Livre blanc

Septembre 2022

The State of Zero Trust Security 2022

Évaluation de la maturité de la gestion des identités et des accès dans les entreprises à l'échelle mondiale

Okta France
Tour Europlaza
20 avenue André Prothin
92400 Courbevoie
France

okta

Sommaire

Zero Trust, une approche essentielle à adopter sans tarder

La philosophie qui sous-tend la sécurité Zero Trust — « ne jamais faire confiance, toujours vérifier » — semble avoir touché une corde sensible. Il a fallu des décennies aux entreprises pour renoncer à une approche binaire de la sécurité et accepter que, dans un monde dominé par le cloud, il n'existe aucun périmètre à défendre et les cybercriminels sont toujours présents dans nos réseaux. Aujourd'hui, les cadres dirigeants partout dans le monde adoptent le framework de sécurité Zero Trust, qui est passé en peu de temps du statut de concept à la mode à celui d'avantage stratégique, puis d'impératif métier. D'après la définition 2022 de Forrester, « le Zero Trust est un modèle de sécurité de l'information qui, par défaut, refuse l'accès aux applications et aux données (...) Le Zero Trust défend trois principes fondamentaux : par défaut, aucune entité n'est fiable ; un accès sur le principe du moindre privilège est appliqué ; et une surveillance complète de la sécurité est implémentée[1]. »

> Depuis la publication du rapport d'Okta « The State of Zero Trust Security 2021 » l'année dernière, le pourcentage des entreprises ayant des initiatives Zero Trust en cours d'exécution a plus que doublé, passant de 24 % à 55 %.

Okta a publié la première édition de ce rapport « State of Zero Trust » en 2019, et un grand nombre des enjeux qui ont grandement accéléré l'adoption du Zero Trust alors sont toujours d'actualité aujourd'hui. Les travailleurs intellectuels en mode hybride ou à distance passent 65 % moins de temps au bureau qu'avant la pandémie de Covid-19 et rencontrent leur équipe en personne deux jours par semaine[2]. Force est de constater que l'essor du télétravail n'est pas un phénomène ponctuel dû uniquement à la pandémie : il s'agit d'un changement en profondeur dans notre façon de travailler. De même, les failles dans la protection de l'identité, parfois exacerbées par le passage accéléré au cloud et au numérique, continuent de représenter un défi pour les organisations de toutes tailles, car les cybercriminels profitent de la disparition du périmètre réseau et de l'évolution rapide des écosystèmes. L'identité est au cœur de ce défi : l'année dernière, plus de 80 % des brèches observées dans les applications web étaient dues à des compromissions d'identifiants, et les identifiants volés sont la tactique n° 1 utilisée dans les attaques de ransomware[3].

Pour protéger leurs systèmes, données, collaborateurs et clients dans un monde qui change, les entreprises ont dû revoir rapidement et radicalement leur approche de la cybersécurité, et renoncer à des solutions de sécurité héritées créées à une époque où tout était plus simple. Aujourd'hui, cela signifie presque toujours implémenter la sécurité Zero Trust. En adoptant un framework Zero Trust, les entreprises disposent d'une méthodologie pour évaluer en continu leur niveau de sécurité et la maturité relative de leur modèle, puis identifier la solution de sécurité qui leur permettra d'accélérer leur transformation à chaque étape de leur parcours.

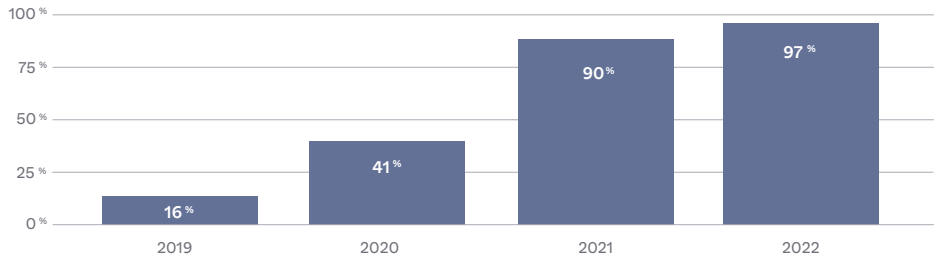
[1] Forrester, « **The Definition of Modern Zero Trust** », Forrester Research, Inc., 24 janvier 2022

[2] Gartner®, « **Strengthen Connection to Culture To Alleviate CEO Concerns About Hybrid Work** », Graham Waller, Alexia Cambon, Rob O'Donohue, Gabriela Vogel, Christie Struckman, Chris Audet, 9 juin 2022

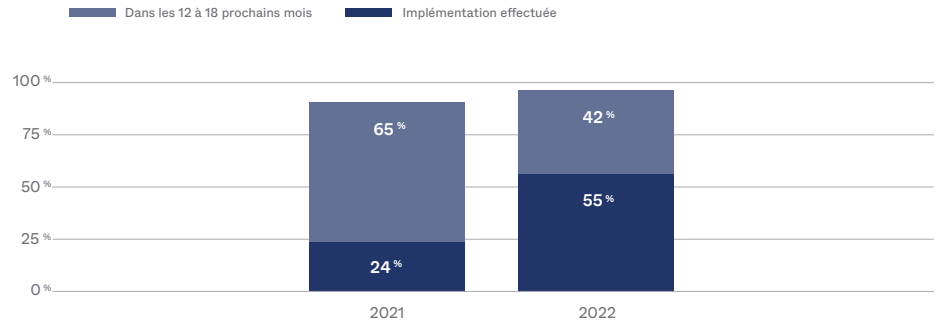
[3] Verizon, « **2022 Data Breach Investigations Report** »

Il y a quatre ans, à peine 16 % des entreprises interrogées déclaraient qu'elles avaient mis en place une initiative Zero Trust ou qu'elles allaient le faire dans les 12 à 18 mois suivants. Aujourd'hui, ce pourcentage est de 97 %.

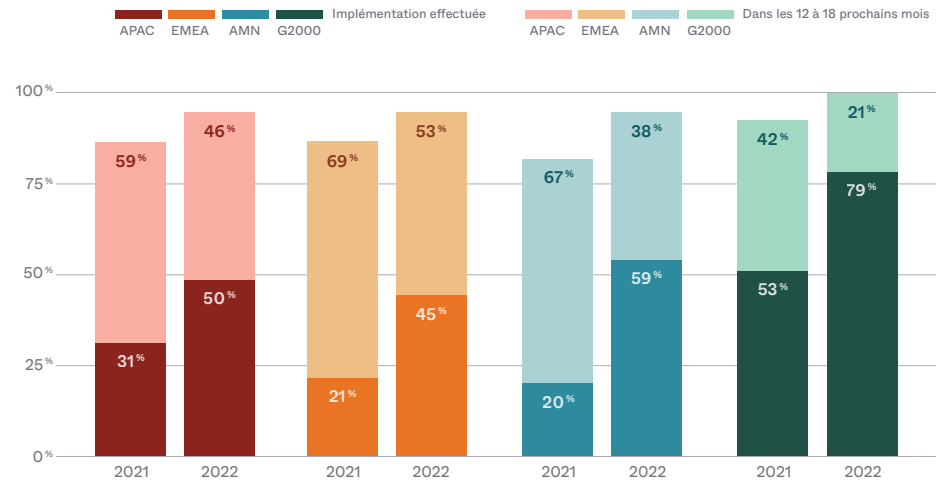
Comparaison annuelle — Toutes les entreprises Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les prochains mois ?



Comparaison annuelle — Toutes les entreprises Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les 12 à 18 prochains mois ?



Comparaison régionale annuelle Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les 12 à 18 prochains mois ?

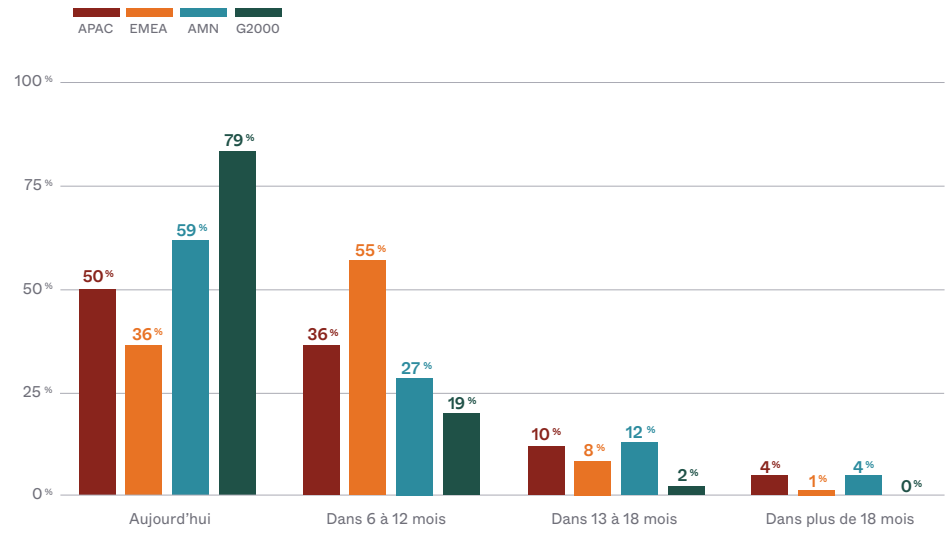


Comme le rapport de cette année le montre clairement, cet état d'esprit est partagé dans le monde entier : presque toutes les entreprises interrogées ont déjà lancé une initiative Zero Trust ou défini un plan pour en démarrer une dans les mois qui viennent. Dans tous les cas, elles ont l'obligation de progresser vite. Par exemple, en 2021, le gouvernement fédéral des États-Unis a mandaté, **par décret**, le développement de l'architecture Zero Trust dans tous les organismes publics fédéraux.

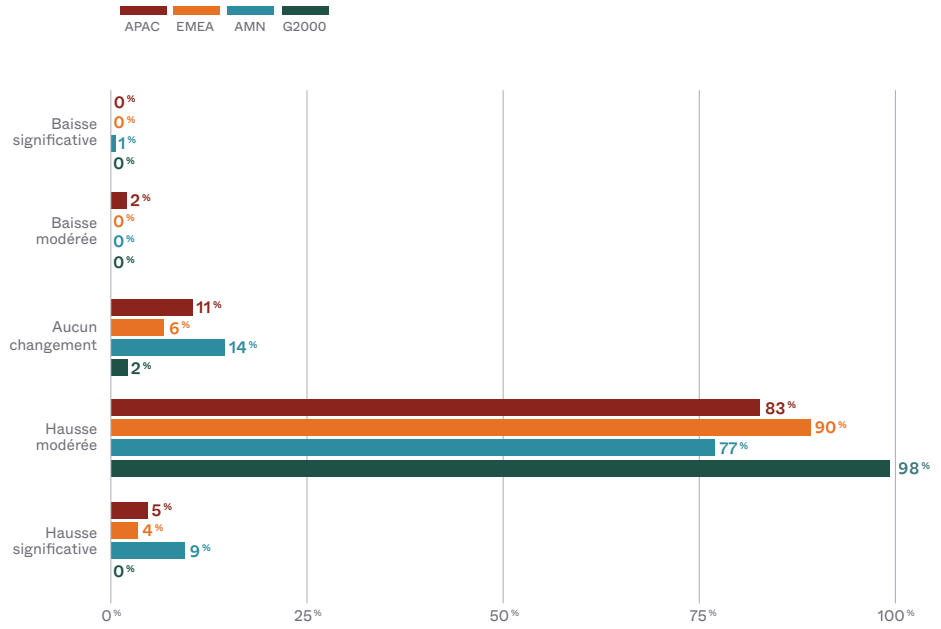
Et le stade de la simple planification est largement dépassé : la vitesse à laquelle les entreprises ont mis cette philosophie en action est stupéfiante. En 2021, 24 % des entreprises indiquaient avoir déjà entamé un parcours Zero Trust ; cette année, ce chiffre a plus que doublé, passant à près de 55 %. Dans toutes les régions où nous avons mené notre enquête — Europe, Moyen-Orient et Afrique (EMEA), Asie-Pacifique (APAC) et Amérique du Nord (AMN), ainsi que les entreprises du classement Global 2000 (G2000) —, plus de 85 % des personnes interrogées indiquent que leur entreprise avait décidé une hausse annuelle modérée, voire significative dans certains cas, de leur budget Zero Trust.

Notre enquête mondiale révèle sans ambiguïté que les projets Zero Trust sont indépendants de la taille de l'entreprise, de sa situation géographique ou de son secteur d'activité. De même, toutes les personnes interrogées mentionnent que leur entreprise avance à un rythme régulier vers l'établissement d'une sécurité Zero Trust. Dans ce rapport, nous montrons comment les entreprises progressent aujourd'hui du point de vue de l'identité (un aspect clé de l'approche Zero Trust) et nous étudierons ensuite l'évolution de leur parcours Zero Trust de manière plus générale lors des mois et années à venir.

Comparaison régionale Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les prochains mois ?

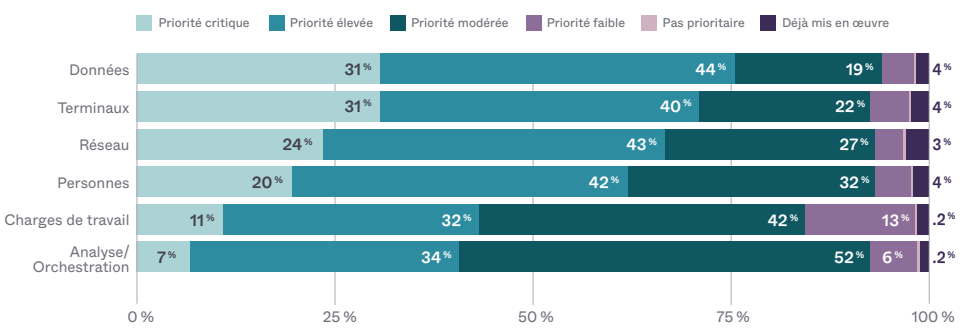


Comparaison régionale Comment votre budget Zero Trust a-t-il évolué (le cas échéant) dans les 12 derniers mois ?



Pour la 4e année de son rapport « State of Zero Trust Security », Okta a interrogé plus de 700 responsables sécurité dans le monde entier — plus que lors des autres éditions — afin d'évaluer l'étape à laquelle leur entreprise est arrivée dans son parcours Zero Trust. Nous leur avons demandé de détailler les initiatives spécifiques que leur entreprise a déjà mises en place, ainsi que leur priorisation à court et à long terme. En nous basant sur le framework Zero Trust popularisé par Forrester et CISA (Cybersecurity and Infrastructure Security Agency), nous avons examiné les priorités qui comptent le plus aujourd'hui dans le cadre des initiatives Zero Trust. Sans surprise, les données, les réseaux et les terminaux sont toujours cités comme des catégories prioritaires, mais cela devrait changer selon nous, à mesure que les entreprises prendront pleinement conscience que le périmètre de sécurité est désormais davantage axé sur les utilisateurs que sur le réseau. La catégorie des utilisateurs devrait donc peu à peu s'imposer elle aussi comme prioritaire. L'identité est un puissant multiplicateur de performances pour les initiatives de sécurité Zero Trust, comme nous le verrons en détail plus tard.

Toutes les entreprises à l'échelle mondiale Classez les exigences Zero Trust suivantes selon les priorités de votre entreprise.



Chaque entreprise se forge son propre parcours Zero Trust, d'après ses pratiques sectorielles, priorités métier, budgets et investissements d'infrastructure existants, entre autres facteurs. Mais si les parcours sont uniques, l'objectif reste le même : partout dans le monde, les entreprises reconnaissent désormais que l'établissement d'une infrastructure Zero Trust fiable est essentiel pour poser les bases d'un avenir sûr et évolutif.

Points à retenir

Le Zero Trust est désormais bien plus qu'un phénomène de mode
Pour les entreprises du monde entier, l'adoption d'une mentalité Zero Trust pour la sécurité est devenue le paradigme par défaut. De fait, la plupart d'entre elles ont déjà mis en place des initiatives allant dans ce sens et recherchent activement des solutions spécifiques pour accélérer leur parcours. Les problèmes de sécurité sont un moteur de plus en plus fort : depuis longtemps, les entreprises s'efforcent de trouver le juste équilibre entre sécurité et facilité d'utilisation. Et tandis que ce second aspect a pris le dessus jusqu'à présent, cette année, la balance penche de l'autre côté. En moyenne, les personnes interrogées attribuent désormais une priorité légèrement plus élevée aux projets de sécurité.

En sécurité d'entreprise, pas de remède miracle
Le Zero Trust est un principe directeur solide, mais atteindre cet objectif constitue une tâche complexe qui exige un grand nombre de solutions de pointe étroitement intégrées et fonctionnant ensemble de façon transparente. Chaque entreprise possède son propre point de départ ainsi que des ressources et priorités différentes, ce qui génère des parcours uniques pour atteindre le même but : une vraie sécurité Zero Trust.

L'identité est fondamentale pour faire du Zero Trust une réalité
Malgré toutes leurs différences, les entreprises du monde entier comprennent désormais que l'identité est cruciale pour mettre en place une sécurité et une stratégie Zero Trust solides. Elles ne ménagent pas leurs efforts pour sécuriser le nouveau périmètre — l'identité — dans le cadre de leurs initiatives Zero Trust. Les stratégies spécifiques de gestion des identités et des accès (IAM) qu'elles mettent en place pour soutenir ces initiatives se composent de cinq phases distinctes, comme nous le détaillons dans ce rapport.

Le rôle de l'identité dans la sécurité Zero Trust

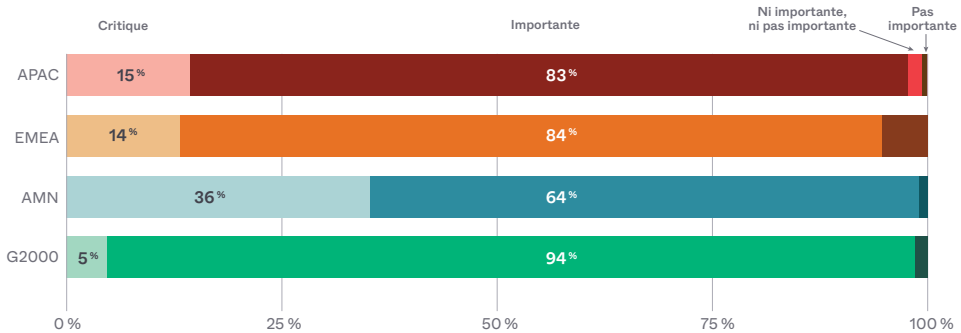
L'identité au cœur des solutions Zero Trust

L'identité n'est pas le seul composant d'un framework Zero Trust complet, mais c'est la base de toute stratégie Zero Trust. Garantir que chaque personne possède toujours le niveau d'accès adapté aux bonnes ressources au bon moment n'a jamais été aussi important pour la sécurité, la gestion, la conformité et d'autres préoccupations de premier plan. Le parcours Zero Trust de chaque entreprise est unique, car chacune possède ses propres impératifs métier, pile technologique et priorités stratégiques. Mais, partout dans le monde, on observe un consensus croissant sur le fait qu'une approche du Zero Trust axée sur l'identité permet aux organisations de tirer pleinement profit de l'IAM, en l'intégrant à d'autres solutions de sécurité critiques, pour en faire un puissant point de contrôle central et assurer une gouvernance intelligente de l'accès des utilisateurs, terminaux, données et réseaux.

