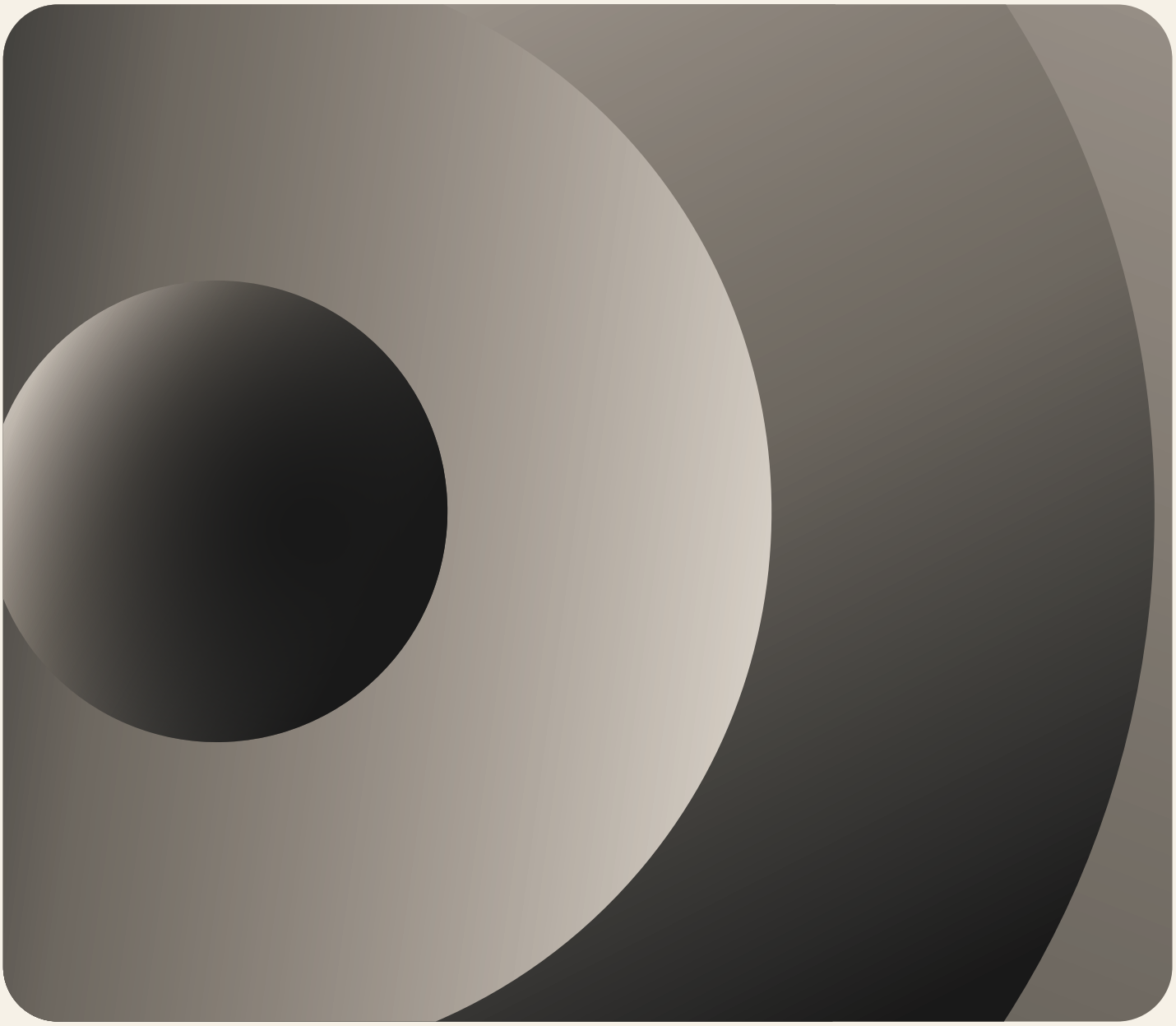
2023

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

The State of Zero Trust Security 2023



okta

Sommaire

Méthodologie

Méthodologie de l'enquête

En avril 2023, Okta, en collaboration avec Qualtrics, a mené une enquête mondiale auprès des décideurs concernés par la sécurité des informations dans un large éventail de secteurs d'activité. Les décideurs sont définis comme des collaborateurs occupant un poste de direction et responsables des décisions d'achat de technologies. L'enquête a été menée en anglais et en japonais par le biais de panels Qualtrics dans 13 pays. 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 », « répondants » ou « participants à l'enquête ».

Participants à l'enquête

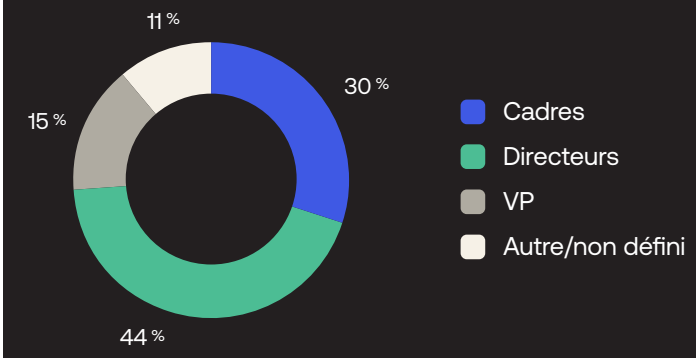
L'échantillon comportait au total 860 décideurs dans le domaine de la sécurité des informations, provenant de trois régions : NAM (États-Unis et Canada), EMEA (Allemagne, Danemark, Finlande, France, Irlande, Pays-Bas, Royaume-Uni, Norvège et Suède) et APJ (Japon et Australie). Ce rapport s'intéresse surtout au secteur public, à la santé, aux services financiers et aux logiciels, mais d'autres secteurs d'activité sont également représentés. (Les régions et les secteurs d'activité sont identifiés par les personnes interrogées.) Le secteur public inclut des organisations des trois régions du monde, mais au niveau national et non local. Les groupes interrogés incluent des cadres, des vice-présidents et des directeurs. L'enquête ne ciblait pas les collaborateurs ou clients d'Okta en particulier.

Détails de la méthodologie

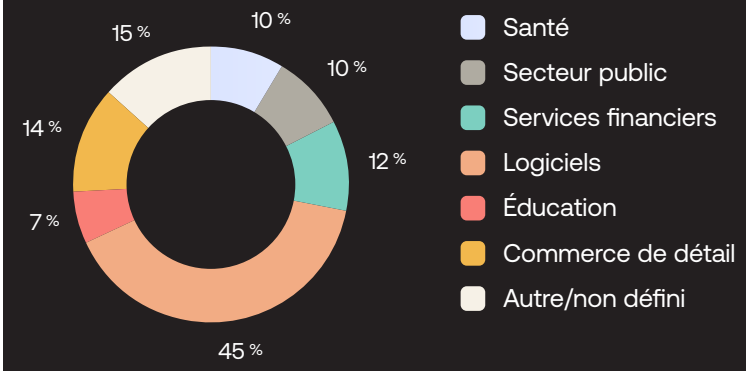
Dans les tableaux du présent rapport, les réponses appartenant aux catégories « Monde » ou « Tous » incluent des répondants de toutes les régions (qu'ils appartiennent ou non aux régions NAM, EMEA ou APJ) et de tous les secteurs (et pas uniquement des quatre secteurs plus particulièrement ciblés). Pour des raisons pratiques, nous arrondissons les données des tableaux au chiffre le plus proche, y compris à zéro dans le cas où le nombre est inférieur à 0,5. C'est la raison pour laquelle les totaux de certains tableaux ne correspondent pas exactement à 100 %. Les tableaux peuvent aussi totaliser plus de 100 % lorsque les personnes interrogées ont répondu oui à plusieurs questions connexes (par exemple en indiquant avoir entrepris une initiative spécifique, mais également avoir l'intention de le faire à l'avenir). ■

Données démographiques des participants à l'enquête

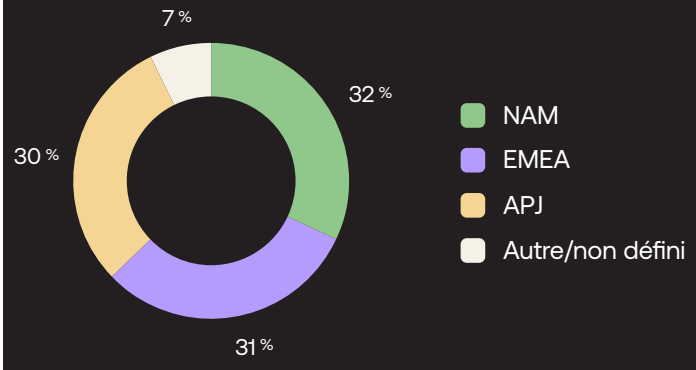
Rôle du participant



Secteur d'activité de l'entreprise



Région de l'entreprise



Le Zero Trust, du statut d'objectif à celui de projet

L'adoption du Zero Trust gagne du terrain au sein des entreprises qui cherchent à protéger leurs collaborateurs, leurs ressources et leur infrastructure.

Il y a dix ans, le Zero Trust ne représentait guère plus qu'un idéal de sécurité à l'horizon lointain. C'est John Kindervag, chercheur chez Forrester, qui a inventé le terme en 2010 pour désigner un principe de sécurité devenu nécessaire et répondant à la maxime « ne jamais faire confiance, toujours vérifier ». Depuis lors, le Zero Trust a connu une évolution rapide : d'un simple principe philosophique, il est devenu un objectif à atteindre, puis une réalité dans le quotidien des entreprises. Aujourd'hui, comme le révèle notre enquête annuelle « State of Zero Trust Security », jamais les entreprises n'ont été aussi nombreuses à l'avoir adopté en tant que stratégie d'entreprise, et à prendre des mesures concrètes pour implémenter une véritable sécurité Zero Trust dans les mois qui viennent.

En fait, pour la première fois depuis 2019, année de la première publication du rapport « State of Zero Trust Security », le nombre d'organisations qui possèdent déjà une stratégie Zero Trust dépasse de loin celles qui en sont toujours au stade de la planification (ou l'estiment superflue). La tendance s'est donc clairement inversée.

Face à la multiplication des brèches et des vols de données, ainsi qu'aux conseils prescriptifs du NIST et de la CISA, ce phénomène n'est guère surprenant. Selon le rapport 2022 Annual Data Breach Report de l'ITRC (Identity Theft Resource Center), l'année dernière, les États-Unis ont connu 1 802 brèches de données qui ont impacté plus de 422 millions de personnes. Comme toujours, l'identité est au cœur de ces attaques incessantes : l'étude 2022 Identity Fraud Study de Javelin estime les pertes dues à la seule usurpation d'identité aux États-Unis à 43 milliards de dollars en 2022 — ce qui reste malgré tout un progrès comparé aux 52 milliards de 2021. Selon un rapport du ministère américain de la Justice publié en 2023, « l'usurpation d'identité intervient dans la plupart des délits majeurs et aucun pays n'est épargné. Elle constitue donc une menace nationale et mondiale pour la sécurité de toutes les nations et de leurs citoyens. »

Pour combattre les menaces modernes et les cybercriminels chevronnés, nous sommes persuadés que les équipes de sécurité d'entreprise n'ont d'autre choix que d'adhérer au principe fondamental du Zero Trust : « ne jamais faire confiance, toujours vérifier ». Une stratégie de sécurité Zero Trust jette les bases permettant aux organisations de dépasser les approches traditionnelles de la cybersécurité, inadaptées aux environnements intégrant le cloud, et de positionner l'identité comme le facteur déterminant de leur niveau de sécurité. Pour de nombreuses entreprises, l'identité est restée pendant longtemps le domaine exclusif des équipes IT. Aujourd'hui, comme le montre notre enquête, le contrôle est largement (et parfois, totalement) passé entre les mains de l'équipe de sécurité. Mais les équipes SecOps ne sont pas les seules à profiter du Zero Trust : les entreprises qui adoptent cette bonne pratique peuvent véritablement tirer parti de la gestion des identités dans toute leur infrastructure réseau et ainsi gagner en efficacité, en plus d'offrir des expériences de meilleure qualité à leurs collaborateurs et à leurs clients.

Les tendances macroéconomiques et l'innovation cloud ont conduit les organisations modernes à adopter des écosystèmes hybrides/multicloud plus complexes, avec des ressources distribuées et des environnements IT désormais accessibles à des effectifs variés et sans frontières, dont les partenaires, les prestataires et les fournisseurs externes. L'identité est le fil conducteur qui les relie tous et aujourd'hui, une gestion robuste des identités est considérée comme une infrastructure critique, indispensable au maintien d'une collaboration efficace et sécurisée de ces équipes internationales complexes. Comme le montrent les données de cette année, les entreprises multiplient les efforts pour renforcer la gestion de leurs terminaux mobiles, ajouter l'authentification unique (SSO) et l'authentification multifacteur (MFA) pour les collaborateurs internes et externes, automatiser leurs workflows de provisioning/déprovisioning et, de manière générale, mettre en place des initiatives Zero Trust efficaces pour protéger leur personnel et leurs ressources d'entreprise.

L'implémentation du Zero Trust est un long parcours. En effet, bouleverser des pratiques et des processus en place depuis des dizaines d'années, reconstruire des piles de sécurité et prendre des décisions d'investissement et d'abandon de solutions logicielles en place présentent leur lot de défis, même dans les meilleures circonstances — ce qui est loin d'être le cas dans la conjoncture économique actuelle. Mais avec les bonnes technologies et les bons fournisseurs, les multinationales représentées dans notre enquête annuelle se simplifient la tâche et progressent à grands pas. Ce rapport a pour but d'aider les organisations à comprendre où et comment les entreprises innovantes et à forte croissance mettent en place des initiatives de sécurité Zero Trust. De cette façon, il leur sera plus facile d'identifier les mesures à prendre pour passer du simple objectif à la concrétisation du projet dans leur propre parcours organisationnel.

Les initiatives Zero Trust se multiplient

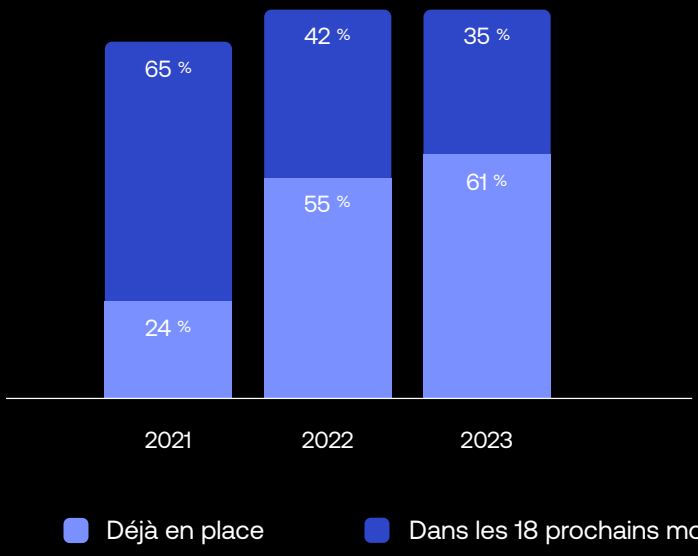
Le nombre d'organisations ayant mis en place une initiative Zero Trust définie connaît une augmentation sans précédent. En 2021, moins d'une entreprise interrogée sur quatre avait mis en place une sécurité Zero Trust. En 2022, elles étaient plus de la moitié et cette année, le pourcentage a encore augmenté pour atteindre 61 %. À l'inverse, le nombre d'entreprises qui prévoient toujours d'implémenter une initiative Zero Trust dans les 12 à 18 prochains mois diminue d'année en année, à mesure que les entreprises progressent dans la réalisation de leur projet. Aujourd'hui, plus de 6 entreprises interrogées sur 10 sont à un stade assez avancé de leur parcours Zero Trust, et les autres en sont pour la plupart à l'étape de la planification.

Si nous analysons les données plus en détail, notamment les résultats selon la taille de l'entreprise, nous constatons que les organisations de plus petite taille (comptant entre 500 et 999 employés) sont moins susceptibles d'avoir une initiative de sécurité Zero Trust définie en place que les plus grandes. En revanche, parmi les entreprises comptant entre 5 000 et 9 999 collaborateurs, trois sur quatre déclarent avoir un projet Zero Trust défini en place. À tous les niveaux, seule une petite minorité des organisations (moins de 10 % dans tous les cas) n'ont pas d'initiative Zero Trust, ni l'intention d'en développer une dans les 18 prochains mois.

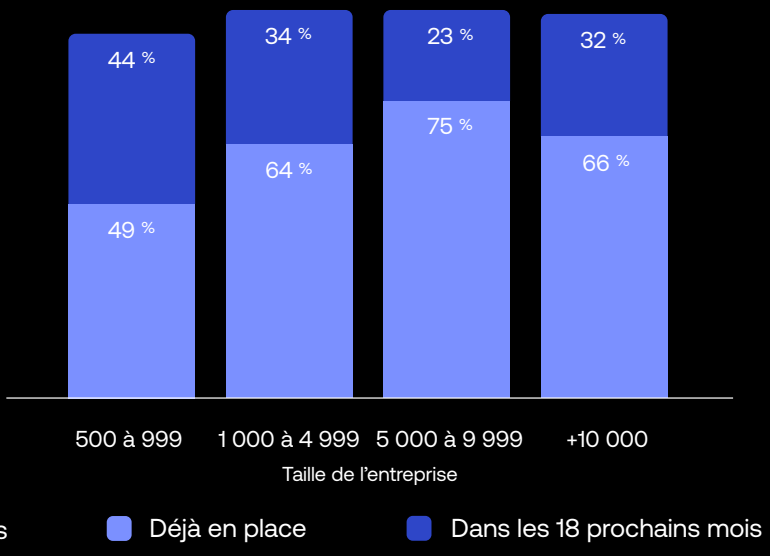
Partout dans le monde, les projets Zero Trust deviennent une réalité

À l'échelle mondiale, 61 % des entreprises possèdent une initiative de sécurité Zero Trust en place, 28 % prévoient d'en implémenter une dans les 6 à 12 prochains mois et 7 % dans les 13 à 18 mois. Cette tendance générale se maintient dans toutes les régions. L'Amérique du Nord conserve son avance en ce qui concerne les initiatives déjà en place, mais les organisations des régions EMEA et APJ comblent rapidement leur retard. Qui plus est, pratiquement toutes celles qui n'ont pas encore adopté le Zero Trust prévoient de le faire dans les 6 à 12 mois ou les 13 à 18 mois à venir.

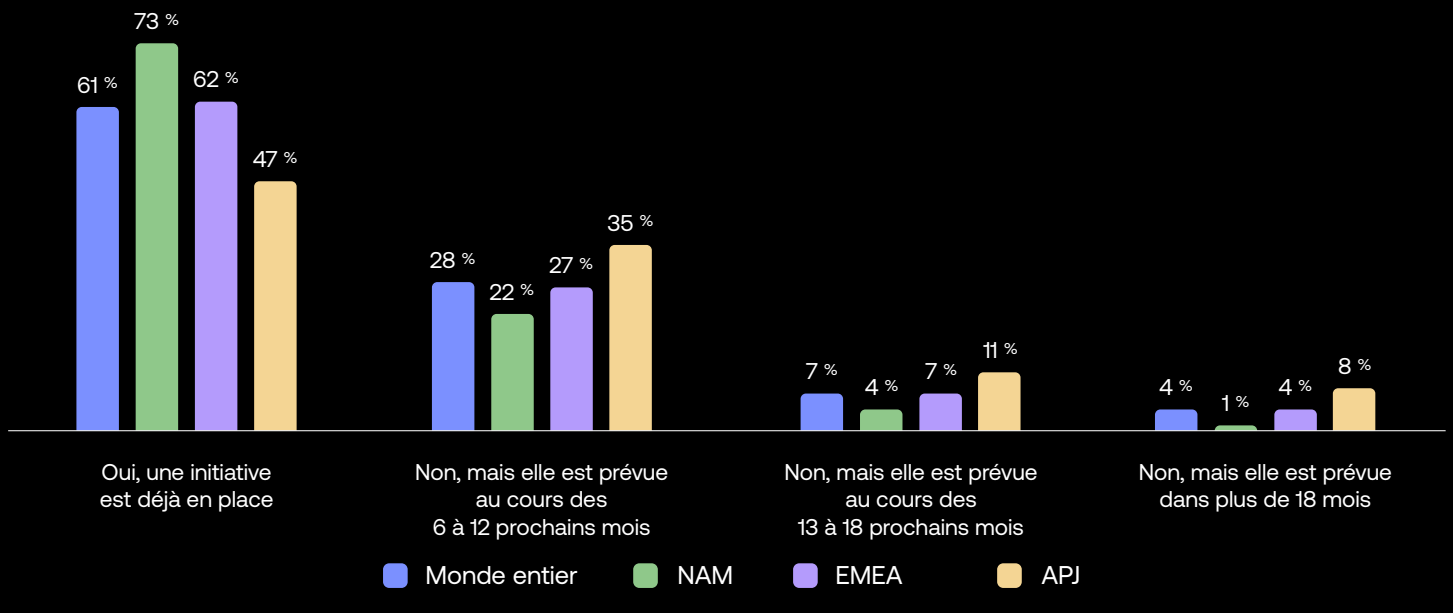
Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle d'en mettre en œuvre une dans les 18 prochains mois ?
Tous les répondants



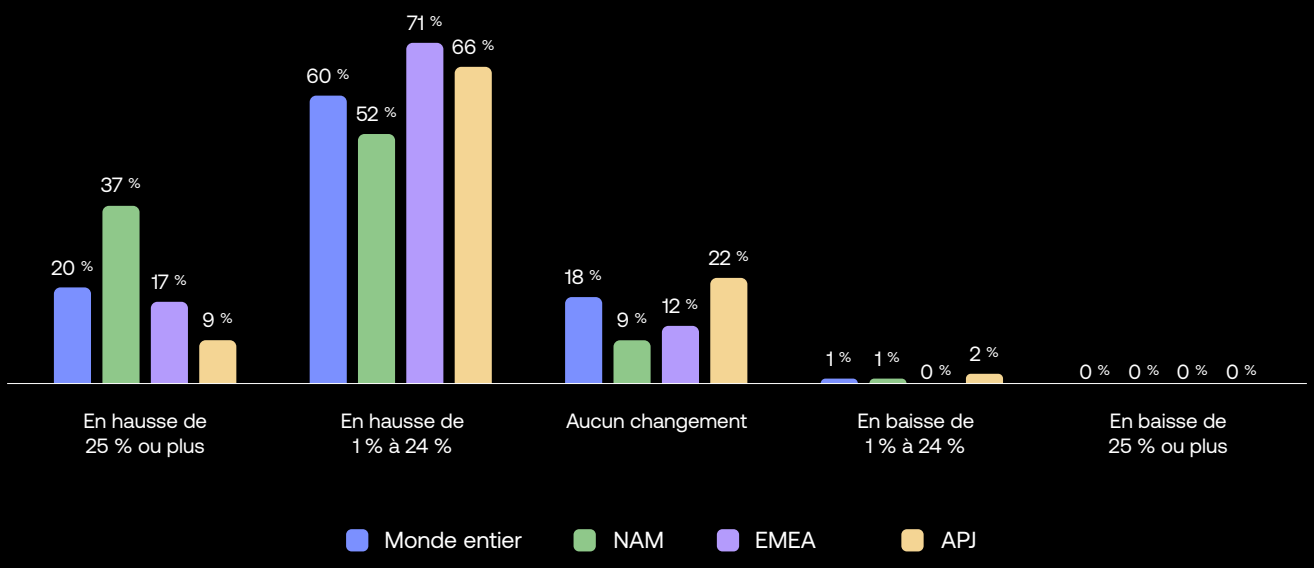
Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les 18 prochains mois ?
Comparaison par taille d'entreprise



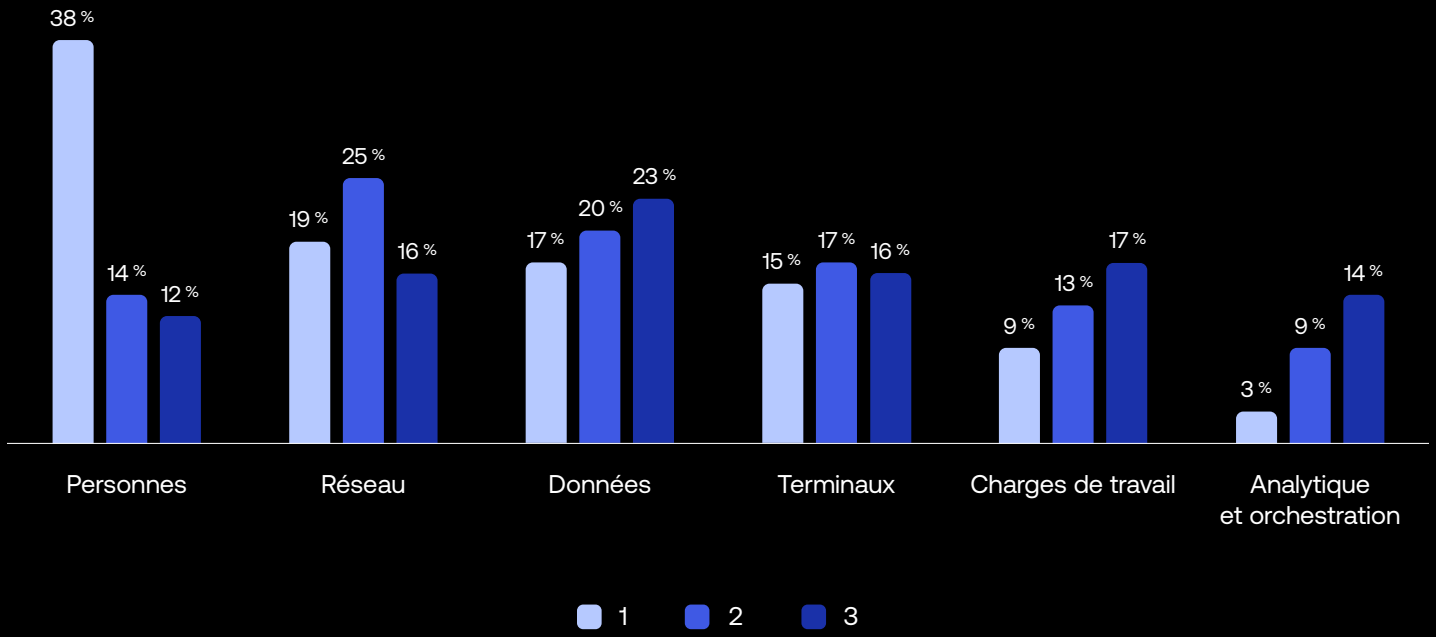
Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les prochains mois ?
Comparaison régionale



Comment votre budget Zero Trust a-t-il évolué (le cas échéant) au cours des 12 à 18 derniers mois ?
Comparaison régionale



Classez les domaines suivants selon leur priorité dans les projets de sécurité de votre entreprise (1 = la plus élevée, 3 = la plus faible)
Tous les répondants



Les budgets restent bons pour les initiatives Zero Trust

À une époque où les facteurs macro-économiques dictent les compressions des coûts et les coupes de personnel dans l'ensemble des régions et des secteurs, les budgets alloués aux initiatives de sécurité Zero Trust semblent virtuellement intouchables. En fait, pour la majorité des entreprises interrogées, ces budgets ne sont pas simplement stables, ils ont augmenté au cours des 12 à 18 derniers mois. À l'échelle mondiale, 60 % des organisations ont observé une augmentation de 1 à 24 % de ces budgets depuis l'année dernière et une entreprise sur cinq a même connu une augmentation plus marquée. Moins de 3 % des organisations interrogées ont vu leur budget diminuer, et ce, quelle que soit la région.

