eBook

Exploiter la puissance et le potentiel de l'identité unifiée

Cinq effets positifs
pour votre entreprise

okta

Le rôle critique de l'identité

L'identité joue un rôle clé dans la sécurité d'aujourd'hui. Dans un monde dominé par le cloud et où systèmes et applications sont étroitement connectés, l'identité détermine si les données sensibles d'une entreprise sont protégées ou vulnérables.

Les acteurs malveillants n'ont pas mis longtemps à considérer l'identité comme une cible majeure. Pourtant, la plupart des entreprises, tous secteurs confondus, sont encore souvent mal préparées à leurs assauts. Alors que les attaques liées à l'identité progressent au rythme de 180 % par an, il faut en moyenne 290 jours à une entreprise pour circonscrire une brèche (2024 Data Breach Investigations Report, Verizon).

Le principal problème est la fragmentation des identités sur l'ensemble des systèmes technologiques et de sécurité. Sans une approche unifiée de la sécurité des identités, les mesures d'atténuation des risques mises en place perdent de leur efficacité, et les équipes IT et sécurité doivent composer avec des outils inefficaces, incapables de lutter contre les menaces complexes actuelles.

Pour redresser la barre, les entreprises doivent déployer une stratégie de sécurité intégrée et axée sur l'identité. Cette stratégie doit permettre de détecter les risques au sein des systèmes IT et de sécurité, de répondre à l'aide de mesures d'atténuation en temps réel et de prévenir les attaques futures au moyen d'une orchestration de la sécurité et de la gouvernance des identités centralisées.

Guide pour une identité évolutive

Cet eBook explique comment les entreprises peuvent concevoir une stratégie de sécurité unifiée et basée sur l'identité, mais aussi :

- Comment une identité fragmentée peut compliquer l'atténuation des risques
- Pourquoi une entreprise moderne a besoin d'une approche de la sécurité axée sur l'identité
- Les cinq principaux effets d'une stratégie de sécurité unifiée

Pour une sécurité efficace, l'identité est la clé

Le monde des entreprises est totalement différent de ce qu'il était il y a cinq ans à peine. Avec la généralisation du travail hybride, la productivité est désormais tributaire de la mise en place d'un réseau décentralisé et étroitement connecté de collaborateurs à temps plein, de sous-traitants, de clients et de partenaires pouvant accéder aux ressources et aux réseaux de n'importe où dans le monde. L'adoption accélérée des services cloud et des applications SaaS simplifie cette connectivité en facilitant la connexion, la collaboration et la création d'expériences clients sécurisées au travers de modalités de plus en plus flexibles.

Mais cette évolution radicale du travail modifie fondamentalement la manière dont nous sécurisons nos activités et nos clients. Les anciens paradigmes de sécurité — pendant longtemps axés sur les périmètres réseau et les déploiements on-premise — ne sont tout simplement pas adaptés à l'ère des applications cloud natives et de la collaboration à distance. Comme les spécialistes de la sécurité le proclament depuis des années, le concept traditionnel d'un périmètre de sécurité n'a plus de raison d'être.

Gérer correctement les identités — avec une visibilité sur qui a accès à quoi, dans quelles conditions et depuis quel emplacement — est essentiel pour garantir la sécurité et des expériences fluides. Dans la conception moderne du Zero Trust, les notions de terminaux et réseaux « de confiance » ne sont plus applicables. Les entreprises doivent permettre à leurs collaborateurs décentralisés et en mode hybride de se connecter de n'importe quel terminal, réseau et emplacement, tout en veillant à ce que les clients puissent accéder aux services en toute sécurité, avec des interactions simples et fluides.

Les acteurs malveillants sont parfaitement conscients que l'identité est devenue le nouveau champ de bataille de la cybersécurité. Les attaques liées à l'identité sont désormais la principale méthode d'accès non autorisé aux informations sensibles. En 2024, 80 % des brèches de données avaient pour origine des identifiants volés et/ou des attaques de phishing (2024 Data Breach Investigations Report, Verizon).

L'identité est donc bel et bien la pierre angulaire d'une sécurité de pointe. Pour atteindre des niveaux Zero Trust de protection contre les menaces, favoriser une collaboration fluide et des expériences client sécurisées, ou encore améliorer la productivité, les entreprises se doivent d'adopter une approche globale et intégrée de la sécurité des identités.