> “
> L'époque de l'approche binaire des réseaux et des périmètres est révolue. En effet, c'est l'identité qui constitue désormais le nouveau périmètre.
>
> John McLeod, CISO, NOV Inc.

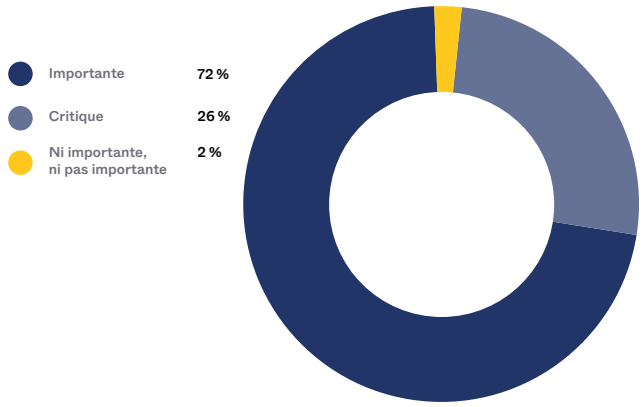
Quelle est l'importance de l'identité ? D'après notre enquête de cette année, 80 % des entreprises déclarent que l'identité est importante pour leur stratégie de sécurité Zero Trust globale, et 19 % vont jusqu'à indiquer que l'identité est critique pour l'activité. En d'autres termes, 99 % des entreprises pensent que l'identité est un facteur majeur de leur stratégie Zero Trust. En particulier chez les CISO (Chief Information Security Officer) et les autres cadres dirigeants, 26 % vont jusqu'à dire que l'identité est critique pour l'activité, parmi les 98 % qui estiment qu'elle est importante. C'est donc sans surprise que Gartner® mentionne les « systèmes de protection de l'identité » dans l'un de ses derniers articles, « 7 Top Trends in Cybersecurity for 2022 », en expliquant que « l'usage abusif d'identifiants [figure parmi] les principales méthodes employées par les cybercriminels pour accéder aux systèmes et atteindre leurs objectifs[4] ». Si cette tendance existe depuis des années, la hausse récente et inattendue des détections et divulgations d'attaques de ce type fait de cette question une priorité pour de nombreuses entreprises.

Comparaison régionale Quelle est l'importance de l'identité dans votre stratégie de sécurité Zero Trust globale ?



[4] Gartner®, « 7 Top Trends in Cybersecurity for 2022 », Susan Moore, 13 avril 2022

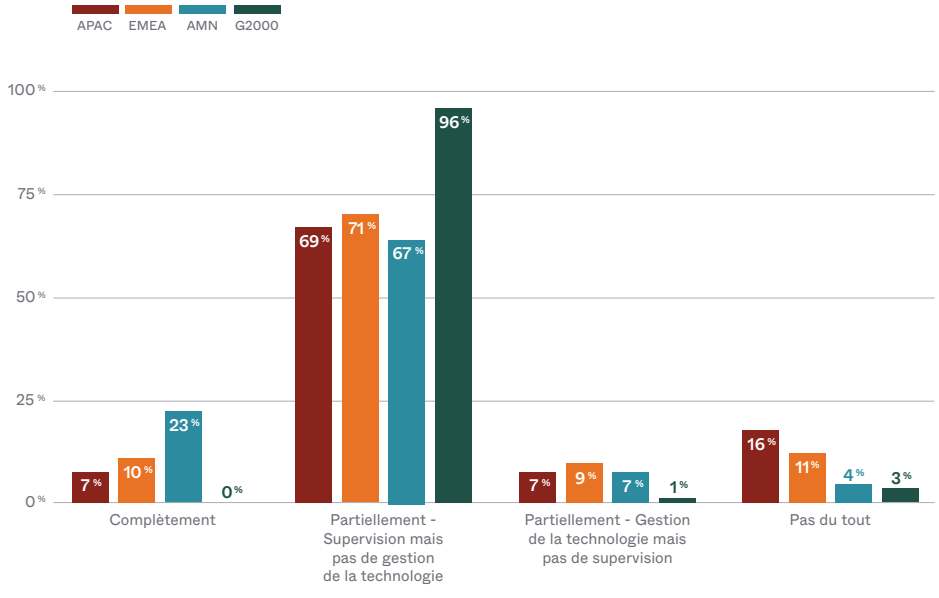
Cadres dirigeants interrogés Quelle est l'importance de l'identité dans votre stratégie de sécurité Zero Trust globale ?



À l'heure où ces organisations s'efforcent de déployer des solutions de gestion des identités dans le cadre de leurs initiatives Zero Trust et de leur stratégie de sécurité globale, la réussite repose sur la collaboration étroite des équipes IT et sécurité. La sécurité a toujours été une activité collective, mais, à mesure que les menaces gagnent en sophistication, les entreprises doivent élaborer des plans exhaustifs et interfonctionnels afin d'abattre les derniers silos. Cela peut générer de nouveaux problèmes, comme nous l'expliquerons par la suite, notamment la difficulté logistique de faire respecter à un nombre croissant d'utilisateurs les décisions concernant l'identité.

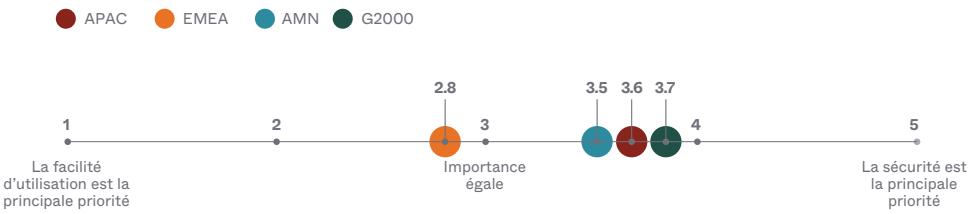
Notre enquête 2022 révèle que les équipes sécurité des entreprises du classement Forbes Global 2000 ont plus de chances de réussir l'intégration de leurs technologies IAM à leurs projets de sécurité que celles des petites entreprises, même si, partout dans le monde, davantage d'équipes sécurité assurent au moins un contrôle partiel sur l'IAM. Dans la zone EMEA, 71 % des équipes sécurité fournissent au moins un contrôle partiel sur la technologie, ce qui représente une légère baisse par rapport à l'année dernière. Dans les zones APAC et Amérique du Nord, par contre, ces chiffres n'ont presque pas changé.

Comparaison régionale Dans quelle mesure les équipes sécurité gèrent-elles les identités et les accès dans votre entreprise ?



Pour assurer à la fois leur sécurité et leur compétitivité aujourd'hui, les entreprises doivent rendre leurs ressources disponibles aux utilisateurs autorisés tout en se protégeant des cybercriminels. Or, trouver l'équilibre entre facilité d'utilisation et sécurité est un défi permanent. Au début de la pandémie de Covid-19, de nombreuses entreprises ont accordé une énorme importance à la facilité d'utilisation. Elles devaient faire en sorte que leurs effectifs à distance accèdent facilement aux outils et aux ressources dont ils avaient besoin pour être productifs. Cependant, en 2022, la tendance a commencé à s'inverser, et une majorité d'entreprises attribuent maintenant un niveau de priorité supérieur à la sécurité par rapport à la facilité d'utilisation. Ce glissement de priorité est plus prononcé dans les zones APAC et Amérique du Nord, la région EMEA démontrant une priorisation plus équilibrée entre ces deux impératifs. Pourquoi la balance penche-t-elle maintenant en faveur de la sécurité ? Les entreprises ayant établi des pratiques solides de travail à distance et hybride exploitent déjà les investissements réalisés lors de la pandémie en matière de facilité d'utilisation. Elles peuvent donc aujourd'hui accuser un retard dans leur sécurité. Mais de plus en plus, elles comprennent qu'il n'est plus nécessaire de choisir entre sécurité forte et facilité d'utilisation optimisée. (Pensez à l'authentification sans mot de passe, par exemple.) En accordant la priorité au renforcement de leurs mesures de sécurité, elles peuvent en même temps obtenir une meilleure facilité d'utilisation.

Comparaison régionale Quelle importance relative accordez-vous respectivement à la sécurité et à la facilité d'utilisation au sein de votre entreprise ?



Adoption de l'identité pour les initiatives Zero Trust

Les cinq phases de la maturité Zero Trust

Les entreprises ont pleinement adopté la philosophie de base du Zero Trust au niveau macro — ainsi que le rôle crucial de l'identité dans ce framework. Mais passent-elles pour autant à l'action ? En nous basant sur le modèle d'adoption de l'identité d'Okta visant à soutenir les stratégies Zero Trust, nous avons décidé d'examiner quelques projets spécifiques liés à l'identité que certaines entreprises mènent actuellement ou prévoient de mener dans le cadre de leurs initiatives Zero Trust. Notre modèle décompose le parcours vers le Zero Trust en cinq phases. L'objectif est d'aider les entreprises à comprendre comment leurs pairs hiérarchisent leurs projets liés à l'identité : le travail déjà accompli, celui qui vient de commencer et les initiatives qui seront prioritaires dans les mois à venir.

> La gestion des accès est devenue une source fiable pour la sécurité axée sur l'identité[5].
>
> Gartner®, *Magic Quadrant™ for Access Management*

Lorsque les entreprises s'efforcent d'implémenter une architecture Zero Trust exploitable qui repose sur des pratiques de sécurité axées sur l'identité, nous constatons qu'elles passent par cinq phases de maturité distinctes :

Phase 1 : modèle traditionnel
Les entreprises qui viennent de démarrer leur transformation cloud essaient d'anticiper les défis de l'adoption du cloud ou sont déjà en train de les affronter : annuaires déconnectés, surface de risque qui s'accroît, incidence croissance des attaques basées sur l'identité. La phase 1 consiste à mettre en place les premières étapes de l'établissement d'une sécurité Zero Trust.

Projets clés liés à l'identité correspondant à cette phase :

- Connecter les annuaires de collaborateurs aux applications cloud critiques pour obtenir une visibilité sur qui accède à quoi, quel que soit le lieu où se trouvent les utilisateurs
- Implémenter l'authentification multifacteur (MFA) pour les collaborateurs afin d'assurer une protection contre le vol d'identifiants

Phase 2 : modèle émergent
Dans la phase 2, en règle générale, les entreprises étendent l'adoption du cloud et leur environnement cloud. Elles tentent d'exploiter l'efficacité et l'évolutivité de cette technologie, tout en essayant de sécuriser et de simplifier les accès utilisateurs, afin de permettre à leurs effectifs à distance ou hybrides de rester sûrs et productifs.

Projets clés liés à l'identité correspondant à cette phase :

- Implémenter le MFA pour les utilisateurs externes, par exemple les partenaires commerciaux et prestataires
- Implémenter le SSO (Single Sign-On) pour les collaborateurs, sur les applications compatibles
- Activer la réinitialisation en libre-service des facteurs et réduire les coûts d'assistance
- Automatiser le provisioning et le déprovisioning des applications

Phase 3 : modèle de maturation
Dans cette phase, les entreprises ont développé des processus et impératifs métier concernant le travail dynamique et à distance. Elles ont besoin d'outils leur permettant d'offrir en toute confiance à une équipe mondiale complexe un accès 24h/24, 7j/7 adapté aux ressources de l'entreprise[5], tout en restant conformes aux exigences réglementaires.

[5] Gartner®, « *Magic Quadrant™ for Access Management* », Henrique Teixeira, Abhyuday Data, Michael Kelley, 1er novembre 2021

Projets clés liés à l'identité correspondant à cette phase :

- Étendre le SSO à tous les utilisateurs externes autorisés
- Automatiser le provisioning et le déprovisioning pour les collaborateurs et les utilisateurs externes selon un modèle basé sur les rôles
- Créer des politiques imposant la prise en charge du SSO sur les applications nouvelles et existantes
- Activer la gestion des accès à privilèges sur l'infrastructure cloud
- Intégrer des informations sur les menaces issues des terminaux et applications cloud aux outils de gestion des événements et informations de sécurité (SIEM)

Phase 4 : modèle élevé

Les entreprises à cette phase tentent de consolider leurs investissements cloud en terminant leur transformation digitale, en décidant de renforcer ou d'abandonner les technologies héritées, selon le cas, et en protégeant les applications personnalisées clés pouvant représenter des failles de sécurité.

Projets clés liés à l'identité correspondant à cette phase :

- Associer différents facteurs d'authentification aux différents groupes d'utilisateurs en fonction du risque, ce qui amène à réduire les coûts de licence
- Ajouter l'accès sécurisé aux API
- Implémenter des politiques d'accès basées sur le contexte
- Déployer des outils faisant office de proxy pour moderniser les technologies héritées
- Utiliser des capacités d'orchestration de la sécurité pour répondre de façon dynamique à l'évolution du paysage des menaces

Phase 5 : modèle évolué

Les entreprises dans cette phase ont posé les bases de la sécurité Zero Trust axée sur l'identité. Elles peuvent exploiter en toute confiance cette connaissance situationnelle en temps réel pour prendre des décisions d'accès informées et modifier des décisions existantes basées sur la mise à jour continue des informations. Elles peuvent continuer à affiner leur sécurité : rendre l'accès plus sûr, par le biais d'une sécurité périphérique, et plus simple, en étendant l'accès passwordless convivial à toutes les ressources de l'entreprise.

Projets clés liés à l'identité correspondant à cette phase :

- Déployer un accès passwordless à l'échelle de l'entreprise
- Prendre des décisions d'accès au niveau de la couche de données en fonction du niveau de sécurité des utilisateurs et des terminaux

Modèle d'adoption de l'identité pour les initiatives Zero Trust Les cinq étapes de l'adoption de l'identité

Phase 1 - Modèle traditionnel Au début du parcours, réflexion sur le rôle de l'identité dans les stratégies de sécurité

Phase 2 - Modèle émergent Accent sur la simplification de l'expérience utilisateur avec mise en place de contrôles de sécurité pour les applications cloud

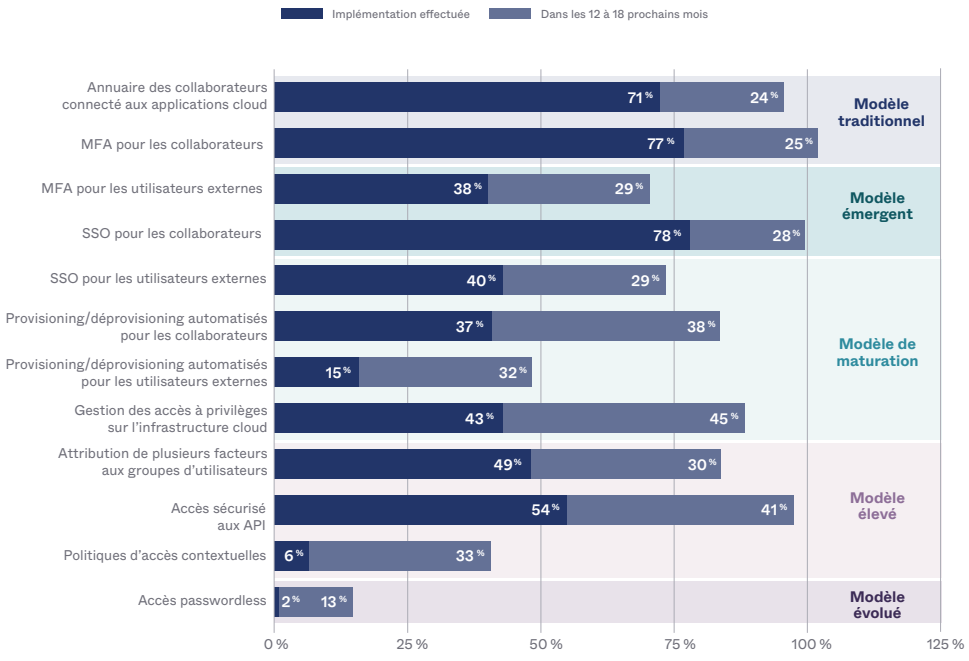
Phase 3 - Modèle de maturation L'identité est considérée comme un élément fondamental des politiques de sécurité et de l'expérience utilisateur

Phase 4 - Modèle élevé Extension des protections aux technologies héritées, et consolidation des stratégies de sécurité et d'identité

Phase 5 - Modèle évolué L'identité est intégrée à une pratique de sécurité moderne qui prend en charge la transformation digitale et applique l'accès sur le principe du moindre privilège

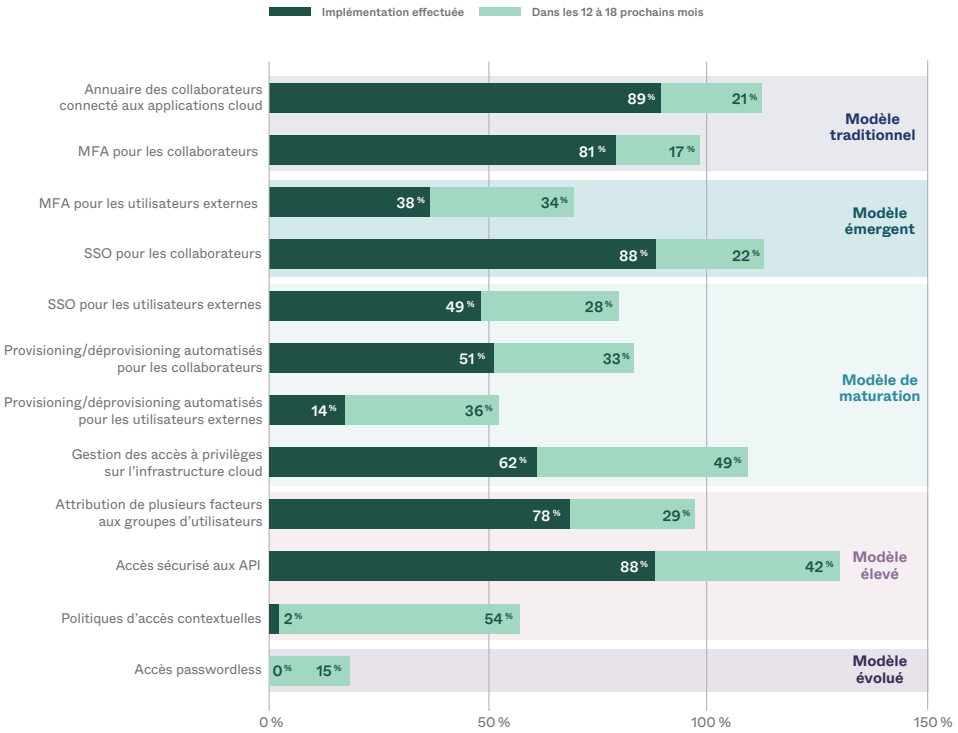
En matière d'investissement Zero Trust, les entreprises semblent agir de façon cohérente avec ce qu'elles annoncent : la grande majorité d'entre elles ont au moins démarré leur parcours de sécurité Zero Trust en lançant des projets critiques liés à l'identité. Notre enquête révèle que plus de 70 % des entreprises interrogées dans le monde ont déjà dépassé la phase 1 (modèle traditionnel). 95 % prévoient de finaliser leurs projets de phase 1 dans les 12 à 18 mois et travaillent sérieusement à des projets liés à l'identité se trouvant plus avant sur la courbe de maturité. Concernant les projets de la phase 2 (modèle émergent), la grande majorité des entreprises interrogées (près de 80 %) ont étendu le SSO à leurs collaborateurs, mais seulement 38 % déclarent avoir étendu le MFA aux utilisateurs externes, ce qui garantit un accès sécurisé aux ressources critiques pour les prestataires, fournisseurs et partenaires commerciaux autorisés. Le Zero Trust ne progresse pas de la même façon après la phase 2, comme expliqué ci-dessous, mais près de 50 % des entreprises interrogées dans le monde ont terminé plusieurs projets liés à l'identité et donc progressé sur la courbe de maturité. Quant aux autres, un pourcentage élevé d'entre elles prévoient de s'attaquer à ces projets dans les mois qui viennent.