Les personnes restent la première priorité des projets de sécurité

Lorsque nous avons demandé aux répondants de classer les trois grands problèmes de sécurité de leur entreprise, les personnes représentaient la première priorité en matière de sécurité, largement en tête, le réseau et les données venant loin derrière en deuxième et troisième places. Si les personnes ont toujours été une priorité majeure, cette année, l'écart s'est encore creusé, reflétant une meilleure compréhension de la fonction critique de l'identité dans les initiatives de sécurité Zero Trust.

Le Zero Trust, du statut d'objectif à celui de projet

Points à retenir

D'un simple plan d'action, le Zero Trust s'est rapidement imposé comme une norme de fonctionnement.

Les organisations qui considéraient au départ le Zero Trust comme un framework théorique ont, pour la plupart, mis leurs plans en œuvre ou sont en passe de le faire. La progression a été spectaculaire : en 2021, seuls 24 % des répondants indiquaient avoir mis en place une initiative stratégique Zero Trust ; l'année dernière, ce chiffre est passé à 55 %, et à 61 % cette année. Cette tendance est observable dans toutes les régions et toutes les entreprises, quelle que soit leur taille. Parmi les quatre secteurs d'activité auxquels nous nous sommes intéressés, les services financiers sont légèrement en tête, 71 % de ces entreprises possédant déjà une sécurité Zero Trust, soit un peu plus que le secteur des logiciels, avec 69 %. En termes de région, l'Amérique du Nord est en tête du peloton, 73 % des entreprises nord-américaines ayant déjà mis en place une initiative de sécurité Zero Trust, et la région APJ ferme la marche avec 47 %. Toutefois, les entreprises de cette région sont les plus susceptibles (35 %) de prévoir la mise en œuvre d'une telle initiative dans les 6 à 12 prochains mois.

Pour la vaste majorité, l'identité est désormais considérée comme critique pour toute stratégie Zero Trust.

Quelle différence en l'espace d'un an ! L'année dernière, 71 % des répondants jugeaient l'identité importante pour leur stratégie de sécurité Zero Trust, mais seuls 27 % estimaient qu'elle était critique pour l'activité. Cette année, la tendance s'est inversée, avec 51 % des répondants déclarant que l'identité est « extrêmement importante » et 40 % « assez importante ». Un tel revirement ne nous surprend pas, dès lors qu'un nombre croissant d'entreprises se rend compte qu'une stratégie robuste de gestion des identités et des accès (IAM) est indispensable à la protection des effectifs et des ressources dans un monde hybride/multicloud.

Les budgets des projets Zero Trust continuent d'augmenter et de résister obstinément aux forces du marché.

Partout dans le monde, les budgets se resserrent face à diverses pressions macroéconomiques, et pourtant les dépenses liées au Zero Trust continuent d'augmenter. Cette année, 80 % des personnes interrogées ont déclaré que les budgets alloués aux initiatives Zero Trust avaient augmenté par rapport à l'année précédente : 60% mentionnent une augmentation du budget comprise entre 1 et 24 %, et 20 % d'entre eux rapportent une hausse substantielle (de 25 % ou plus). Dans les trois dernières éditions du rapport, les coûts restent une préoccupation majeure, mais la multiplication des fraudes et des menaces internes, ainsi que la demande de travail hybride et d'un libre accès au cloud, contraignent les entreprises de toutes tailles et de tous les secteurs à se concentrer sur (et à budgétiser) les mesures de sécurité axées sur l'identité.

Les entreprises cherchant à adopter le Zero Trust doivent encore surmonter de nombreux défis.

Cette année, nos répondants ont cité les coûts et les déficits technologiques comme principaux obstacles à l'adoption du Zero Trust, suivis des réglementations sur la confidentialité/sécurité des données et de la pénurie de talents/compétences. Mais la situation a changé : au cours des années précédentes, une seule préoccupation semblait l'emporter largement sur les autres. Cette année, les défis sont plus équitablement répartis : facilité des intégrations, sensibilisation à la solution, conformité des audits et adhésion des parties prenantes. Dans le même ordre d'idées, le contrôle des équipes sur l'IAM au sein des entreprises est fondamentalement passé du domaine IT à un modèle de responsabilité partagée géré essentiellement par les équipes de sécurité. ■

L'identité au cœur du Zero Trust

Les entreprises du monde entier prennent conscience du rôle essentiel de l'identité dans une sécurité de pointe.

Dans un monde où les périmètres réseau traditionnels ont pratiquement disparu, l'identité s'impose comme le nouveau périmètre et c'est là que doit commencer la défense. Le contrôle de l'identité de chaque personne et de chaque machine à chaque tentative d'accès à vos ressources — d'où que ce soit dans le monde et depuis un large éventail de terminaux, autorisés ou non — est l'enjeu de notre époque.

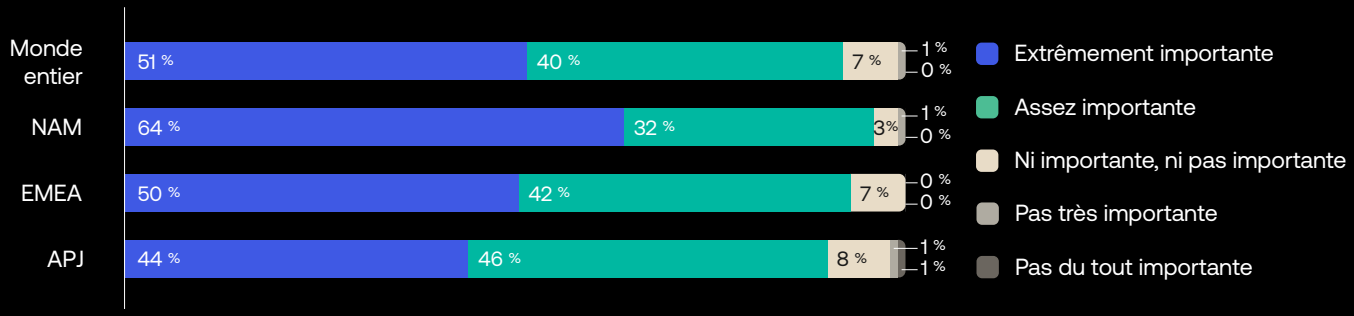
Mais c'est aussi la réussite de l'entreprise qui se joue ici. Comme le montrent les données de cette année, les entreprises, tous secteurs et tailles confondus, se rendent compte que l'identité n'est pas simplement un enjeu de sécurité, mais aussi le moyen de développer l'activité en toute sécurité afin de générer de nouveaux revenus, d'améliorer la fidélité des clients, de protéger leurs ressources et la réputation de leur marque, et bien plus encore.

Ces tendances se reflètent dans les résultats de notre enquête 2023, qui révèle la volonté des entreprises d'accorder une plus grande importance à l'identité dans le cadre de leurs initiatives Zero Trust. À l'échelle mondiale, plus de la moitié de nos répondants déclarent que l'identité est extrêmement importante pour leur stratégie de sécurité Zero Trust, soit une hausse considérable par rapport à ceux qui le pensaient déjà en 2022, constatée par ailleurs dans toutes les régions, comme nous le verrons par la suite.

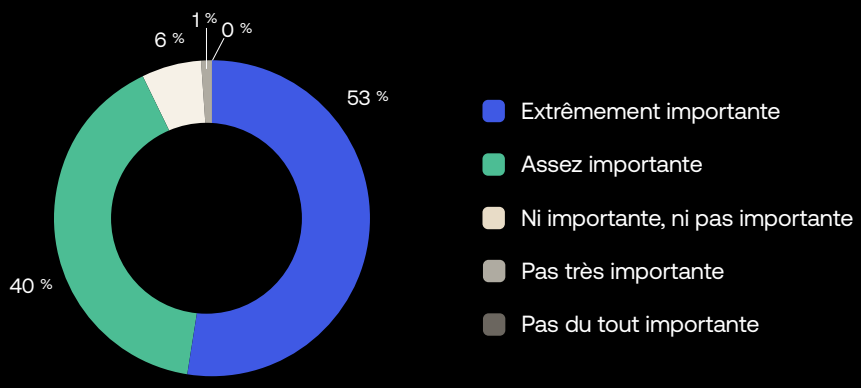
« Les leaders IT alignent leurs investissements en solutions IAM sur les objectifs de sécurité, mais aussi métier. S'il est mis en œuvre efficacement, l'IAM crée un processus sécurisé pour l'autorisation, l'application des politiques ainsi que le provisioning et déprovisioning, ce qui réduit les points de friction et optimise les opérations métier (...) une source potentielle d'améliorations tant en termes de sécurité que de productivité. »

— Identity-Defined Security Alliance.
2022 Trends in Securing Digital Identities

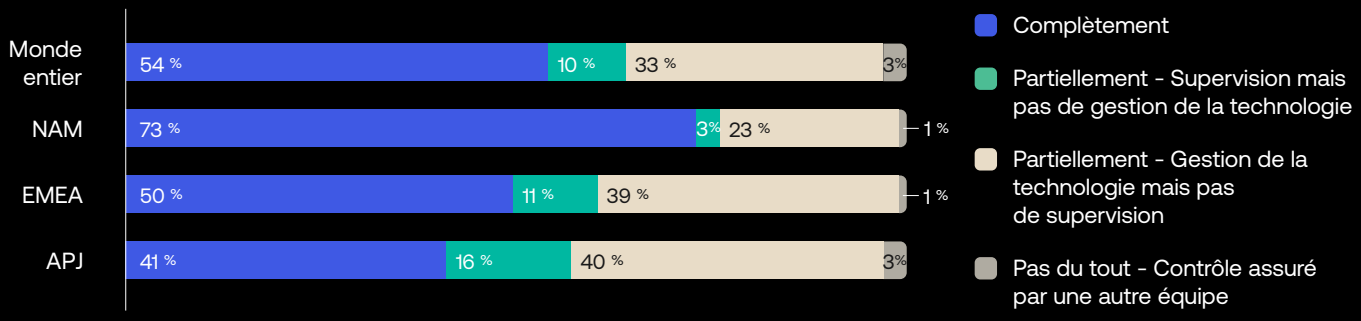
Quelle est l'importance de l'identité dans votre stratégie de sécurité Zero Trust globale ?
Comparaison régionale



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



Dans quelle mesure les équipes sécurité gèrent-elles la solution IAM dans votre entreprise ?
Comparaison régionale



Remarque : la somme des colonnes n'est pas toujours égale à 100 % en raison de l'utilisation de la méthode d'arrondi à l'entier le plus proche.

L'importance de l'identité est indéniable

Aujourd'hui, le rôle critique de l'identité dans les initiatives Zero Trust ressort de manière encore plus évidente. L'année dernière, seuls 27% de toutes les entreprises interrogées déclaraient que l'identité était extrêmement importante pour leur stratégie de sécurité Zero Trust globale ; cette année, ce pourcentage atteint 51 %. Par région, l'Amérique du Nord ouvre la marche, près de deux tiers des répondants considérant l'identité comme extrêmement importante et près d'un tiers comme assez importante. Les régions EMEA et APJ peuvent encore être en butte à certains obstacles perceptuels puisque 7 % et 8 % des répondants respectivement estiment l'identité « ni importante, ni pas importante ». Dans la région APJ, certains (2 %) la considèrent même comme très peu importante.

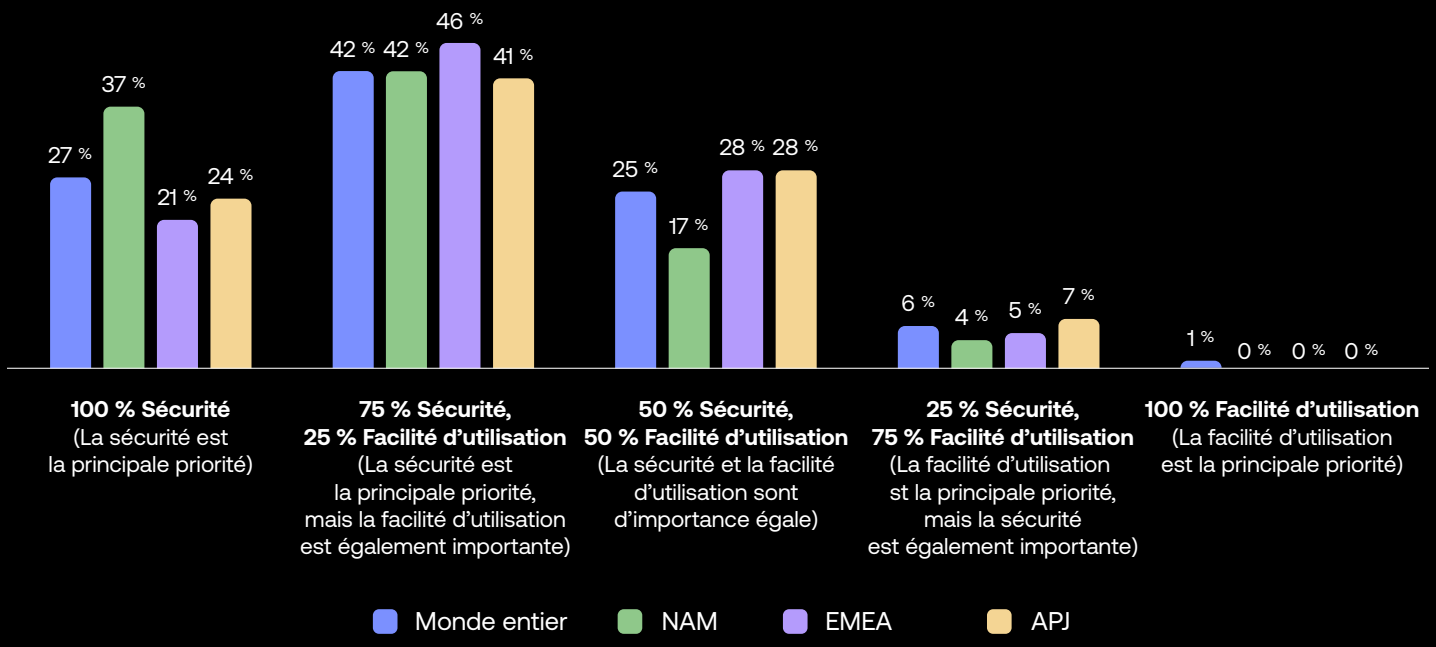
L'adhésion des dirigeants

La vaste majorité des dirigeants interrogés continuent de considérer l'identité comme une priorité, comme c'était le cas dans le rapport de l'année dernière. Plus de la moitié d'entre eux estiment l'identité extrêmement importante pour une stratégie Zero Trust et 40 % déclarent qu'elle est assez importante. (L'année dernière, seuls 29 % des dirigeants interrogés jugeaient l'identité critique pour l'activité.) Point à retenir : la perception du rôle critique de l'identité dans une sécurité de pointe se généralise.

La responsabilité de l'IAM change de mains

Pour comprendre à quel point l'approche de sécurité a changé, il suffit de se demander qui a le contrôle de la solution IAM dans l'entreprise. Pendant longtemps, l'identité a été essentiellement du ressort de l'équipe IT, mais ces dernières années, elle est progressivement devenue une responsabilité de l'équipe de sécurité compte tenu de la prévalence des menaces basées sur l'identité, comme le phishing par exemple. (L'année dernière, 74 % des brèches impliquaient une interaction humaine, selon le rapport 2023 Data Breach Investigations Report de Verizon.) Les équipes de sécurité sont désormais responsables de la gestion des identités et des accès dans la moitié des organisations de l'EMEA et, pour l'Amérique du Nord, ce pourcentage s'élève à 73 %. Cette responsabilité est plus partagée dans la région APJ, où seulement 41 % des organisations confient la gestion de l'IAM aux équipes de sécurité, tandis que 56 % d'entre elles leur confient soit la supervision des identités, soit la gestion des technologies, mais pas les deux.

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



Globalement, la sécurité est devenue une priorité plus importante que la facilité d'utilisation

La surface d'attaque a considérablement augmenté dans les réseaux hybrides/multicloud d'aujourd'hui, laissant les organisations de plus en plus vulnérables aux menaces basées sur l'identité. En conséquence, les entreprises ont — parfois totalement — revu leurs priorités en faveur de la sécurité plutôt que de la facilité d'utilisation. À l'échelle mondiale, plus de deux entreprises sur trois estiment que la sécurité est leur priorité absolue, ou que le rapport est de trois quarts/un quart en faveur de la sécurité par rapport à la facilité d'utilisation. Cela dénote une nette évolution par rapport à la situation de 2021 où la priorité allait à la facilité d'utilisation en raison de la pandémie et de la nécessité de mettre en place une structure de télétravail. Les répondants de l'EMEA étaient moins nombreux à déclarer que la sécurité était leur principale priorité (21 %) par rapport aux entreprises d'Amérique du Nord (37 %).

Maturité des identités collaborateurs

Les entreprises ont fini par comprendre la valeur de la gestion des identités. Toute la difficulté consiste à mettre ces principes en pratique.

Il faut du temps pour mettre en place une stratégie Zero Trust. De plus, comme la gestion de projets complexes, de priorités changeantes et de besoins croissants demande du temps et des ressources, en l'absence de frameworks clairs, les organisations peuvent éprouver bien des difficultés à appréhender leurs vulnérabilités et à évaluer leurs progrès. Le modèle de maturité des identités collaborateurs d'Okta, expliqué ci-dessous, peut aider les entreprises à contextualiser les aspects relatifs à l'identité de leurs parcours Zero Trust et à évaluer leurs progrès. Ce parcours en plusieurs phases demande du temps, mais à mesure qu'elles mettent en place une sécurité axée sur l'identité, les entreprises renforcent progressivement leur protection : diminution de la surface d'attaque, réponse accélérée en cas d'attaque, réduction des coûts IT et de la charge d'administration. De manière générale, elles gagnent en sécurité, en efficacité et en agilité. Dans les pages suivantes, nous passerons rapidement en revue les 4 stades de ce parcours.

Maturité des identités collaborateurs

Les quatre stades

Stade 1 : Fondamental Consolidation et simplification	• Diminution des tâches de gestion manuelles • Réduction de la surface de risque • Consolidation des annuaires
Stade 2 : Extension Ajout de contrôles de sécurité	• Automatisation de l'onboarding et de l'offboarding • Amélioration de la productivité IT • Diminution de la charge d'administration
Stade 3 : Avancé Automatisation et amélioration de l'expérience	• Connexion de tous les systèmes d'identité • Automatisation de tous les processus d'administration • Mise hors service des technologies héritées
Stade 4 : Stratégique Optimisation et extension de l'identité	• Modernisation de l'expérience d'accès • Élimination des risques liés aux mots de passe • Extension de la maturité numérique

Stade 1 : Fondamental

Consolidation et simplification

Pour les entreprises qui en sont au premier stade, les objectifs consistent généralement à réduire les tâches de gestion manuelles et à renforcer les défenses contre les attaques basées sur l'identité. À ce stade, les organisations cherchent à limiter la gestion manuelle des utilisateurs et des applications, tout en renforçant leurs défenses. Avec des initiatives disjointes et ponctuelles, elles risquent d'augmenter involontairement leur surface d'attaque et de multiplier indûment le nombre d'annuaires.

Parmi les initiatives à réaliser en priorité au premier stade, citons la consolidation des systèmes d'identité, l'implémentation de SSO et MFA de base avec des politiques d'accès basées sur les rôles, la création d'une architecture haute disponibilité, l'ajout de normes SLA et l'établissement d'un inventaire des applications on-premise et cloud.

Stade 2 : Extension

Ajout de contrôles de sécurité

Au stade 2, les entreprises cherchent généralement à améliorer la productivité IT et à réduire les délais et les coûts d'administration. À ce stade, elles sont parfois trop dépendantes des mots de passe et des processus manuels, par exemple pour l'onboarding et l'offboarding des utilisateurs. Les objectifs sont l'augmentation de la productivité, l'allègement de la charge de gestion des administrateurs IT et la simplification de l'accès utilisateur aux applications.

Parmi les projets à envisager au stade 2, citons : l'extension du MFA à l'ensemble des applications, prestataires et partenaires commerciaux, la consolidation des contrôles d'accès et de sécurité pour l'ensemble des applications cloud et on-premise, l'implémentation du contrôle d'accès basé sur les rôles et de politiques d'accès dynamiques, ainsi que le déploiement d'outils de surveillance et d'audit de la conformité et de la sécurité.

Stade 3 : Avancé

Automatisation et amélioration de l'expérience

Au stade 3, les entreprises automatisent les éventuels processus manuels toujours en place et consolident tous les systèmes d'identité en une seule solution de gestion unifiée. Elles accélèrent ainsi l'efficacité de leurs effectifs dynamiques, tout en consolidant et en éliminant simultanément les technologies héritées pour mettre en place des systèmes connectés et capables de communiquer.

Les projets d'identité à envisager ici incluent le contrôle des accès basé sur les attributs et sur les rôles, et l'application du principe du moindre privilège aux API, à l'infrastructure critique et aux applications. En outre, les entreprises doivent chercher à adopter une recertification planifiée des accès utilisateurs et à implémenter un accès sécurisé sans mot de passe à l'infrastructure critique.

Stade 4 : Stratégique

Optimisation et extension de l'identité

À ce stade, les entreprises sont protégées par des systèmes axés sur l'identité et interconnectés, capables d'optimiser la sécurité et l'efficacité de toute l'entreprise. Elles peuvent désormais se concentrer sur des objectifs plus stratégiques, comme l'amélioration des expériences d'accès et l'élimination des risques liés aux mots de passe.

Elles doivent chercher à adopter l'authentification sans mot de passe dans tout l'environnement, à déployer des processus entièrement automatisés pour la prévention des incidents, la détection et la réponse, à mettre en place un accès à flux tendu (JIT) basé sur les risques, et à s'assurer qu'il ne reste plus aucun privilège établi.

Maturité des identités collaborateurs

Concrétisation des initiatives Zero Trust

Au départ simple théorie, le concept Zero Trust de « ne jamais faire confiance, toujours vérifier » est rapidement devenu une réalité grâce à la priorité donnée à l'identité et à l'adoption massive de telles initiatives par les entreprises les plus innovantes. Celles-ci jettent les bases d'une nouvelle sécurité, à commencer par l'extension du MFA et du SSO aux collaborateurs, aux utilisateurs externes, ainsi qu'aux applications, API et autres composants clés de leur infrastructure réseau. Dans toutes les régions, nous constatons qu'un nombre croissant d'organisations s'attaquent à des projets Zero Trust de plus en plus complexes et leurs progrès sont encourageants.

Motivées par des effectifs de plus en plus variés et dispersés, qui incluent des collaborateurs, prestataires, partenaires et fournisseurs nécessitant tous un accès fiable et instantané, les entreprises partout dans le monde progressent à grands pas vers une sécurité Zero Trust renforcée, reposant sur l'identité. Par exemple, les entreprises donnent la priorité au MFA pour les utilisateurs externes : 34 % des répondants cette année ont mis en place une telle mesure de sécurité pour les utilisateurs externes et 33 % pour les collaborateurs.