Transformez l'identité en avantage stratégique

Si l'identité représente le plus grand risque de sécurité pour votre entreprise, elle constitue aussi votre plus belle opportunité. En reconnaissant son rôle clé et en modernisant les fonctions de gestion des identités, dont l'identité client, vous pouvez atténuer les risques, damer le pion aux cybercriminels et profiter d'avantages majeurs. Une stratégie de sécurité bien conçue contribue à une connectivité plus rapide, à une collaboration plus agile, à une conformité simplifiée et à une sécurité renforcée.

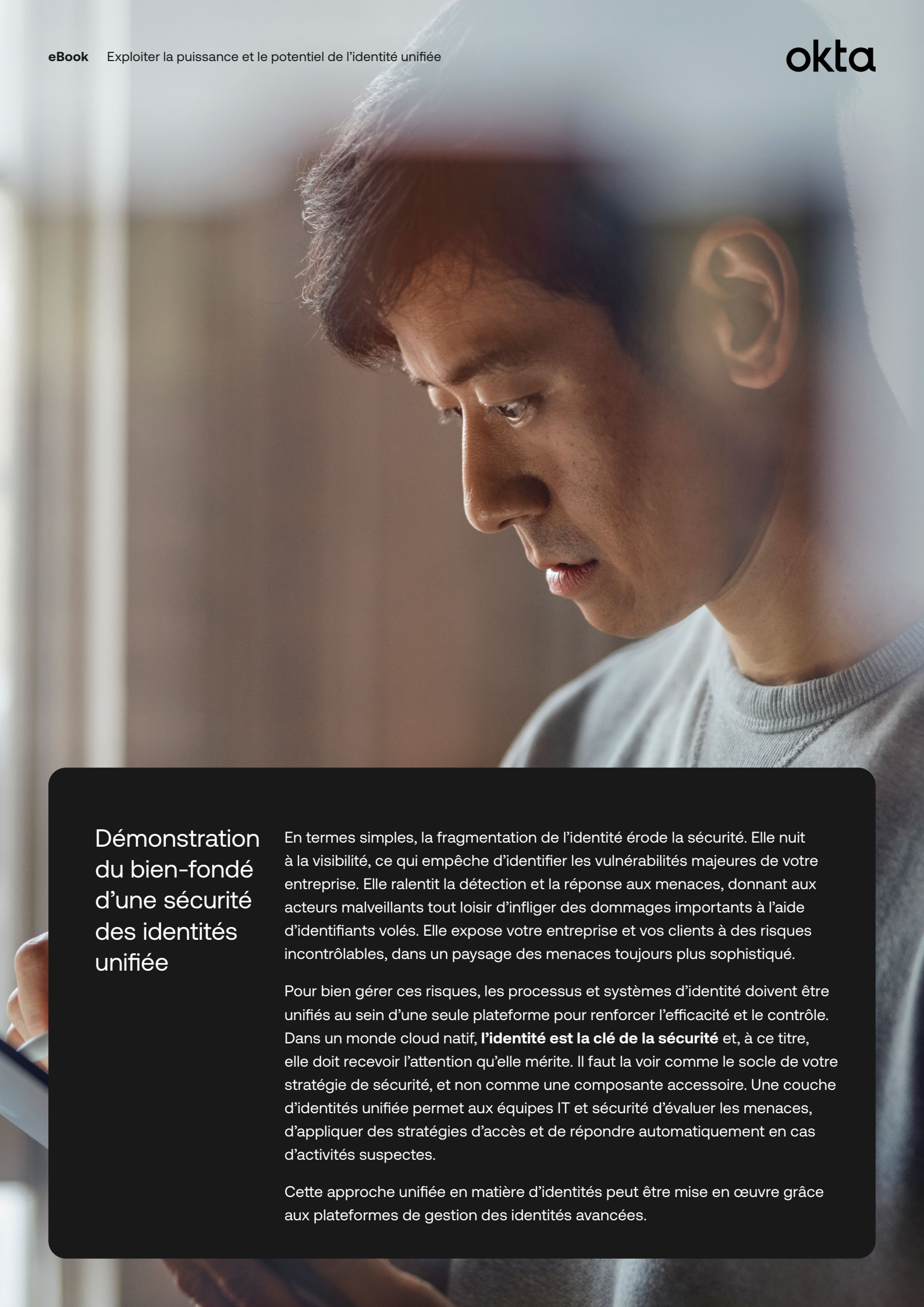
Des identités fragmentées créent des zones d'ombre dangereuses