Toutes les entreprises à l'échelle mondiale Adoption de l'identité pour les initiatives Zero Trust



Concernant le groupe des entreprises du classement Forbes Global 2000, près de 100 % d'entre elles prévoient de finaliser leurs projets de phase 1 dans les 18 mois à venir (si ce n'est pas déjà fait). En outre, dans les mêmes délais, au moins la moitié d'entre elles comptent venir à bout des projets des phases 1 à 4, et commencer à travailler sur la phase 5.

Entreprises du classement Global 2000 Quels projets votre entreprise a-t-elle déjà implémentés jusqu'à présent et quelles sont ses priorités dans les 12 à 18 prochains mois ?



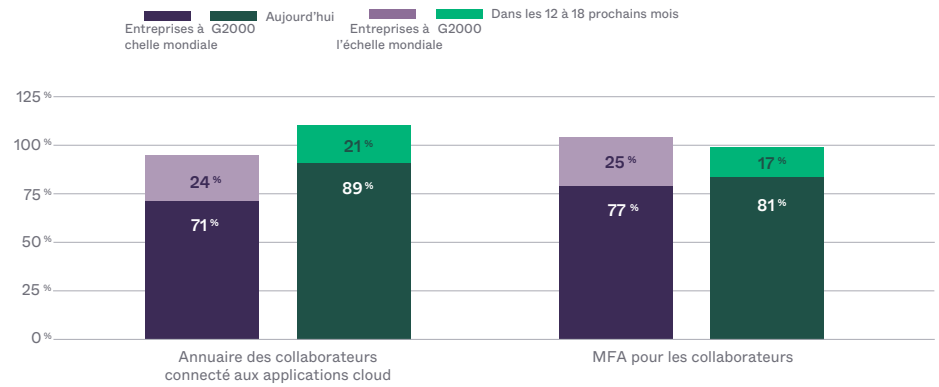
Phase 1 : modèle traditionnel

Au début d'un parcours Zero Trust, les entreprises se retrouvent face à des défis de base liés à l'identité, comme les annuaires déconnectés, une surface de risque qui s'étend et une déferlante d'attaques basées sur l'identité. Pour mesurer leur progression à cette phase de la courbe de maturité, nous leur avons demandé si leurs annuaires de collaborateurs étaient connectés à leurs applications cloud et si elles avaient implémenté le MFA pour les collaborateurs. Nous avons découvert que, même en phase 1, les entreprises arrivent à trouver des solutions efficaces pour attribuer aux bons utilisateurs l'accès approprié aux bonnes ressources, en ajoutant plusieurs couches de sécurité à leur processus d'authentification.

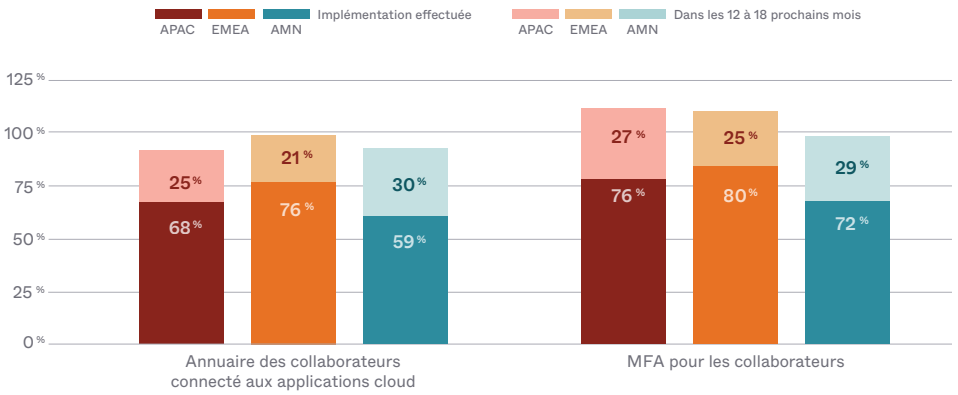
D'après notre rapport, près de 100 % des entreprises à l'échelle mondiale et des entreprises du classement Global 2000 interrogées prévoient de finaliser les projets de la phase 1 liés à l'identité dans les 18 prochains mois. Étendre le MFA aux collaborateurs est le projet le plus adopté parmi tous les participants à l'enquête,

et 100 % des entreprises interrogées dans toutes les régions planifient l'adoption du MFA pour les collaborateurs sous 18 mois dans le contexte de leur stratégie globale de protection de l'identité. Un pourcentage inférieur indique que l'annuaire de leur entreprise est déjà connecté aux applications cloud, mais nombre de ces entreprises sont peut-être toujours en pleine migration vers le cloud. Elles se donnent généralement 18 mois pour atteindre cet objectif.

Phase 1 — Toutes les entreprises à l'échelle mondiale et les entreprises du classement Global 2000
Quels projets votre entreprise a-t-elle déjà implémentés jusqu'à présent et quelles sont ses priorités dans les 12 à 18 prochains mois ?



Phase 1 — Comparaison régionale Quels projets votre entreprise a-t-elle déjà implémentés jusqu'à présent et quelles sont ses priorités dans les 12 à 18 prochains mois ?

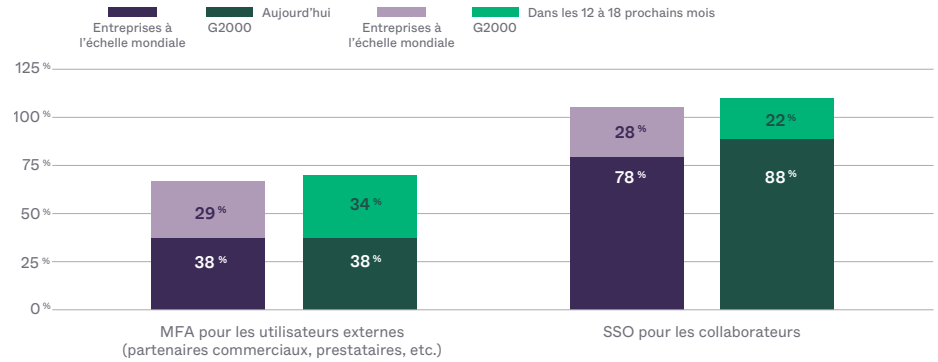


Phase 2 : modèle émergent

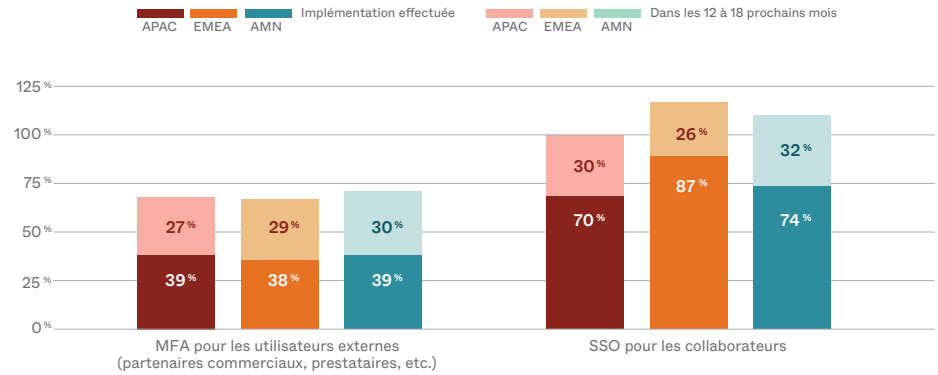
Dans cette phase, les entreprises tentent souvent de corréler les activités se déroulant sur des systèmes disparates, après avoir apporté des changements tels qu'une hausse des applications cloud utilisées et/ou une fusion-acquisition, ce qui nécessite de simplifier l'accès des utilisateurs. Pour évaluer les progrès en phase 2, nous avons demandé aux personnes interrogées si leur entreprise avait déjà déployé le MFA pour les utilisateurs externes, ce qui inclut les partenaires commerciaux et prestataires, et si elle avait étendu le SSO aux collaborateurs afin de simplifier leur accès aux outils dont ils ont besoin pour être productifs.

D'après les données recueillies, plus de la moitié des entreprises interrogées dans chaque région prévoient de finaliser la phase 2 dans les 12 à 18 mois à venir (si ce n'est pas déjà fait). Dans leur activité, de plus en plus d'entreprises s'appuient non seulement sur des collaborateurs travaillant à distance, mais aussi sur des prestataires, des bénévoles, des fournisseurs et d'autres partenaires différents de leurs employés à temps plein. Ces personnes représentent une problématique de sécurité croissante, et étendre le MFA à ces utilisateurs externes est une priorité majeure dans toutes les régions pour faire en sorte que les ressources restent accessibles et sécurisées. Les entreprises, quelle que soit leur taille, ont quasiment toutes établi le MFA pour les utilisateurs externes, tandis que le SSO pour les collaborateurs semble davantage en place dans les entreprises du classement Global 2000 que dans les petites entreprises (88 % contre 78 %).

Phase 2 — Toutes les entreprises à l'échelle mondiale et les entreprises du classement Global 2000
Quels projets votre entreprise a-t-elle déjà implémentés jusqu'à présent et quelles sont ses priorités dans les 12 à 18 prochains mois ?



Phase 2 — Comparaison régionale Quels projets votre entreprise a-t-elle déjà implémentés jusqu'à présent et quelles sont ses priorités dans les 12 à 18 prochains mois ?



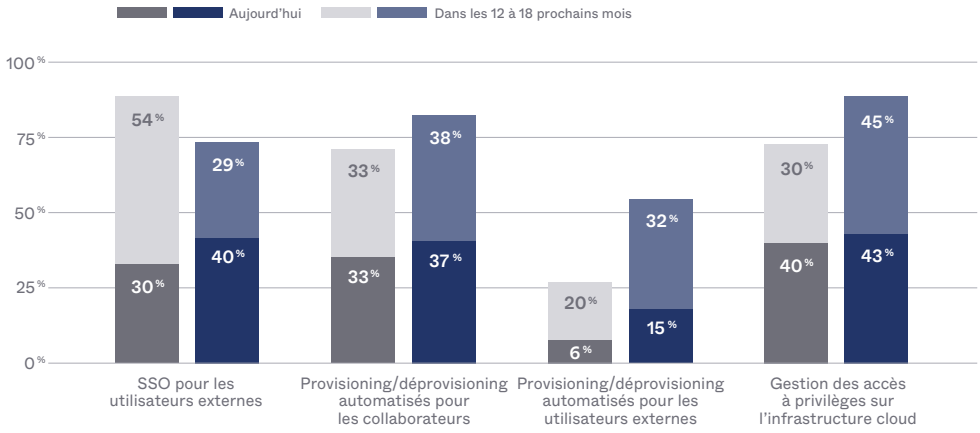
Phase 3 : modèle de maturation

Les entreprises en phase de maturation rencontrent des défis complexes, par exemple des exigences de conformité et réglementaires plus strictes, une infrastructure hybride et le besoin de soutenir des équipes étendues, très actives, dynamiques et partiellement ou principalement à distance. Pour relever ces défis, elles ne doivent pas cantonner leurs projets IAM aux collaborateurs et au réseau hérité, mais les appliquer aussi à un nombre toujours croissant d'utilisateurs externes ainsi qu'à un cloud ou à une infrastructure multicloud en expansion.

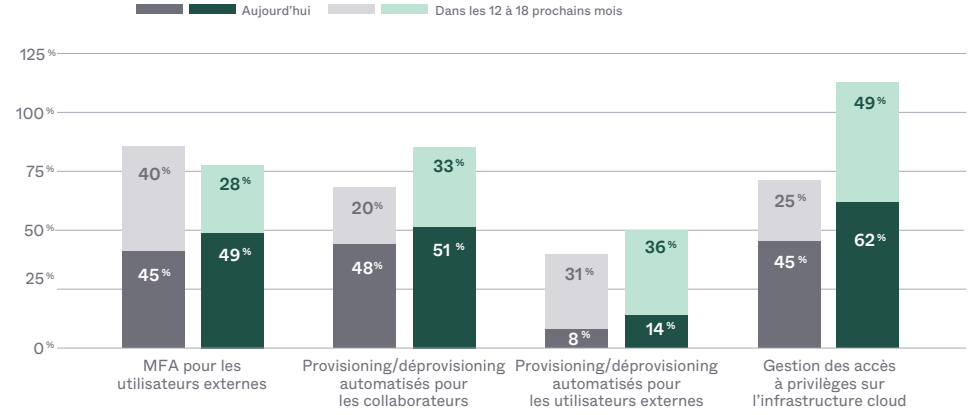
Pour évaluer les avancées en phase 3, nous avons demandé aux personnes interrogées si leur entreprise avait déjà automatisé le provisioning et le déprovisioning des collaborateurs et des utilisateurs externes, et si elle offrait la gestion des accès à privilèges sur son infrastructure cloud.

Moins d'entreprises ont atteint cette phase que les deux précédentes, mais près de la moitié des entreprises à l'échelle mondiale et du classement Global 2000 pensent finaliser leurs initiatives de phase 3 d'ici fin 2023. Pour les 18 mois à venir, les entreprises de la région APAC accordent davantage d'importance à l'automatisation du provisioning et du déprovisioning des collaborateurs, et à la gestion des accès à privilèges pour l'infrastructure cloud. Elles prévoient une hausse de l'adoption respectivement de 22 % à 76 % et de 44 % à 88 %. Les entreprises interrogées dans la zone Amérique du Nord comptent doubler l'adoption des accès à privilèges sur l'infrastructure cloud, et prévoient d'étendre le SSO aux utilisateurs externes, tout ceci sous 12 à 18 mois. De façon quasi similaire, les entreprises interrogées de la zone EMEA prévoient d'au moins doubler l'adoption des accès à privilèges sur l'infrastructure cloud, pour atteindre les 100 % dans les 18 prochains mois.

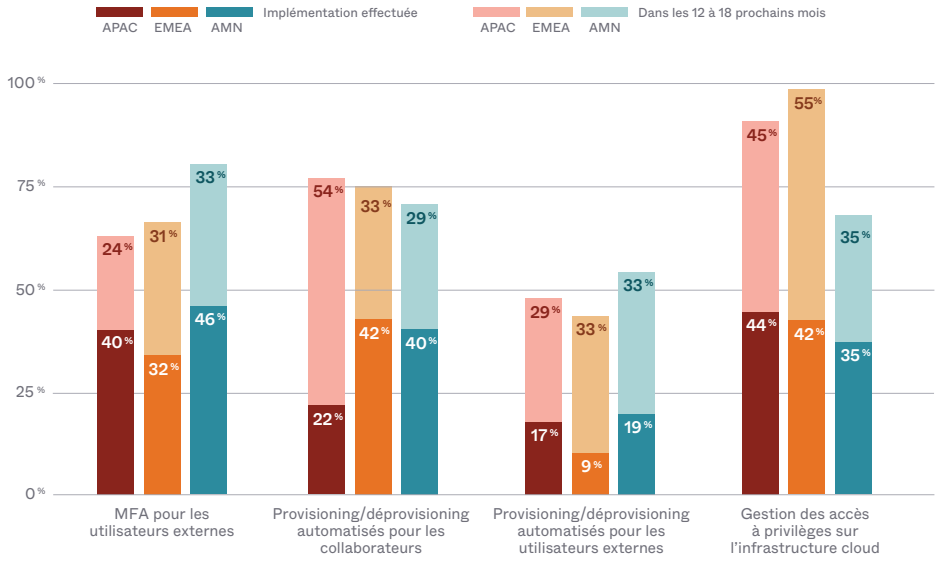
Phase 3 — Comparaison annuelle — Toutes les entreprises à l'échelle mondiale Quels projets votre entreprise a-t-elle déjà implémentés jusqu'à présent et quelles sont ses priorités dans les 12 à 18 prochains mois ?



Phase 3 — Comparaison annuelle — Entreprises du classement Global 2000 Quels projets votre entreprise a-t-elle déjà implémentés jusqu'à présent et quelles sont ses priorités dans les 12 à 18 prochains mois ?

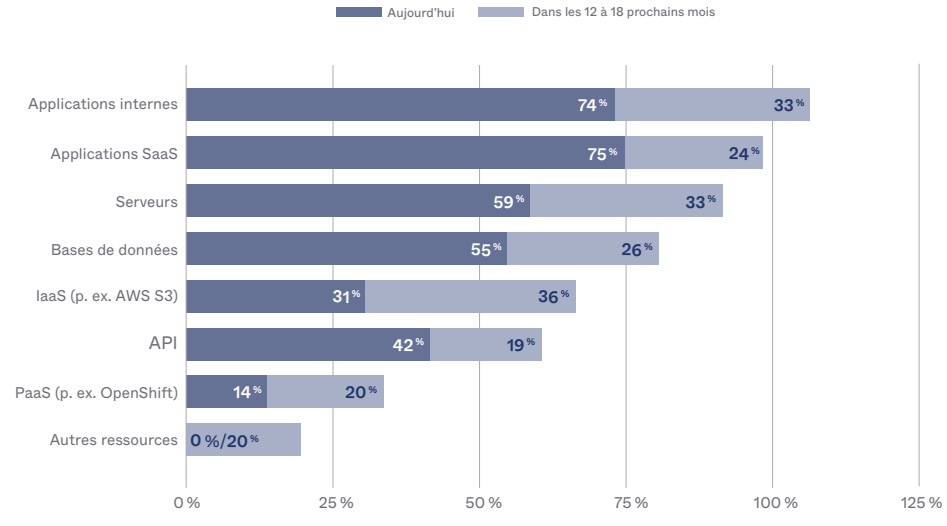


Phase 3 — Comparaison régionale Quels projets votre entreprise a-t-elle déjà implémentés jusqu'à présent et quelles sont ses priorités dans les 12 à 18 prochains mois ?