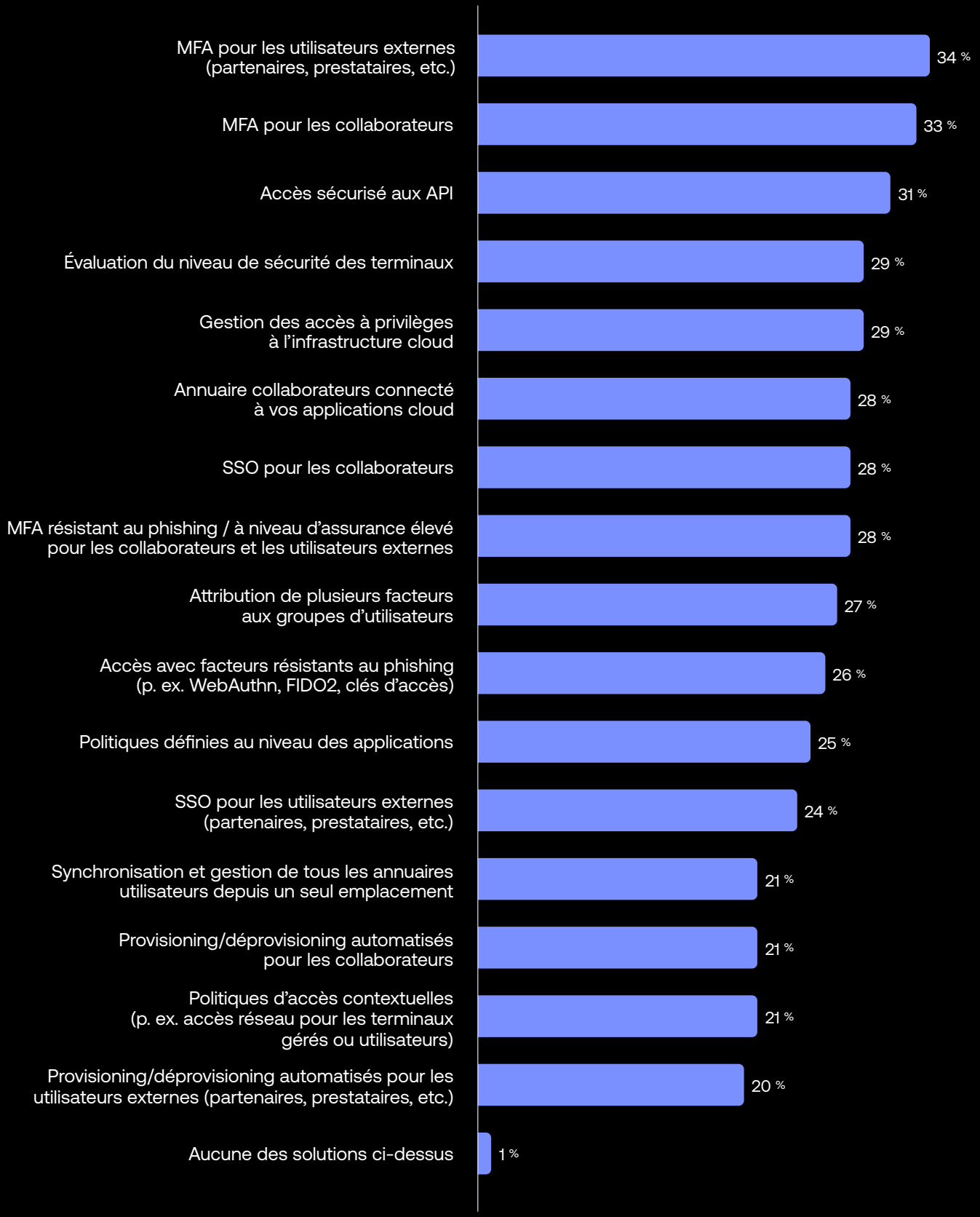
Si l'on s'en réfère aux données par secteur d'activité, les principales initiatives de sécurité déjà mises en place par les organisations interrogées sont les suivantes :

- **Secteur de la santé :** MFA pour les utilisateurs externes, MFA pour les collaborateurs et connexion des annuaires aux applications cloud
- **Secteur public :** MFA pour les utilisateurs externes, accès sécurisé aux API et MFA pour les collaborateurs
- **Services financiers :** MFA pour les collaborateurs, MFA pour les utilisateurs externes et gestion des accès à privilèges à l'infrastructure cloud
- **Logiciels :** MFA pour les collaborateurs, accès sécurisé aux API et MFA pour les utilisateurs externes

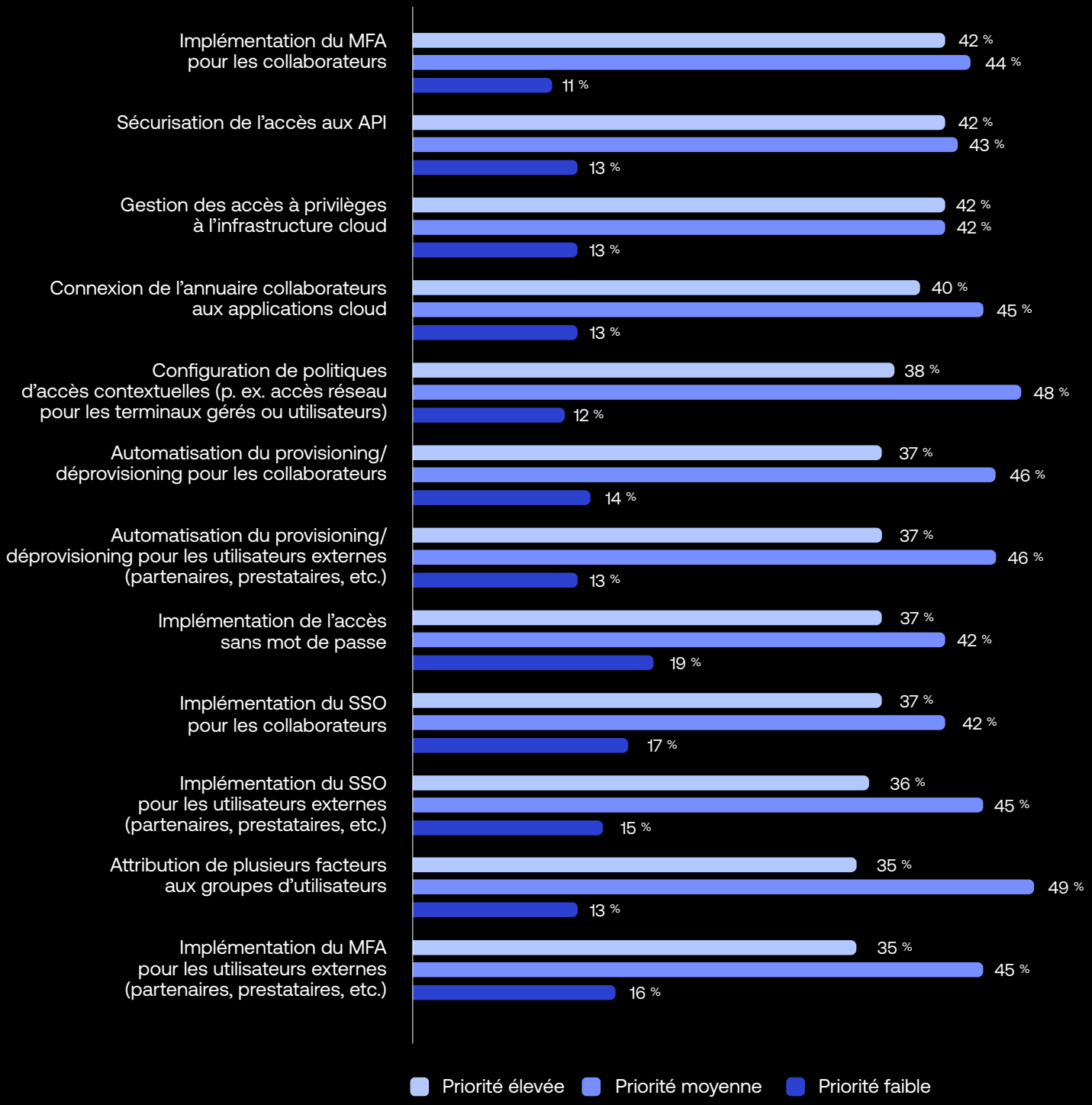
En ce qui concerne les initiatives de sécurité toujours à l'étude au sein des entreprises interrogées, les données de cette année révèlent une répartition assez uniforme, les trois grandes implémentations prévues étant la gestion des accès à privilèges au cloud, la sécurisation de l'accès aux API et l'implémentation du MFA pour les collaborateurs.

En 2021 et 2022, le déploiement du MFA et du SSO pour les collaborateurs venait en tête de la liste de mesures de sécurité déjà implémentées par les répondants, suivi de près par la connexion des annuaires collaborateurs aux applications cloud. En 2021, la principale priorité pour les 12 à 18 mois à venir était le SSO pour les utilisateurs externes et en 2022, la gestion des accès à privilèges à l'infrastructure cloud.

Parmi les initiatives de sécurité suivantes, lesquelles avez-vous déjà implémentées ?
Tous les répondants



Classez les initiatives de sécurité suivantes par ordre de priorité pour votre organisation dans les 12 à 18 prochains mois.
Tous les répondants



Remarque : la somme des colonnes n'est pas toujours égale à 100 % en raison de l'utilisation de la méthode d'arrondi à l'entier le plus proche.

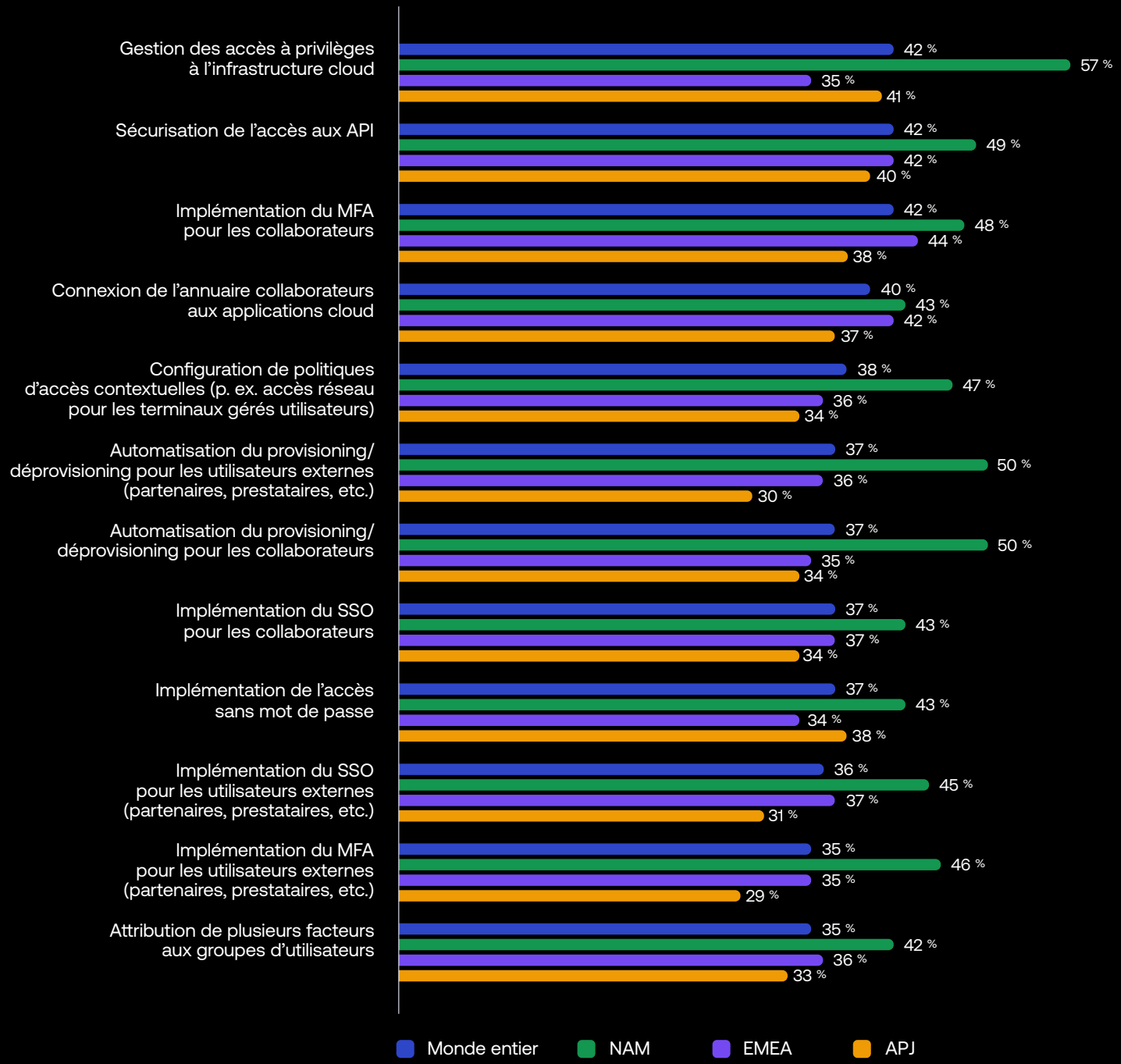
Maturité des identités collaborateurs

Planification des implémentations

2021	1	SSO pour les utilisateurs externes (57 %)
	2	Politiques d'accès contextuelles (43 %)
	3	MFA pour les utilisateurs externes, tels que les partenaires et prestataires (42 %)
2022	1	Gestion des accès à privilèges à l'infrastructure cloud (45 %)
	2	Sécurisation de l'accès aux API (41 %)
	3	Automatisation du provisioning/déprovisioning pour les collaborateurs (38 %)
2023	1	Gestion des accès à privilèges à l'infrastructure cloud (42 %)
	2	Sécurisation de l'accès aux API (42 %)
	3	MFA pour les collaborateurs internes (42 %)

Chaque année, nous demandons aux participants à l'enquête de dresser la liste de solutions Zero Trust qu'ils prévoient d'implémenter dans les 12 à 18 prochains mois. Sur la base des trois premières réponses données chaque année, plusieurs tendances intéressantes semblent émerger. En 2021, les entreprises étaient surtout déterminées à implémenter le MFA et le SSO pour les utilisateurs externes et à renforcer les politiques d'accès. Comme ces mesures ont déjà été déployées par de nombreuses organisations, leur priorité va désormais à la sécurisation de l'accès à privilèges au cloud et de l'accès aux API, ainsi qu'à l'automatisation du provisioning/déprovisioning pour les collaborateurs (l'année dernière) et l'implémentation du MFA pour les collaborateurs (cette année).

Quelles initiatives de sécurité sont prioritaires pour votre organisation au cours des 12 à 18 prochains mois ? (Le tableau ne renseigne que les initiatives à « priorité élevée ».)
Comparaison régionale



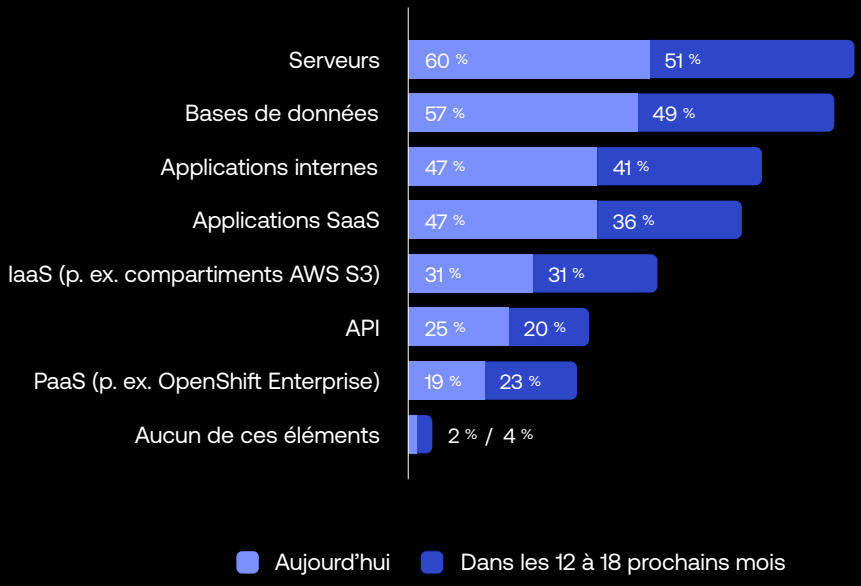
Les entreprises d'Amérique du Nord accordent une priorité plus élevée aux initiatives de sécurité

Une analyse approfondie des résultats de notre enquête révèle l'émergence de variations régionales. Les répondants sont plus susceptibles d'accorder une priorité plus élevée aux initiatives de sécurité de tous types en Amérique du Nord — la gestion de l'accès à privilèges au cloud et l'automatisation du provisioning/déprovisioning venant en tête en termes d'initiatives de sécurité prévues spécifiques. Dans l'EMEA, les initiatives prioritaires sont l'implémentation du MFA pour les collaborateurs, la sécurisation de l'accès aux API et la connexion de l'annuaire collaborateurs aux applications cloud. Globalement, pour les entreprises de la région APJ, aucune initiative n'émerge comme véritablement prioritaire, la répartition étant ici assez uniforme en termes des initiatives prévues. Viennent en tête la gestion des accès à privilèges à l'infrastructure cloud et la sécurisation de l'accès aux API, suivies de près par l'implémentation du MFA pour les collaborateurs, l'implémentation de l'accès sans mot de passe et la connexion des annuaires collaborateurs aux applications cloud.

Maturité des identités collaborateurs

Protection de l'authentification

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



Remarque : la somme des colonnes n'est pas toujours égale à 100 % car les répondants peuvent sélectionner deux réponses.

Les serveurs et les bases de données représentent les ressources les plus susceptibles de bénéficier d'une protection MFA/SSO

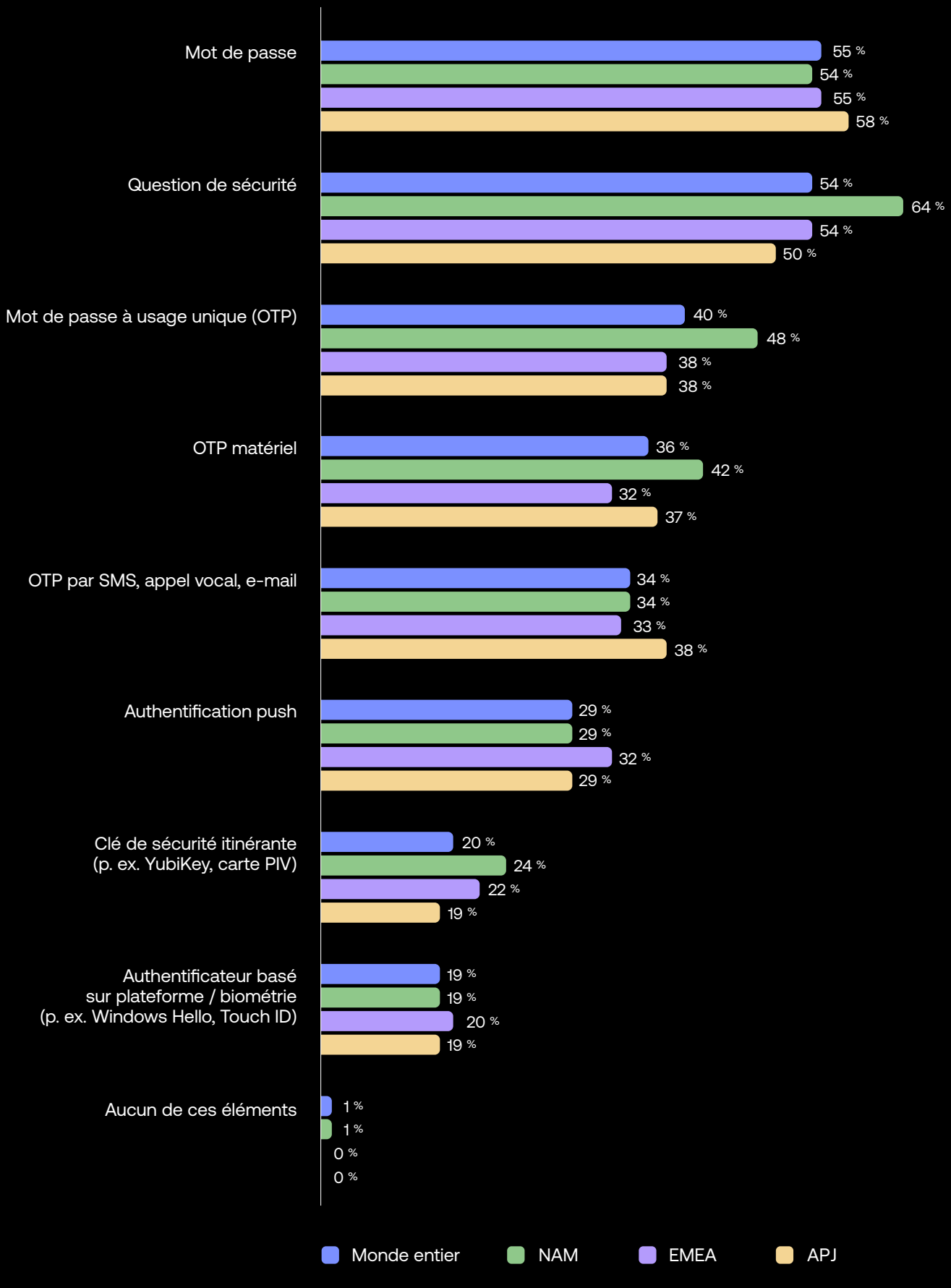
Dans le rapport de l'année dernière, la priorité allait à l'extension du MFA et du SSO aux applications internes et aux applications SaaS. Cette année, elle s'oriente vers des composants réseau essentiels : 3 répondants sur 5 (60 %) déclarent déjà utiliser le MFA et/ou le SSO pour les serveurs. De plus, la protection des bases de données reposant sur l'identité gagne également du terrain, 57 % des répondants ayant déjà étendu le MFA et/ou le SSO à celles-ci. L'analyse des données au niveau des régions ne montre pas d'écart significatif : les serveurs, les bases de données et les applications (internes et SaaS) figurent parmi les principales catégories citées par les entreprises des régions NAM, EMEA et APJ, tant en termes de mesures déjà appliquées que prévues.

Des authentificateurs plus robustes gagnent du terrain sur les mots de passe

Les mots de passe restent encore et toujours la norme en matière d'authentification, et ce, en dépit de leur fiable niveau d'assurance. Ils sont encore utilisés dans les entreprises de plus de la moitié de nos répondants, tous pays confondus. Les questions de sécurité (facteurs à faible assurance également) viennent en deuxième place, au niveau mondial et dans les régions EMEA et APJ, tandis qu'elles se classent en première position en Amérique du Nord. Globalement, les entreprises restent très nombreuses à utiliser des facteurs à faible assurance (les deux précités ainsi que les mots de passe à usage unique générés par matériel et ceux communiqués par e-mail, SMS et appel vocal), alors qu'il est relativement facile de les compromettre.

Les facteurs à niveau d'assurance moyen comme les mots de passe à usage unique via un jeton matériel et l'authentification push sont utilisés par un nombre moindre d'organisations (respectivement 36 % et 29 %). Seulement 19 % des entreprises ont recours à des facteurs à niveau d'assurance élevé comme les authentificateurs basés sur une plateforme et la biométrie. Selon nos prévisions, le MFA va continuer de se généraliser tandis que des réglementations de plus en plus strictes contraindront certains secteurs comme les services financiers et le secteur public à adopter l'authentification sans mot de passe et d'autres facteurs d'authentification résistants au phishing, offrant un niveau d'assurance élevé.