Ce changement radical dans nos habitudes de travail, à savoir la transition vers une productivité et une collaboration plus distribuées qui priorisent la vitesse et l'agilité, a également altéré la composition et la structure des piles technologiques et de sécurité dans pratiquement tous les secteurs. Le temps où les entreprises faisaient appel à un seul fournisseur pour toutes leurs solutions, sous un même accord de licence d'entreprise, est révolu. Les organisations les plus performantes dépendent désormais d'un écosystème de solutions de pointe qui prennent en charge leurs besoins spécifiques — qu'il s'agisse de l'activité métier, de la sécurité ou des expériences clients. Leur capacité à développer leur activité, à protéger leur entreprise et à offrir des interactions fluides et sécurisées aux clients dépend dès lors de leur faculté à *connecter* ces solutions et à *maximiser leur valeur.*

Néanmoins, il faut admettre que cette approche crée des piles technologiques toujours plus étendues, que les équipes IT et sécurité éprouvent bien des difficultés à configurer et à gérer. Trop souvent, cela donne lieu à des environnements IT fragmentés dont les ressources et les identités sont dispersées entre différents systèmes et infrastructures.

Conséquences d'une identité fragmentée

- Manque de visibilité sur la posture de sécurité en temps réel et les autorisations individuelles dans l'ensemble des systèmes et applications de l'entreprise
- Réponses tardives qui permettent aux acteurs malveillants d'exploiter les vulnérabilités liées à l'identité, avec à la clé des brèches coûteuses et préjudiciables
- Pratiques chronophages et fastidieuses en matière d'octroi des autorisations utilisateurs, qui exposent les contrôles d'accès au risque d'erreurs humaines



Démonstration du bien-fondé d'une sécurité des identités unifiée

En termes simples, la fragmentation de l'identité érode la sécurité. Elle nuit à la visibilité, ce qui empêche d'identifier les vulnérabilités majeures de votre entreprise. Elle ralentit la détection et la réponse aux menaces, donnant aux acteurs malveillants tout loisir d'infliger des dommages importants à l'aide d'identifiants volés. Elle expose votre entreprise et vos clients à des risques incontrôlables, dans un paysage des menaces toujours plus sophistiqué.

Pour bien gérer ces risques, les processus et systèmes d'identité doivent être unifiés au sein d'une seule plateforme pour renforcer l'efficacité et le contrôle. Dans un monde cloud natif, **l'identité est la clé de la sécurité** et, à ce titre, elle doit recevoir l'attention qu'elle mérite. Il faut la voir comme le socle de votre stratégie de sécurité, et non comme une composante accessoire. Une couche d'identités unifiée permet aux équipes IT et sécurité d'évaluer les menaces, d'appliquer des stratégies d'accès et de répondre automatiquement en cas d'activités suspectes.

Cette approche unifiée en matière d'identités peut être mise en œuvre grâce aux plateformes de gestion des identités avancées.

Effets positifs d'une stratégie de sécurité unifiée, axée sur l'identité

Personne ne conteste la nécessité d'unifier et de consolider les processus et systèmes d'identité. Tout le problème, pour la plupart des entreprises, est de transformer cette philosophie en stratégie concrète.

Une stratégie de sécurité unifiée et axée sur l'identité englobe une série de résultats concrets qui, ensemble, possèdent une incidence mesurable sur la façon dont votre entreprise protège les ressources critiques, sécurise les interactions clients, simplifie les workflows quotidiens et améliore les performances de toutes les opérations métier.