Étendre le MFA et le SSO, ces deux piliers de la sécurité et de la facilité d'utilisation telles qu'elles se conçoivent aujourd'hui, est une pratique qui va bientôt se généraliser. Ainsi, près de 75 % de toutes les entreprises interrogées dans le monde indiquent avoir déjà étendu le MFA, le SSO ou les deux aux applications internes et SaaS (Software-as-a-Service). Au moins 99 % d'entre elles prévoient de le faire dans les 12 à 18 mois, si elles n'y sont pas déjà quasiment parvenues. L'extension du SSO, du MFA ou des deux à l'IaaS (Infrastructure-as-a-Service) devrait faire un bond prodigieux dans les 12 à 18 mois, car les entreprises partout dans le monde cherchent à sécuriser l'accès à ces ressources essentielles. L'adoption devrait quant à elle plus que doubler d'ici 2023, passant de 31 % à 67 %.

Toutes les entreprises à l'échelle mondiale À quelles catégories de ressources avez-vous déjà étendu le SSO et/ou le MFA ? (Sélectionnez toutes les réponses pertinentes)

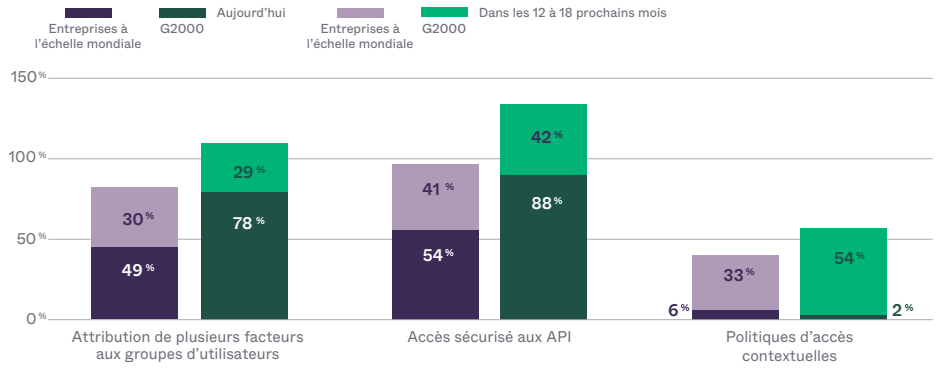


Phase 4 : modèle élevé

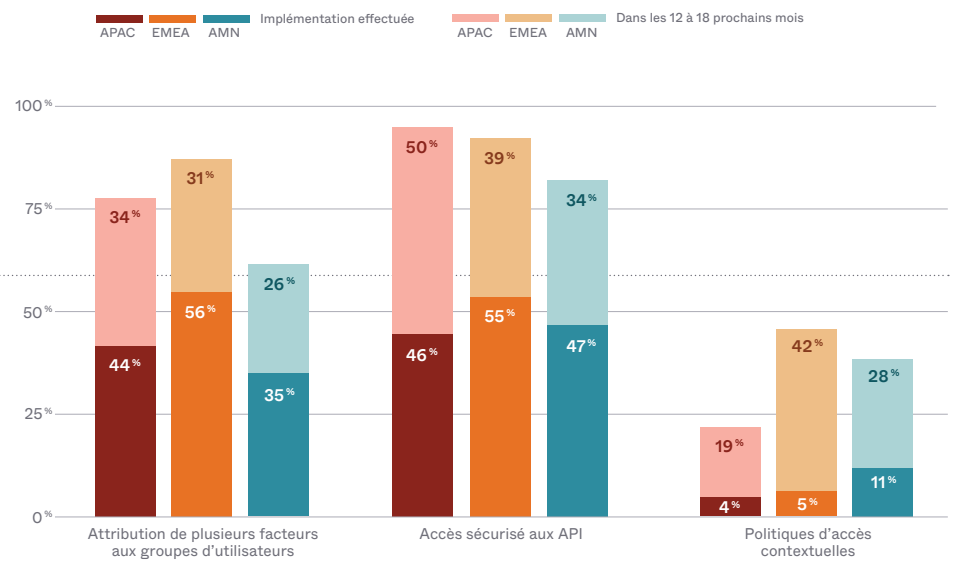
Les entreprises les plus avancées sur la courbe de maturité maîtrisent les fondamentaux de la sécurité Zero Trust basée sur l'identité, et disposent des outils et processus leur permettant de relever des défis liés à l'identité de plus en plus complexes. Nous avons mesuré les progrès réalisés dans les projets suivants de la phase 4 : les entreprises sont-elles prêtes à attribuer plusieurs facteurs d'authentification aux différents groupes d'utilisateurs pour réduire les points de friction, augmenter la productivité des effectifs à distance et prendre en charge une sécurité de type « ne jamais faire confiance, toujours vérifier » ? Ont-elles ajouté un accès sécurisé aux API ? Ont-elles implémenté des politiques d'accès contextuelles ?

Toutes les entreprises du classement Global 2000 interrogées pensent venir à bout de leurs projets liés à l'identité dans les 12 à 18 mois, notamment l'attribution de plusieurs facteurs aux différents groupes d'utilisateurs et la sécurisation de l'accès aux API. Au moins la moitié d'entre elles prévoient de finaliser la phase 4 dans les mêmes délais, en plaçant l'accent sur la définition de politiques d'accès contextuelles permettant de déterminer la fiabilité des terminaux au moment de la tentative d'accès, l'endroit où la tentative est effectuée, l'utilisateur et/ou la ressource concernés, et d'autres données critiques. Les entreprises interrogées de la zone Amérique du Nord sont pour l'instant en retard sur leurs homologues des régions APAC et EMEA en ce qui concerne les projets de déploiement de plusieurs facteurs aux groupes d'utilisateurs et de sécurisation de l'accès aux API, mais elles devraient progresser considérablement dans les mois qui viennent.

Toutes les entreprises à l'échelle mondiale et du classement Global 2000 — Quels projets votre entreprise a-t-elle déjà implémentés jusqu'à présent et quelles sont ses priorités dans les 12 à 18 prochains mois ?

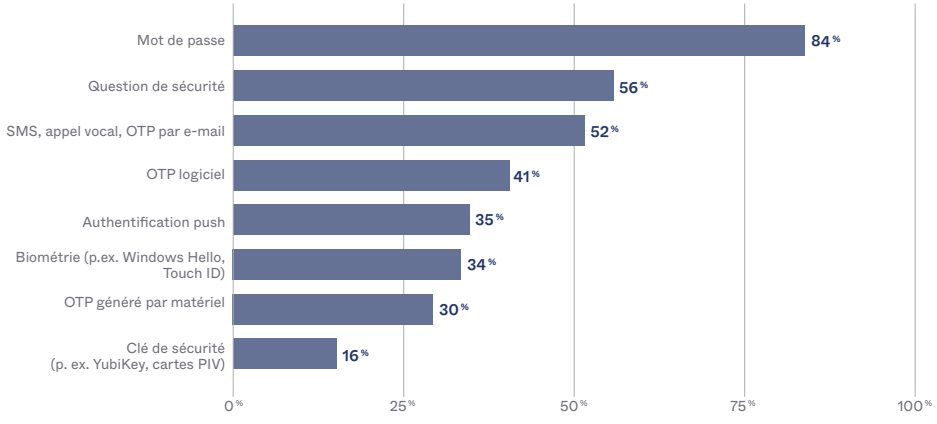


Phase 4 — Comparaison régionale Quels projets votre entreprise a-t-elle déjà implémentés jusqu'à présent et quelles sont ses priorités dans les 12 à 18 prochains mois ?



Sans surprise, les mots de passe continuent d'être le facteur de sécurité le plus utilisé, ce qui représente un problème récurrent, d'autant que la combinaison « 123456 » reste encore et toujours le mot de passe le plus courant[6]. Sur une note plus positive, d'après le rapport annuel d'Okta **Businesses at Work, 2022** publié plutôt cette année, les entreprises continuent de renforcer leur utilisation du MFA et remplacent peu à peu les facteurs à faible niveau d'assurance, comme les mots de passe, par d'autres facteurs à niveau d'assurance plus élevé. Le pourcentage des entreprises qui persistent à utiliser les mots de passe pour vérifier l'identité de leurs utilisateurs internes et externes a diminué de dix points cette année, passant à 84 %. Sur la même période, l'adoption d'une authentification push présentant des facteurs à niveau d'assurance plus élevé a augmenté de 20 points.

Toutes les entreprises à l'échelle mondiale Sélectionnez les facteurs d'authentification que votre entreprise utilise pour vérifier l'identité des utilisateurs internes et externes. (Sélectionnez toutes les réponses pertinentes)

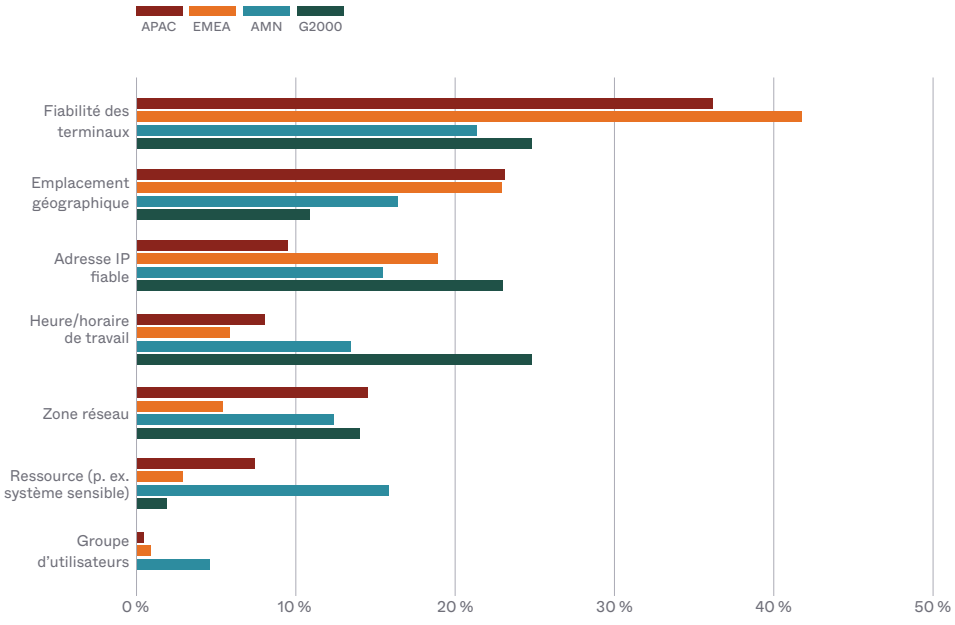


[6] Okta, « **Businesses at Work, 2022** »

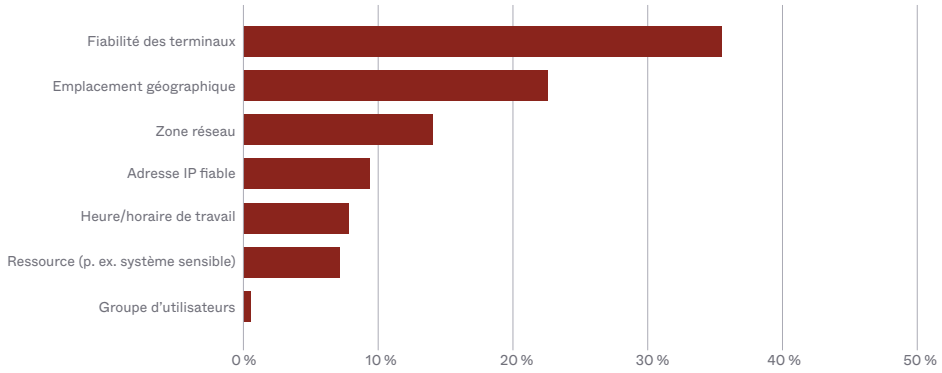
> “Les mots de passe compromis sont généralement la première étape de la chaîne de frappe d’une compromission. C’est la méthode employée par les cyberattaquants pour obtenir un accès initial avant de se déplacer latéralement dans le réseau, puis de procéder à une élévation des privilèges. L’utilisation des seuls mots de passe n’est plus une option viable ou défendable pour authentifier les identités et protéger nos ressources numériques.
>
> Trey Ray, Manager of Cybersecurity, FedEx

Dans le monde entier, les personnes interrogées citent les terminaux fiables, l’emplacement géographique et les adresses IP fiables en tant qu’attributs les plus importants pour la gestion et l’approbation des accès aux ressources internes. Dans toutes les régions, la fiabilité des terminaux (c’est-à-dire, le fait que le terminal soit géré, connu, vérifié et intègre) est l’attribut critique n° 1. Mais, il y a des variations régionales. Ainsi, les personnes interrogées dans la zone APAC estiment que la zone réseau est un attribut plus critique que la fiabilité des adresses IP, tandis qu’en Amérique du Nord, la ressource elle-même (par exemple une base de données sensible) est jugée aussi importante que l’emplacement géographique et la fiabilité des adresses IP. Parmi les entreprises du classement Global 2000, l’emplacement géographique est considéré comme un facteur bien moins critique. L’heure d’accès et la zone réseau sont considérées comme un peu plus importantes que la fiabilité des adresses IP, ce qui renvoie l’emplacement géographique en cinquième place des attributs les plus importants.

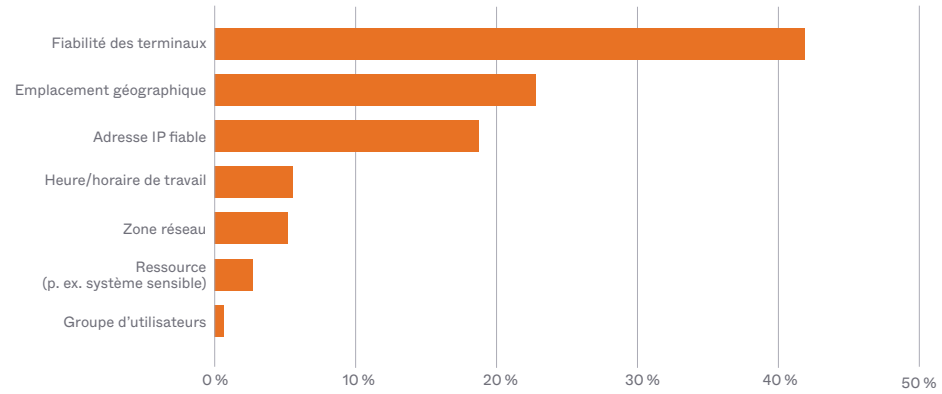
Comparaison régionale Classez les trois facteurs les plus critiques dans le contrôle et l’approbation des accès à vos ressources internes.



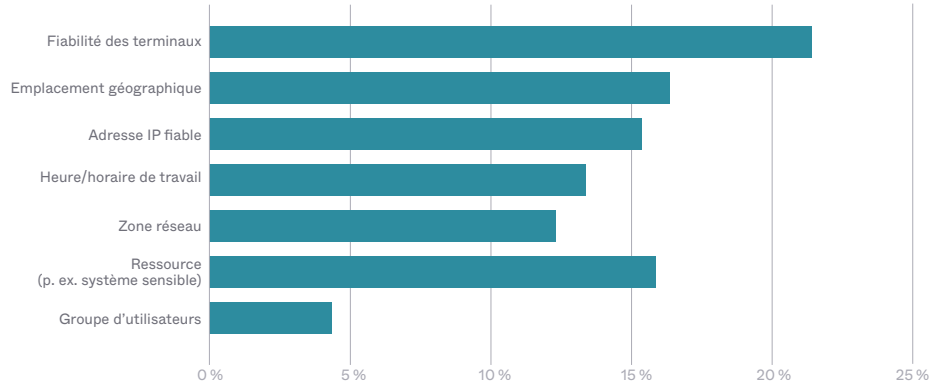
APAC Classez les trois facteurs les plus critiques dans le contrôle et l'approbation des accès à vos ressources internes.



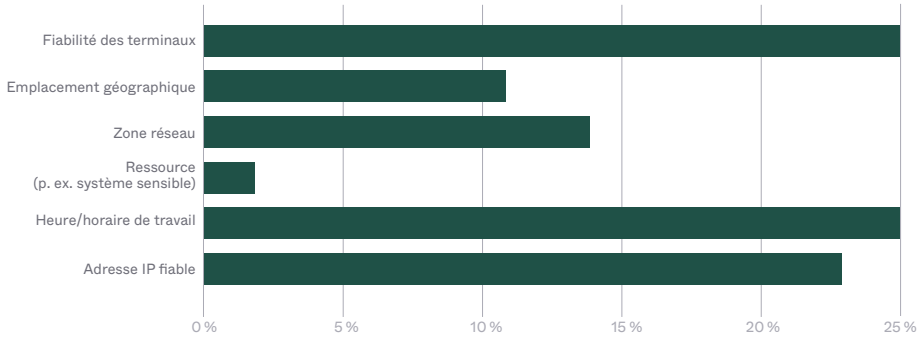
EMEA Classez les trois facteurs les plus critiques dans le contrôle et l'approbation des accès à vos ressources internes.



AMN Classez les trois facteurs les plus critiques dans le contrôle et l'approbation des accès à vos ressources internes.



Entreprises du classement Global 2000 Classez les trois facteurs les plus critiques dans le contrôle et l'approbation des accès à vos ressources internes.