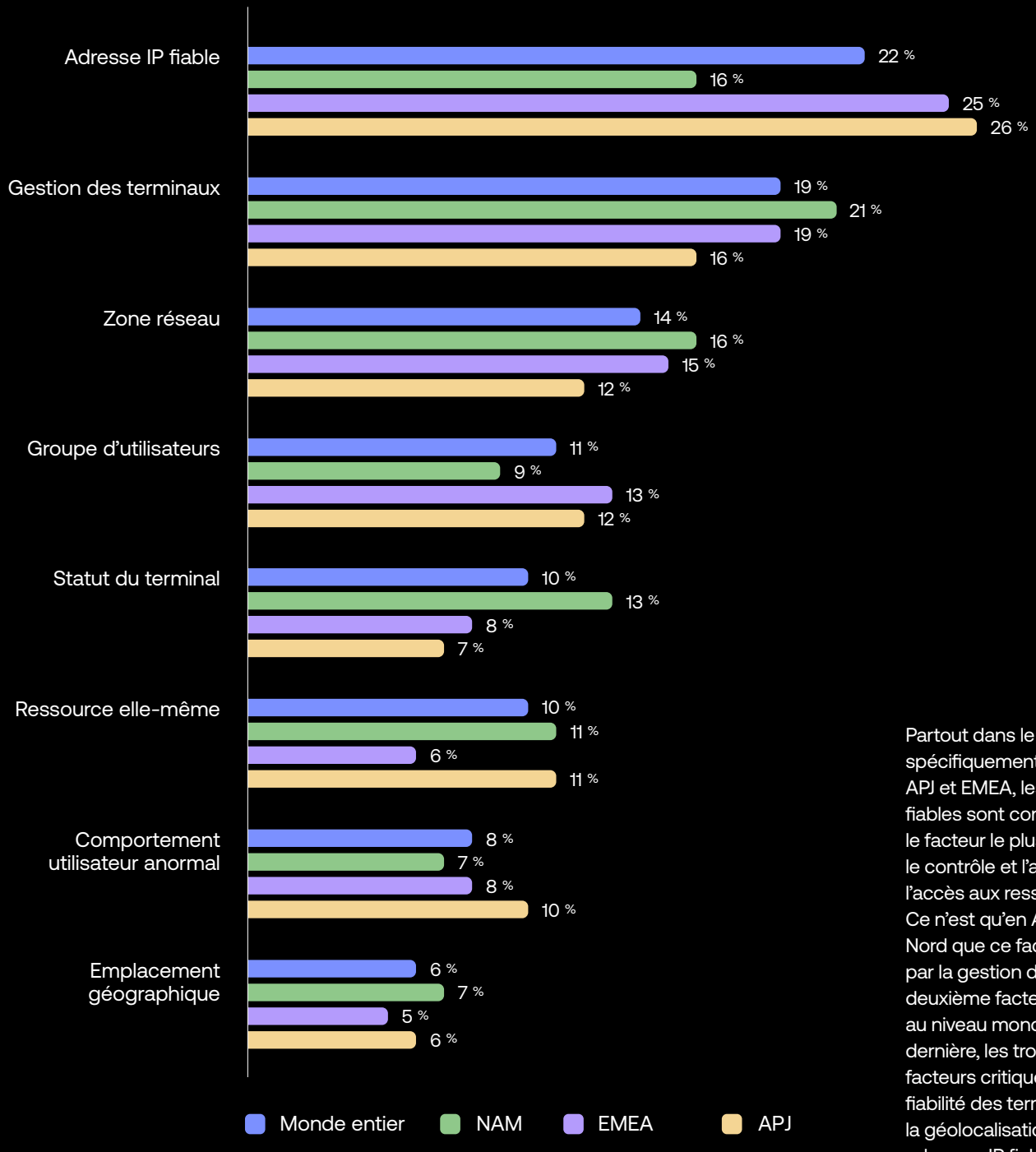
Sélectionnez les facteurs d'authentification que votre entreprise utilise pour vérifier l'identité des utilisateurs internes et externes.
Comparaison régionale



Maturité des identités collaborateurs

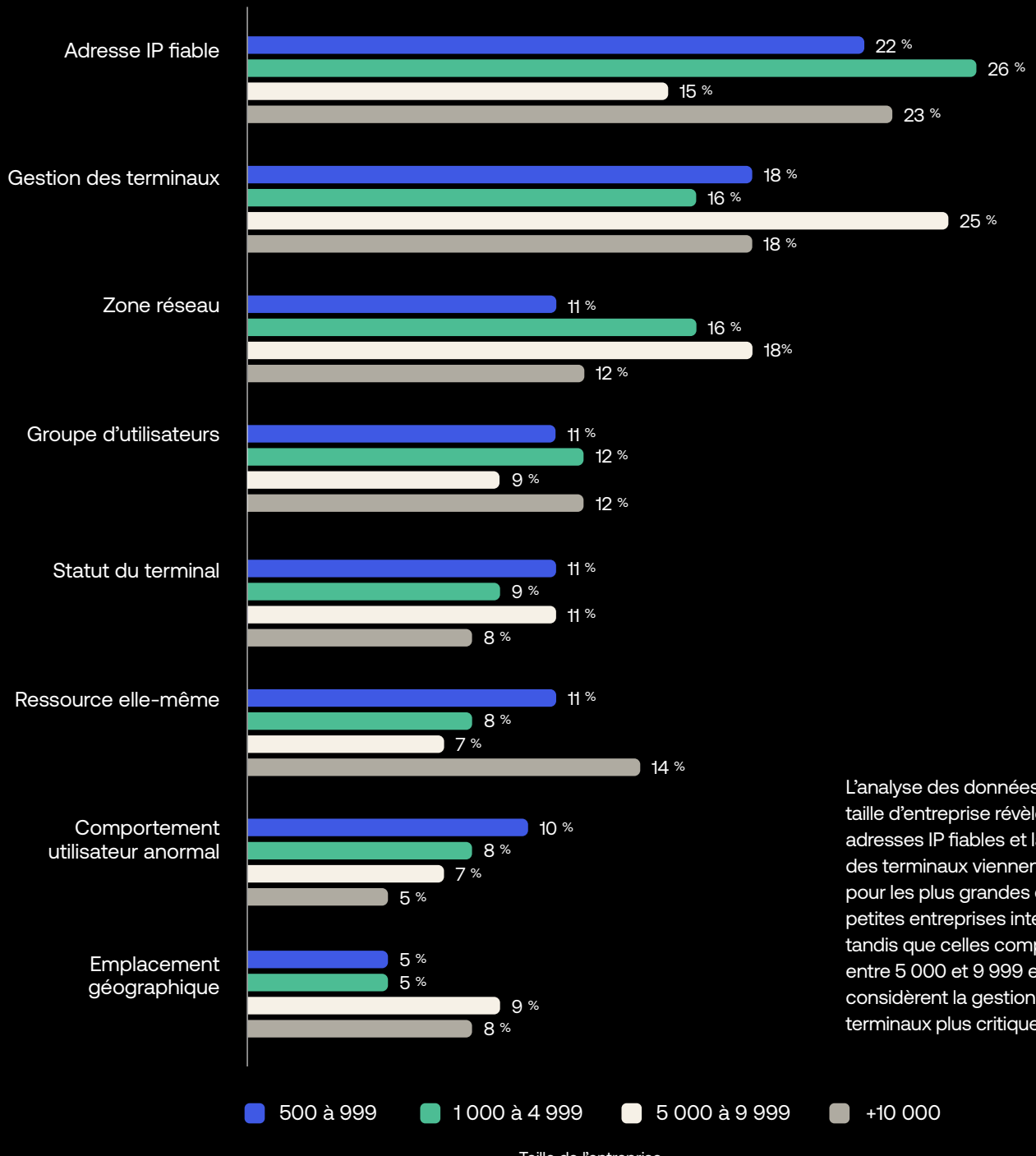
Approbation de l'accès aux ressources internes

Quels sont les facteurs les plus critiques dans le contrôle et l'approbation des accès à vos ressources internes ?
Comparaison régionale



Partout dans le monde, mais plus spécifiquement dans les régions APJ et EMEA, les adresses IP fiables sont considérées comme le facteur le plus critique pour le contrôle et l'approbation de l'accès aux ressources internes. Ce n'est qu'en Amérique du Nord que ce facteur est devancé par la gestion des terminaux (le deuxième facteur le plus critique au niveau mondial). L'année dernière, les trois premiers facteurs critiques étaient la fiabilité des terminaux, la géolocalisation et les adresses IP fiables.

Quels sont les facteurs les plus critiques dans le contrôle et l'approbation des accès à vos ressources internes ?
Par taille de l'entreprise



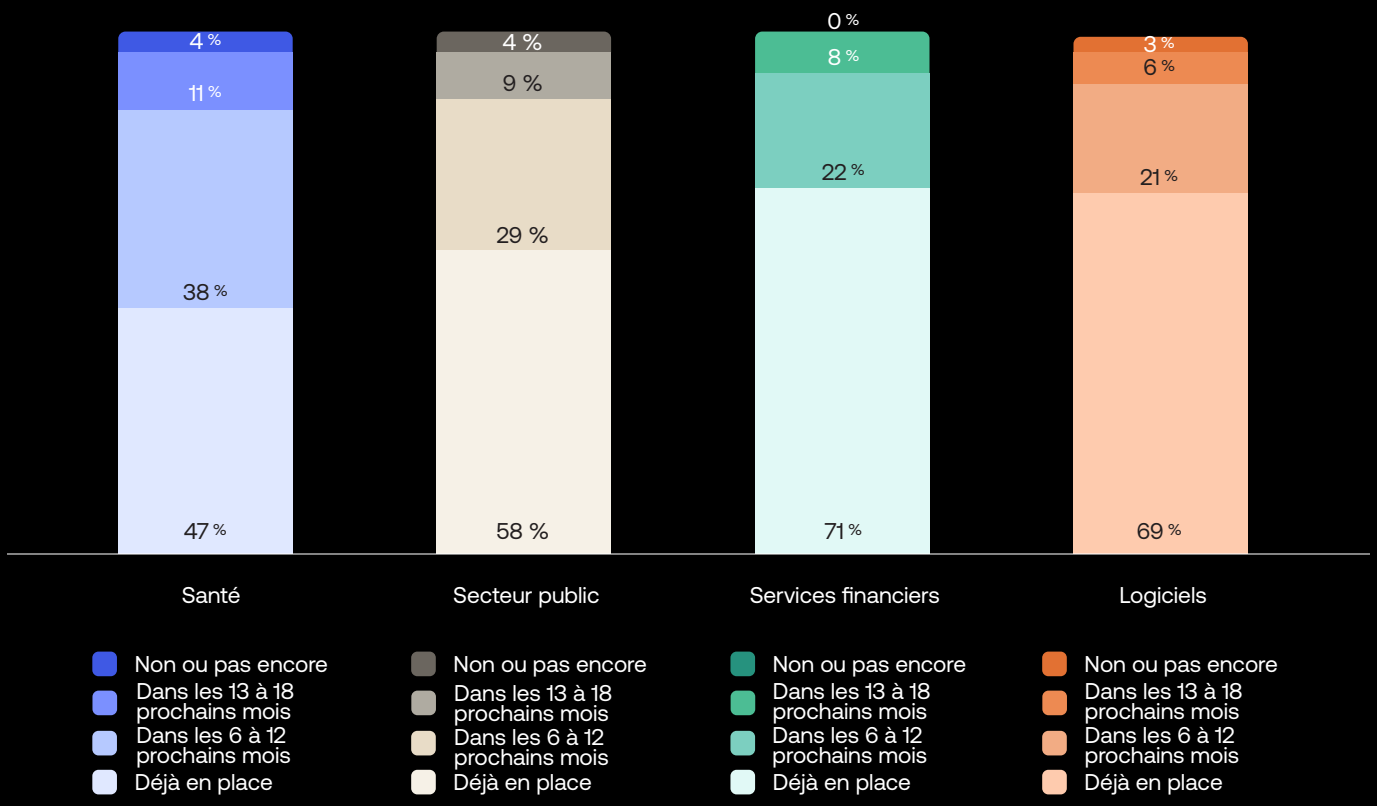
L'analyse des données par taille d'entreprise révèle que les adresses IP fiables et la gestion des terminaux viennent en tête pour les plus grandes et les plus petites entreprises interrogées, tandis que celles comptant entre 5 000 et 9 999 employés considèrent la gestion des terminaux plus critique. ■

Progression du Zero Trust par secteur d'activité

Analyse détaillée des principaux secteurs d'activité

Le parcours vers une sécurité Zero Trust varie considérablement d'un secteur à l'autre, au même titre que les priorités et les pratiques des entreprises. L'enquête de cette année s'intéresse une nouvelle fois aux données de quatre secteurs clés : la santé, le secteur public, les services financiers et les logiciels. Les trois premiers étant très réglementés, ils ont plus de motivations d'investir dans des initiatives de sécurité Zero Trust pour préserver la protection et la conformité de leurs écosystèmes. Dans l'ensemble, les quatre secteurs semblent avoir progressé depuis l'année dernière, mais tâtonnent encore pour véritablement tirer parti de la sécurité Zero Trust.

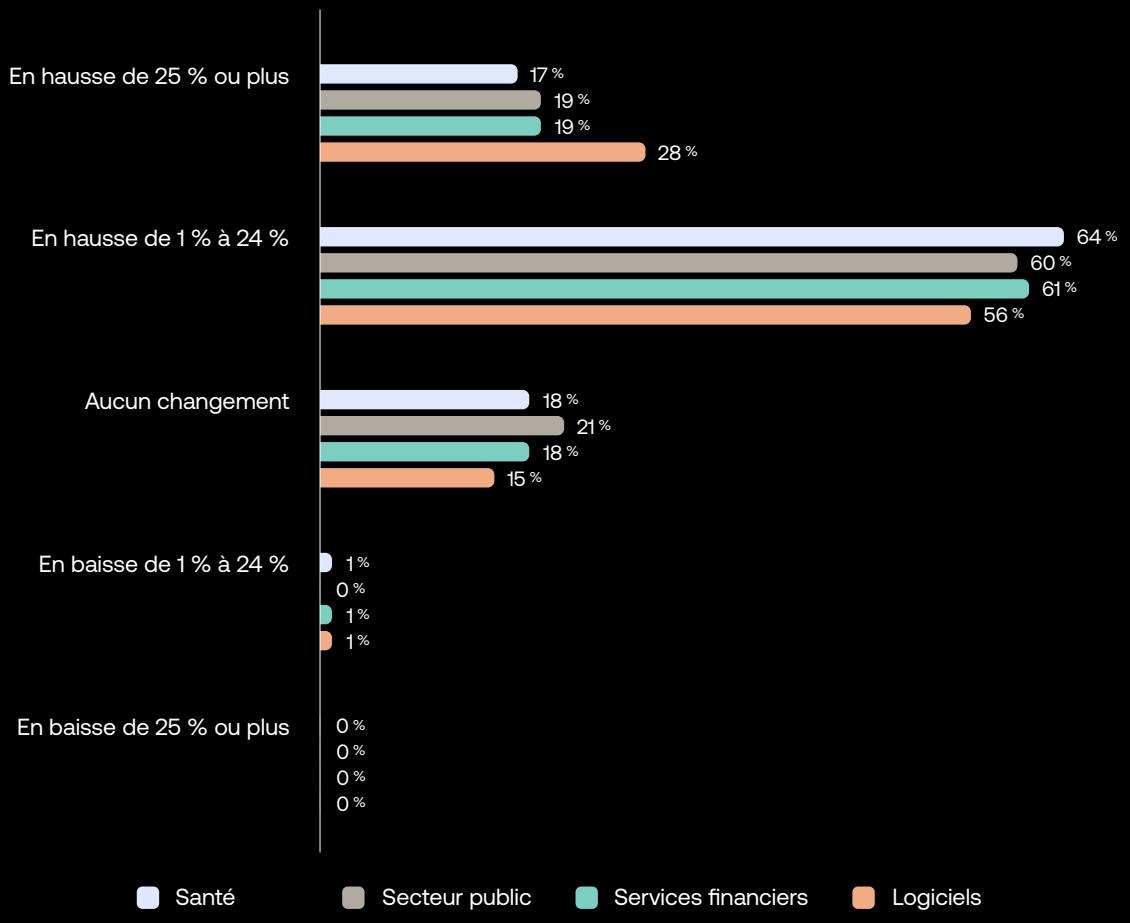
Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les 12 à 18 prochains mois ?
Comparaison par secteur



Les secteurs des services financiers et des logiciels sont en tête en matière d'adoption du Zero Trust

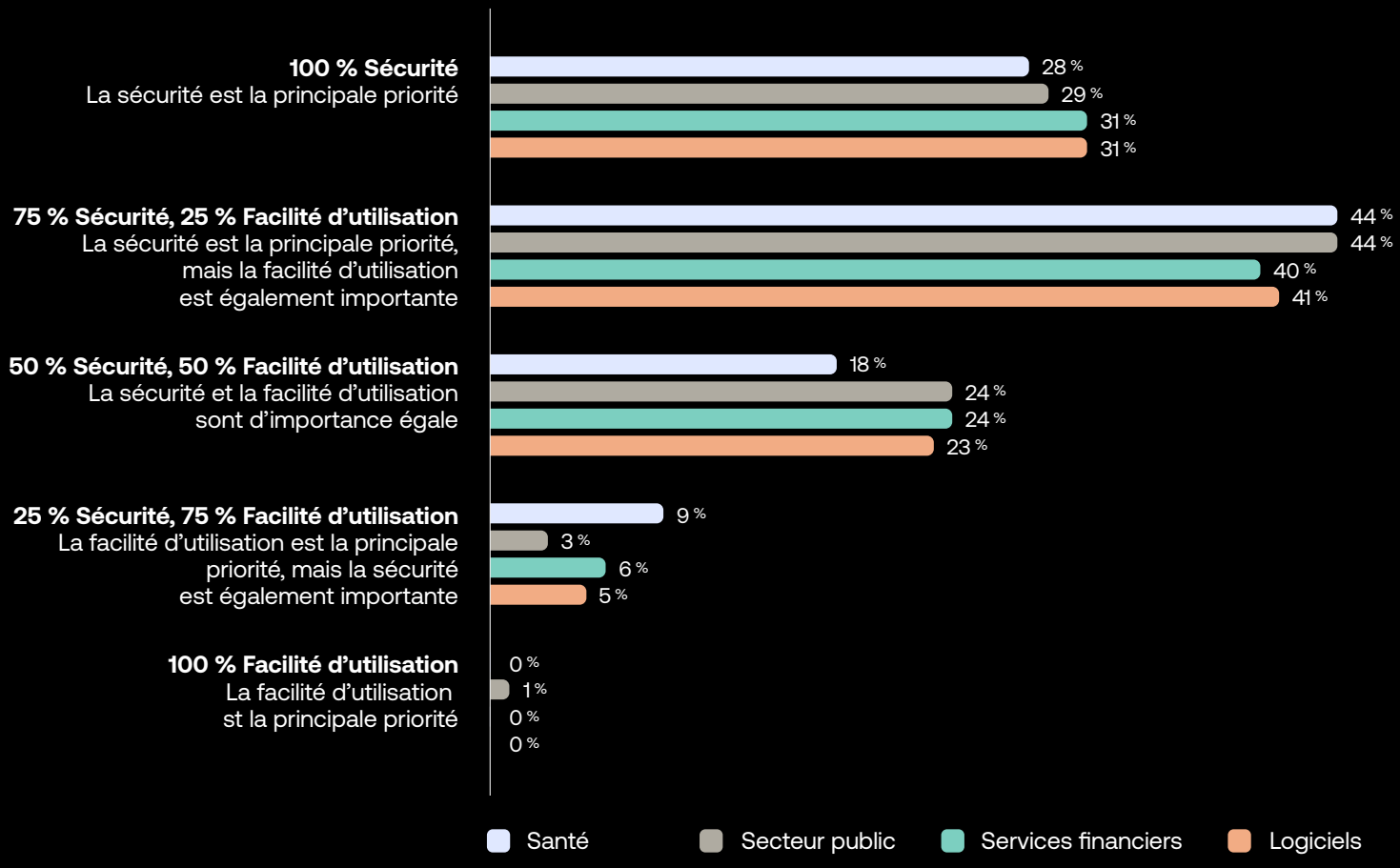
Tous secteurs confondus, l'enquête de cette année révèle une véritable volonté d'implémenter le Zero Trust. Parmi les répondants des quatre secteurs cibles, ils sont à peine 4 % à avoir déclaré n'avoir « aucune initiative Zero Trust en place et aucune prévue dans les 18 prochains mois ». Les entreprises de services financiers et d'édition de logiciels sont les plus susceptibles d'avoir mis en place une initiative à l'heure actuelle (respectivement 71 % et 68 %). Elles sont suivies de près par le secteur public et la santé, comme nous le verrons dans les pages suivantes.

Comment le budget alloué par votre entreprise aux initiatives de sécurité Zero Trust a-t-il évolué (le cas échéant) au cours des 12 derniers mois ?
Comparaison par secteur



En dépit des pressions macroéconomiques forçant la compression des coûts dans d'autres départements, les entreprises des quatre secteurs étudiés continuent de délier les cordons de la bourse pour les initiatives de sécurité Zero Trust. Parmi les organisations interrogées dans ces quatre secteurs, environ quatre sur cinq ont rapporté une augmentation des budgets alloués aux initiatives de sécurité l'année dernière, et pratiquement aucune d'entre elles n'a vu son budget sécurité diminuer.

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



Comme le montre clairement ce graphique, c'est la sécurité qui l'emporte. D'après le rapport 2022 Data Breach Report de l'Identity Theft Resource Center, des brèches de données se produisent désormais près de cinq fois par jour. Dans un tel contexte, rien d'étonnant à ce que la facilité d'utilisation soit reléguée au second plan. Parmi les répondants des quatre secteurs interrogés sur leurs priorités, la réponse la plus fréquente était d'accorder la primauté à la sécurité sur la facilité d'utilisation selon un rapport 75/25. La deuxième réponse la plus probable, pour tous, est de considérer la sécurité comme une priorité absolue. Minimiser la friction pour les collaborateurs et les prestataires reste important, mais dans les secteurs très réglementés, le risque d'une violation de conformité ou de sécurité l'emporte largement sur celui d'une expérience utilisateur non optimale.

Progression du Zero Trust par secteur d'activité

Santé

Le secteur de la santé est parfois moins prompt à évoluer, mais les organisations continuent d'avancer dans la planification et l'exécution des projets Zero Trust. La majorité des répondants du secteur ont déjà mis en place une initiative Zero Trust ou prévoient d'en démarrer une dans un proche avenir. Et bien que la plupart hésitent toujours à abandonner les facteurs d'authentification risqués, à faible niveau d'assurance, ces organisations sont nombreuses à reconnaître l'importance de l'identité et à adopter le MFA et le SSO pour les utilisateurs internes et externes, ainsi que pour les bases de données et d'autres ressources.

Les phases de définition et planification du Zero Trust se rapprochent des 100 %

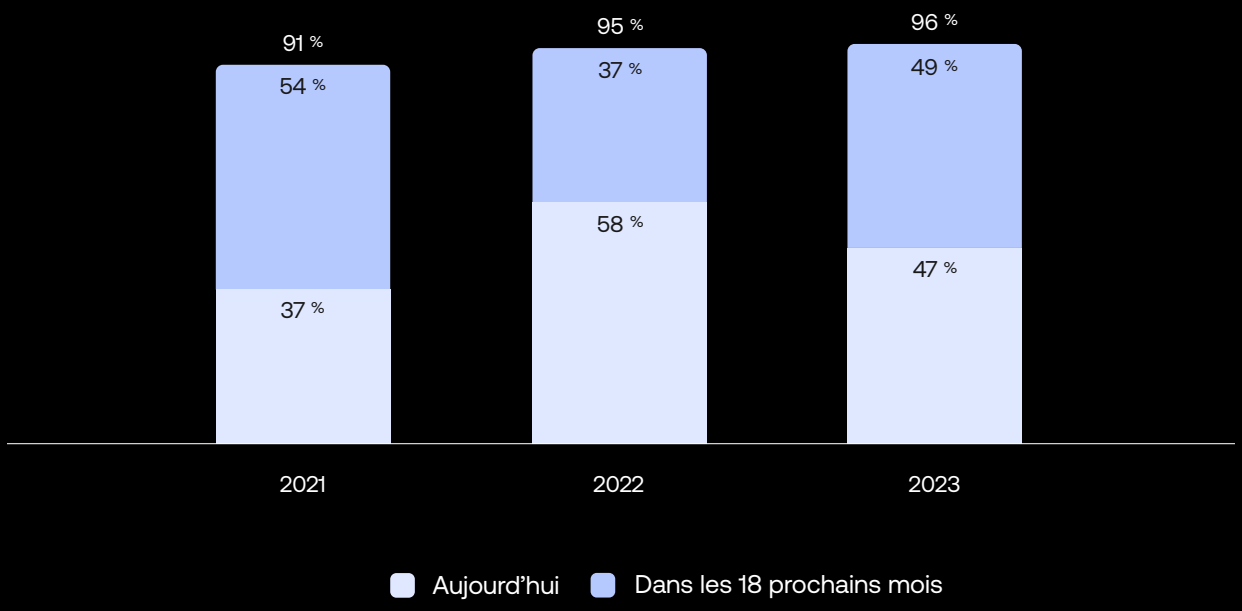
Au cours des trois dernières années, nous avons vu l'intérêt du secteur de la santé vis-à-vis des initiatives Zero Trust fluctuer, mais peu. À l'exception de 4 % d'entre elles, toutes les organisations interrogées cette année déclarent avoir mis en place une initiative Zero Trust ou prévoient de le faire dans les 18 prochains mois. En outre, le nombre total d'organisations qui ont mis en place une initiative ou prévoient de le faire à court terme se rapprochent chaque année un peu plus des 100 %. (Par rapport à l'année dernière, le nombre d'organisations qui déclarent avoir déjà mis en place une initiative a légèrement baissé, peut-être en raison de la diminution des dépenses IT en 2022 constatée par le Wall Street Journal — tendance qui semble s'inverser à l'heure actuelle.) Dans l'ensemble, nous nous attendons à ce qu'un nombre croissant d'organisations du secteur de la santé mettent en œuvre une sécurité Zero Trust, tandis que celles qui l'ont déjà fait continueront d'avancer dans leur parcours.

Le secteur de la santé reste un peu à la traîne, mais entend combler son retard

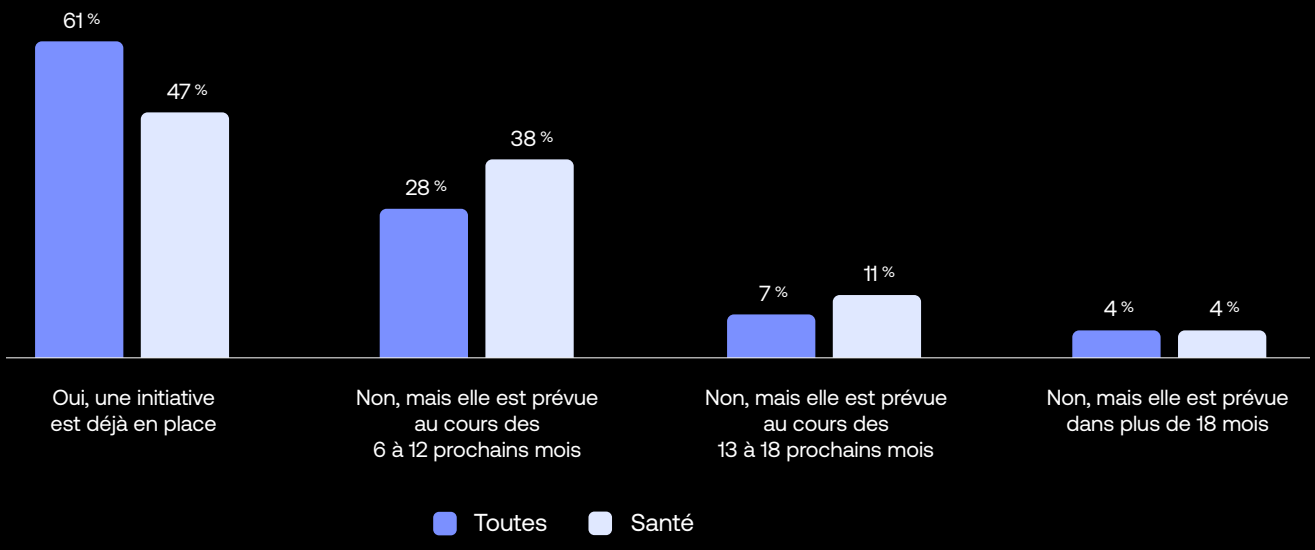
À l'examen des chiffres du secteur de la santé par rapport à ceux de l'ensemble de l'échantillon, nous constatons qu'un nombre moindre a mis en place une initiative Zero Trust par rapport à la moyenne mondiale. Toutefois, ces entreprises ne ménagent pas leurs efforts pour combler leur retard et sont loin devant les autres en ce qui concerne les plans des 6 à 12 prochains mois. En effet, 38 % des organisations du secteur de la santé prévoient une implémentation au cours de cette période, alors que ce pourcentage n'est que de 28 % pour les organisations à l'échelle mondiale.

Interrogés sur l'importance de l'identité dans leur stratégie de sécurité Zero Trust, plus de 9 répondants sur 10 estiment l'identité très ou assez importante. Ce n'est guère surprenant compte tenu des informations d'identification personnelles sensibles qui doivent être impérativement protégées par les organismes de santé (et qui sont par ailleurs au centre des réglementations sectorielles).

