

2026

Enquête mondiale 2026 sur l'état de l'authentification

Perceptions vs Réalité :
Les lacunes de la sécurité
de l'authentification

yubico



okta

Sommaire

Synthèse	1
L'écart d'adoption	3
Maîtrise des méthodes d'authentification modernes	4
Piégé par le modèle d'intégration par défaut	5
Quand le travail déborde sur la vie personnelle	6
Le biais d'optimisme et la menace non humaine	7
Euros et bon sens : l'explosion des attaques par phishing dopées à l'IA	8
Fin du phishing « évident »	9
Deepfakes et taux de réussite élevés	10
Saurez-vous repérer le bot ? (Spoiler : les experts n'y sont pas parvenus)	11
Avenir de l'agentique : sécuriser les identités non humaines	12
L'obligation de vérification	13
Quand la délégation devance les contrôles de sécurité	14
L'exigence d'une intervention humaine	15
Analyse par région	16
Créer une nouvelle architecture de sécurité	18
Conclusion	20
Présentation des entreprises et méthodologie	22

Synthèse

Pendant des années, les stratégies de sécurité des entreprises ont reposé sur un postulat fondamental selon lequel sensibiliser les utilisateurs suffisait à renforcer la sécurité. Les responsables de la cybersécurité savent clairement ce qu'il faut faire pour protéger les organisations et les individus : adopter l'authentification multi-facteurs (MFA) et se préparer aux menaces pilotées par IA susceptibles d'aggraver les failles de sécurité existantes.

Mais il arrive encore bien trop souvent que les connaissances en matière de sécurité ne se traduisent pas dans la pratique, laissant les organisations vulnérables. Autrement dit, le fossé entre savoir et faire persiste.

Les conclusions de ce rapport suggèrent que le décalage constaté n'est pas d'ordre éducatif, mais plutôt d'ordre structurel. Tant au travail qu'en dehors, les difficultés rencontrées lors des connexions et la fatigue provoquée par les demandes d'authentification poussent même les professionnels les plus avertis à systématiquement opter pour la solution de facilité. La crainte de se retrouver bloqué hors de ses comptes personnels peut renforcer cette tendance et inciter les utilisateurs à revenir à des mots de passe simples et à une authentification multi-facteurs (MFA) par SMS, qu'ils connaissent bien. Pour s'affranchir des moyens d'authentification par défaut peu sûrs, tels que les noms d'utilisateur et les mots de passe, il est important de reconnaître que même les experts les plus qualifiés restent sujets aux biais comportementaux humains et aux angles morts opérationnels. L'enjeu n'est donc pas de changer les comportements des utilisateurs, mais de modifier l'infrastructure sous-jacente. Les entreprises doivent donc éliminer les procédures héritées par défaut et les remplacer, sur l'ensemble de leurs systèmes, par une authentification fluide et résistante au phishing.

Ces dernières années, nous avons interrogé des professionnels du monde entier pour déterminer dans quelle mesure ils mettent en œuvre des pratiques de cybersécurité efficaces chaque jour. Et cette année, Yubico a adopté une nouvelle approche en faisant équipe avec Okta pour interroger près de 2 000 professionnels de la cybersécurité et de l'informatique dans neuf pays. Ces professionnels évoluent au quotidien dans le domaine de la sécurité. Ils élaborent des politiques, gèrent les accès et savent mieux que quiconque à quel point les mots de passe classiques peuvent facilement céder face à une attaque.

Près

2,000

Professionnels De La
Technologie Et De La
Sécurité

9

Pays

Au-delà des mots de passe et de la sensibilisation

Nos conclusions révèlent une opportunité majeure pour les organisations de moderniser leurs pratiques de cybersécurité en redéfinissant leur architecture de sécurité. Alors que l'expertise et la sensibilisation aux méthodes d'authentification sécurisées n'ont jamais été aussi élevées, notre enquête montre que même les professionnels de la sécurité continuent de s'appuyer sur les processus existants fondés sur les mots de passe, mis en place lors de l'intégration des nouveaux collaborateurs. Or, tant que les entreprises continueront à attribuer des mots de passe lors des processus d'intégration, les employés continueront à les utiliser.