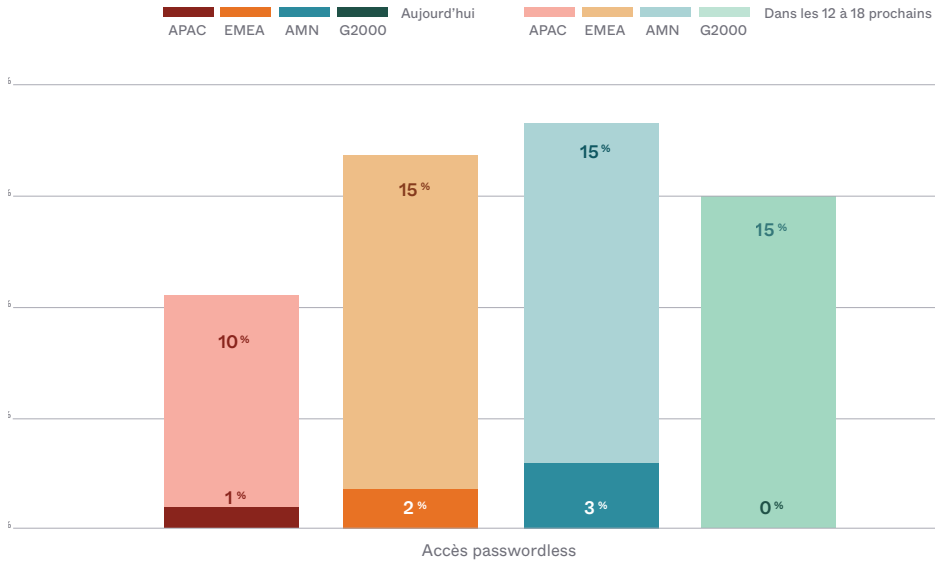


Phase 5 : modèle évolué

Les entreprises qui se trouvent en phase 5 ont déjà migré leurs opérations vers une plateforme cloud, comme Amazon Web Services (AWS), Google Cloud (GCP) ou Microsoft Azure. Elles se concentrent désormais sur l'automatisation et l'adoption d'une sécurité périphérique. Dans cette phase, l'accent n'est plus placé sur la mise en œuvre des projets Zero Trust clés présentés dans les phases précédentes, mais sur l'optimisation de la gestion du cycle de vie des utilisateurs, l'application d'un contrôle des accès sécurisé aux serveurs et l'implémentation d'un accès passwordless à l'aide de facteurs à niveau d'assurance élevé tels que les facteurs séquentiels, les connexions biométriques via Web Authentication (WebAuthn) et les clés de sécurité Universal 2nd Factor (U2F).

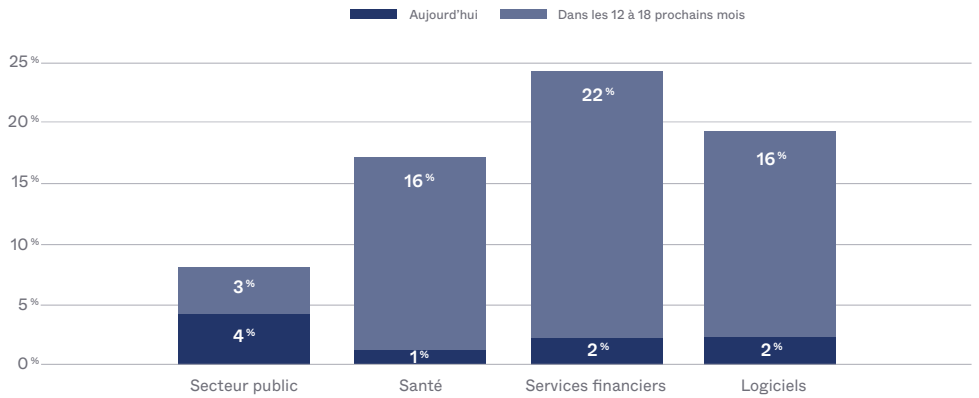
Constat encourageant : les entreprises interrogées dans toutes les régions prévoient d'accélérer l'adoption de l'accès passwordless sous 12 à 18 mois. Cette tendance est particulièrement positive compte tenu du fait que plus de la moitié des brèches de données actuelles impliquent des identifiants faibles ou volés, les compromissions d'identifiants étant en grande partie responsables de la hausse des attaques de ransomware et autres attaques basées sur l'identité[3]. Les entreprises nord-américaines sont en tête de peloton dans ce domaine. Elles sont plus nombreuses à proposer un accès passwordless, et de nombreuses entreprises interrogées dans cette région ont établi une feuille de route allant dans ce sens.

Comparaison régionale Offrez-vous déjà un accès passwordless ou prévoyez-vous de le faire dans les 12 à 18 prochains mois ?



Si l'on examine les données par secteur d'activité, près de 22 % des entreprises interrogées dans le secteur de services financiers indiquent qu'elles prévoient d'adopter l'accès passwordless dans les 12 à 18 mois, et 16 % dans les secteurs des soins de santé et des logiciels. Les organismes publics sont à la traîne, puisque seulement 7 % d'entre eux proposent déjà l'accès passwordless ou prévoient de le faire dans les mois qui viennent.

Comparaison sectorielle Offrez-vous déjà un accès passwordless ou prévoyez-vous de le faire dans les 12 à 18 prochains mois ?



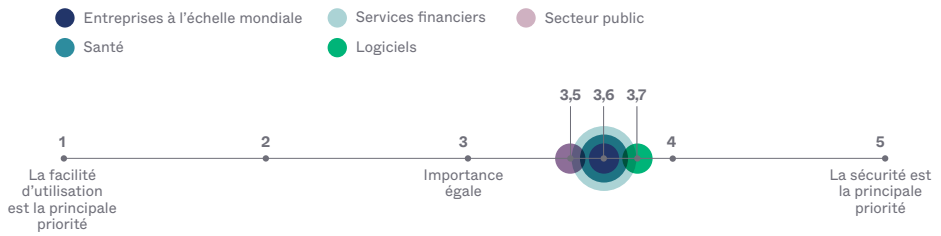
Secteurs d'activité

Progression du Zero Trust par secteur d'activité

Chaque secteur d'activité (et entreprise, bien entendu) possède ses propres pratiques, priorités et obligations, et tend de ce fait à emprunter un parcours Zero Trust légèrement différent. Dans notre enquête 2022, nous avons examiné plus en détail quatre secteurs d'activité clés : les soins de santé, les services financiers, les logiciels et, pour la première fois, les organismes publics. Notre but était de mieux cerner l'influence des besoins uniques des entreprises dans ces secteurs sur l'adoption de solutions Zero Trust. En particulier, nous avons souhaité découvrir comment ces secteurs parviennent à équilibrer ces impératifs souvent contradictoires que sont la sécurité et la facilité d'utilisation.

De fait, les entreprises parviennent à concilier ces deux exigences. Il est intéressant de noter que les personnes interrogées cette année accordent, en moyenne, une légère priorité à la sécurité par rapport à la facilité d'utilisation — une nouveauté par rapport à 2021 où cette dernière dépassait de peu la sécurité. Par exemple, des secteurs comme celui des soins de santé réduisent leur dépendance à l'égard des facteurs à faible niveau d'assurance comme les mots de passe, qui sont très vulnérables aux attaques basées sur les identifiants. Dans tous les secteurs d'activité ciblés, les entreprises citent les mêmes quatre principaux défis à l'implémentation d'une stratégie de sécurité Zero Trust : en 2022, le plus grand défi est la pénurie de talents et de compétences, suivie par l'adhésion des parties prenantes, les coûts et la sensibilisation à l'importance des solutions de sécurité appuyant le Zero Trust.

Quelle importance relative accordez-vous respectivement à la sécurité et à la facilité d'utilisation au sein de votre entreprise ?

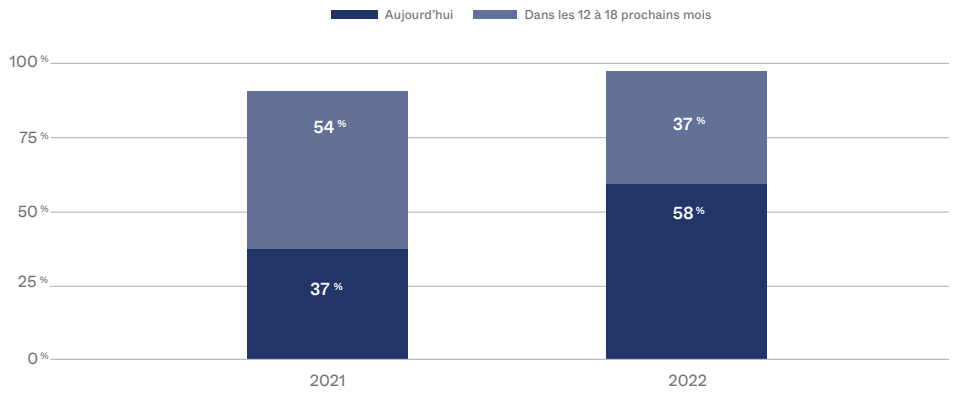


Secteurs clés

Santé

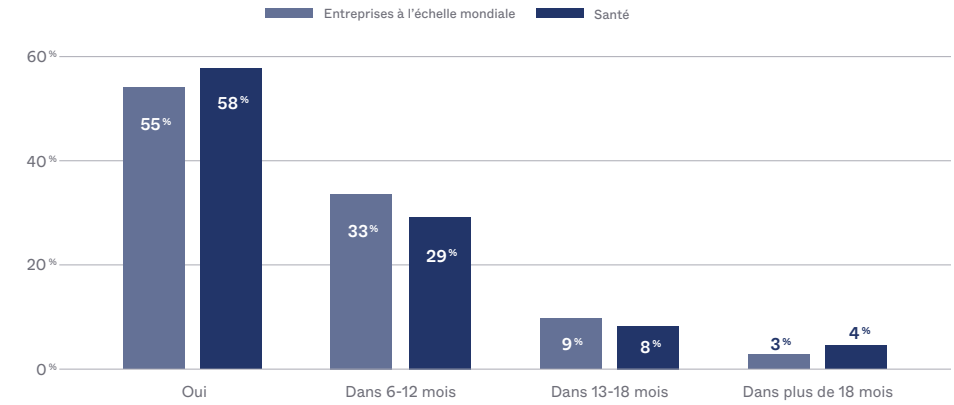
Les dernières entreprises du secteur des soins de santé qui n'ont pas encore adopté le Zero Trust ont au moins élaboré des plans allant dans ce sens. Le pourcentage des entreprises interrogées ayant mis en place une initiative Zero Trust ou prévoyant de le faire au cours des 12 à 18 prochains mois est passé de 91 % en 2021 à 96 % en 2022. 58 % des entreprises de ce secteur ont déjà commencé à implémenter leurs projets Zero Trust, ce qui représente une augmentation de près de 21 points par rapport à l'année dernière (37 %). La majorité des entreprises interrogées n'ayant pas encore défini d'initiative Zero Trust prévoient de le faire sous 6 à 12 mois, ce qui reste dans la logique d'une exécution à court terme.

Comparaison annuelle — Santé Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les 12 à 18 prochains mois ?

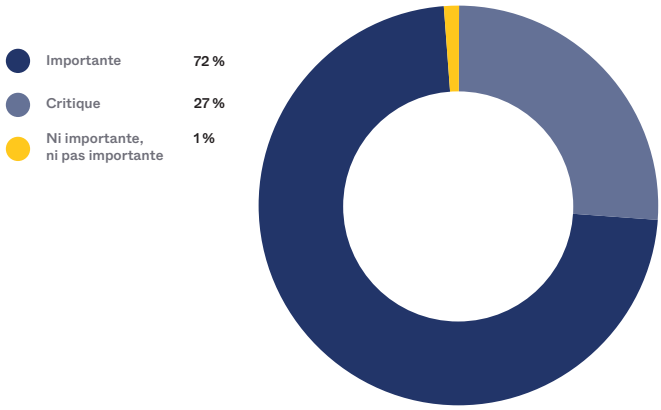


98 % affirment que l'identité joue un rôle significatif dans leur stratégie globale de sécurité Zero Trust. Dans ce pourcentage, 72 % estiment que l'identité est importante et 27 % qu'elle est critique. En outre, ils mettent ces stratégies en pratique : la majorité des entreprises interrogées dans ce secteur ont déjà lancé une initiative Zero Trust, et la plupart des autres prévoient d'en démarrer une dans les 6 à 12 mois. Les principaux projets liés à l'identité qu'elles comptent mener à bien dans ce laps de temps comprennent l'extension du SSO aux collaborateurs et la sécurisation de l'accès aux API.

Comparaison — Toutes les entreprises à l'échelle mondiale vs. le secteur de la santé Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les mois qui viennent ?

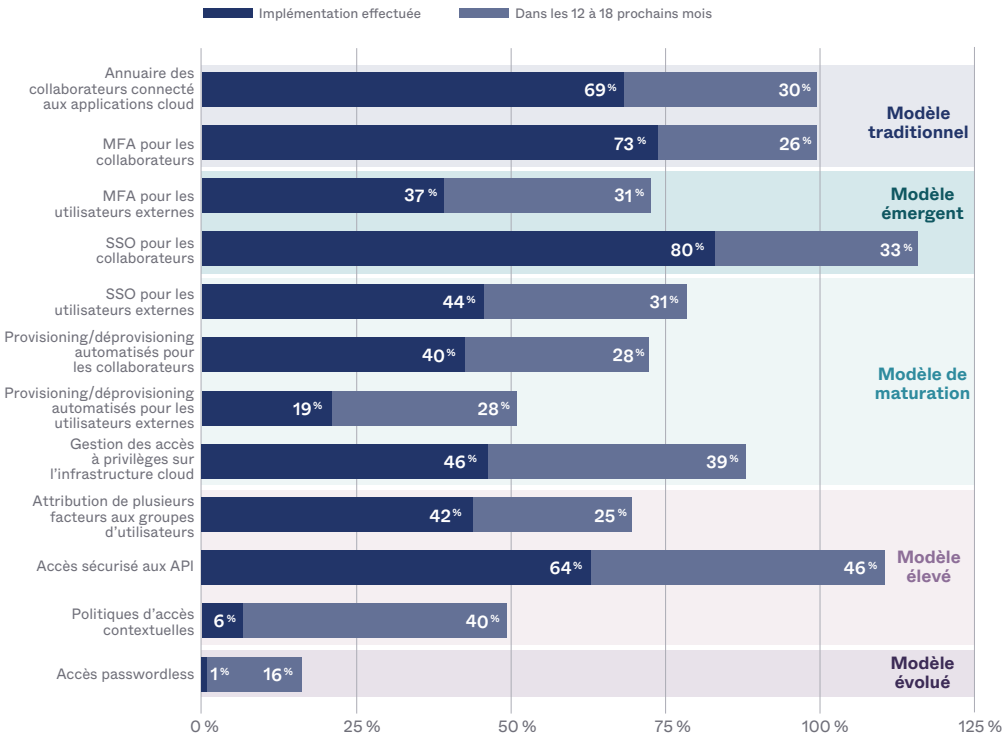


Santé Quelle est l'importance de l'identité dans votre stratégie de sécurité Zero Trust ?

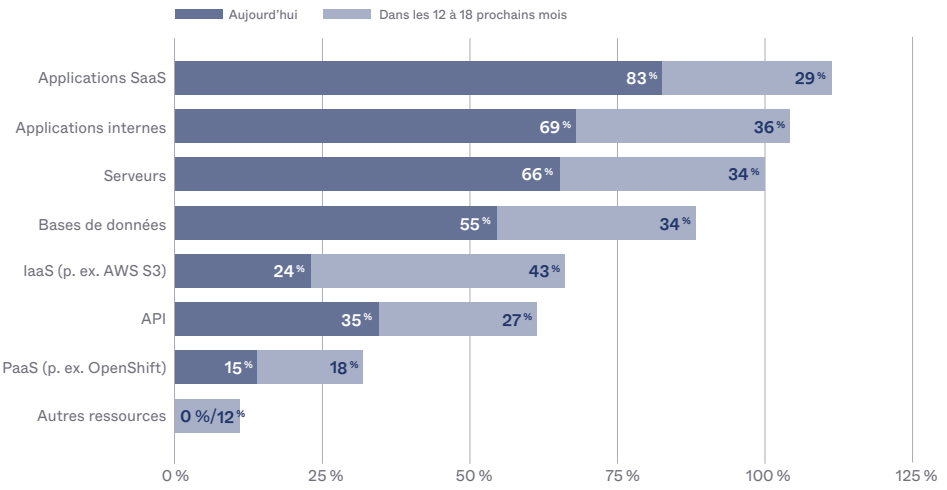


Mais, dans ce secteur, l'une des plus grandes avancées dans les mois à venir sera l'ajout de politiques d'accès contextuelles : seules 6 % des entreprises interrogées déclarent avoir déjà mis en place ces politiques, mais 40 % d'entre elles prévoient de les déployer dans les 12 à 18 mois à venir. Toutes les personnes interrogées dans ce secteur déclarent que leur entreprise planifie d'étendre le SSO, le MFA ou les deux aux applications SaaS, aux applications internes et aux serveurs dans un délai de 12 à 18 mois. Elles accordent également beaucoup d'importance à l'IaaS. Le nombre des entreprises interrogées qui pensent étendre le SSO, le MFA ou les deux à cette catégorie de ressources devrait presque tripler dans les mois qui viennent.

Santé Parmi les initiatives suivantes, lesquelles votre entreprise a-t-elle déjà implémentées ou prévoit-elle d'implémenter dans les 12 à 18 prochains mois ?

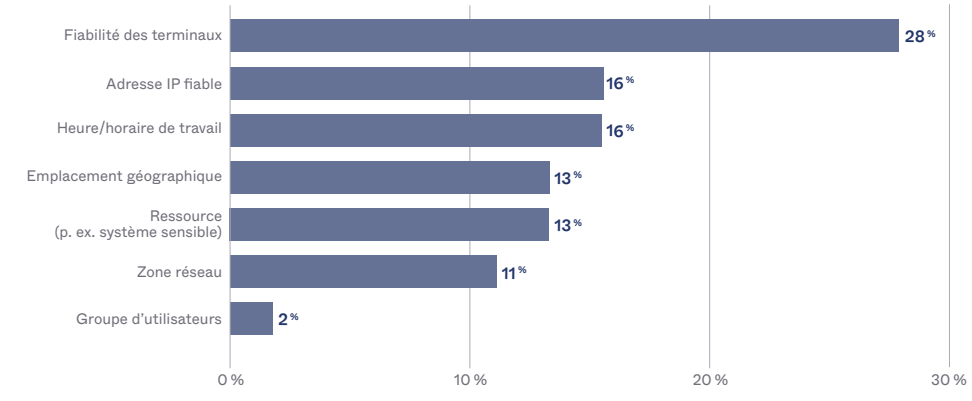


Santé À quelles catégories de ressources avez-vous déjà étendu le SSO et/ou le MFA ?