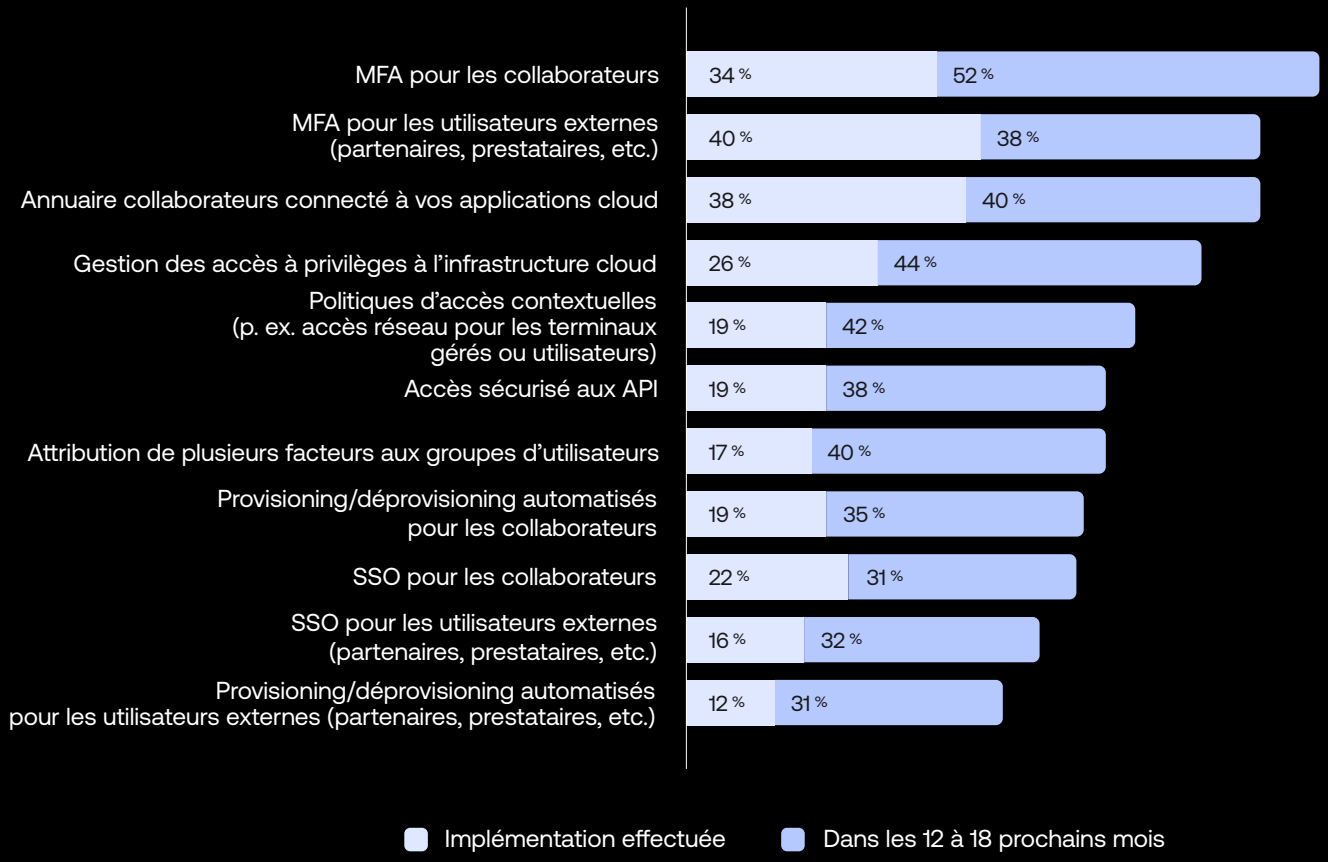
Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les 18 prochains mois ?
Comparaison par année dans le secteur de la santé



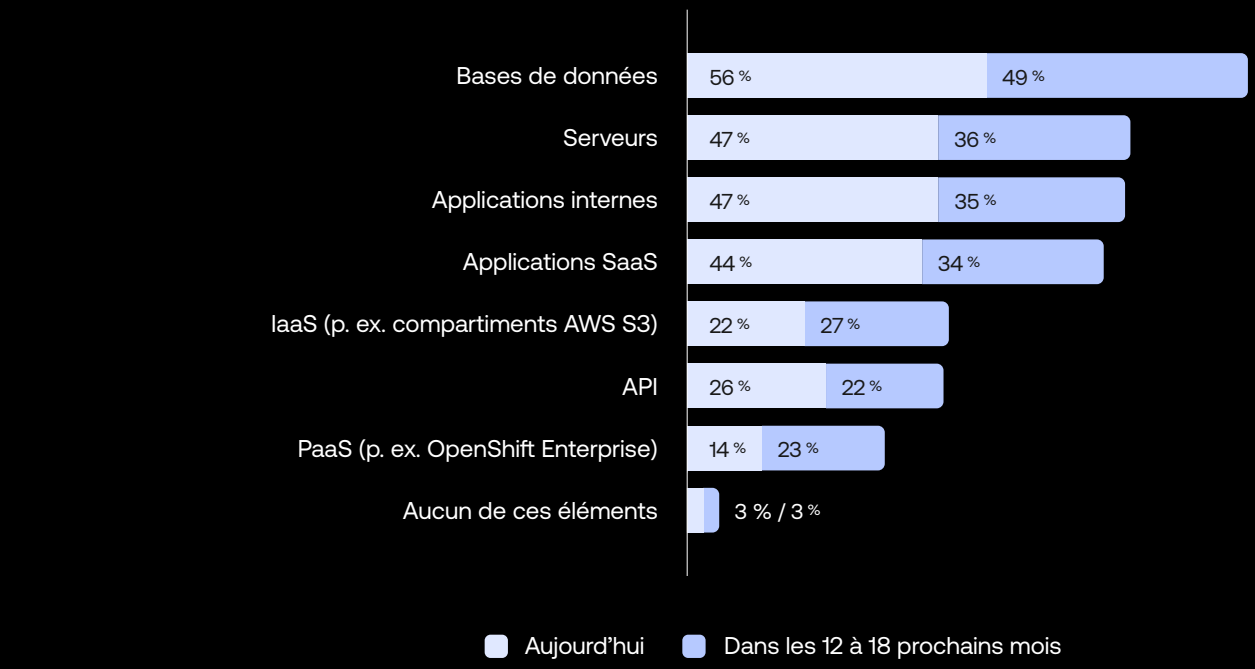
Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les prochains mois ?
Secteur de la santé vs tous les autres participants à l'enquête



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, ou prévoyez-vous de le faire dans les 12 à 18 prochains mois ?
Santé



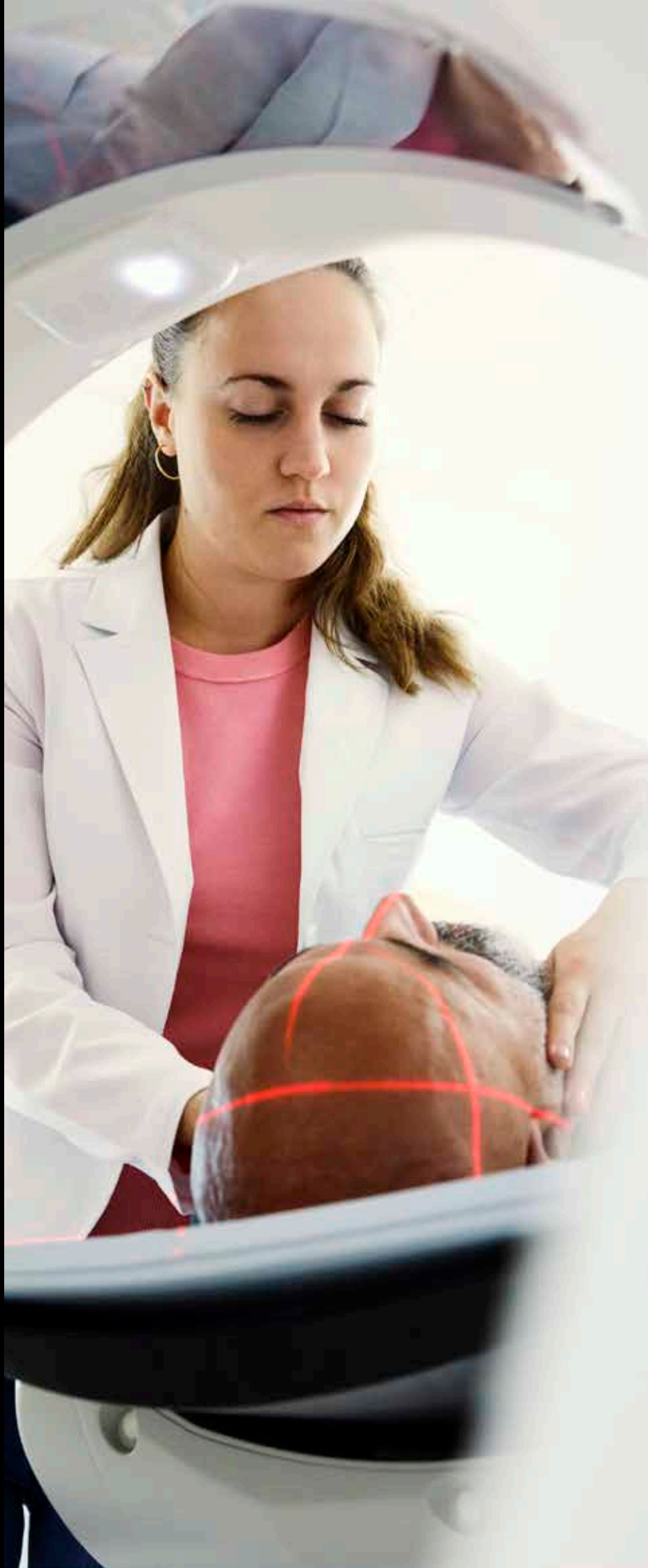
Remarque : la somme des colonnes n'est pas toujours égale à 100 % car les répondants peuvent sélectionner deux réponses.

Principales initiatives du secteur de la santé : MFA et connexion des annuaires

Le MFA pour les collaborateurs et pour les utilisateurs externes figure depuis toujours parmi les initiatives prioritaires des organisations du secteur et c'est encore le cas cette année. La connexion des annuaires collaborateurs aux applications cloud complète le trio de tête en ce qui concerne les initiatives de sécurité déjà implémentées. Plus d'un tiers des organisations interrogées ont déjà mis en place le MFA pour les collaborateurs et, en ce qui concerne les projets prévus dans un avenir proche, l'ajout du MFA pour les collaborateurs arrive en tête avec 52 %. Toujours pour les projets en prévision, d'autres initiatives, telles que le SSO et le provisioning automatisé, sont moins prioritaires pour ces organisations cette année.

Les bases de données, les serveurs et les applications dans le trio de tête pour la protection par SSO/MFA

Les organisations de santé sont les plus susceptibles d'avoir étendu la protection par SSO et/ou MFA aux bases de données. En effet, comme celles-ci peuvent héberger des informations sensibles et confidentielles sur les patients, elles représentent une cible très prisée par les cybercriminels. Mais l'extension du SSO/MFA aux serveurs ainsi qu'aux applications internes et SaaS n'est pas loin derrière, en termes d'adoption actuelle et future pour les entreprises de ce secteur.



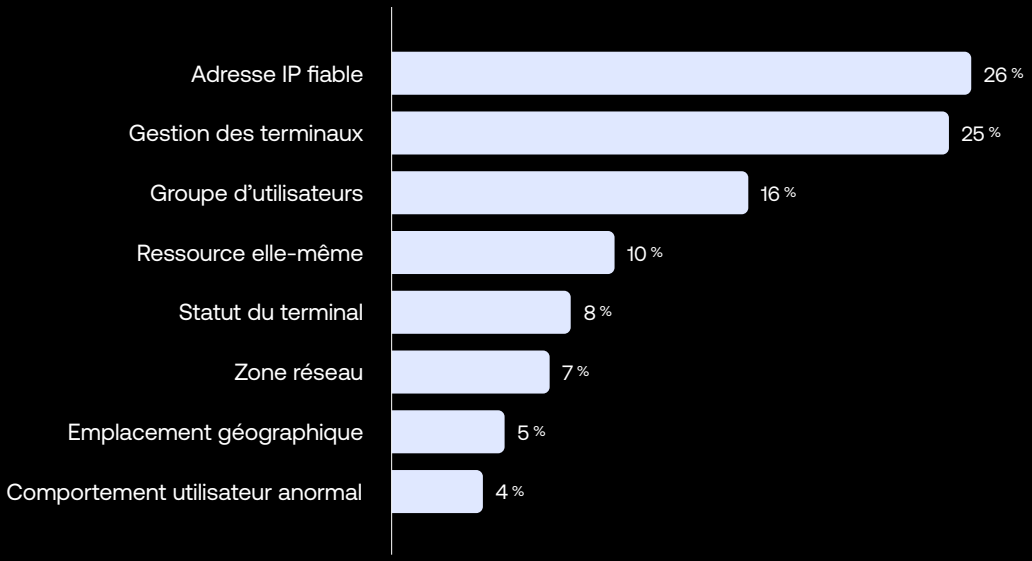
Les adresses IP fiables et la gestion des terminaux considérés comme principaux facteurs de contrôle des accès

Plus de la moitié de toutes les organisations du secteur de la santé interrogées considèrent les adresses IP fiables ou la gestion des terminaux comme le facteur prioritaire pour le contrôle et l'approbation de l'accès aux ressources internes, ce qui est aussi le cas pour les répondants à l'échelle mondiale. Les groupes d'utilisateurs et les ressources elles-mêmes sont les deux facteurs suivants pour le contrôle et l'approbation des accès.

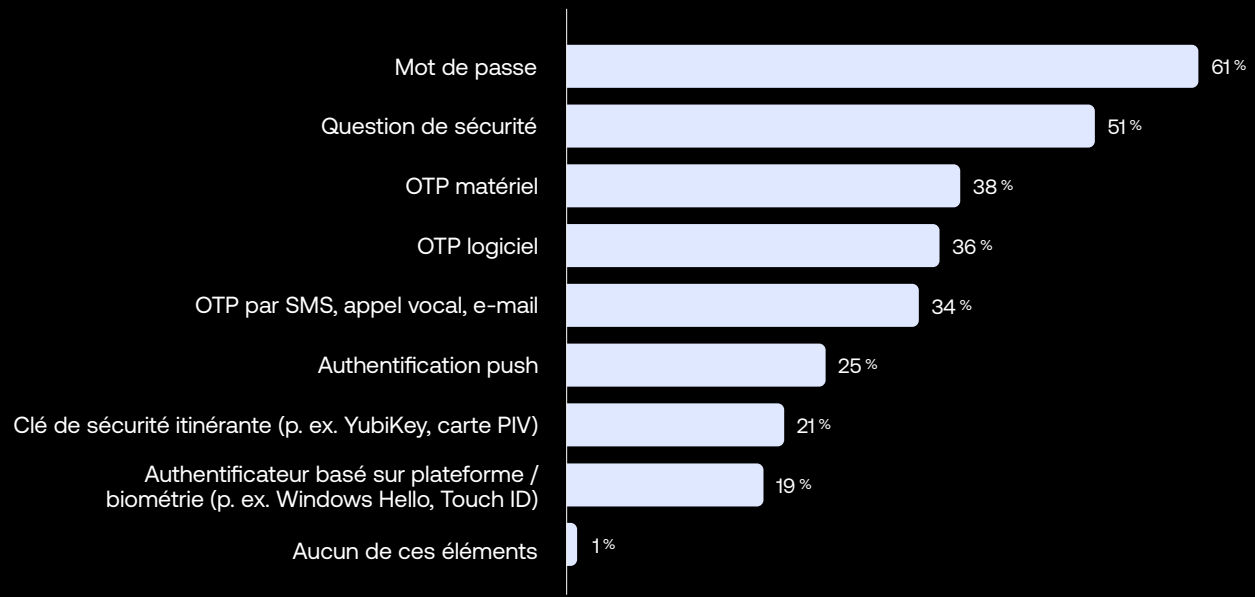
Les mots de passe et les questions de sécurité sont les principaux facteurs d'authentification du secteur de la santé

Les mots de passe restent le premier facteur d'authentification pour les organisations du secteur (61 %). Par conséquent, un futur sans mot de passe est encore loin pour ce secteur. Les questions de sécurité viennent en deuxième position et sont utilisées par plus de la moitié des entreprises interrogées. Les mots de passe à usage unique (OTP) de quelque catégorie que ce soit — matériel, logiciel ou par SMS/appel vocal/e-mail — occupent la troisième place, pratiquement à égalité. Quant aux authentificateurs basés sur une plateforme et à la biométrie, ils figurent parmi les facteurs d'authentification les moins usités.

Classez le facteur le plus critique dans le contrôle et l'approbation des accès à vos ressources internes.
Santé



Sélectionnez les facteurs d'authentification que votre organisation utilise pour vérifier l'identité des utilisateurs internes et externes.
Santé



Progression du Zero Trust par secteur d'activité

Secteur public

S'il est bien un secteur sous pression pour renforcer sa sécurité avec le Zero Trust, c'est le secteur public. En Amérique du Nord, par exemple, la stratégie Zero Trust fédérale aux États-Unis exige expressément que toutes les agences fédérales mettent en œuvre des normes de cybersécurité spécifiques et atteignent certains objectifs précis d'ici septembre 2024 pour renforcer les défenses du gouvernement contre des campagnes de menaces persistantes et toujours plus sophistiquées. Et c'est loin d'être la seule directive gouvernementale américaine. Il en existe d'autres, par exemple le document National Cybersecurity Strategy publié par la Maison-Blanche et le plan Zero Trust Strategy and Roadmap du ministère américain de la Défense.

Cette année, nous avons interrogé des entités publiques en Amérique du Nord, EMEA et APJ. (Ce rapport concerne uniquement les administrations publiques au niveau national et non local.) Les résultats de l'enquête révèlent que 58 % d'entre elles ont déjà mis en place une initiative Zero Trust et 38 % prévoient de le faire d'ici peu. Ces organisations utilisent le SSO et/ou le MFA pour protéger leurs ressources les plus importantes et déploient un périmètre de sécurité renforcé pour préserver leur infrastructure et leurs ressources.

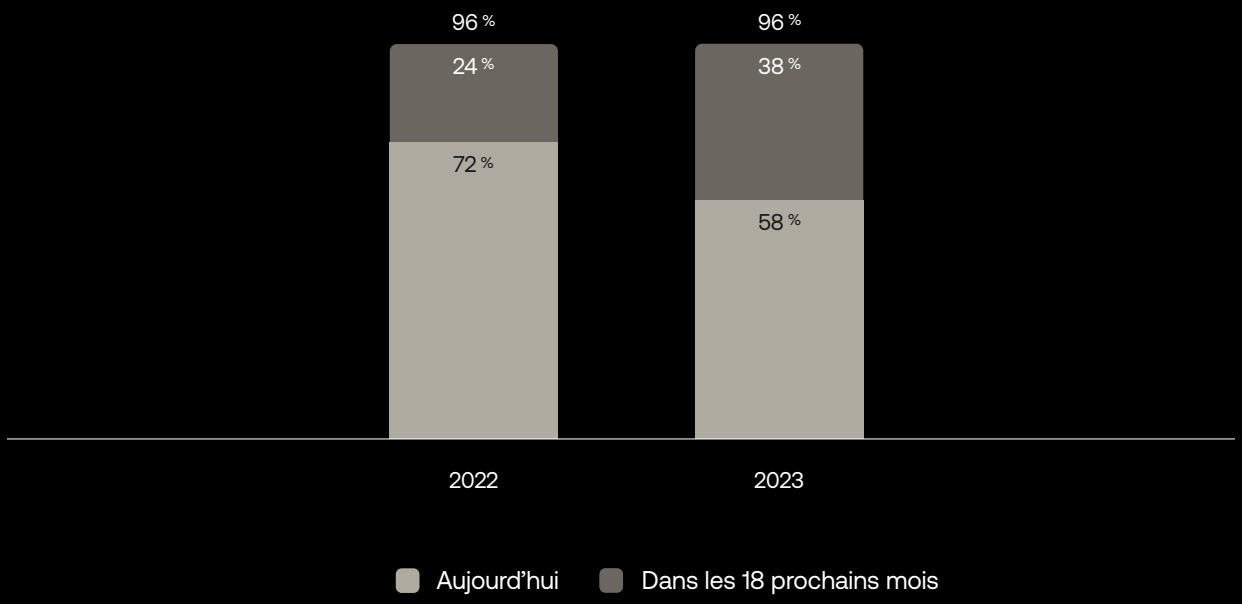
La vaste majorité des organisations du secteur public ont déjà mis en chantier des initiatives Zero Trust

Les chiffres restent stables en ce qui concerne l'engagement vis-à-vis du Zero Trust. Entre 2022 et 2023, le pourcentage des organisations du secteur public ayant déjà mis en place une initiative Zero Trust ou prévoyant de le faire dans un proche avenir s'est maintenu à 96 %. Parmi les organisations interrogées l'année dernière, 72 % avaient mis en place une initiative Zero Trust. Il est toutefois intéressant de noter que les répondants du secteur public de l'année dernière provenaient essentiellement d'Amérique du Nord (86 %). Cette année, nous avons élargi la portée de l'enquête : seuls 31 % des organismes publics interrogés cette année proviennent d'Amérique du Nord et, dans cet échantillon plus large, 58 % déclarent avoir déjà mis en place une initiative Zero Trust et 38 % avoir prévu de la démarrer d'ici peu.

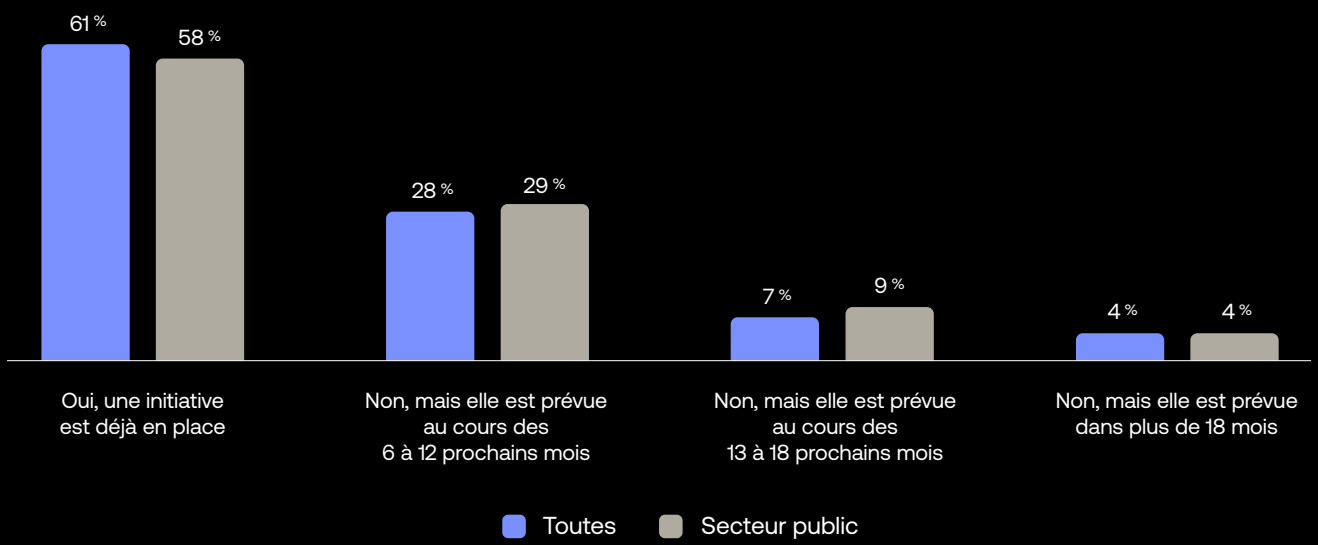
Les organismes du secteur public accusent un retard en ce qui concerne les initiatives en place, mais elles sont plus nombreuses en termes d'initiatives prévues

Cette année, les organisations du secteur public interrogées suivent de près la moyenne mondiale en ce qui concerne les initiatives de sécurité Zero Trust déjà en place : 61 % de l'ensemble des organisations interrogées possèdent un tel programme, contre 58 % dans le secteur public. Par contre, près d'un tiers des entités publiques prévoient d'en lancer un dans les 6 à 12 prochains mois — très souvent pour respecter des directives gouvernementales —, ce qui est légèrement supérieur à la moyenne mondiale.