En matière de phishing, plutôt que de compter sur l'inspection visuelle des utilisateurs pour détecter les anomalies subtiles révélant une page web frauduleuse, les équipes de sécurité tournées vers l'avenir reconnaissent qu'une authentification résistante au phishing constitue la protection ultime, car celle-ci supprime toute intervention humaine dans les décisions de sécurité. À l'inverse, les méthodes d'authentification modernes assurent la sécurité au moment même de l'accès, grâce à un échange cryptographique de nonces signés et à une vérification du domaine. Elles garantissent ainsi que, même si un utilisateur tombe dans le piège d'une tentative de phishing, l'authentification échouera automatiquement et l'attaque sera complètement bloquée.

En résumé : la sensibilisation à la sécurité n'est pas le principal obstacle à la sécurité des entreprises. Le véritable frein réside dans les frictions opérationnelles et les pratiques par défaut obsolètes qui ne tiennent pas compte de l'identité avant, pendant et après l'authentification. Pour combler cette lacune, il est nécessaire d'aller au-delà de la sensibilisation et d'imposer une authentification résistante au phishing et adossée à du matériel, pour chaque identité, humaine ou non.

yubico



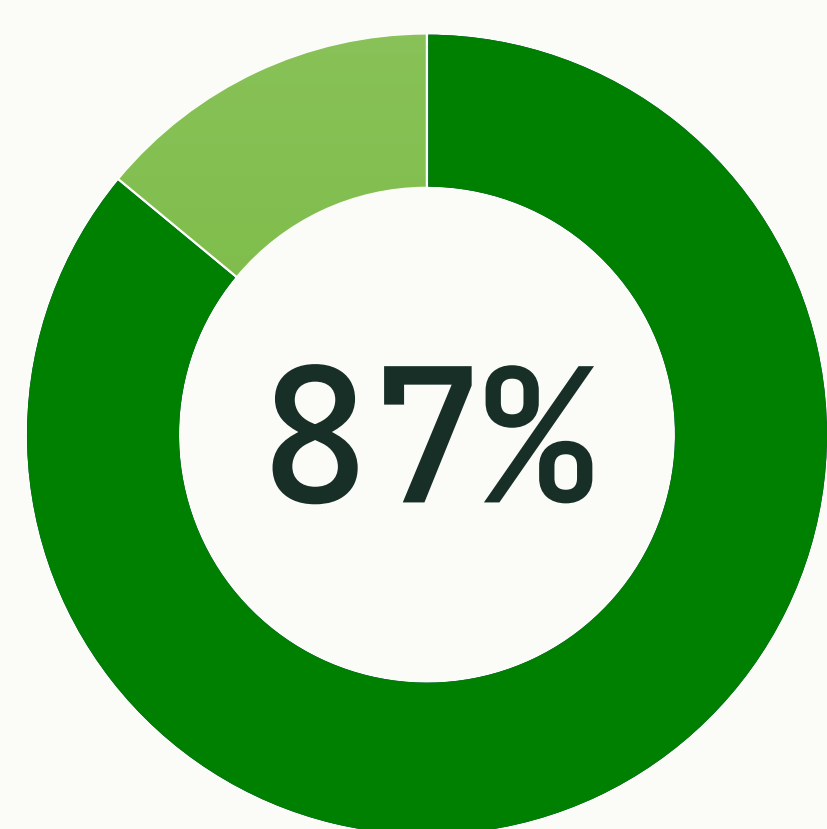
L'écart d'adoption



Maîtrise des méthodes d'authentification modernes

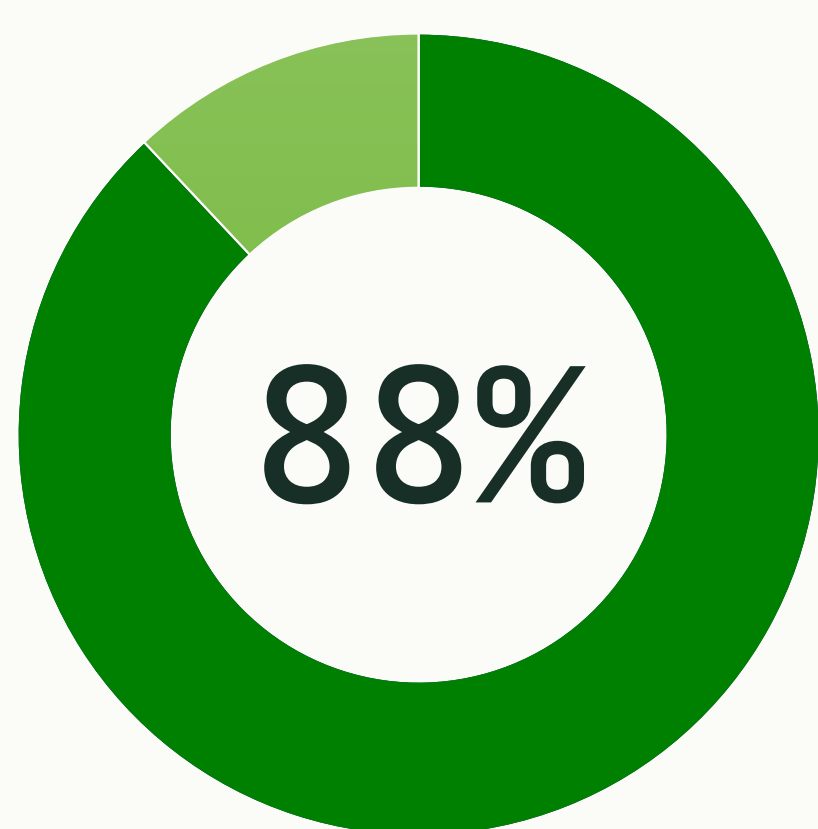
Les équipes de sécurité des entreprises possèdent une connaissance approfondie du domaine. Lorsqu'on leur demande d'évaluer les contrôles d'accès, elles identifient les passkeys matérielles comme le moyen le plus sûr **(31 %)**, devant les applications d'authentification mobiles **(29 %)** et les passkeys synchronisées **(27 %)**.

Leur connaissance de ces technologies est indéniable : **87 %** sont familières avec les passkeys, **82 %** ont suivi une formation à la sécurité proposée par leur employeur, et seuls **3 %** n'ont jamais utilisé une passkey. Sur le papier, ces professionnels sont donc parfaitement à même d'identifier les outils de référence pour protéger les entreprises, les employés et les clients contre les cybermenaces.



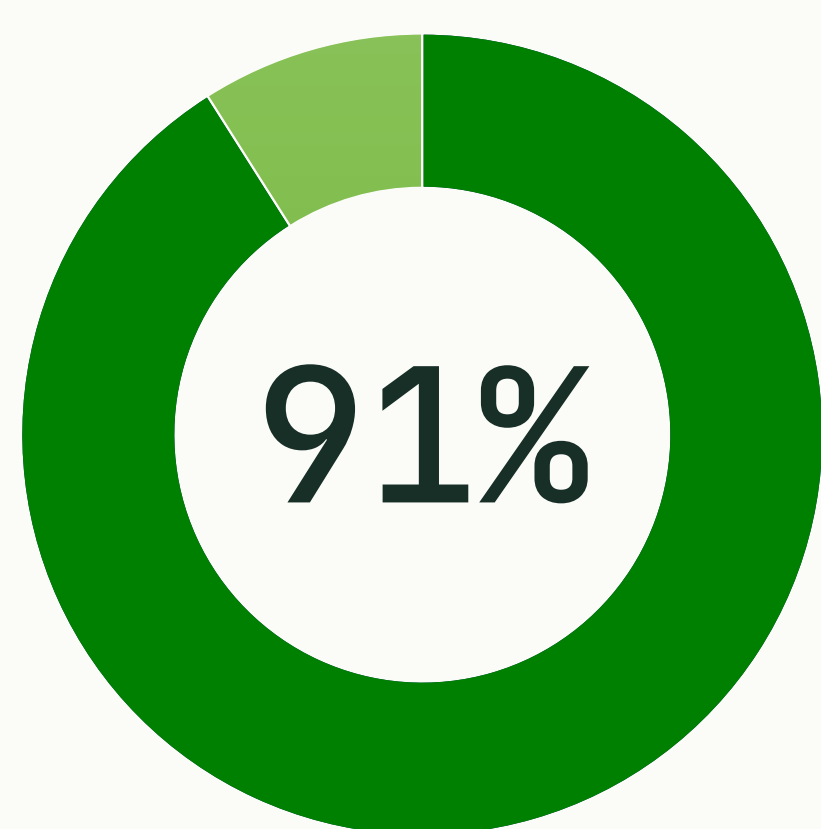
Sensibilisation élevée

87 % des professionnels de la sécurité connaissent les clés d'accès (passkeys), et **31 %** reconnaissent explicitement les clés d'accès liées à l'appareil et reposant sur un composant matériel comme l'identifiant le plus sécurisé disponible