Effet 1 : visibilité sur les menaces visant l'identité et remédiation en temps réel

Effet 2 : élimination totale des privilèges permanents et application systématique du principe du moindre privilège

Effet 3 : mise en œuvre éprouvée des principes Zero Trust

Effet 4 : contrôle renforcé des identités non humaines et machines

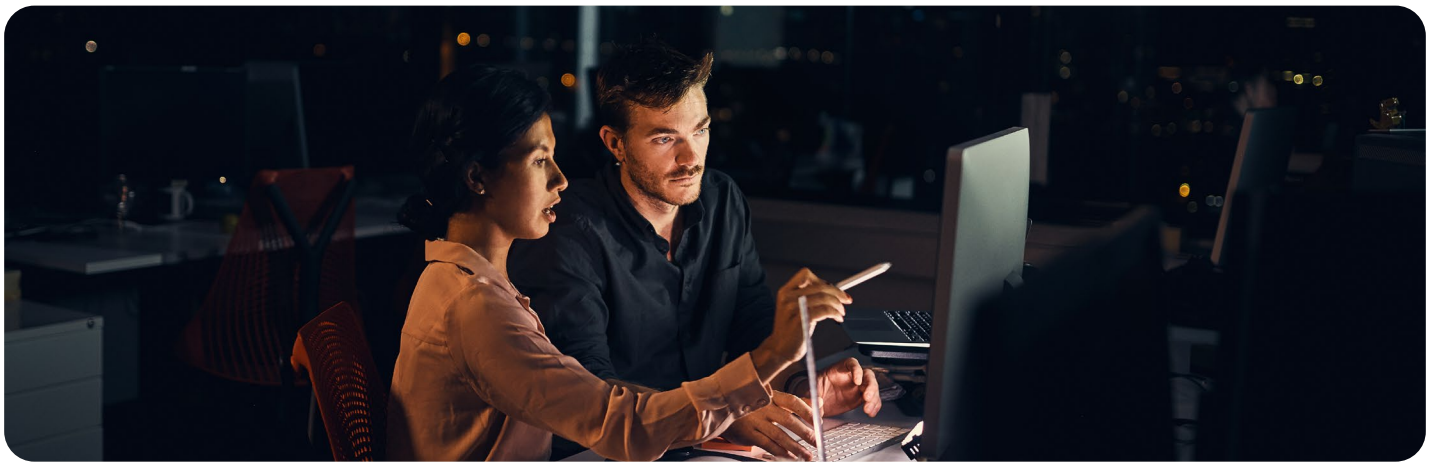
Effet 5 : rentabilisation maximale des investissements en technologies et sécurité

Des résultats concrets avec Okta

Okta Platform vous offre la possibilité d'adopter une approche robuste et extrêmement simplifiée de la sécurité axée sur l'identité. Grâce à un large éventail de produits et fonctionnalités, Okta propose une protection de bout en bout contre les menaces sophistiquées sans alourdir vos workflows ou expériences utilisateurs. De plus, en unifiant l'orchestration de l'identité, Okta offre une visibilité incomparable sur les signaux et politiques dans vos environnements IT, sécurité et clients, et vos équipes sont armées pour neutraliser les risques en temps réel.

Effet 1

Visibilité sur les menaces visant l'identité et remédiation en temps réel



Les piles technologiques et de sécurité fragmentées génèrent un volume considérable de données sur les risques et menaces potentielles. Vos équipes se retrouvent contraintes de passer en revue les logs et d'identifier elles-mêmes les risques à traiter en priorité, ce qui rend la remédiation en temps réel quasi impossible.

Pour accélérer cette atténuation des risques, vous avez impérativement besoin d'une vue complète et centralisée de votre profil de risques liés à l'identité. Cette visibilité doit par ailleurs vous permettre de synthétiser et de prioriser tous les signaux générés par vos outils de sécurité pour les transformer en informations exploitables en temps réel. Pour les entreprises gérant des identités clients, cela revient à détecter et à résoudre les usurpations de comptes et les identifiants compromis en temps réel pour conserver la confiance des clients et protéger les données sensibles.

De plus, la remédiation ne peut pas se reposer sur des actions manuelles et lentes. Votre solution d'identité doit associer des informations en temps réel à des workflows de remédiation automatisés qui peuvent être adaptés aux besoins spécifiques de votre entreprise.

Tout cela est possible grâce à une identité unifiée. En unifiant votre pile de sécurité avec une solution d'identité moderne, vous pouvez intégrer vos mesures de résistance au phishing à un Risk Engine axé sur l'identité pour bénéficier d'une visibilité complète sur les menaces visant l'identité au fur et à mesure qu'elles apparaissent et évoluent. Que ce soit pour protéger les collaborateurs ou les clients, un tel niveau de visibilité est indispensable dans le paysage actuel et c'est ce que vous procure une identité unifiée.