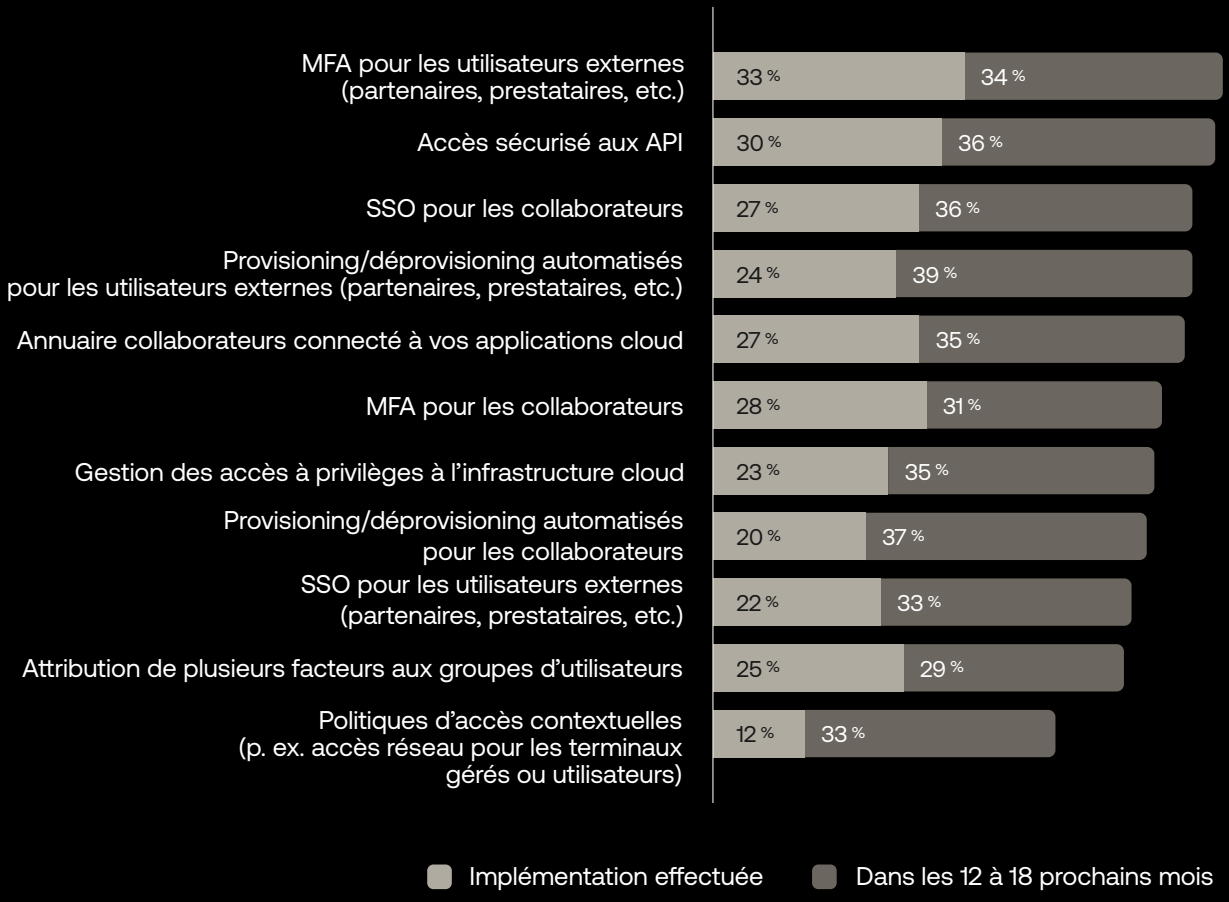
Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les 18 prochains mois ?
Comparaison par année dans le secteur public



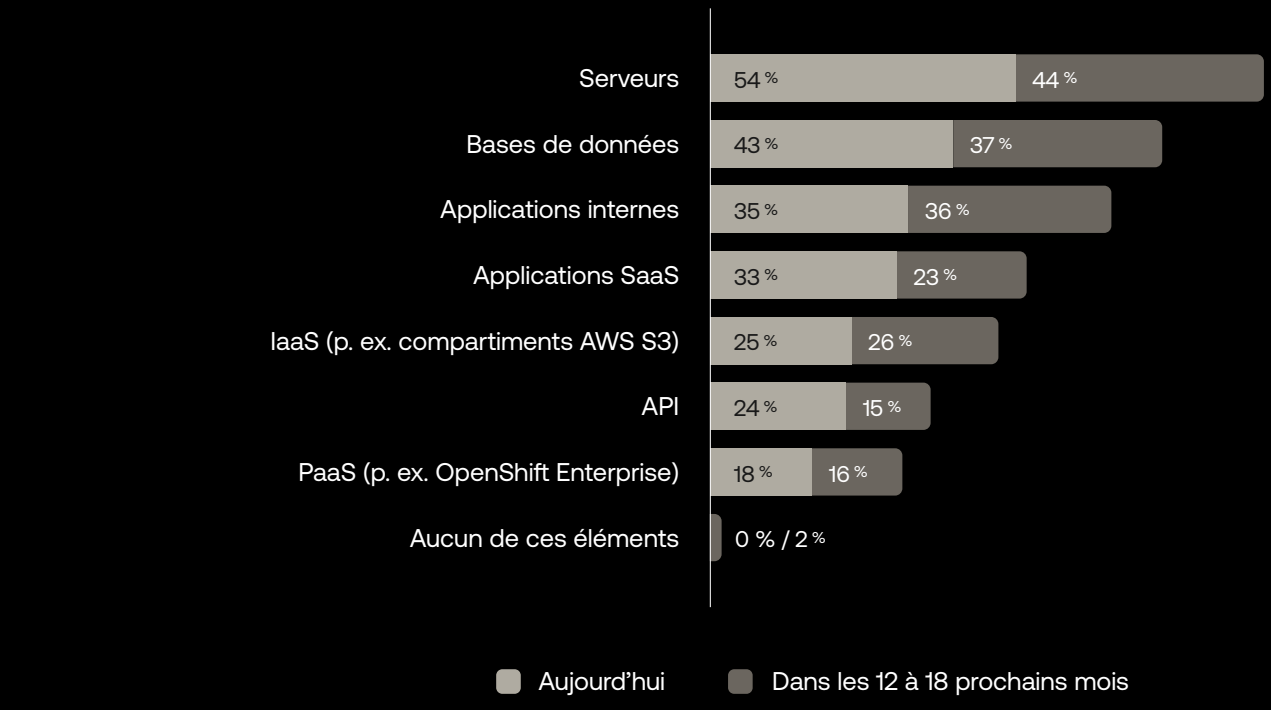
Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les prochains mois ?
Secteur public vs tous les autres participants à l'enquête



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



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 ?
Secteur public



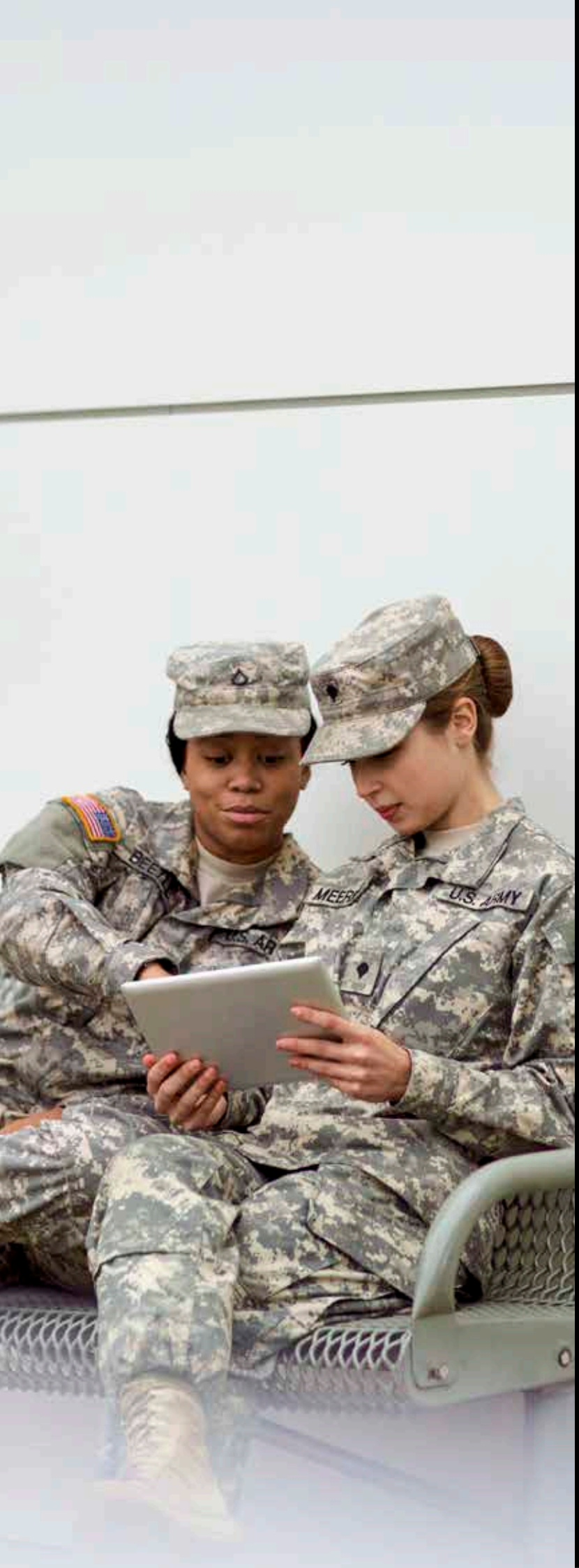
Remarque : la somme des colonnes n'est pas toujours égale à 100 % car les répondants peuvent sélectionner deux réponses.

Les principales initiatives du secteur public sont le MFA pour les utilisateurs externes et l'accès sécurisé aux API

Les entités gouvernementales du monde entier font appel à un large éventail de partenaires externes ou de prestataires étrangers. Dès lors, il n'est guère surprenant que les principales initiatives du secteur public soient le MFA pour les utilisateurs externes (y compris les partenaires et fournisseurs tiers) et la sécurisation de l'accès aux API, qui représentent respectivement 33 % et 30 % des organisations interrogées. Parmi les entités interrogées, 34 % prévoient d'étendre le MFA à ces utilisateurs externes au cours des 12 à 18 prochains mois. En ce qui concerne les priorités du secteur public, le SSO pour les collaborateurs et le provisioning/déprovisioning automatisés pour les utilisateurs externes occupent les troisième et quatrième places.

La protection par SSO/MFA étendue en priorité aux serveurs et bases de données

Les serveurs et les bases de données sont les premiers à bénéficier d'une protection SSO/MFA dans le secteur public. Plus de la moitié des organisations du secteur interrogées ont déjà appliqué le SSO et/ou le MFA aux serveurs et 43 % ont appliqué l'un de ces types d'authentification ou les deux aux bases de données. Viennent ensuite les applications SaaS et internes, un tiers des organisations ayant déjà mis en place le SSO et/ou le MFA pour celles-ci, suivies par les solutions IaaS, les API et les plateformes PaaS.



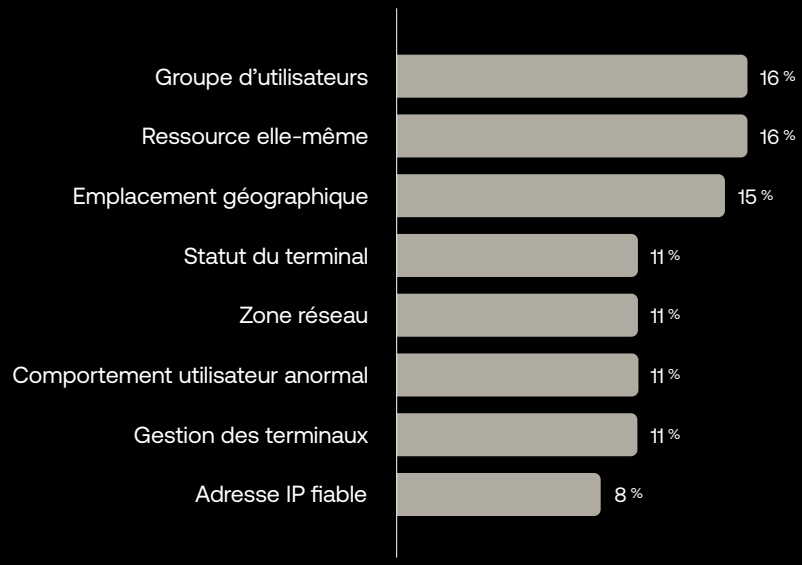
Les groupes d'utilisateurs et les ressources sont les deux facteurs les plus critiques pour l'accès aux ressources

Les organisations du secteur public sont tout particulièrement attentives à protéger leurs ressources numériques contre les tentatives d'accès non autorisées. Les principaux facteurs de contrôle et d'approbation de l'accès aux ressources internes sont les groupes d'utilisateurs, la ressource elle-même et l'emplacement géographique, suivis des autres facteurs, à peu près tous dans la même proportion.

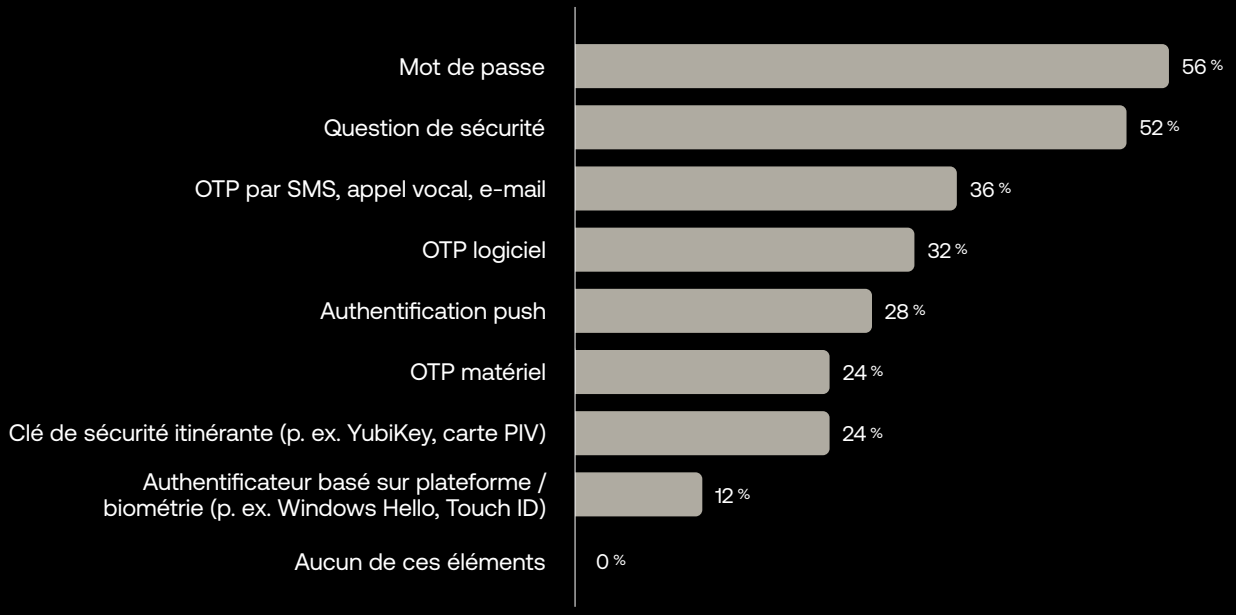
Les mots de passe et les questions de sécurité restent les deux premières mesures de contrôle de l'identité des utilisateurs

Le secteur public continue de faire confiance à des facteurs d'autorisation à niveau d'assurance faible, comme c'est le cas dans les autres secteurs étudiés lors de cette enquête, avec les mots de passe et les questions de sécurité restant les facteurs les plus souvent cités par les répondants. La situation risque toutefois de changer sous peu étant donné la popularité croissante de facteurs à niveau d'assurance plus élevé, comme les mots de passe à usage unique logiciels et matériels, ou ceux envoyés par SMS/appel vocal/e-mail. (En raison de leur nature éphémère, les mots de passe à usage unique sont intrinsèquement plus sûrs que les mots de passe et questions de sécurité stockés dans un emplacement physique et donc plus faciles à pirater.) ■

Classez le facteur le plus critique dans le contrôle et l'approbation des accès à vos ressources internes.
Secteur public



Sélectionnez les facteurs d'authentification que votre organisation utilise pour vérifier l'identité des utilisateurs internes et externes.
Secteur public



Progression du Zero Trust par secteur d'activité

Services financiers

Les entreprises de services financiers constituent des cibles de choix pour les cyberattaquants et n'ont pas été épargnées par les brèches de sécurité ces dernières années. Au moins 79 entreprises américaines de ce secteur ont signalé des brèches de données ayant affecté 1 000 consommateurs ou plus en 2022. Pour les plus graves d'entre elles, le nombre de victimes s'élève à plusieurs millions. Pour ces entreprises, le Zero Trust représente clairement la voie à suivre pour sécuriser leurs systèmes et données clients critiques. Aujourd'hui, plus de deux tiers de toutes les entreprises de services financiers ont déjà mis en place une initiative Zero Trust et le tiers restant déclare avoir un projet en chantier.

7 entreprises de services financiers sur 10 disposent aujourd'hui d'une stratégie Zero Trust

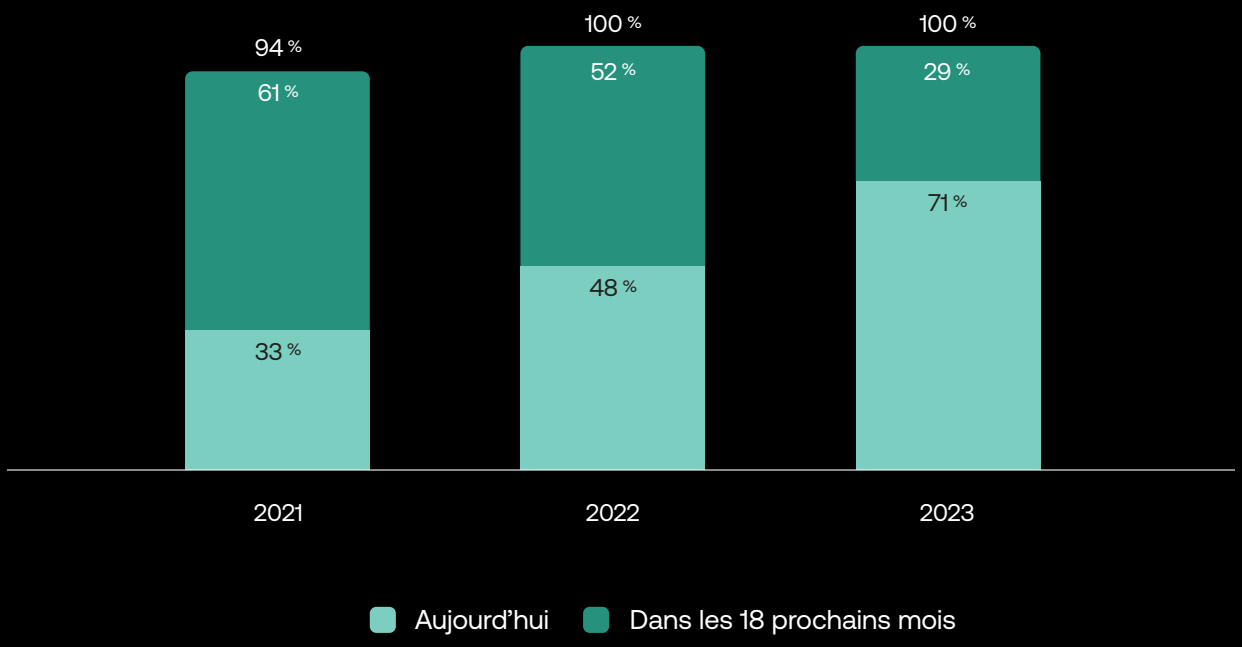
Les brèches de sécurité peuvent s'avérer extrêmement onéreuses : 4,45 millions de dollars par brèche, selon IBM et son rapport Cost of a Data Breach 2023. Rien de surprenant, dès lors, à ce qu'un nombre croissant d'entreprises de services financiers mettent en place des initiatives Zero Trust chaque année. En 2021, seul un tiers des répondants du secteur avait déclaré disposer d'une initiative Zero Trust définie. En 2022, ce pourcentage s'élevait à près de 50 %. Cette année, 71 % des entreprises interrogées affirment avoir mis en place une stratégie Zero Trust. Il s'agit d'une croissance impressionnante en seulement trois ans.

Le secteur des services financiers, chef de file des initiatives Zero Trust

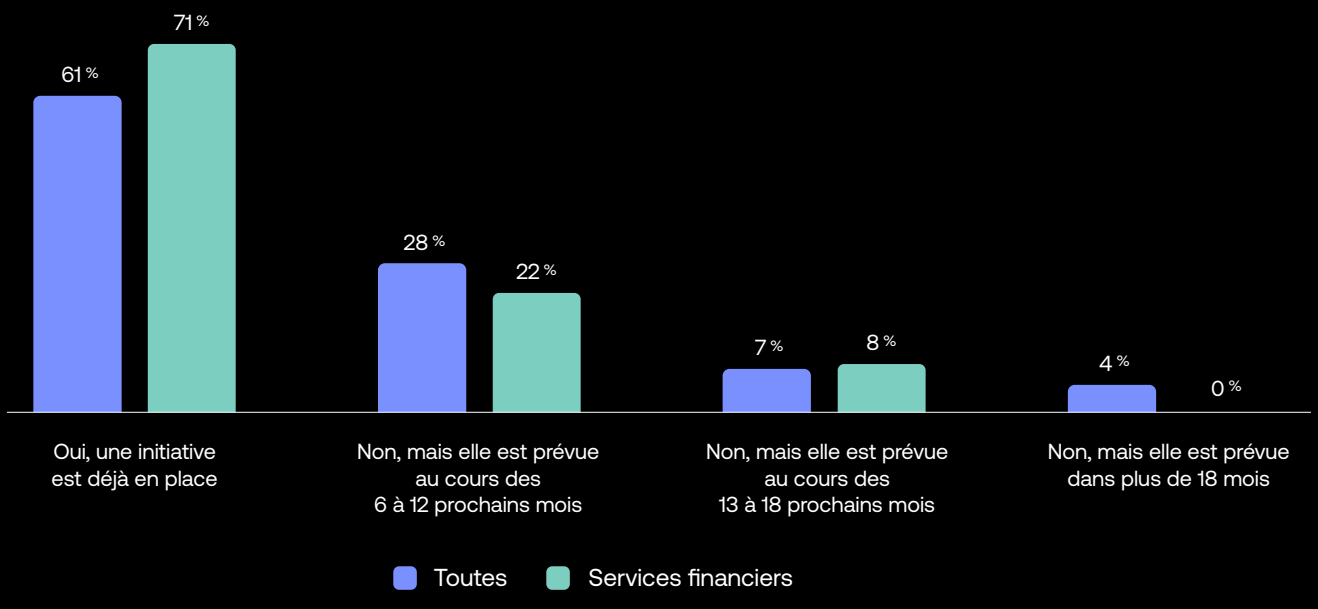
Plus de deux tiers des entreprises de services financiers ont déjà lancé une initiative Zero Trust. 22 % prévoient de le faire dans les 12 prochains mois et 8 % dans les 18 mois qui viennent. En ce qui concerne les initiatives déjà en place, le secteur dépasse la moyenne mondiale et l'ensemble des entreprises de ce secteur interrogées déclarent soit avoir mis en place une initiative Zero Trust, soit prévoir de le faire dans les 18 prochains mois.

En ce qui concerne la valeur de l'identité dans une stratégie Zero Trust, le secteur des services financiers apparaît convaincu de ce principe. Plus de 90 % des répondants estiment l'identité extrêmement ou assez importante dans une stratégie Zero Trust, près de la moitié la jugeant extrêmement importante. Seuls 2 % la considèrent comme peu ou très peu importante.

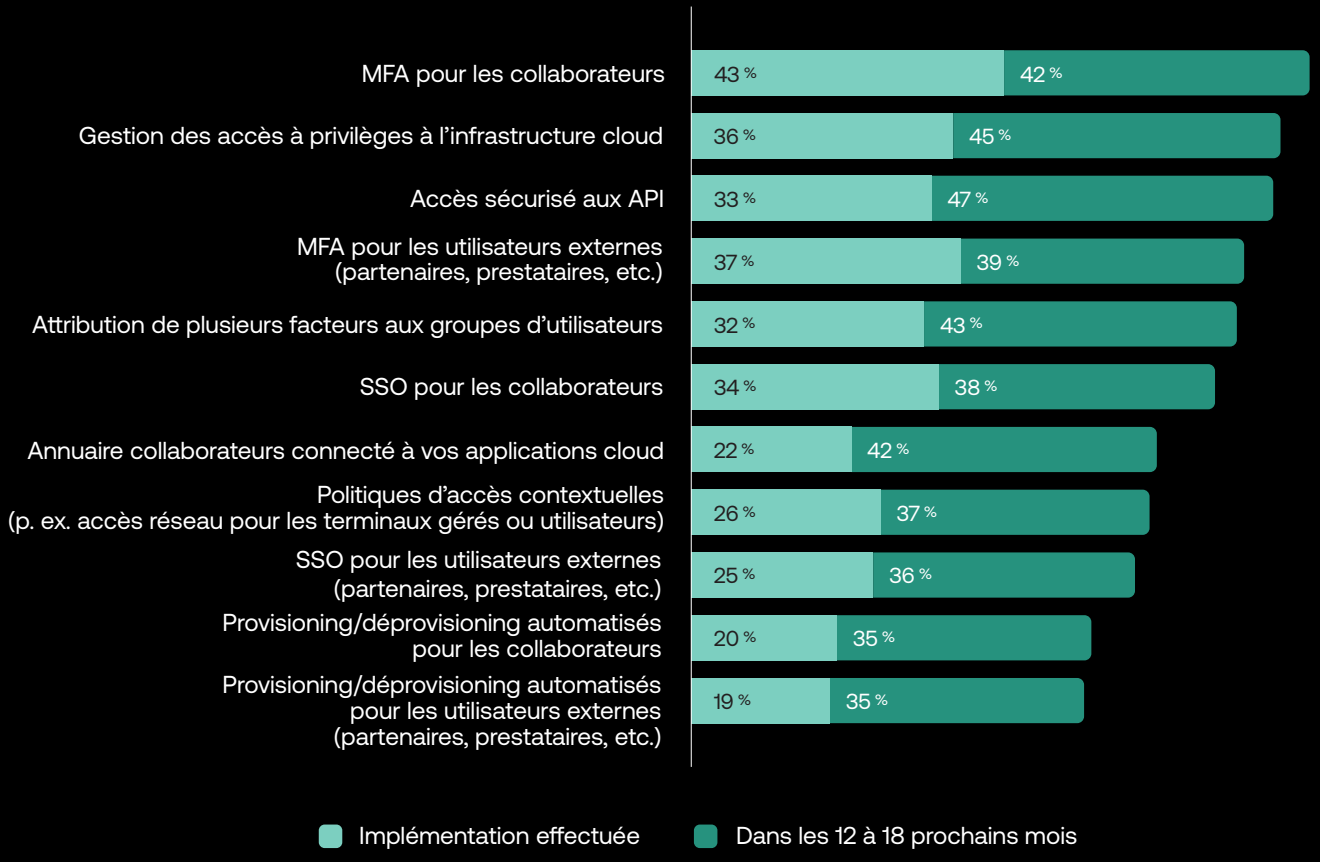
Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les 18 prochains mois ?
Comparaison par année dans le secteur des services financiers