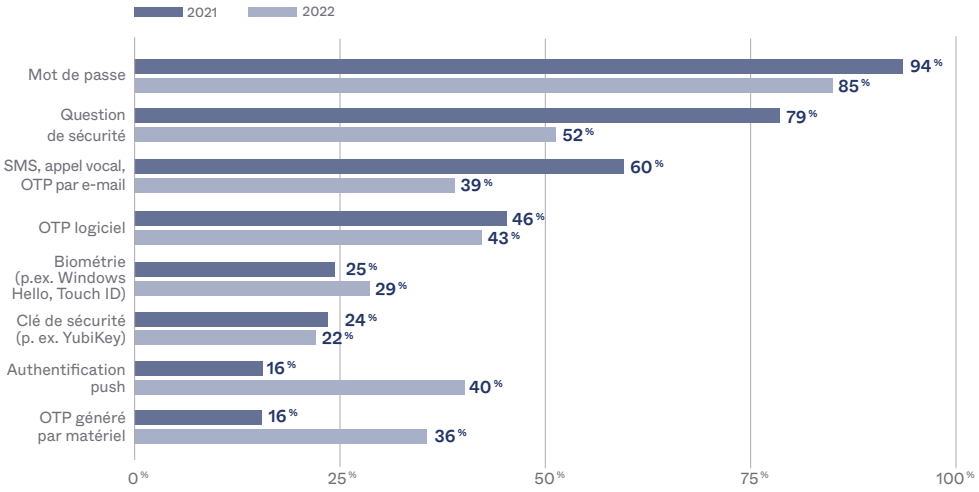
Dans ce secteur, en 2022, les trois facteurs jugés les plus critiques pour contrôler et approuver l'accès aux ressources internes sont la fiabilité des terminaux, l'emplacement géographique et la fiabilité des adresses IP. Bien que la fiabilité des terminaux arrive largement en tête des priorités mentionnées, d'autres facteurs sont presque aussi importants : l'heure, l'horaire de travail et la ressource elle-même (par exemple si elle très sensible).

Santé Indiquez le facteur principal dans le contrôle et l'approbation des accès à vos ressources internes.



D'une année à l'autre, le pourcentage des établissements de soins de santé qui utilisent des mots de passe (faible niveau d'assurance) a baissé, tandis que l'adoption de l'authentification push (niveau d'assurance plus élevé) est passée de 16 % l'année dernière à plus de 40 % cette année, ce qui représente une augmentation bienvenue.

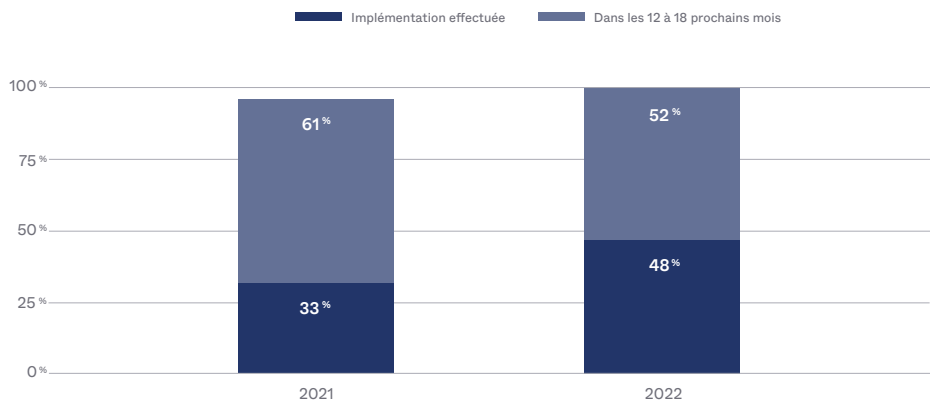
Comparaison annuelle — Santé Sélectionnez les facteurs d'authentification que votre entreprise utilise actuellement pour vérifier l'identité des utilisateurs internes et externes.



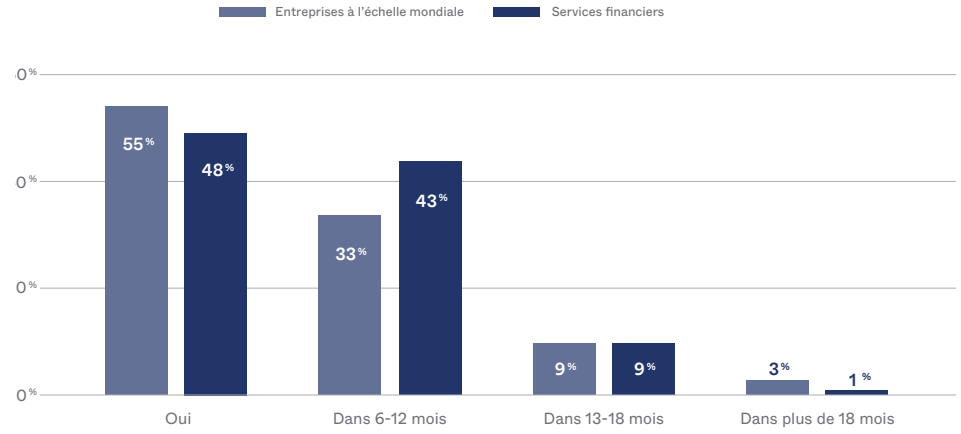
Services financiers

Dans le secteur des services financiers, le Zero Trust est clairement dans tous les esprits : presque 100 % des entreprises interrogées déclarent qu'elles prévoient de lancer dans les 12 à 18 mois une initiative en vue de son adoption. En fait, près de la moitié des entreprises interrogées (48 %) ont déjà mis en place ce type de projet, contre environ un tiers l'année dernière, ce qui représente une augmentation bienvenue de 15 points.

Comparaison annuelle — Services financiers Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les 12 à 18 prochains mois ?

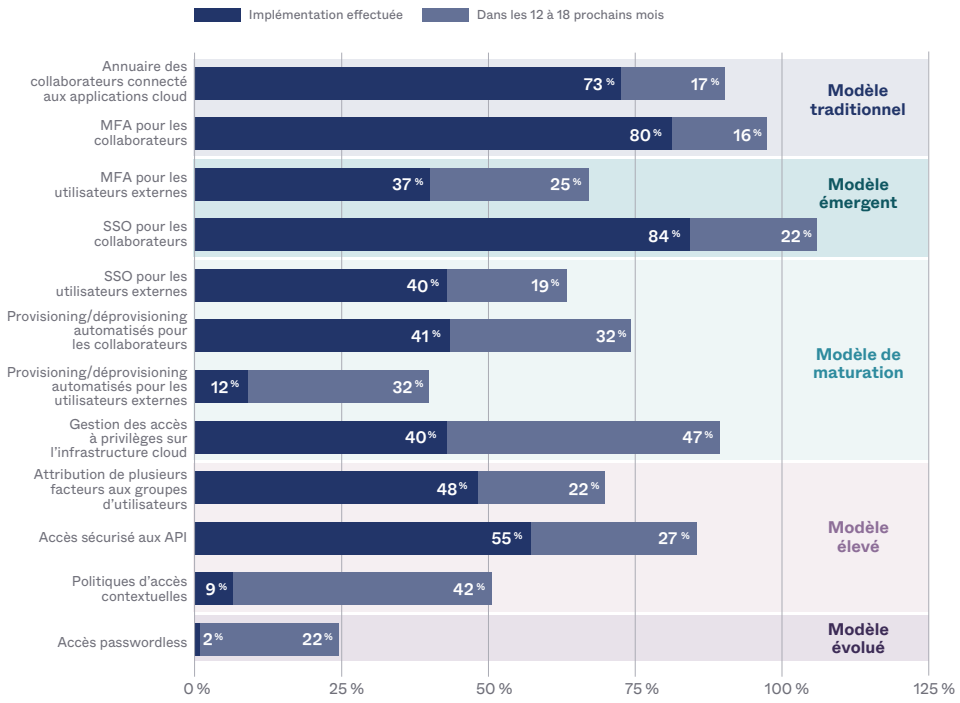


Comparaison — Toutes les entreprises à l'échelle mondiale vs. le secteur des services financiers
Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les mois qui viennent ?



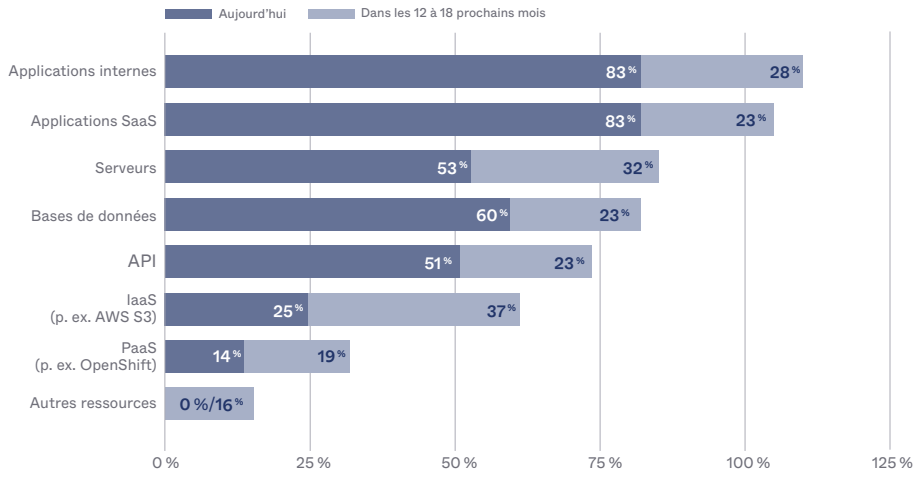
Dans la plupart des cas, les travaux de définition de ces projets sont d'ailleurs déjà en cours. La grande majorité des entreprises financières interrogées n'ayant encore mis en place aucune initiative Zero Trust prévoient de le faire dans les 6 à 12 prochains mois. Globalement, si ce secteur peut sembler à l'heure actuelle légèrement en retard dans sa maturité Zero Trust par rapport à d'autres secteurs, les établissements financiers ont élaboré des plans spécifiques et actifs pour progresser de façon significative et rattraper ce retard à court terme.

Services financiers Parmi les initiatives suivantes, lesquelles votre entreprise a-t-elle déjà implémentées ou prévoit-elle d'implémenter dans les 12 à 18 prochains mois ?



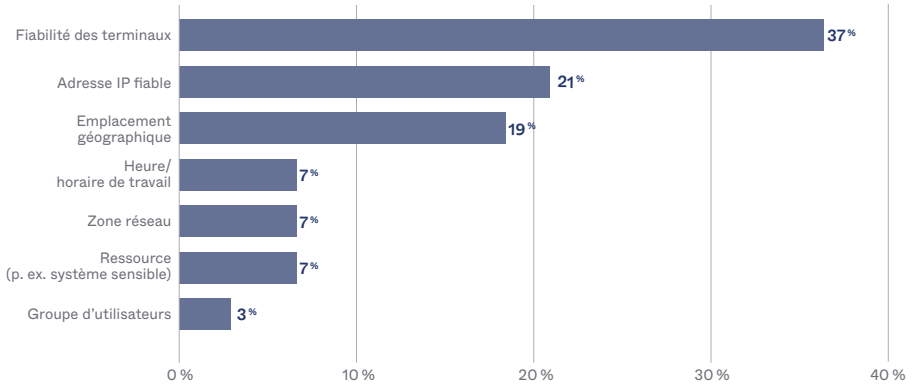
Toutes les entreprises de services financiers que nous avons interrogées ont déjà étendu le SSO, le MFA ou les deux aux applications SaaS et internes, ou prévoient de le faire dans les 12 à 18 mois. Plus précisément, elles entendent augmenter leurs facteurs de vérification lors de l'authentification. Cela signifie étendre autant que possible le SSO à tous les terminaux, y compris pour accéder aux applications SaaS et on-premise, et adopter le MFA chaque fois que c'est possible, en particulier sur les applications sensibles qui traitent des paiements et des mouvements, ainsi que pour tous les accès à privilèges. L'IaaS est un autre projet lié à l'identité sur lequel les établissements de services financiers prévoient de se concentrer dans les mois qui viennent. Les plans déjà en place actuellement permettraient de plus que doubler le taux actuel d'adoption de l'IaaS d'ici fin 2023. Dans l'ensemble, près de 75 % des établissements financiers, si ce n'est plus, comptent étendre le SSO, le MFA ou les deux aux serveurs, aux bases de données et aux API dans les 18 prochains mois.

Services financiers À quelles catégories de ressources avez-vous déjà étendu le SSO et/ou le MFA, ou prévoyez-vous de le faire dans les 12 à 18 prochains mois ?

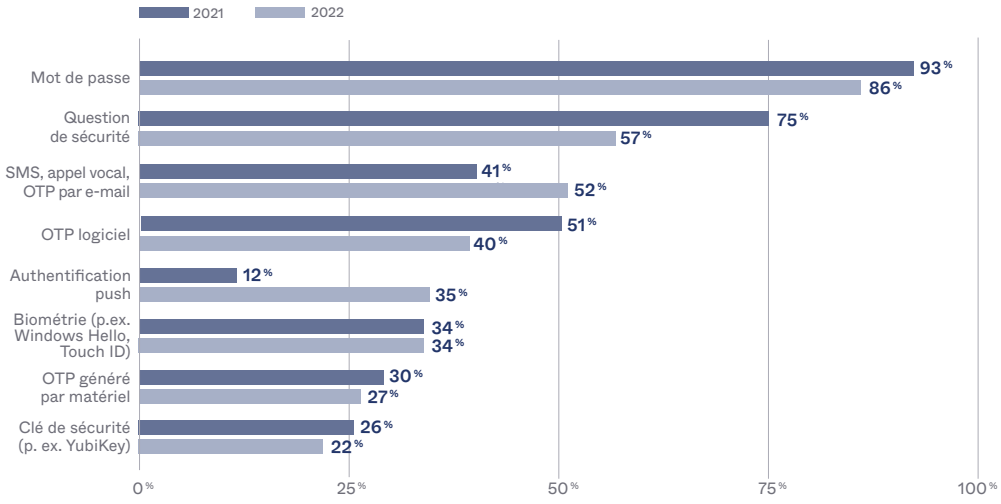


Pour les personnes interrogées dans ce secteur, la fiabilité des terminaux est le facteur le plus critique pour contrôler et approuver l'accès aux ressources internes. Plus de 36 % d'entre elles le citent comme leur facteur d'authentification n° 1. Le pourcentage des entreprises utilisant des mots de passe et des questions de sécurité comme facteurs d'authentification a diminué depuis l'année dernière, tandis que l'on constate une augmentation de plus de 20 points des entreprises qui utilisent l'authentification push, un facteur à niveau d'assurance plus élevé.

Services financiers Classez les facteurs les plus critiques dans le contrôle et l'approbation des accès à vos ressources internes.



Comparaison annuelle — Services financiers Sélectionnez les facteurs d'authentification que votre entreprise utilise actuellement pour vérifier l'identité des utilisateurs internes et externes.

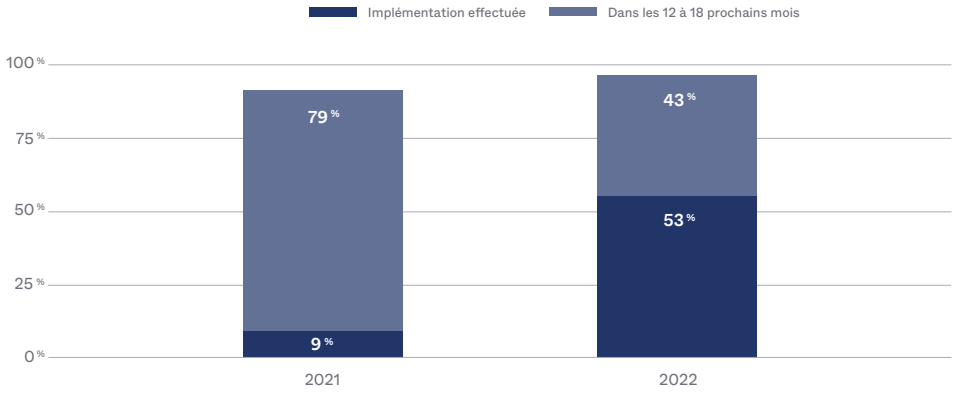


Logiciels

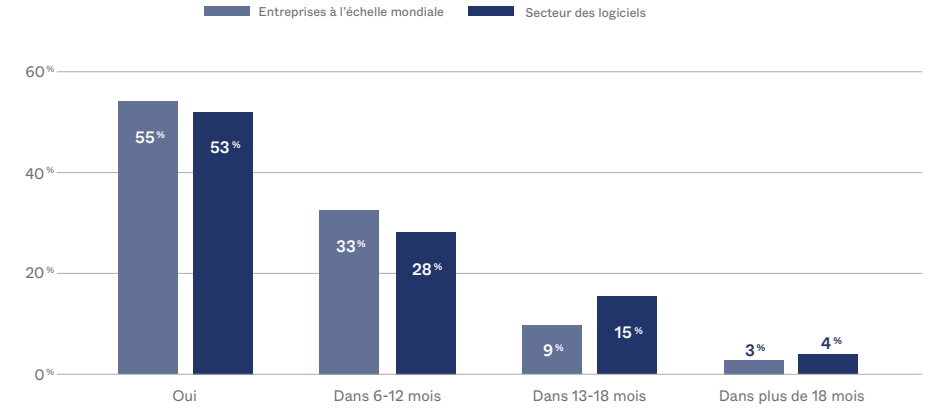
Dans le rapport de l'année dernière, le secteur des logiciels était nettement à la traîne par rapport aux autres secteurs cibles de notre enquête. Cependant, les entreprises interrogées exprimaient une forte détermination à réaliser des progrès significatifs dans les initiatives de sécurité Zero Trust au cours des 12 à 18 mois suivants. Elles y sont parvenues avec brio. En 2021, seulement 9 % d'entre elles avaient déjà mis en place une initiative Zero Trust et 79 % prévoyaient d'en lancer une. Cette année, le nombre d'entreprises ayant une initiative en cours a presque atteint les 53 %, et près de 43 % d'entre elles pensent définir un projet dans les 12 à 18 prochains mois, ce qui signifie que 96 % des entreprises de ce secteur ont

au moins commencé leur parcours. Nous constatons la même progression rapide dans l'adoption de la sécurité Zero Trust : les éditeurs de logiciels ont l'intention d'agir rapidement. Ils ont accéléré l'élaboration de leur stratégie Zero Trust et prévoient généralement de l'implémenter sous 6 à 12 mois.

Comparaison annuelle — Logiciels Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les 12 à 18 prochains mois ?

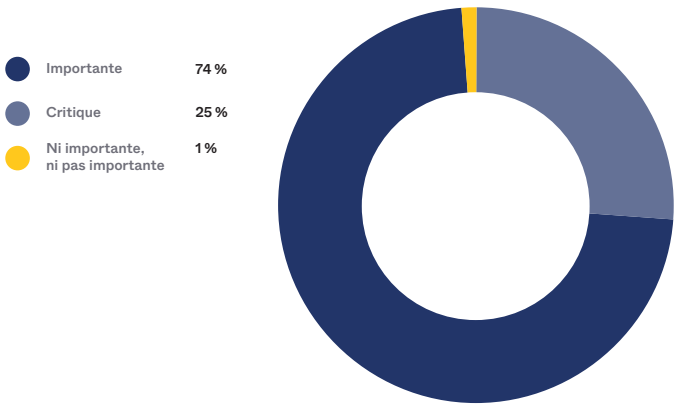


Comparaison — Toutes les entreprises à l'échelle mondiale vs. le secteur des logiciels Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les mois qui viennent ?