Avec Okta

Identity Threat Protection avec Okta AI

- Bénéficiez d'une visibilité en temps réel sur les menaces dans l'ensemble de vos systèmes, terminaux et types d'utilisateurs afin de profiter d'une posture de sécurité proactive.
- Tirez parti des signaux tiers et des données first-party d'Okta pour avoir accès à des informations plus pertinentes et accélérer la détection des menaces.
- Répondez rapidement aux menaces avec des actions automatisées personnalisables, par exemple le déclenchement d'un MFA ou la déconnexion des utilisateurs compromis.

Okta FastPass

- Déployez une authentification passwordless résistante au phishing pour offrir une expérience utilisateur fluide et sûre.
- Vérifiez la posture de sécurité des terminaux au cours de l'authentification pour éviter tout accès non autorisé.
- Renforcez la sécurité à la connexion afin d'identifier rapidement les activités inhabituelles et y répondre.
- Bloquez les applications non fiables avant qu'elles puissent exploiter les processus d'authentification.

Effet 2

Élimination totale des privilèges permanents et application systématique du principe du moindre privilège

Appliquer le principe du moindre privilège aux accès dans toute l'entreprise peut sembler un défi permanent et insurmontable — surtout avec une pile d'identité fragmentée qui repose essentiellement sur des intégrations manuelles.

Les solutions d'identité modernes vous procurent les outils et les fonctionnalités nécessaires pour transformer l'accès en flux tendu (JIT) en un cadre réel applicable. En unifiant la gouvernance des identités et la gestion des accès à privilèges, les entreprises peuvent centraliser la visibilité sur les personnes bénéficiant d'une autorisation d'accès et mettre en place des contrôles très granulaires pour cet accès.

Une solution de sécurité des identités unifiée simplifie également la gestion des identités en consolidant la gouvernance, la gestion des accès à privilèges et d'autres fonctions liées à l'identité au sein d'une même plateforme. Cette centralisation permet d'implémenter des politiques d'accès cohérentes et de renforcer la sécurité des données les plus critiques de votre entreprise.

Avec Okta

Okta Identity Governance

- Bénéficiez d'une vue unifiée des accès dans tous les systèmes et applications afin de renforcer le contrôle et la supervision.
- Simplifiez les autorisations grâce à un accès basé sur les rôles et les groupes afin que les bonnes personnes disposent de l'accès approprié.
- Assurez aux nouvelles recrues un accès approprié dès le premier jour, ce qui accélère leur productivité et réduit les risques.
- Automatisez les changements de rôle et le déprovisioning pour maintenir la posture de sécurité.

Okta Privileged Access

- Protégez les informations confidentielles ou sensibles avec des contrôles d'accès sûrs.
- Personnalisez les protocoles d'accès afin de les harmoniser avec des cas d'usage et des utilisateurs spécifiques.
- Bénéficiez d'une visibilité élevée sur les activités protégées afin d'améliorer les audits et la gestion des risques.
- Simplifiez les demandes d'accès grâce à des intégrations conviviales qui accélèrent les workflows sans nuire à la sécurité.

Okta Integration Network

Le catalogue de préintégrations d'Okta, riche de plus de 7 000 entrées, vous aide à acquérir une visibilité sur l'accès à la vaste majorité des composants de votre pile technologique, au moyen d'un point de contrôle unique.

Google Workspace slack salesforce HubSpot zoom

Effet 3

Mise en œuvre éprouvée des principes Zero Trust

Alors que la plupart des entreprises se sont engagées depuis longtemps à en respecter les principes, peu d'entre elles opèrent réellement dans un framework Zero Trust. En effet, tout comme l'application du principe du moindre privilège, la mise en place du Zero Trust avec une pile d'identité fragmentée exige une surveillance manuelle de tous les instants que les administrateurs peinent à exécuter.

Une approche unifiée de la sécurité axée sur l'identité est essentielle pour confirmer (avec un haut niveau de confiance) que votre entreprise a concrètement entrepris de mettre en place des opérations Zero Trust. Grâce à l'unification de votre pile technologique sous une plateforme moderne de gestion des identités, il est plus facile pour votre entreprise d'appliquer les principes Zero Trust à toute la pile technologique et de démontrer cette conformité. Il n'est plus nécessaire de vérifier manuellement les autorisations de chaque utilisateur dans l'ensemble des systèmes et applications. L'identité unifiée remplace les tâches fastidieuses (et sujettes à erreur) par une analyse automatisée, ce qui renforce le niveau de confiance et de protection contre les menaces avec moins de ressources.