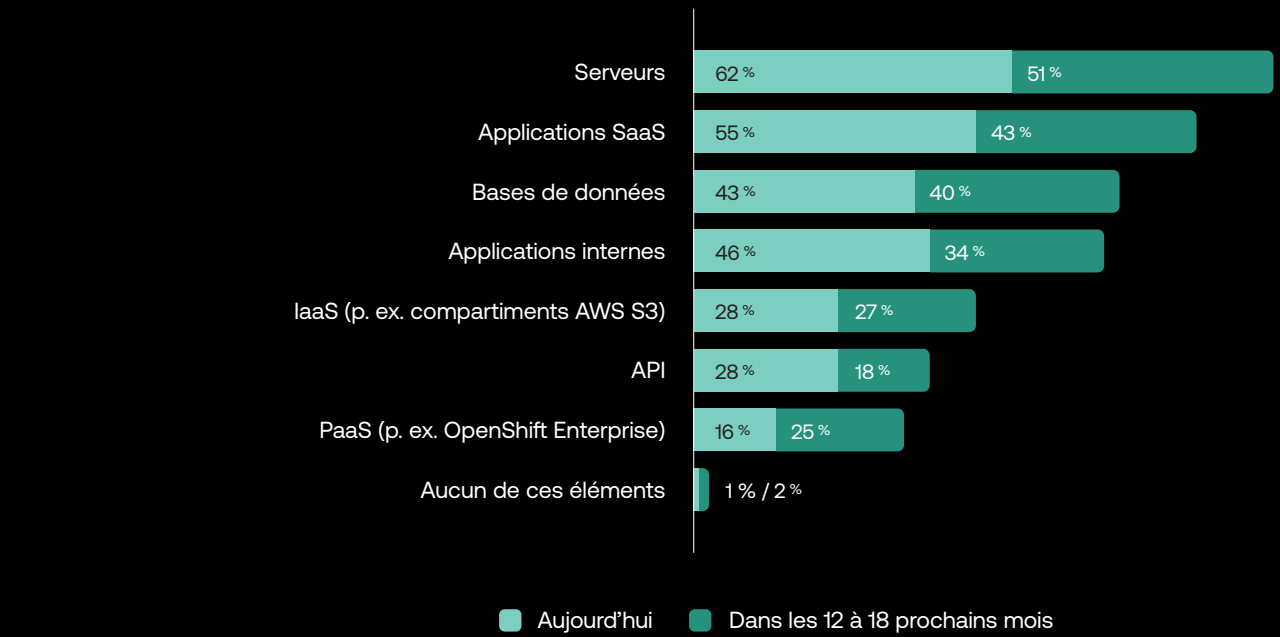
Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les prochains mois ?
Secteur des services financiers vs tous les autres participants à l'enquête



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



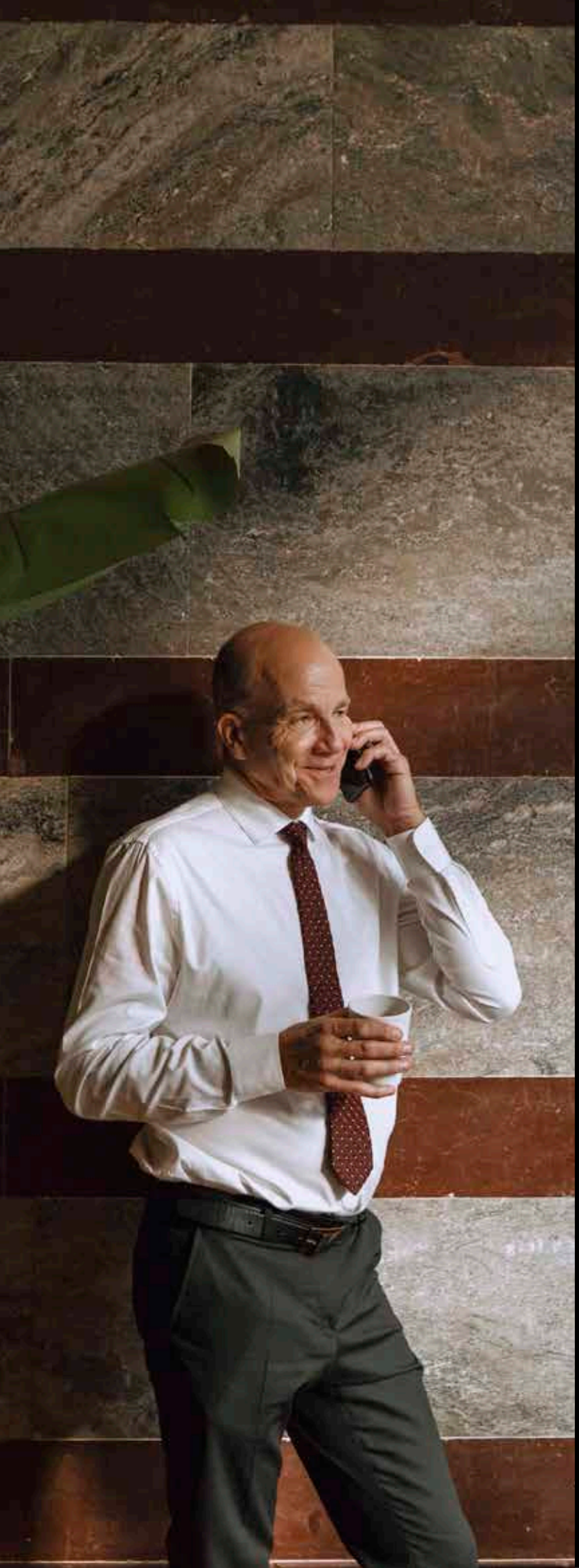
Remarque : la somme des colonnes n'est pas toujours égale à 100 % car les répondants peuvent sélectionner deux réponses.

Principales initiatives pour les services financiers : MFA et gestion des accès à privilèges

Cette année, c'est le MFA pour les collaborateurs qui vient en tête des initiatives Zero Trust prises par les entreprises de services financiers : 43 % l'ont déjà implémenté et 42 % prévoient de le faire dans les 12 à 18 mois. Cette mesure est suivie par la gestion des accès à privilèges au cloud (36 %), puis par l'accès sécurisé aux API (33 %). Les projets les moins prioritaires pour ce secteur sont le SSO pour les utilisateurs externes et le provisioning/déprovisioning automatisés.

Le SSO et/ou le MFA sont appliqués principalement aux serveurs et aux applications SaaS

Les entreprises de services financiers surveillent de près leurs serveurs : 62 % ont déjà appliqué le SSO et/ou le MFA pour protéger leur accès et 51 % prévoient de le faire à court terme. (Les répondants pouvaient choisir les deux options.) Les applications SaaS, les bases de données et les applications internes complètent la liste des principales ressources auxquelles les entreprises de services financiers appliquent (ou prévoient d'appliquer) ces mesures de sécurité axées sur l'identité.



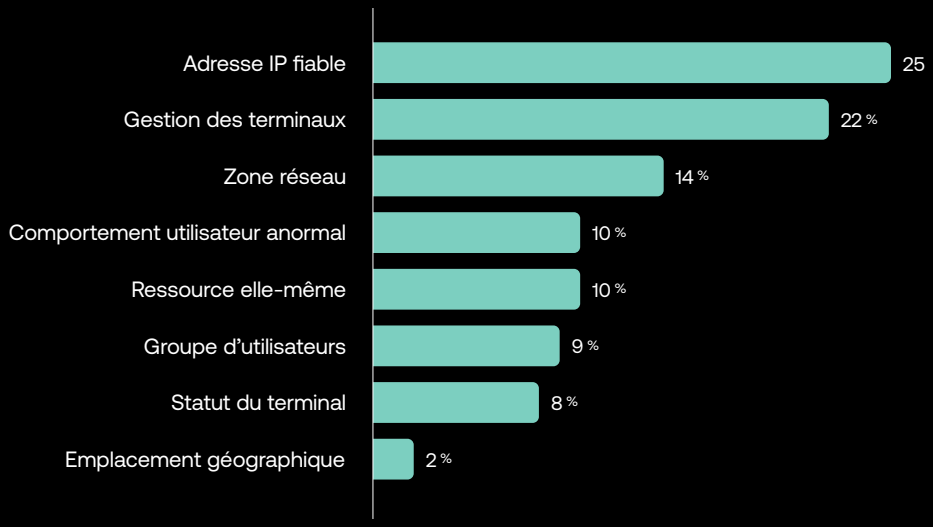
Les adresses IP fiables et la gestion des terminaux sont les principaux facteurs d'approbation des accès

Dès lors qu'il s'agit de contrôler et d'approuver l'accès aux ressources internes, les entreprises de ce secteur veulent vraiment connaître votre emplacement et le terminal utilisé. Une entreprise interrogée sur quatre cite comme principal facteur d'approbation des accès les adresses IP fiables et 22 % la gestion des terminaux. Viennent ensuite la zone réseau, les comportements utilisateurs inhabituels et la ressource elle-même, l'emplacement géographique étant le facteur le moins important cité.

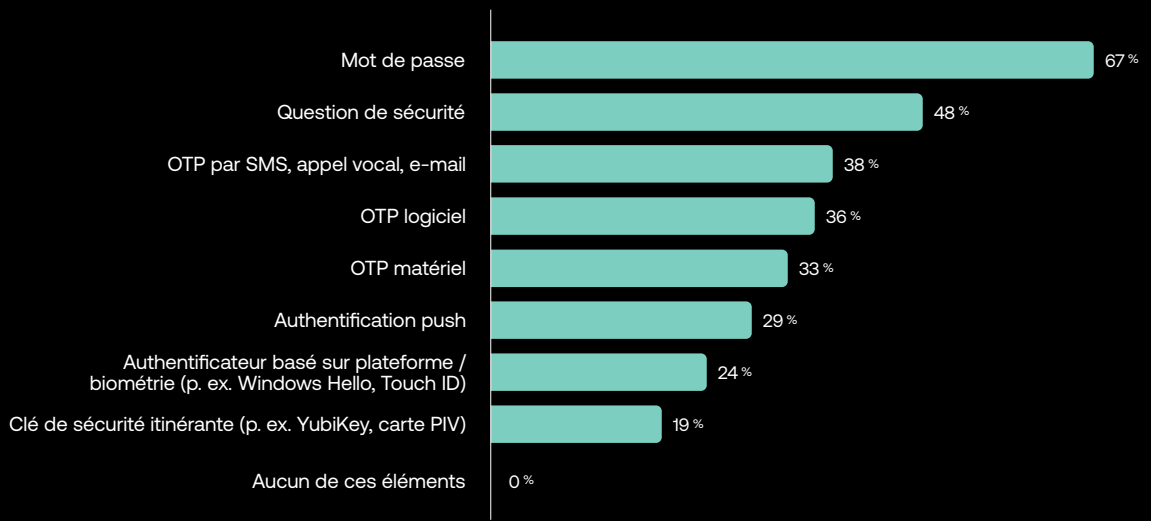
Principaux facteurs d'authentification du secteur des services financiers : mots de passe et questions de sécurité

Les mots de passe restent le tout premier facteur d'authentification pour les entreprises de services financiers puisque deux tiers des répondants l'utilisent actuellement. Les questions de sécurité basées sur la connaissance occupent la deuxième place (48 %) et les options OTP (mot de passe à usage unique) sont citées par un tiers des répondants du secteur.

Classez le facteur le plus critique dans le contrôle et l'approbation des accès à vos ressources internes.
Services financiers



Sélectionnez les facteurs d'authentification que votre organisation utilise pour vérifier l'identité des utilisateurs internes et externes.
Services financiers



Progression du Zero Trust par secteur d'activité

Logiciels

Les années précédentes, le secteur des logiciels était parfois à la traîne par rapport aux autres secteurs cibles de notre enquête. Mais il comble progressivement son retard et les initiatives Zero Trust du secteur ont bien progressé, dépassant la moyenne mondiale, même si le secteur n'est pas soumis à des réglementations aussi strictes que les autres secteurs. En particulier, les éditeurs de logiciels cherchent davantage à renforcer l'authentification et se fondent sur des facteurs d'authentification à niveau d'assurance plus élevé que les autres secteurs du rapport.

Deux tiers des entreprises du secteur ont des initiatives Zero Trust en place

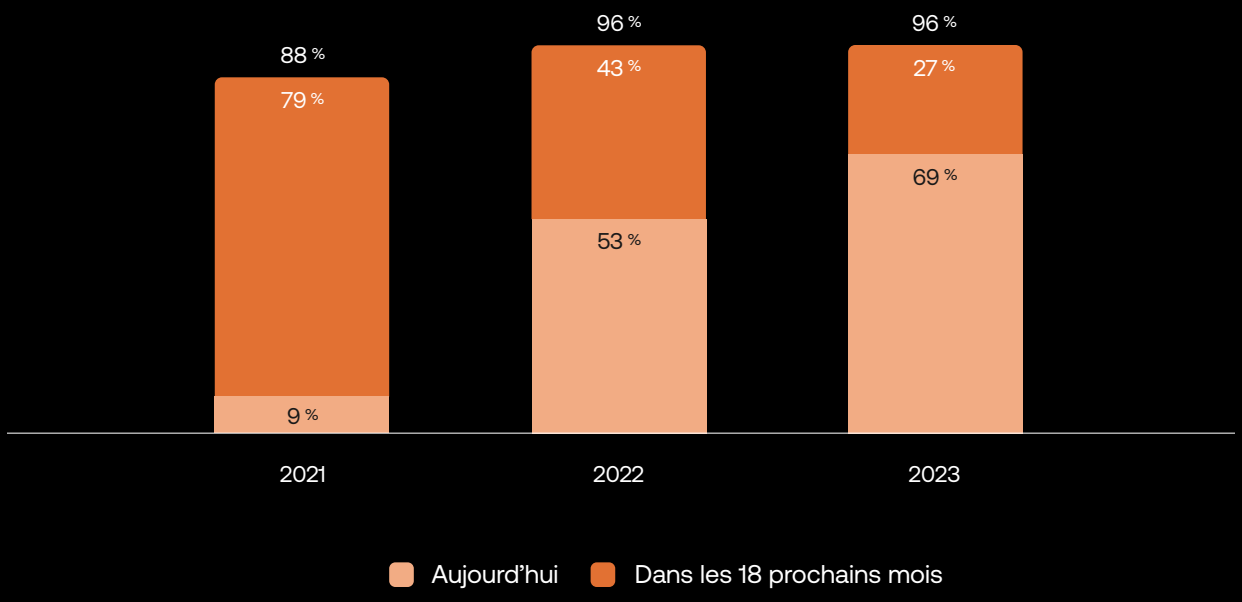
Les entreprises de ce secteur comblent rapidement leur retard sur les autres organisations de notre échantillon dans leur parcours Zero Trust. Alors que le rapport 2021 indiquait que moins d'un répondant sur 10 avait mis en place une initiative Zero Trust dans ce secteur, ce chiffre s'élève aujourd'hui à pratiquement 70 %, le reste ayant déclaré son intention d'en lancer une dans un futur proche. Seulement 4 % des entreprises interrogées n'ont pas mis d'initiative Zero Trust en place et ne prévoient pas de le faire dans les 18 prochains mois.

Le secteur des logiciels est en tête en matière de déploiement d'initiatives Zero Trust

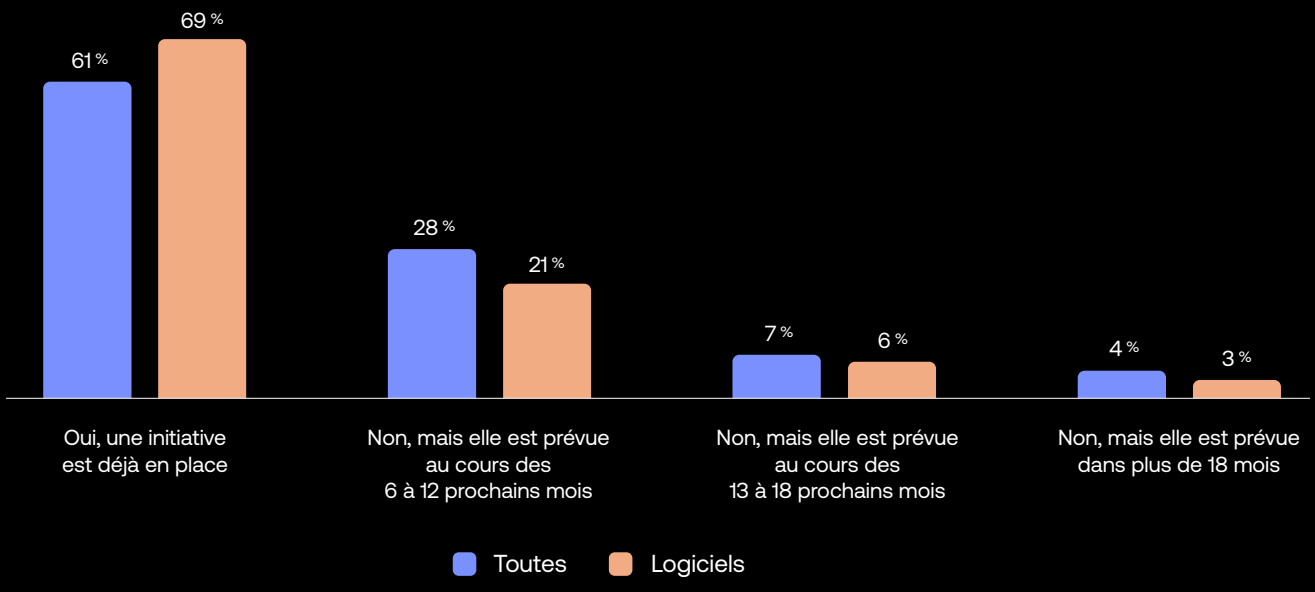
Ces entreprises font mieux que la moyenne mondiale au niveau des initiatives Zero Trust définies déjà mises en place (69 % contre 61 % pour l'ensemble des répondants). Celles qui n'en possèdent pas encore prévoient de lancer un tel projet dans les 6 à 12 prochains mois (21 %), dans les 13 à 18 prochains mois (6 %) ou dans plus de 18 mois (3 %).

Aucun autre secteur de notre enquête ne comprend mieux la valeur de l'identité dans une stratégie Zero Trust. Interrogés sur l'importance de l'identité dans leur stratégie de sécurité Zero Trust, plus de 9 répondants sur 10 déclarent que l'identité est très importante (54 %), assez importante (37 %), et moins de 1 % lui accorde très peu d'importance.

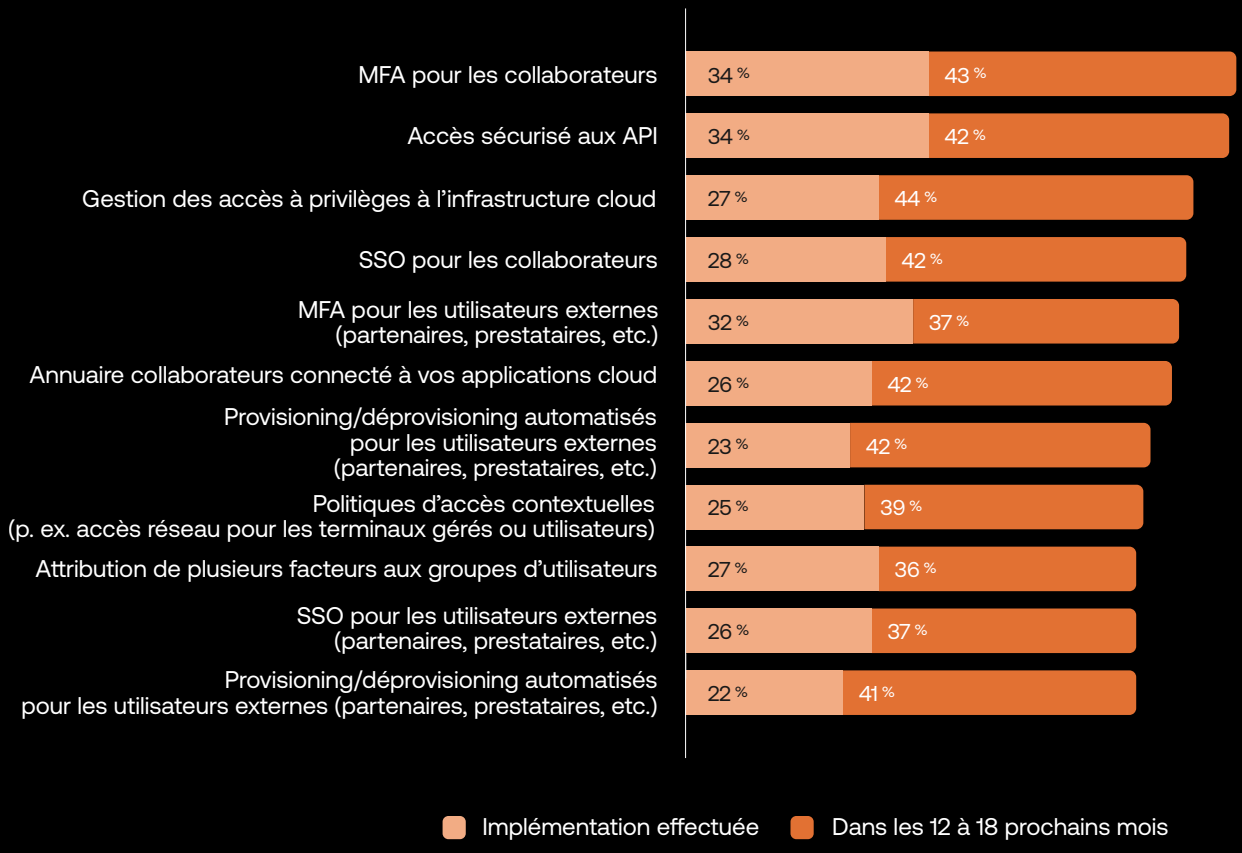
Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les 18 prochains mois ?
Comparaison par année dans le secteur des logiciels



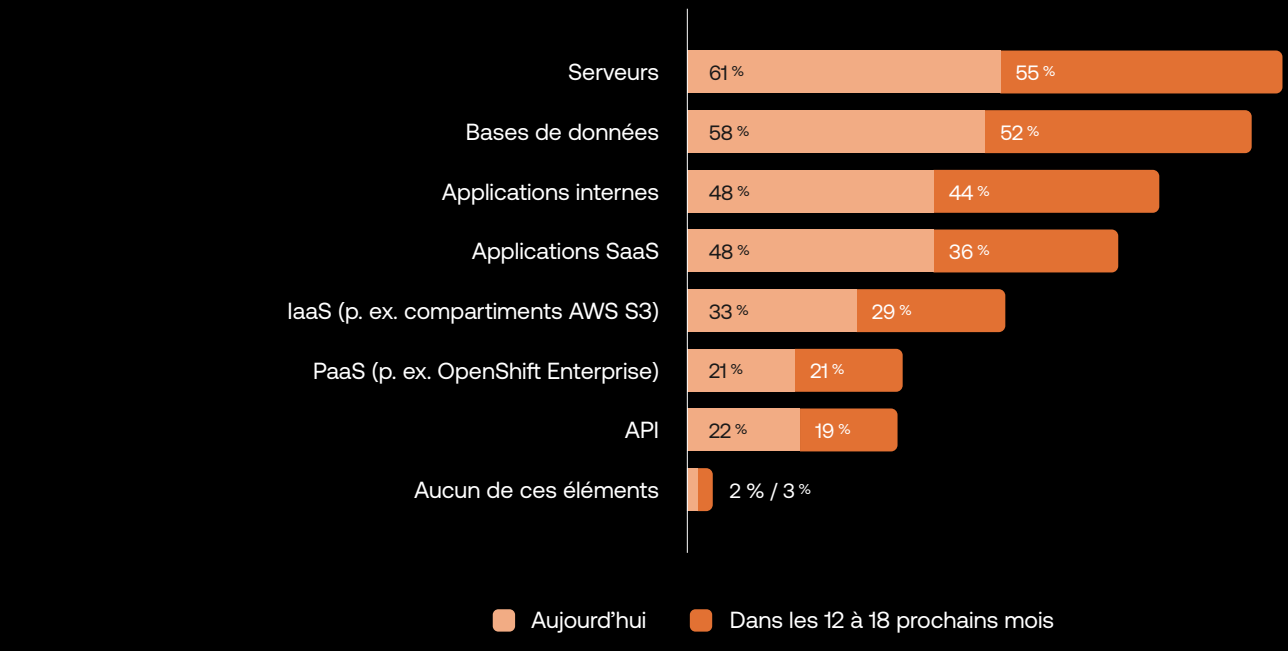
Votre entreprise a-t-elle défini une initiative de sécurité Zero Trust ou prévoit-elle de le faire dans les prochains mois ?
Secteur des logiciels vs tous les autres participants à l'enquête



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



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 ?
Logiciels



Remarque : la somme des colonnes n'est pas toujours égale à 100 % car les répondants peuvent sélectionner deux réponses.

Principales initiatives dans le secteur des logiciels : MFA pour les collaborateurs et sécurité des API

Le MFA pour les collaborateurs et l'accès sécurisé aux API revêtent une importance égale pour les éditeurs de logiciels interrogés. Dans chacune de ces catégories, 34 % des répondants déclarent avoir déjà mis en place une initiative et plus de deux sur cinq prévoient d'en implémenter une des deux, voire les deux, dans les 12 à 18 prochains mois. Le MFA pour les utilisateurs externes occupe la troisième place, avec 32 % des entreprises du secteur déclarant avoir déjà implémenté une telle mesure.

Principales ressources visées par l'extension du SSO/MFA : serveurs et bases de données

Cette année, les entreprises du secteur pensent toutes à protéger l'accès à leurs serveurs (61 %) et à leurs bases de données (58 %) en étendant le SSO et/ou le MFA à ceux-ci. Parmi les entreprises interrogées, 48 % supplémentaires déclarent que les applications internes sont actuellement protégées par le SSO et/ou le MFA et le même pourcentage indique avoir protégé les ressources SaaS avec cette mesure de sécurité.

