonctionnalités prévues en juillet 2024 :

- **Cookies de session liés aux terminaux pour les applications Okta —** Des cookies de session liés aux terminaux empêcheront la relecture des sessions Okta en exigeant une preuve de possession d'une clé privée stockée sur le terminal d'un utilisateur. Cette mesure permet de renforcer la liaison entre la session et le terminal afin de réduire le risque de vol de tokens ou d'attaques par relecture.
- **Amélioration de la fonction Bot Detection —** Permet de renforcer les fonctions de détection et de protection contre les bots à l'aide de scores d'outils tiers et de signaux de composants déployés en périphérie.
- **Code CAPTCHA par défaut renforcé —** Par défaut, les événements qui déclenchent l'affichage d'un CAPTCHA dans Okta Customer Identity Cloud exigeront une demande d'authentification dont la complexité sera proportionnelle au risque observé.
- **Extension du contrôle de gestion des sessions et renforcement de la sécurité des tokens —** Offre un contrôle programmable complet des sessions pour permettre aux clients de développer leurs propres tableaux de bord de sessions et de personnaliser l'expérience utilisateur.
- **Accélération des comptes de service des solutions SaaS et des hyperscalers** en tant que ressources protégées dans Okta Privileged Access.
- **Inscription de FastPass limitée aux terminaux gérés —** Okta offrira aux administrateurs un contrôle accru en autorisant la préinscription des utilisateurs dans Okta Verify et FastPass à l'aide d'une solution de gestion des terminaux mobiles (MDM). Les clients pourront ainsi limiter les inscriptions dans l'authentificateur aux terminaux gérés.
- **Ajout de nouveaux guides de bonnes pratiques intégrés aux produits —** Okta fournira des guides supplémentaires intégrés aux produits pour aider les clients à adhérer aux bonnes pratiques afin de protéger leurs tenants Okta.

Renforcement de l'infrastructure d'entreprise d'Okta

Nous intensifions nos investissements pour renforcer nos systèmes d'entreprise et auxiliaires (attachés à l'environnement de production).

Disponibles depuis peu	Mises à jour prévues en avril 2024	Mises à jour prévues en juillet 2024
• Suppression de tous les accès personnels aux comptes Google Chrome • Surveillance et détection renforcées pour tous les comptes de service • Assainissement des archives HTTP (fichiers HAR) dans l'Okta Help Center pour détecter les données sensibles • Gestion du code source et surveillance des bases de données améliorées	• Extension de la résistance au phishing à tout le cycle de vie des collaborateurs • Automatisation de la découverte et du reporting des comptes de service M2M dans les applications SaaS • Évaluation de la sécurité interne • Évaluation de la sécurité des applications SaaS	• Fonctionnalités de détection et réponse améliorées • Fonctionnalités centralisées et uniformisées pour la gestion des vulnérabilités, des ressources et de la posture de sécurité cloud (CSPM) • Reporting centralisé et normalisé pour la gestion des risques de sécurité • Protection renforcée des ordinateurs portables • Protection renforcée des terminaux mobiles

Disponibles depuis peu :

L'infrastructure d'entreprise d'Okta a fait l'objet d'une série de modifications, mises à niveau et améliorations, dont les suivantes :

- Suppression de tous les accès personnels aux comptes Google Chrome
- Surveillance et détection renforcées pour tous les comptes de service
- Assainissement des archives HTTP (fichiers HAR) dans l'Okta Help Center pour détecter les données sensibles, par exemple les tokens de session
- Gestion du code source et surveillance des bases de données améliorées

Mises à jour prévues en avril 2024 :

- **Extension de la résistance au phishing à tout le cycle de vie des collaborateurs —** Cela fait longtemps que nous avons déployé Okta FastPass pour offrir un MFA avec résistance au phishing. Cette résistance au phishing va être désormais étendue à tout le cycle de vie des collaborateurs, de l'inscription/onboarding à la récupération de comptes.
- **Automatisation de la découverte et du reporting des comptes de service M2M dans les applications SaaS —** Nous allons implémenter un outil destiné à offrir une visibilité complète sur les comptes de service locaux créés dans les applications SaaS, afin d'améliorer la gestion et le renouvellement des secrets utilisés dans le cadre de l'authentification.
- **Évaluation de la sécurité interne —** Okta a conclu un partenariat avec un grand cabinet de conseil international pour réaliser une évaluation complète de ses produits, de son infrastructure et de ses systèmes d'entreprise.
- **Évaluation de la sécurité des applications SaaS** — Okta collabore avec des experts en sécurité tiers pour réaliser des évaluations de sécurité de ses applications SaaS critiques, dont l'Okta Help Center.