Culture de sécurité proactive

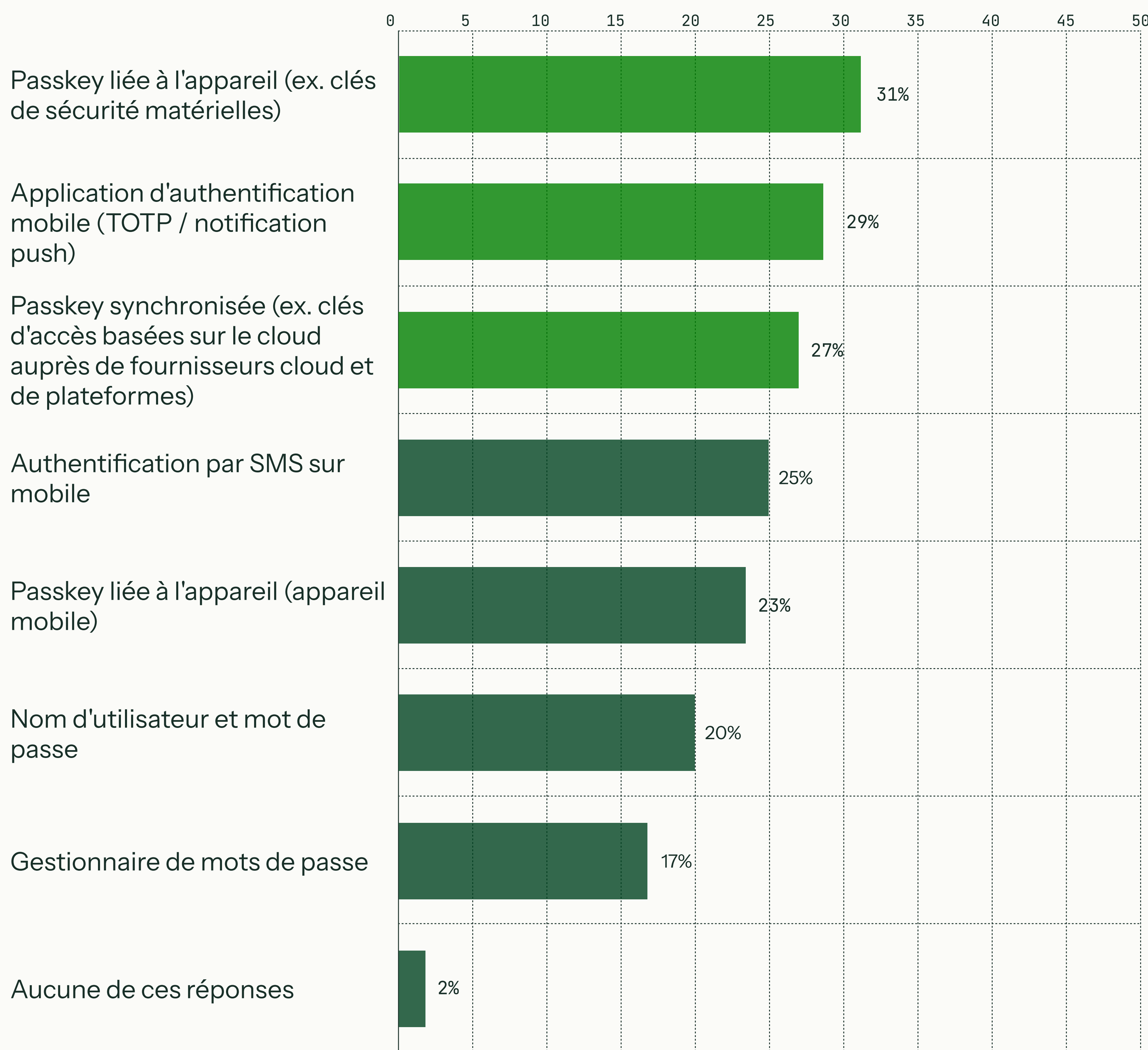
88 % des responsables de la sécurité se disent confiants quant à la posture de sécurité actuelle de leur organisation, ce qui traduit des investissements importants dans les outils, l'infrastructure et la formation des équipes.



Prêts pour l'ère de l'IA

91 % des dirigeants reconnaissent l'importance de l'authentification des agents d'IA, faisant preuve d'une préparation visionnaire face aux identités non humaines.

Selon vous, quelles sont les méthodes d'authentification les plus sécurisées ?



Piégé par le modèle d'intégration par défaut

Malgré leur expertise, leurs habitudes quotidiennes ressemblent à celles des employés non techniques. Les noms d'utilisateurs et mots de passe restent le moyen que les professionnels de la sécurité utilisent le plus couramment pour se connecter à leurs comptes professionnels (**43 %**), tandis que les passkeys matérielles se classent parmi les méthodes les moins utilisées au quotidien, avec **25 %**.