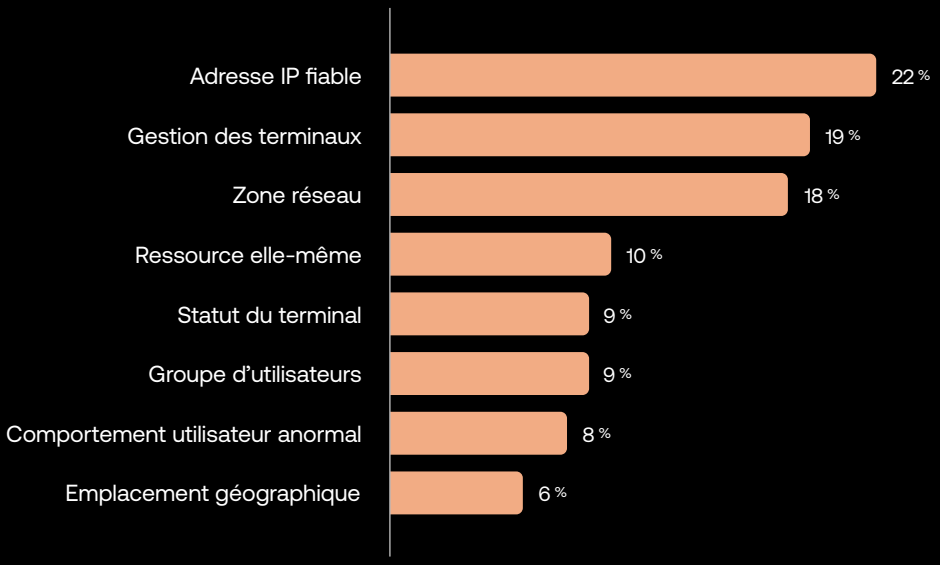
Principaux facteurs pour l'accès aux ressources : adresses IP fiables et gestion des terminaux

Pour contrôler l'accès aux ressources internes, 22 % des éditeurs de logiciels considèrent les adresses IP fiables comme le facteur prioritaire. Pour 19 %, c'est la gestion des terminaux, la zone réseau (18 %) occupant la troisième place. Environ une entreprise sur 10 cite les ressources individuelles (par exemple, des systèmes sensibles) comme principal facteur et 9 % le statut des terminaux ou le groupe d'utilisateurs. L'emplacement géographique est le facteur le moins prioritaire pour les éditeurs de logiciels interrogés.

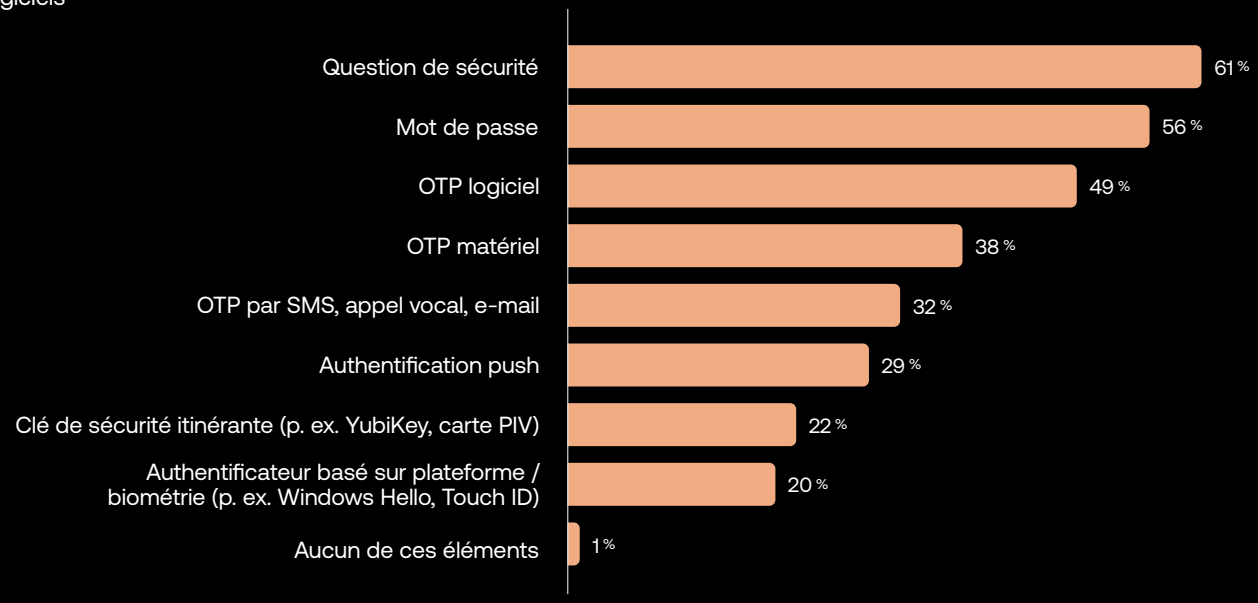
Les questions de sécurité supplantent les mots de passe comme premier facteur d'authentification

Parmi nos quatre secteurs cibles, celui des logiciels est le seul à ne pas sélectionner les mots de passe (dont le manque de fiabilité est établi) comme premier facteur d'authentification. Les mots de passe occupent toujours la deuxième place, puisqu'ils sont toujours utilisés par 56 % des répondants, mais le fait que les questions de sécurité soient en tête (pour 61 % des entreprises interrogées) indique que dans ce secteur au moins, les mots de passe semblent perdre du terrain. Il vaut la peine de souligner, cependant, que les questions de sécurité et les mots de passe sont tous deux des facteurs à niveau d'assurance faible, qu'il conviendrait de remplacer par des facteurs à niveau d'assurance plus élevé comme les mots de passe à usage unique, qui gagnent en popularité.

Classez le facteur le plus critique dans le contrôle et l'approbation des accès à vos ressources internes.
Logiciels



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



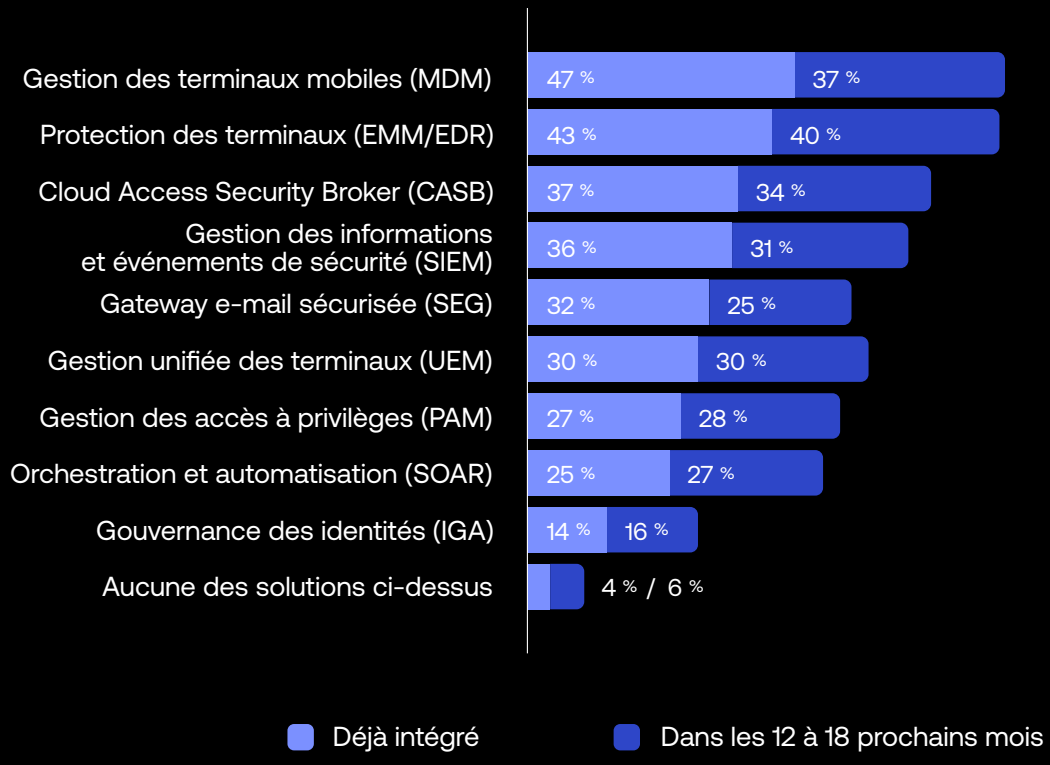
Une sécurité axée sur l'identité

L'évolution de l'écosystème d'entreprise

Si l'identité constitue désormais le nouveau périmètre de sécurité, il ne faut aucun doute que la gestion des identités se trouve dès lors au cœur de la stratégie de sécurité. Les organisations hybrides/multicloud actuelles doivent s'assurer que leur solution IAM fonctionne de concert avec les systèmes de sécurité afin que les équipes de sécurité puissent contrer les menaces internes et externes sans nuire à l'efficacité du personnel authentifié. En d'autres termes, la mise en place d'un véritable écosystème Zero Trust consiste à intégrer les outils de gestion des identités avec les dispositifs de sécurité existants.

Nous avons interrogé les responsables IT et sécurité sur les outils qu'ils avaient déjà intégrés avec leurs systèmes IAM, et ceux qu'ils prévoyaient d'intégrer dans un avenir proche. Ces résultats ont un peu varié par rapport à l'année dernière, où la gestion des informations et des événements de sécurité (SIEM) était la première réponse donnée. Aujourd'hui, la gestion des terminaux mobiles (MDM) est le système le plus largement intégré, selon les participants à l'enquête, et les solutions SIEM, MDM et de protection des terminaux sont les trois systèmes dont l'intégration avec une solution IAM est considérée comme une priorité.

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 ?
Tous les répondants



Intégration prioritaire avec un système IAM en 2023 : la gestion des terminaux mobiles

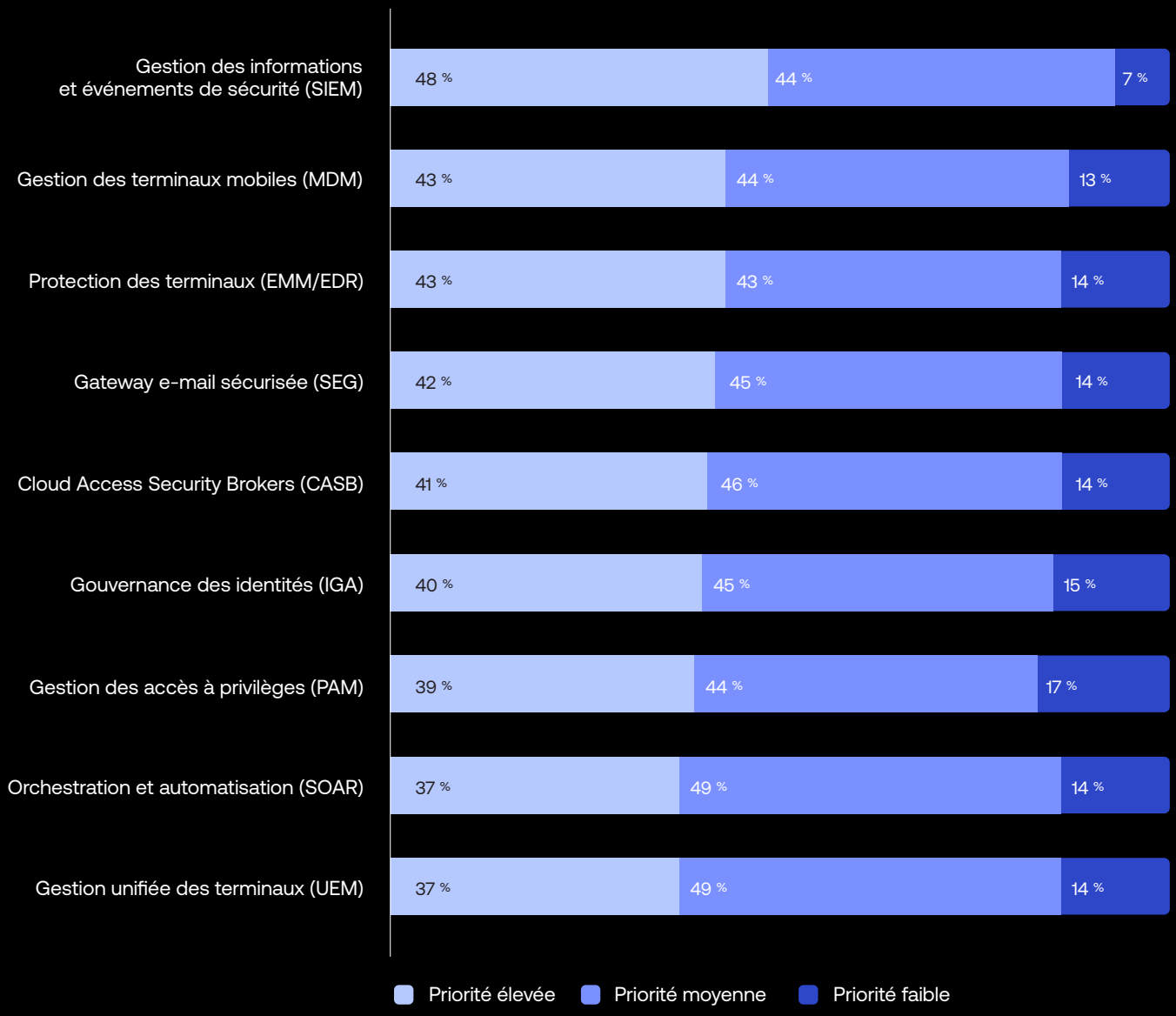
La gestion des terminaux mobiles s'impose comme l'intégration IAM la plus courante dans les résultats de cette année, après une longue progression constante (elle venait en 7e position en 2021 et en 4e position l'année dernière). En 2021, seuls 11 % des répondants avaient intégré une solution MDM avec un système IAM. Aujourd'hui, ce pourcentage s'élève à 47 %, mais 37 % des autres organisations interrogées prévoient de le faire dans les 12 à 18 prochains mois. Le secteur continue de donner la priorité aux intégrations offrant des outils de protection et de surveillance de la sécurité à haute valeur ajoutée et une gestion fiable des terminaux.

Principales préoccupations par région :

- NAM : gestion des terminaux mobiles, CASB et protection des terminaux
- EMEA : SIEM, gateway e-mail sécurisée et gestion unifiée des terminaux
- APJ : gestion des terminaux mobiles, SIEM, SOAR et protection des terminaux

Ces intégrations avec l'IAM peuvent fonctionner conjointement pour simplifier la gouvernance et implémenter en toute sécurité des contrôles des accès basés sur des politiques, des autorisations granulaires ainsi que d'autres automatisations intuitives pour les entreprises tournées vers l'avenir.

Parmi les éléments suivants, lesquels sont pour vous les plus importants à intégrer à une solution IAM pour soutenir une sécurité Zero Trust ?
Priorités à l'échelle mondiale



Les solutions SIEM, MDM et de protection des terminaux en tête des intégrations prioritaires avec l'IAM

Invités à attribuer une priorité élevée, moyenne ou faible aux intégrations potentielles avec l'IAM ci-dessus, les répondants, toutes régions confondues, sont plus enclins à choisir le SIEM en premier (48 %), puis une solution MDM et de protection des terminaux (43 % pour chaque). Les intégrations avec les solutions SOAR et UEM ont généralement une priorité moyenne et le maximum de répondants ayant attribué une priorité faible à l'une des catégories ne dépasse jamais 17 %. ■

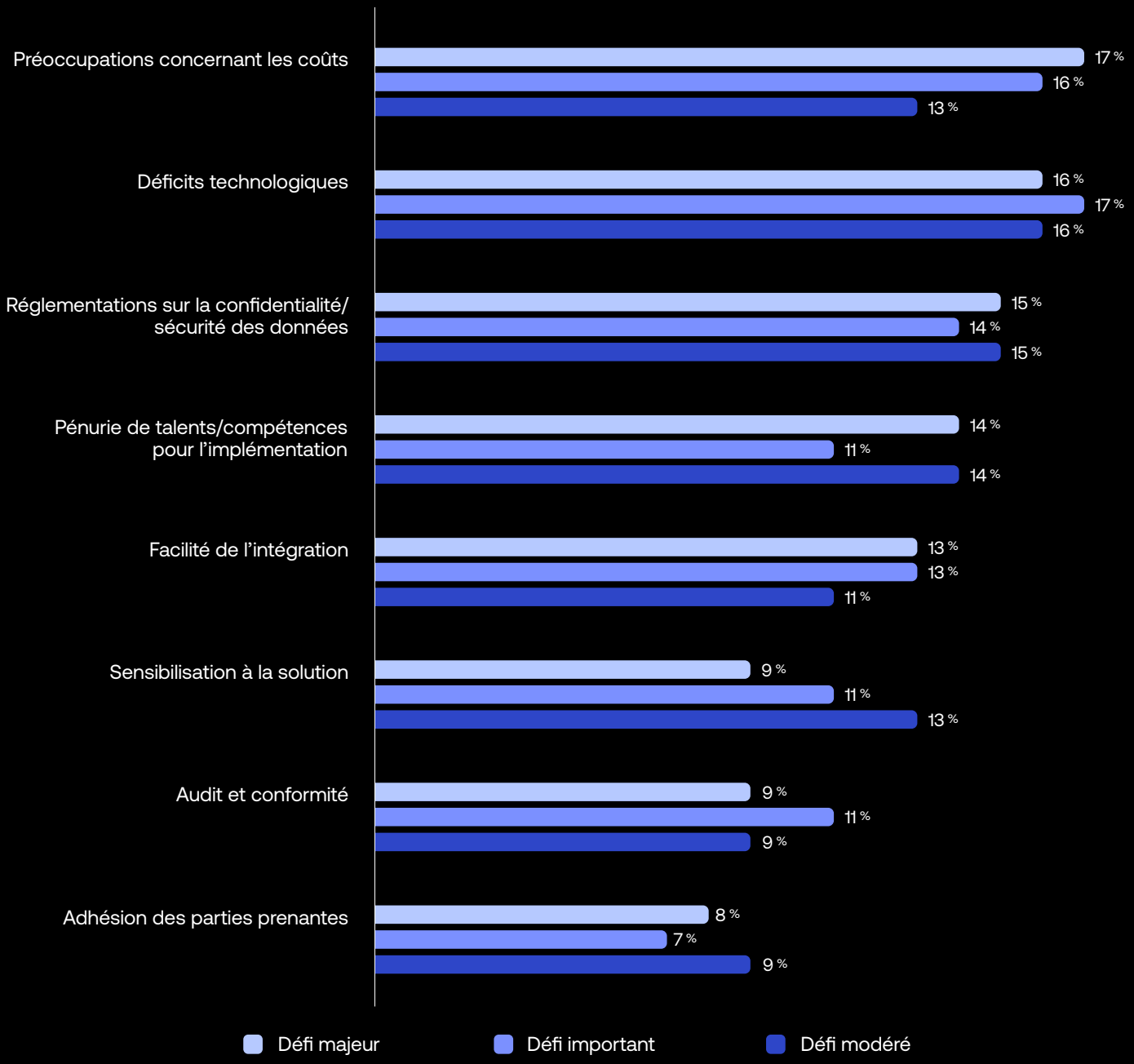
Remarque : la somme des colonnes n'est pas toujours égale à 100 % en raison de l'utilisation de la méthode d'arrondi à l'entier le plus proche.

Le long parcours vers le Zero Trust

Les entreprises surmontent des obstacles systémiques et lancent des initiatives Zero Trust critiques pour l'activité.

Le Zero Trust est le seul moyen de sécuriser efficacement l'entreprise hybride/multicloud moderne : il permet d'automatiser en toute confiance l'accès et le provisioning d'équipes internationales, tout en limitant les risques posés par les menaces internes et externes. La philosophie est désormais bien comprise et, pour la vaste majorité des organisations, tous secteurs, tailles et régions confondus, les plans sont en place ou en cours. Mais sans les bons logiciels, partenaires et processus, il n'est pas toujours facile de mettre ces principes en pratique et de concrétiser les promesses du Zero Trust. Les entreprises du monde entier continuent d'être en butte à une série de problèmes liés à la sécurité, notamment en termes de coûts, déficits technologiques, pénurie de talents et autres, comme l'illustrent les données de notre enquête annuelle.

Les trois principaux défis à l'adoption d'une solution Zero Trust :



Principaux obstacles à l'adoption du Zero Trust cette année : coûts et technologies

Cette année, les répondants ont le plus souvent cité les coûts, les déficits technologiques et les réglementations sur la confidentialité/sécurité des données comme les principaux obstacles à l'implémentation des initiatives de sécurité Zero Trust. La présence des réglementations sur la confidentialité dans le trio de tête est nouvelle, mais les coûts constituent un défi récurrent. En 2021, les coûts étaient le deuxième obstacle le plus souvent cité, le premier étant la pénurie de talents/compétences et le troisième, les déficits technologiques. Dans l'édition de 2022, les coûts venaient en 3e position après la pénurie de talents/compétences et le manque d'adhésion des parties prenantes. Cette année, la pénurie de talents/compétences reste un enjeu assez important, mais le manque d'adhésion des parties prenantes a régressé, sans doute grâce à la validation des principes Zero Trust par des experts reconnus.

À l'examen des données de cette année, les tendances générales varient quelque peu selon la fonction. Pour les cadres dirigeants interrogés, les réglementations sur la confidentialité et la pénurie de talents constituent des obstacles majeurs. Pour les vice-présidents, il s'agit de la facilité de l'intégration et des réglementations sur la conformité. Enfin, pour les directeurs, les principaux enjeux sont la conformité lors des audits et la facilité de l'intégration.

Le long parcours vers le Zero Trust

L’avenir du Zero Trust

Le parcours Zero Trust est différent pour chaque organisation. Pour les entreprises qui veulent moderniser leur sécurité et garder une longueur d’avance sur des menaces en perpétuelle évolution, le déploiement d’un projet stratégique aussi complexe peut poser des défis de taille et durer plusieurs années. Quoi qu’il en soit, le constat est clair : les organisations progressent dans la réalisation de leurs projets, augmentent le budget alloué aux initiatives Zero Trust, même en cette période d’incertitude économique, et renforcent progressivement la sécurité du cloud.

Pour mettre en œuvre un véritable modèle Zero Trust, les entreprises doivent trouver des solutions à leurs enjeux de confidentialité et de sécurité des données (y compris les directives réglementaires), tout en préservant la productivité de leurs effectifs. Elles ont besoin de solutions faciles et rapides à intégrer dans leurs écosystèmes et piles technologiques pour valoriser autant que possible leurs investissements. Par ailleurs, elles doivent relever des défis récurrents tels que la pénurie de talents et compétences.

Sur le plan positif, il semble plus facile d’obtenir l’adhésion des parties prenantes et les avantages offerts par une gestion efficace des identités sont désormais clairement visibles. La plupart des dirigeants d’entreprise sont aujourd’hui conscients que la valeur du Zero Trust va au-delà de la sécurité : il s’agit aussi d’un moteur d’activité stratégique qui améliore l’expérience des collaborateurs et des clients, facilite la collaboration au sein d’équipes hybrides et est essentiel à la mise en place d’expériences fluides et sécurisées contribuant à renforcer la confiance des clients et à générer des revenus.

La sécurisation du nouveau périmètre de l’identité est sans doute le principal défi des entreprises aujourd’hui. Cela étant, la mise en place d’une véritable sécurité Zero Trust, axée sur l’identité, permet de tirer pleinement parti de toute la puissance du cloud et de profiter des nouvelles opportunités qu’il présente en termes d’agilité, d’innovation et de croissance.

Le long parcours vers le Zero Trust

Rappel des principaux points à retenir

- **D'un simple plan d'action, le Zero Trust s'est rapidement imposé comme une norme de fonctionnement.**

  Alors qu'hier encore, il restait un objectif difficilement réalisable, il est devenu aujourd'hui une réalité opérationnelle. La majorité des entreprises ont déjà déployé une initiative Zero Trust et s'appuient sur celle-ci pour renforcer leur sécurité et conserver leur avantage concurrentiel. Celles qui n'en ont pas encore possèdent néanmoins, pour la plupart, un plan défini en projet ou en cours.

- **Pour la vaste majorité, l'identité est désormais considérée comme critique pour toute stratégie Zero Trust.**

  Pour les entreprises hybrides/multicloud et agiles actuelles, l'identité constitue désormais le nouveau périmètre, et une gestion des identités performante représente une stratégie essentielle à leur succès et leur offre la possibilité de se développer en toute confiance.

- **Les budgets des projets Zero Trust continuent d'augmenter et de résister obstinément aux forces du marché.**

  Même en période d'incertitude économique, rien n'arrête les attaques externes ni les menaces internes, et rien ne vient réduire les budgets de sécurité. Les entreprises restent déterminées à renforcer leurs défenses grâce à des initiatives de sécurité axées sur l'identité.

- **Les entreprises cherchant à adopter le Zero Trust doivent encore surmonter de nombreux défis.**

  La conception, la planification et l'implémentation d'une stratégie de sécurité Zero Trust est une initiative complexe qui fait intervenir de nombreuses parties prenantes. Pour y parvenir, chaque entreprise doit suivre son propre chemin, souvent parsemé d'embûches telles que la conformité aux réglementations sur la confidentialité, les déficits technologiques, la compression des coûts et d'autres facteurs.

Vous souhaitez en savoir plus, ou déterminer où se positionne votre organisation dans le modèle de maturité Okta en matière d'identités collaborateurs ? Consultez notre livre blanc.

À propos d'Okta

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

Clause de non-responsabilité

Le présent document et toute recommandation concernant vos pratiques de sécurité ne constituent pas des conseils juridiques, commerciaux ou de sécurité. Le contenu de ce document revêt un caractère purement informatif et pourrait ne pas refléter les normes de sécurité et les réglementations les plus récentes, ou tous les problèmes juridiques ou de sécurité pertinents. Pour obtenir de tels conseils, il vous revient de vous adresser à votre conseiller juridique ou à tout autre conseiller professionnel et de ne pas vous en remettre aux recommandations formulées dans le présent document. Okta décline toute responsabilité quant aux pertes ou dommages pouvant résulter de la mise en œuvre des recommandations fournies dans le présent document.

okta

Okta France
Tour Europlaza
20 avenue André Prothin
92400 Courbevoie - France
info@okta.com
+33 01 85 64 08 80