Mises à jour prévues en juillet 2024 :

- **Fonctionnalités de détection et réponse améliorées —** Nous prévoyons de déployer des solutions pour améliorer nos fonctionnalités de détection et réponse, y compris un nouvel outil de gestion des dossiers d'incidents de sécurité, une nouvelle plateforme de threat intelligence et des fonctionnalités de surveillance du Dark Web supplémentaires.
- **Reporting centralisé et normalisé pour la gestion des vulnérabilités, des ressources et de la posture de sécurité cloud (CSPM) —** Nous prévoyons de déployer la solution d'un fournisseur unique pour centraliser toutes les informations liées aux vulnérabilités dans nos environnements de production et d'entreprise.
- **Reporting centralisé et normalisé pour la gestion des risques de sécurité —** Nous déploierons la solution d'un seul fournisseur pour centraliser la gestion des risques et des problèmes liés à notre programme de gouvernance, de gestion des risques et de la conformité, y compris la gestion des risques liés aux tiers.
- **Protection renforcée des ordinateurs portables —** Nous limiterons davantage les modalités d'utilisation des ordinateurs portables d'Okta par les collaborateurs. Alors que nous avons déjà supprimé l'accès administrateur local pour tous les collaborateurs de l'entreprise, nous prévoyons de le supprimer également pour les développeurs et ingénieurs exemptés.
- **Protection renforcée des terminaux mobiles —** Nous serons inflexibles quant à la sécurité des terminaux mobiles. Même si le produit Okta Verify renforce la posture de sécurité des terminaux, notamment grâce aux codes PIN, au chiffrement et au contrôle des versions du système d'exploitation, nous exigerons aussi un logiciel MDM pour accéder à nos applications d'entreprise.

Promouvoir les bonnes pratiques auprès des clients pour optimiser leur protection

Notre objectif est d'optimiser les bonnes pratiques sectorielles pour rester en phase avec le paysage des menaces.

- **Facteurs résistants au phishing** — 100 % des collaborateurs d'Okta utilisent Okta FastPass et AMFA comme facteurs résistants au phishing. Nous encourageons les clients à réfléchir à la façon dont ils peuvent, eux aussi, incorporer des facteurs résistants au phishing dans leur propre infrastructure d'identité.
- **Inscriptions MFA et libre-service —** Nous tenons à souligner toute l'importance du MFA et à offrir une visibilité accrue aux clients sur toutes les inscriptions MFA (administrateurs et utilisateurs), ainsi que la possibilité de s'inscrire en libre-service.
- **Assistance experte personnalisée —** Notre nouveau service Okta Expert Assist a pour but d'aider les clients à renforcer leur sécurité et à optimiser leur configuration grâce à l'assistance d'un expert en sécurité d'Okta. Nous encourageons les clients à utiliser le service pour bénéficier de recommandations personnalisées.
- **Sensibilisation et formation —** Nous intensifions les formations de sensibilisation au phishing et déployons des méthodes d'authentification avec résistance au phishing.
- **Ajout de nouveaux guides de bonnes pratiques intégrés aux produits —** Okta fournira des guides supplémentaires intégrés aux produits pour aider les clients à adhérer aux bonnes pratiques afin de protéger leurs tenants Okta.

Encourager notre secteur à renforcer la protection contre les attaques ciblant l'identité

Initiatives Okta for Good récentes pour faire progresser le secteur :

- **NetHope's Global Humanitarian Information Sharing & Analysis Center (ISAC) —** Partenariat public-privé conclu entre NetHope, USAID et Okta pour aider les ONG humanitaires mondiales à répondre aux cybermenaces en pleine croissance.
- **Cybersecurity Futures 2030** — Okta a financé cette étude mondiale en partenariat avec l'UC Berkeley Center for Long-term Cybersecurity et le Centre for Cybersecurity du Forum économique mondial. Le but est d'identifier les tendances et les risques de cybersécurité émergents pour le secteur public, le secteur privé et la société civile, et d'améliorer la collaboration pour relever ces futurs défis.
- **Initiative Cybersecurity Workforce Development** – Propose de nouvelles bourses philanthropiques et d'études pour encourager les parcours inclusifs dans les secteurs cyber et technologiques, et résoudre la pénurie de compétences dans le secteur.
- **Portefeuille de subventions de cybersécurité pour les organisations à but non lucratif —** Plus d'un million de dollars a été alloué en deux ans pour encourager l'application des bonnes pratiques de cybersécurité au sein des organisations à but non lucratif.

Conclusion

Okta est déterminé à jouer un rôle de premier plan dans la lutte contre les attaques prenant l'identité pour cible. C'est la raison pour laquelle nous avons lancé l'initiative « Okta Secure Identity Commitment », articulée au autour de 4 piliers :

- Proposer des produits et services d'identité sécurisés de pointe
- Renforcer notre infrastructure d'entreprise
- Promouvoir les bonnes pratiques auprès des clients pour optimiser leur protection
- Encourager notre secteur à renforcer la protection contre les attaques ciblant l'identité

Il s'agit d'un engagement à long terme et nous continuerons d'évoluer en parallèle avec le paysage technologique et des menaces.

À propos d'Okta
Partenaire leader indépendant en matière d'identité, Okta permet à chacun d'utiliser en toute sécurité n'importe quelle technologie, partout, sur n'importe quel terminal ou application. Les plus grandes marques font confiance à Okta en matière d'accès sécurisé, d'authentification et d'automatisation. De par leur flexibilité et neutralité, les solutions Okta Workforce Identity Cloud et Customer Identity Cloud offrent aux dirigeants d'entreprises et aux développeurs la possibilité de se concentrer sur l'innovation et d'accélérer leur transformation digitale, grâce à des solutions personnalisables et plus de 7 000 préintégrations. Nous construisons un monde où l'identité vous appartient. Pour en savoir plus, consultez notre site à l'adresse okta.com/fr.