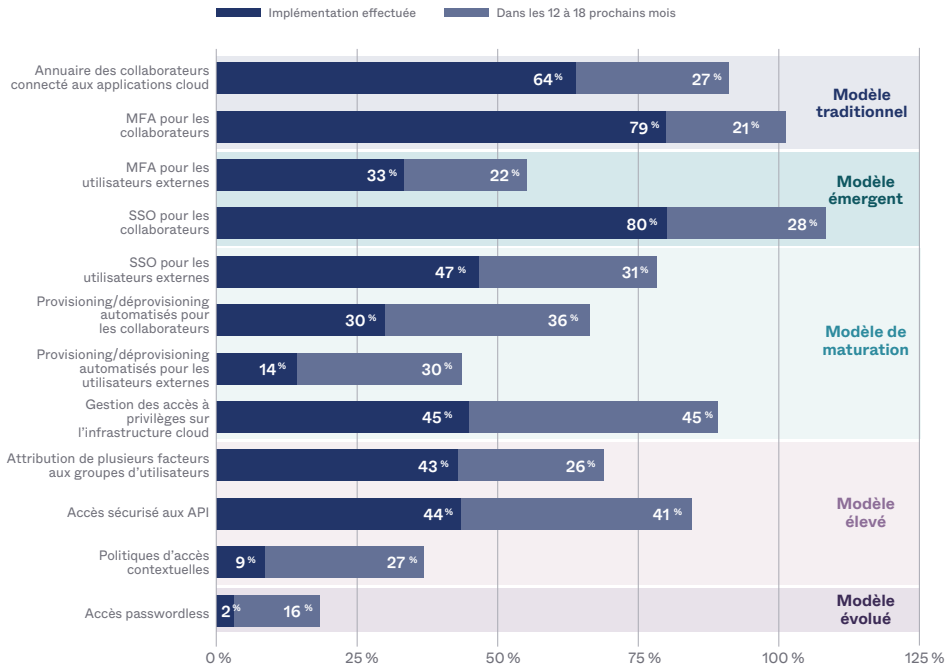
Parmi les entreprises interrogées dans le secteur, 99 % ont déclaré que l'identité était importante ou critique dans leur stratégie Zero Trust globale, 25 % d'entre elles la déclarant critique pour leur activité.

Logiciels Quelle est l'importance de l'identité dans votre stratégie de sécurité Zero Trust ?

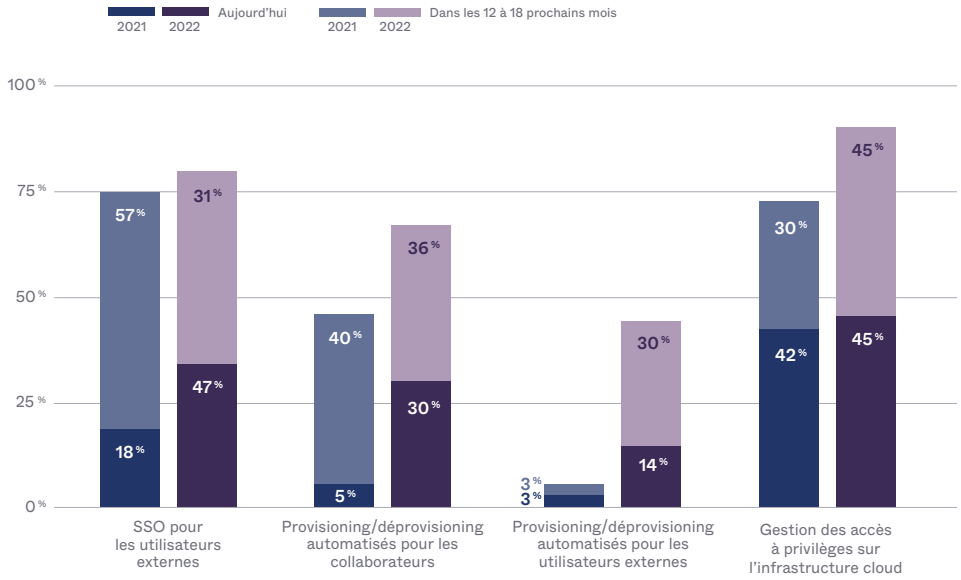


De tous les secteurs interrogés, les entreprises du secteur des logiciels sont celles qui ont le plus avancé d'une année à l'autre dans la phase 3 de la courbe de maturité. Elles ont bien progressé dans l'adoption de projets liés à l'identité, en implémentant le SSO pour les utilisateurs externes, et en automatisant le provisioning et le déprovisioning de tous les utilisateurs. Une belle réussite. Près de 100 % des entreprises du secteur interrogées indiquent qu'elles planifient la mise en place d'un accès à privilèges sur l'infrastructure cloud d'ici fin 2023.

Logiciels Parmi les initiatives suivantes, lesquelles votre entreprise a-t-elle déjà implémentées ou prévoit-elle d'implémenter dans les 12 à 18 prochains mois ?

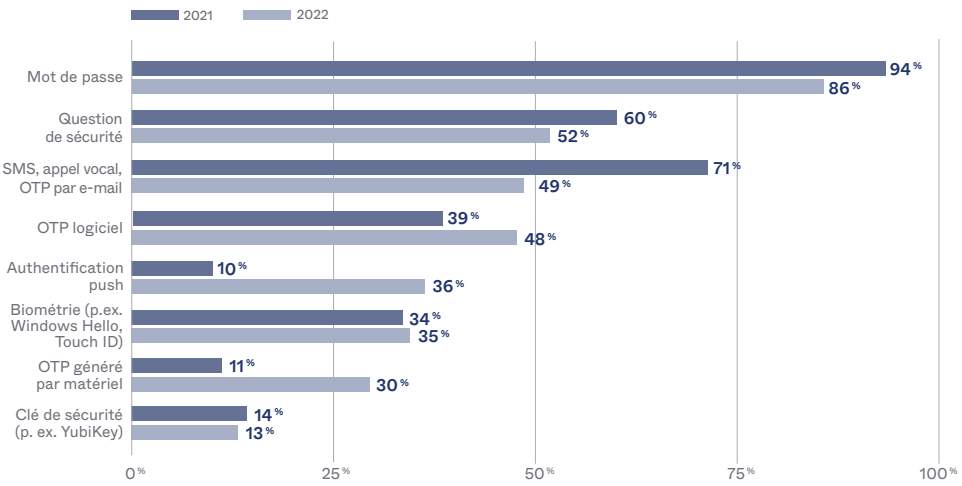


Phase 3 — Comparaison annuelle — Logiciels Parmi les initiatives suivantes, lesquelles votre entreprise a-t-elle déjà implémentées ou prévoit-elle d'implémenter dans les 12 à 18 prochains mois ?



Les facteurs d'authentification à faible niveau d'assurance, notamment les mots de passe, les questions de sécurité, les SMS, les appels vocaux et les e-mails, ont connu un léger recul par rapport à 2021, tandis que l'authentification push a connu une hausse significative.

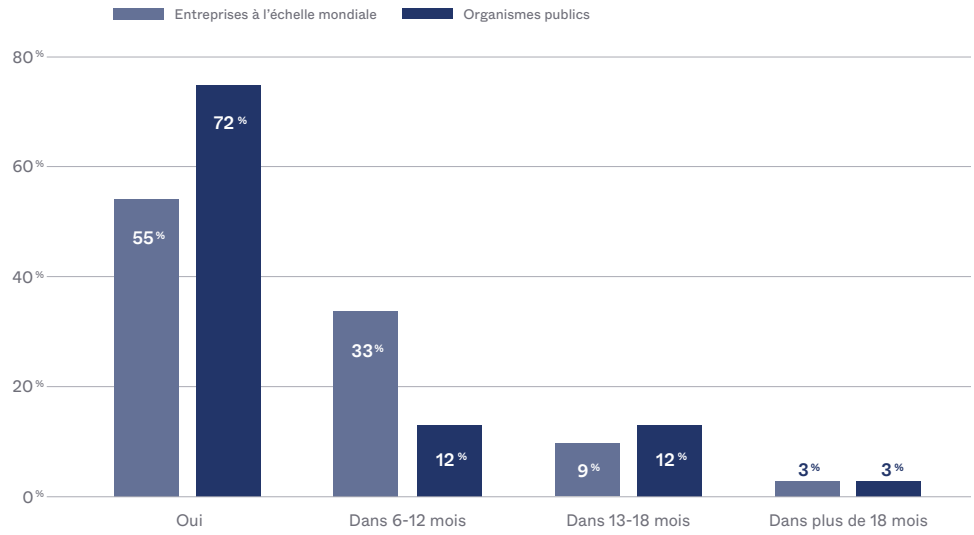
Logiciels Sélectionnez les facteurs d'authentification que votre entreprise utilise actuellement pour vérifier l'identité des utilisateurs internes et externes.



Secteur public

Les organismes du secteur public sont généralement en avance sur leurs homologues d'autres secteurs dans l'adoption d'initiatives Zero Trust. Ils ont en outre déjà planifié leur progression régulière sur la courbe de maturité en adoptant des projets spécifiques liés à l'identité visant à soutenir leur stratégie Zero Trust, qu'ils exécuteront dans les mois qui viennent. Aux États-Unis, les mandats gouvernementaux récents exigeant des actions rapides et décisives en matière de cybermodernisation (pas seulement des améliorations progressives), notamment des actions précises que les agences fédérales doivent mettre en œuvre dans un avenir proche, ont largement contribué à accélérer la transformation des organismes de services publics. D'autres organismes publics mondiaux sont aussi en train de revoir leur approche des impératifs Zero Trust. Au Royaume-Uni, par exemple, le National Cyber Security Centre a publié un outil pratique définissant huit principes de conception d'une architecture Zero Trust, avec des recommandations axées sur l'identité comme « ne faites confiance à aucun réseau, y compris au vôtre[7] ».

Comparaison — Toutes les entreprises à l'échelle mondiale vs. tous les organismes publics
Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les mois qui viennent ?

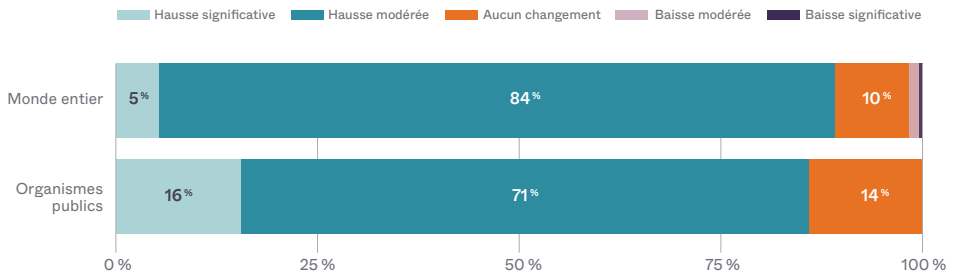


Dans le monde entier, ces 12 derniers mois, un pourcentage plus élevé d'organismes publics ont bénéficié d'une augmentation significative de leur budget afin de soutenir des projets Zero Trust. Dans le cas du gouvernement des États-Unis, la **stratégie Zero Trust fédérale** de la Maison-Blanche ne dispose d'aucun financement, mais les organismes intéressés peuvent demander des fonds du Technology Modernization Fund (TMF)[8] pour soutenir leurs initiatives.

[7] « Zero Trust Architecture Design Principles », National Cyber Security Centre, 23 juillet 2021, Ncsc.gov.uk/collection/zero-trust-architecture/dont-trust-any-network, page au 10 août 2022

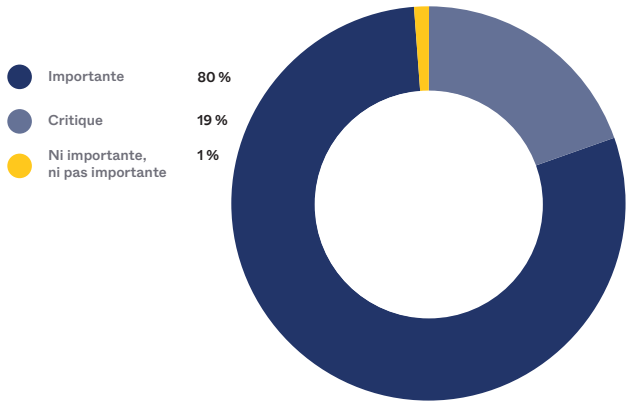
[8] FCW.com, « **How the TMF Helps Agencies Pave the Way Toward Zero Trust** », 2022

Comparaison — Toutes les entreprises à l'échelle mondiale vs. tous les organismes publics
Comment votre budget Zero Trust a-t-il évolué (le cas échéant) dans les 12 derniers mois ?



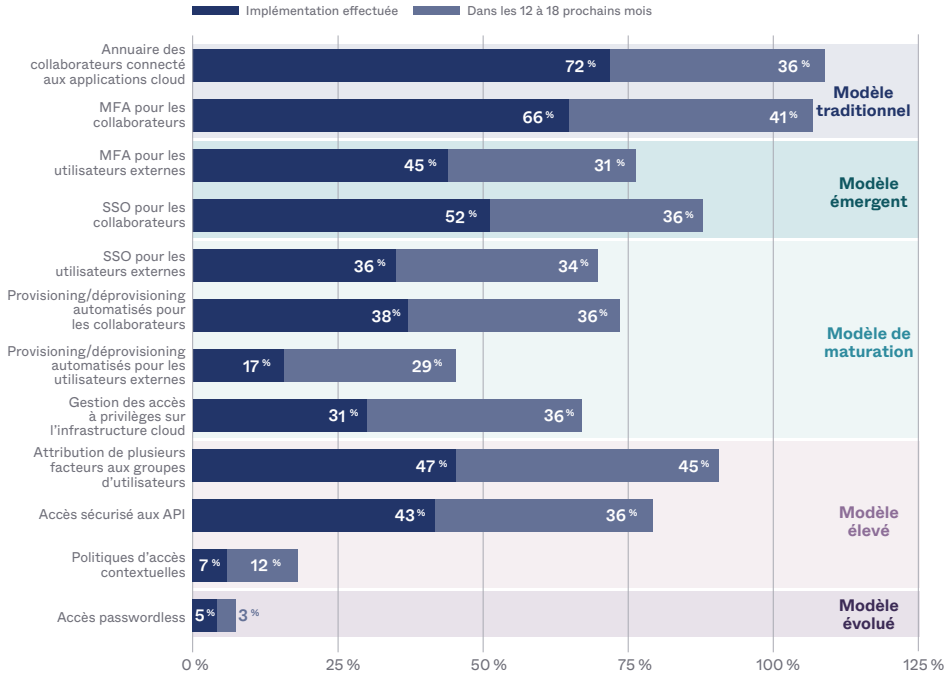
La plupart des organismes publics interrogés dans le monde déclarent que l'identité est importante pour leur stratégie Zero Trust globale, 19 % d'entre eux la jugeant critique. (Aux États-Unis, une nouvelle stratégie Zero Trust fédérale impose qu'un MFA antiphishing soit utilisé pour les effectifs des services publics et constitue une option possible pour les usagers.) En outre, dans le **modèle de maturité Zero Trust du CISA**, l'identité est le premier pilier de la sécurité Zero Trust, ce qui correspond au pilier « Utilisateurs » de l'architecture de référence Zero Trust du ministère américain de la Défense.

Organismes publics Quelle est l'importance de l'identité dans votre stratégie de sécurité Zero Trust ?

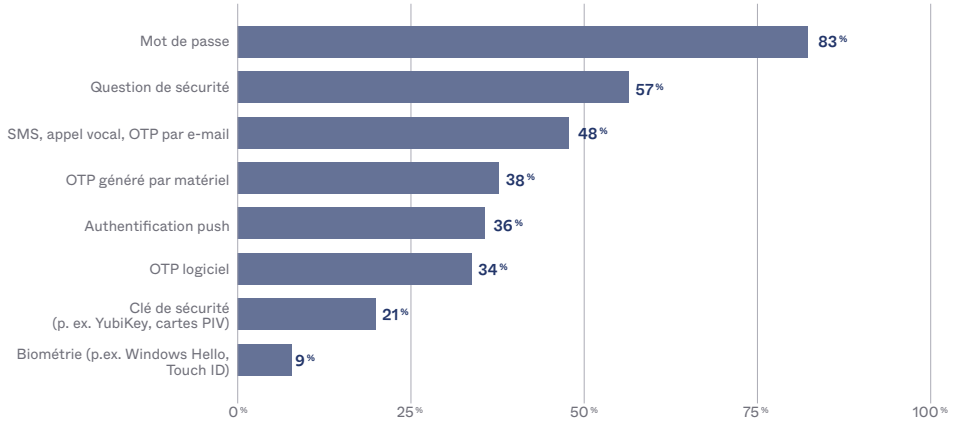


Les organismes publics interrogés prévoient de réaliser des progrès significatifs sur la courbe de maturité dans les 12 à 18 mois. Plus précisément, ils comptent quasiment doubler leur progression dans 6 des 12 projets liés à l'identité de la courbe de maturité, en donnant la priorité à des initiatives telles que le déploiement du MFA pour les collaborateurs et les groupes d'utilisateurs. Par rapport aux autres secteurs d'activité, les services publics semblent avoir pris du retard dans les projets des premières phases de la courbe de maturité, tels que le MFA et le SSO, mais ils se montrent déterminés à adopter ces technologies et à travailler sur de nombreux autres projets dans les mois à venir.

Organismes publics Parmi les initiatives suivantes, lesquelles votre entreprise a-t-elle déjà implémentées ou prévoit-elle d'implémenter dans les 12 à 18 prochains mois ?



Organismes publics Sélectionnez les facteurs d'authentification que votre entreprise utilise actuellement pour vérifier l'identité des utilisateurs internes et externes.