Avec Okta

Identity Security Posture Management

- Exécutez des analyses automatisées de tous vos outils et évaluez votre environnement en fonction d'un ensemble agrégé de frameworks Zero Trust.
- Identifiez de façon proactive les vulnérabilités et les failles de sécurité avant qu'elles soient exploitées.
- Mettez continuellement au jour les failles et erreurs de configuration critiques, notamment une application incohérente du MFA et la multiplication des comptes.
- Appliquez les principes Zero Trust et confirmez-les en quelques minutes (et non en plusieurs jours ou semaines).

Effet 4

Contrôle renforcé des identités non humaines et machines

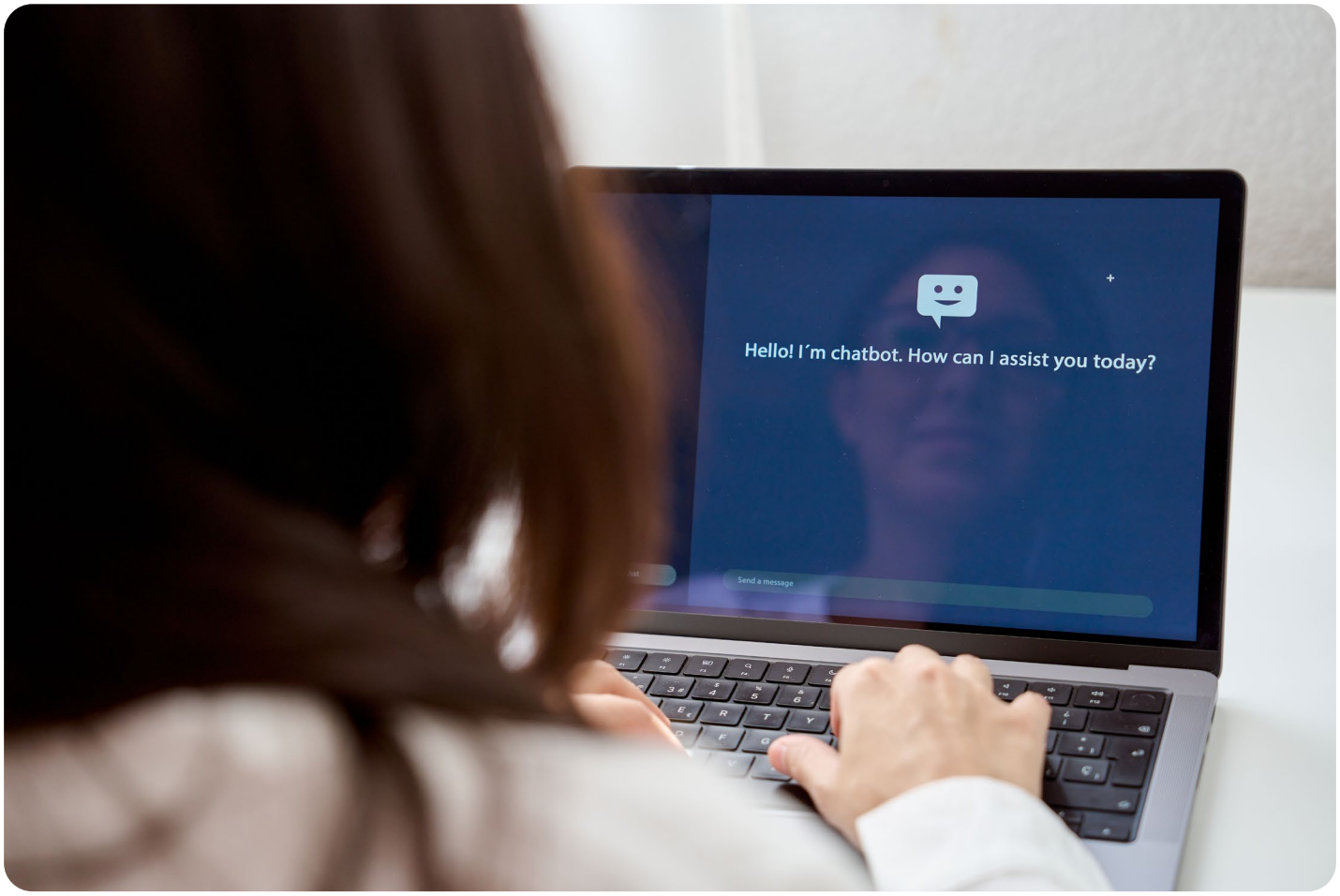
Les identités non humaines (p. ex. celles des machines, services et agents d'IA) accélèrent les capacités essentielles de votre entreprise en matière de collaboration, d'innovation et de productivité générale. Toutefois, elles représentent également un vecteur de menace croissant, généralement non surveillé.