Le Zero Trust aujourd'hui

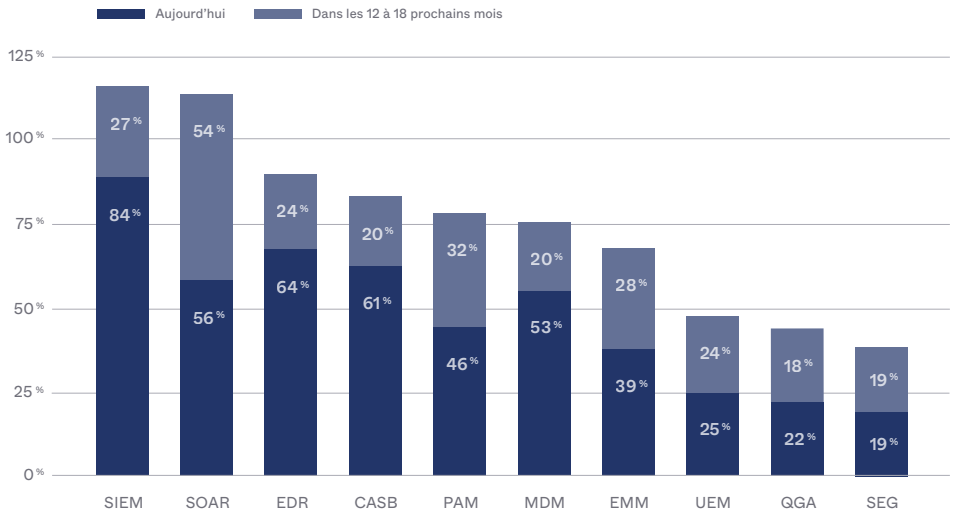
L'écosystème de sécurité axée sur l'identité d'aujourd'hui

Aucune solution ne peut à elle seule prendre en compte tous les aspects des recommandations Zero Trust promues par Forrester, le NIST (National Institute of Standards and Technology) et d'autres organismes. Cependant, l'identité s'est imposée comme une technologie incontournable dans l'ensemble de la pile de sécurité, et il devient de plus en plus clair qu'elle doit être au cœur de la planification de la sécurité, plutôt qu'un élément à ajouter par la suite.

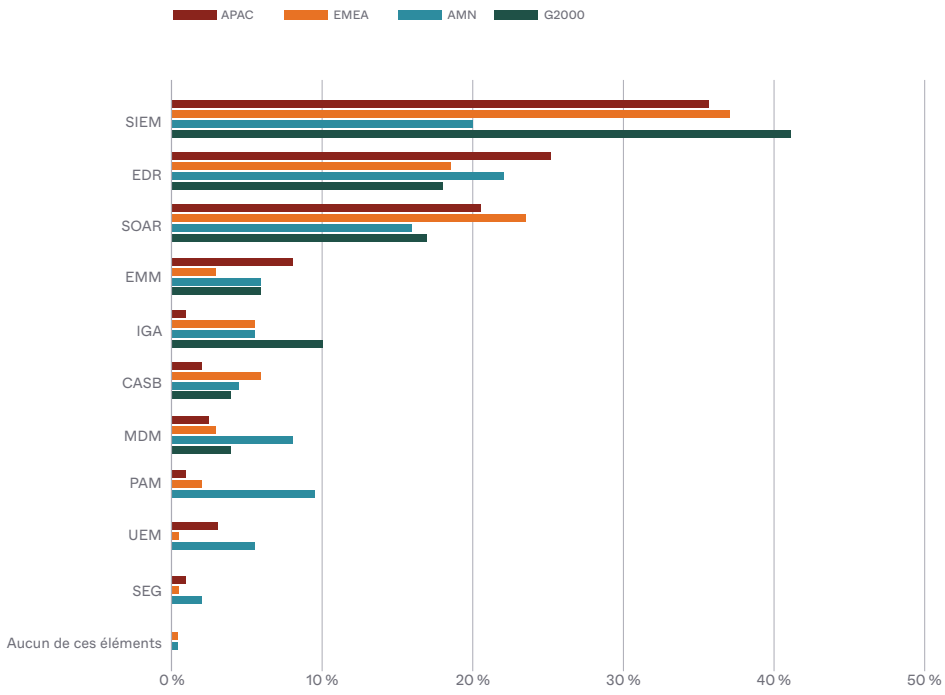
La protection Zero Trust mise en place est plus efficace si l'entreprise parvient à intégrer sa solution IAM à l'ensemble de son architecture de sécurité : gestion des événements de sécurité (SIEM), orchestration et automatisation (SOAR), gestion de la mobilité d'entreprise (EMM), gestion des appareils mobiles (MDM), CASB (Cloud Access Security Broker) et gestion des accès à privilèges (PAM). Par exemple, en coordonnant l'IAM avec le SIEM, les entreprises peuvent trier intelligemment les événements de sécurité potentiels. En intégrant l'IAM au SOAR, elles peuvent bénéficier de réponses de sécurité automatisées mieux informées. En intégrant l'IAM à l'EDR, elles peuvent utiliser l'identité pour corréler de manière centralisée des points de données indépendants qui, ensemble, indiquent qu'une attaque est en cours.

Nous avons demandé aux responsables sécurité quels outils doivent, selon eux, être absolument intégrés à leur solution IAM pour soutenir une sécurité Zero Trust. Dans la plupart des régions, et pour plus de 40 % des entreprises du classement Global 2000 interrogées, le SIEM est cité comme l'élément le plus critique à intégrer. La seule région qui n'a pas désigné le SIEM est l'Amérique du Nord, où l'EDR est mentionné avec une légère avance. En termes d'intégrations IAM actuelles, les solutions les plus fréquemment intégrées aujourd'hui sont le SIEM, l'EDR et le CASB. Ces intégrations sont déjà opérationnelles aujourd'hui dans plus de trois entreprises sur cinq que nous avons interrogées.

Toutes les entreprises à l'échelle mondiale Parmi les éléments suivants, lesquels avez-vous intégrés à votre solution de gestion des identités et des accès, ou prévoyez-vous d'intégrer dans les 12 à 18 prochains mois ? (Sélectionnez toutes les réponses pertinentes)



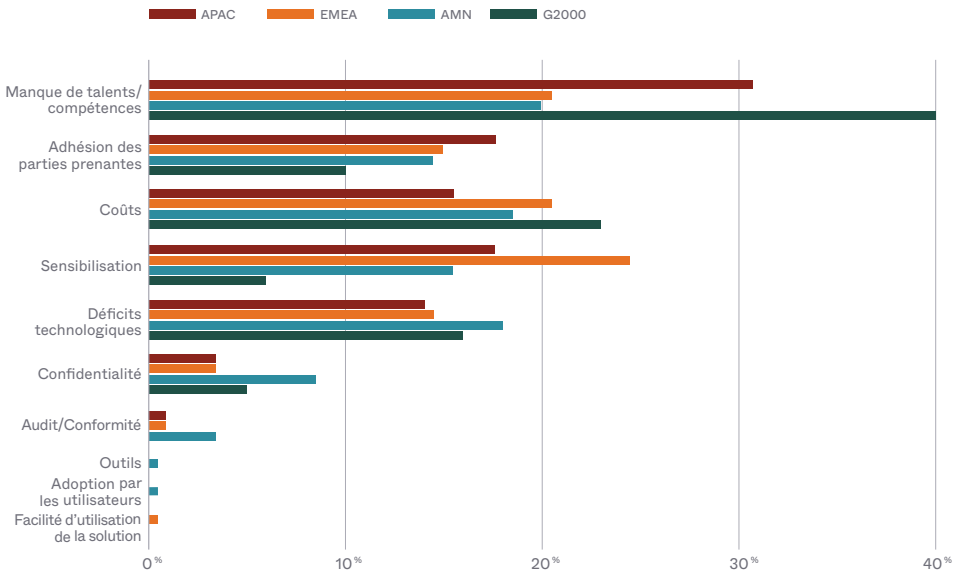
Comparaison régionale Parmi les éléments suivants, lesquels sont pour vous les plus importants à intégrer à une solution IAM pour soutenir une sécurité Zero Trust ?



Les promesses et les défis du Zero Trust

Depuis l'année dernière, les entreprises du monde entier ont accompli des progrès considérables dans leurs initiatives Zero Trust, mais elles sont encore confrontées à un certain nombre de grands défis, comme la nécessité de réaliser des investissements significatifs pour aider leurs équipes à mettre en œuvre de nouvelles technologies. Lorsque nous avons interrogé les responsables sécurité concernant les principaux défis à relever pour implémenter des initiatives Zero Trust spécifiques, leurs réponses ont été révélatrices. La pénurie de talents/compétences est citée comme défi principal en Amérique du Nord, dans la région APAC et par les entreprises du classement Global 2000. Dans la région EMEA, les coûts sont vus comme un défi équivalent, et la sensibilisation (à l'importance de disposer d'une solution soutenant le Zero Trust) est davantage prioritaire encore. Si l'on examine les trois principaux défis de chaque groupe, la pénurie de talents/compétences et les coûts figurent dans le trio de tête de tous les groupes. Ils sont suivis de près par les déficits technologiques en Amérique du Nord et dans la région APAC, et par l'adhésion des parties prenantes dans la région EMEA et dans les entreprises du classement Global 2000.

Comparaison régionale Quels défis votre entreprise rencontre-t-elle dans l'implémentation d'un modèle de sécurité Zero Trust ?



Principaux défis de l'implémentation d'une initiative Zero Trust Classez les trois principaux défis que rencontre votre entreprise dans l'implémentation d'une initiative de sécurité Zero Trust

APAC
1. Pénurie de talents/compétences pour l'implémentation
2. Déficits technologiques
3. Coûts

EMEA
1. Pénurie de talents/compétences pour l'implémentation
2. Adhésion des parties prenantes
3. Coûts

Amérique du Nord
1. Pénurie de talents/compétences pour l'implémentation
2. Déficits technologiques
3. Coûts

Global 2000
1. Pénurie de talents/compétences pour l'implémentation
2. Adhésion des parties prenantes
3. Cost concerns

Toutes les entreprises à l'échelle mondiale
1. Pénurie de talents/compétences pour l'implémentation
2. Adhésion des parties prenantes
3. Coûts

L'avenir du Zero Trust

Compte tenu de la pénurie mondiale de talents et de compétences, les entreprises doivent trouver des solutions qui les aident à progresser dans leur démarche Zero Trust sans nécessiter de budgets, d'effectifs ou de ressources de formation supplémentaires. Ces solutions doivent s'intégrer à leur écosystème de sécurité existant pour en tirer le maximum de valeur. Elles doivent en outre être plus faciles et plus rapides à déployer, et pouvoir évoluer au fur et à mesure que les entreprises se développent et avancent dans leur stratégie Zero Trust. Les problèmes d'adhésion des parties prenantes peuvent, dans certains cas, résulter du fait qu'un département sécurité n'a pas le plein contrôle sur les solutions IAM, et éventuellement d'autres solutions de sécurité, présentes dans l'environnement. D'autres départements moins impliqués dans les initiatives Zero Trust peuvent être réticents à y réaffecter des ressources.

Ces défis sont autant d'opportunités. Les équipes sécurité doivent prendre le temps d'expliquer à ces départements la nécessité de faire progresser ces projets afin d'obtenir leur adhésion. Pour cela, elles peuvent s'inspirer de leurs homologues au sein d'autres entreprises pour savoir comment orchestrer leur approche organisationnelle. Plus important encore, elles doivent travailler avec les partenaires appropriés pour implémenter des solutions Zero Trust qu'elles pourront exploiter quelle que soit la phase à laquelle elles sont parvenues. Elles pourront ainsi découvrir les solutions spécifiques dont elles ont besoin à chaque phase de la courbe de maturité, et pouvant être intégrées à leur infrastructure de sécurité existante, ce qui les aidera à surmonter les défis restants.

Rappel des points à retenir

Tout d'abord, le Zero Trust est désormais bien plus qu'un phénomène de mode. En peu de temps, il est passé du statut d'idée intéressante et de concept théorique, à celui d'impératif métier stratégique. Et les entreprises du monde entier ont défini des plans pour le mettre en place.

Ensuite, il n'y a pas un chemin direct vers le Zero Trust. Chaque entreprise a un point de départ et des priorités différents, ce qui nécessite des solutions différentes et spécifiques à intégrer de manière transparente à un programme de sécurité simple, efficace et performant.

Enfin, l'identité est le moteur du Zero Trust. C'est l'élément qui permet d'être efficace lorsque vous connectez une solution complexe, protégez le nouveau périmètre, équilibrez sécurité et facilité d'utilisation, et gardez vos actifs sécurisés mais accessibles pour vos collaborateurs distants.

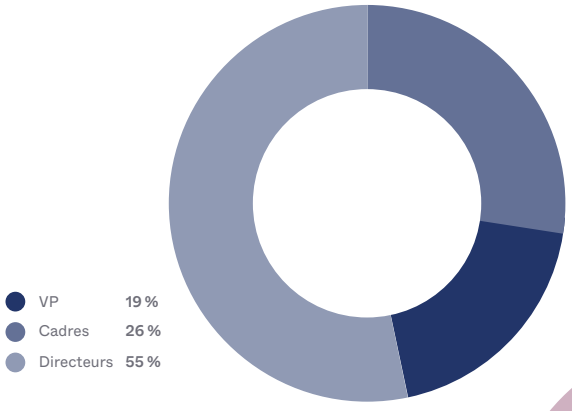
Si vous êtes prêt à découvrir où se situe votre entreprise sur la courbe de maturité, nous avons une ressource qui peut vous aider. Pour en savoir plus, **cliquez ici**.

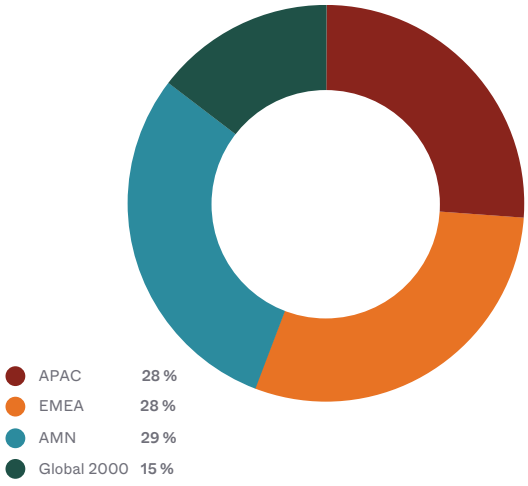
Méthodologie de l'enquête

Okta a commandité à Pulse Q&A une enquête mondiale auprès de 700 décideurs et responsables sécurité dans de nombreuses entreprises et secteurs d'activité. Nous définissons par « décideurs » les personnes responsables des décisions d'achat de technologies. Ce sont eux que notre partenaire Pulse Q&A a interrogés début 2022. Tout au long de ce rapport, nous utilisons les termes « notre enquête » et « l'enquête » pour désigner cette enquête, et nous faisons référence aux personnes qui ont répondu au nom de leur entreprise comme aux « personnes interrogées ».

Participants à l'enquête

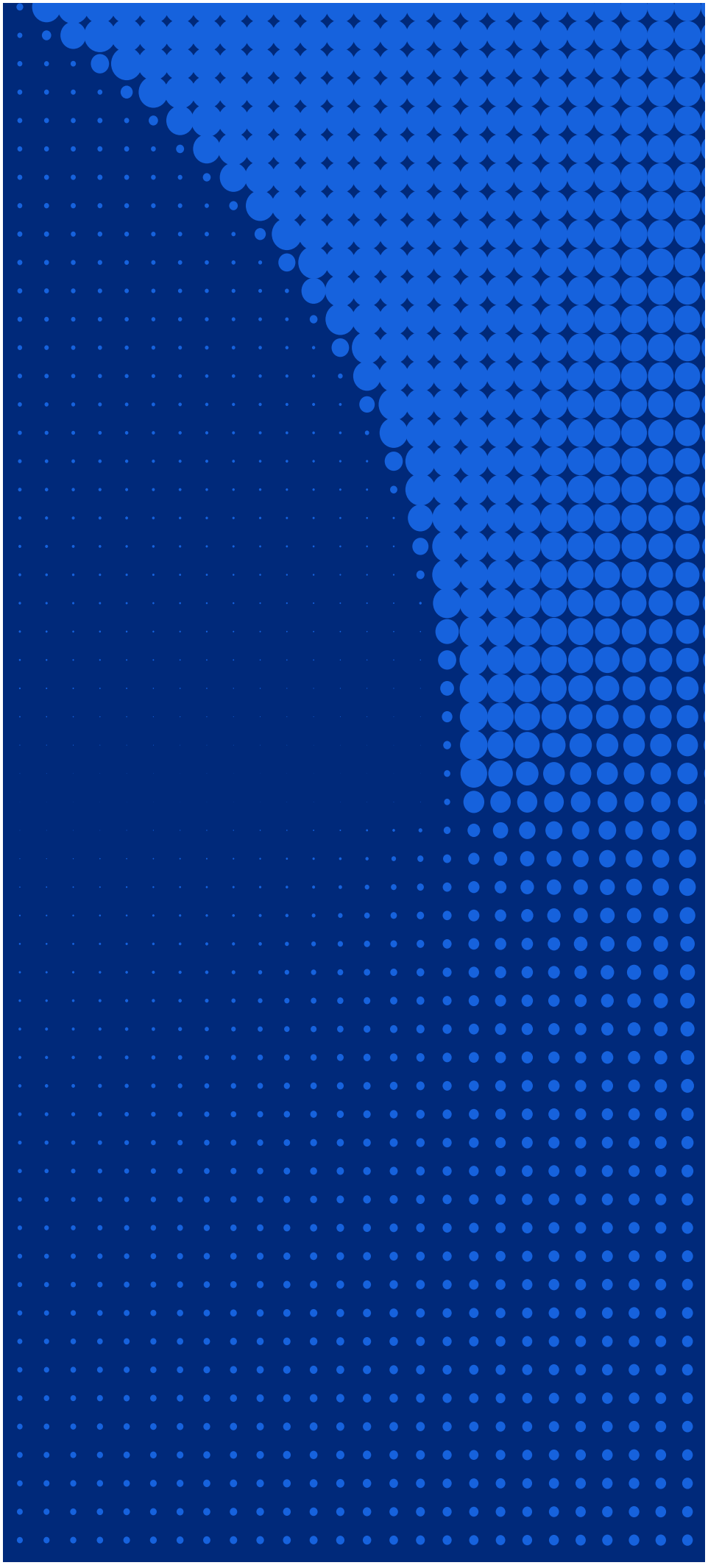
Voici une vue d'ensemble des 700 personnes interrogées et des entreprises qu'elles représentent. Pour les données sectorielles, nous nous sommes concentrés sur quatre secteurs d'activité et trois zones géographiques, ainsi que sur les entreprises du classement Forbes Global 2000. Les responsables sécurité interrogés étaient des vice-présidents, des directeurs ou des cadres, et nous avons utilisé des pourcentages dans chaque segment pour normaliser.





À propos d'Okta

Okta est le leader indépendant des solutions de gestion des identités. Okta Identity Cloud permet aux entreprises de connecter en toute sécurité les bonnes personnes aux bonnes technologies au bon moment. Grâce à plus de 7 000 intégrations avec des applications et fournisseurs d'infrastructures, Okta offre des accès fluides et sécurisés aux personnes et aux organisations, où qu'elles se trouvent, leur donnant ainsi la confiance nécessaire pour réaliser leur plein potentiel. Plus de 15 800 entreprises, dont JetBlue, Nordstrom, Slack, Takeda, Teach for America et Twilio, font confiance à Okta pour les aider à protéger l'identité de leurs collaborateurs et de leurs clients. Pour en savoir plus, rendez-vous sur okta.com/fr.



okta