Une identité unifiée permet d'éviter ce type d'angle mort en vous offrant une visibilité complète sur les identités non humaines de votre pile technologique : elle vous indique leurs emplacements ainsi que les ressources auxquelles elles peuvent accéder. Cette nouvelle visibilité vous permet de surveiller leurs autorisations, de gérer leur accès aux ressources clés à l'aide de contrôles granulaires, et d'intégrer ces identités non humaines à une stratégie de sécurité des identités complète, reposant sur le principe du moindre privilège.

Avec Okta

Identity Security Posture Management

- Découvrez les identités non humaines et bénéficiez d'une vue centralisée des modalités d'accès et des ressources accessibles par celles-ci.
- Définissez des autorisations plus granulaires pour les identités non humaines afin de réduire la surface d'attaque.



Effet 5

Rentabilisation maximale des investissements en technologies et sécurité

L'interconnectivité de votre pile technologique est précisément ce qui permet à ces investissements en technologies de générer une valeur métier. Sans une intégration étroite et harmonieuse des composants de votre pile technologique, il est impossible d'exploiter pleinement la valeur de vos investissements en technologies et sécurité.

Ce constat est tout particulièrement vrai dans le cas de vos outils de sécurité. Chaque solution génère une mine de données et de signaux, mais si ceux-ci restent isolés, il est impossible de préparer ses défenses et de répondre de façon agile et décisive au paysage des menaces actuel — tant pour protéger les systèmes sensibles internes que pour offrir des expériences clients sécurisées.

Une stratégie unifiée et axée sur l'identité libère tout le potentiel de vos piles technologiques et de sécurité étendues, en connectant ces signaux à une plateforme centralisée qui évalue constamment votre posture de sécurité, gère l'accès aux applications et systèmes, protège les identités clients et détermine les stratégies de remédiation automatique.

Témoignages clients

HubSpot

80 % des demandes d'accès désormais résolues grâce à l'automatisation

Delivery Hero

Gain de productivité de 28 800 h grâce à l'élimination des pannes

TakedaID

Déploiement de l'identité 5x plus rapide avec Okta qu'avec une solution interne

Des solutions axées sur l'identité pour vos besoins actuels et futurs

Ces cinq effets positifs sont loin d'être anodins : ils constituent des éléments déterminants de la sécurité et du succès de votre entreprise. Dans un paysage des risques défini par des menaces toujours plus sophistiquées et de nouvelles méthodes d'attaques optimisées par l'IA, l'approche la plus judicieuse pour un avenir sûr et résilient est une sécurité axée sur l'identité.

Pourquoi ? Parce que la sécurité est *la clé* de l'identité. Elle est au cœur de toute stratégie moderne de protection de l'entreprise. Mais pour tenir cette promesse d'une sécurité renforcée, il vous faut éliminer la fragmentation des identités, fléau pour la gestion des risques et la réalisation de la valeur métier. Dans le paysage actuel, une sécurité unifiée et axée sur l'identité aide non seulement les entreprises à garder une longueur d'avance sur les menaces, mais aussi à soutenir les environnements IT fluides nécessaires pour démarquer votre entreprise de la concurrence.

Vous souhaitez en savoir plus sur l'unification de votre stratégie de sécurité à l'aide d'une solution d'identité moderne ? Prenez contact avec notre équipe et découvrez Okta Platform en action.

okta

Okta France
Tour Europlaza
20 avenue André Prothin
92400 Courbevoie – France
+33 01 85 64 08 80