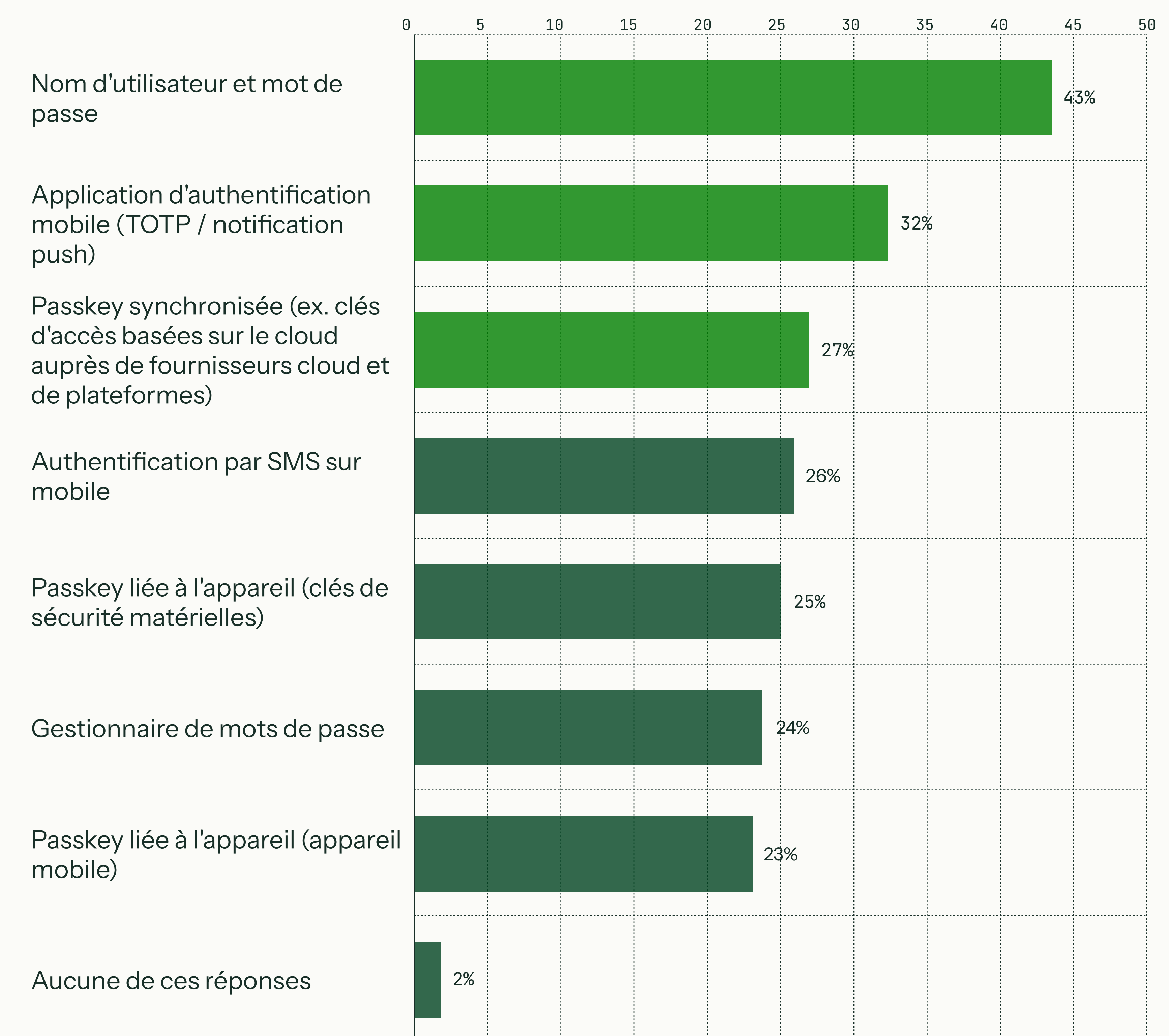
L'enquête révèle que les habitudes de longue date sur le lieu de travail remontent souvent aux méthodes par défaut adoptées dès le premier jour. Plus de la moitié des personnes interrogées (**52 %**) ont reçu des identifiants classiques (nom d'utilisateur et mot de passe) lors de leur prise de fonction, ancrant ainsi des habitudes de connexion qui perdurent au fil du temps.

Les incohérences opérationnelles aggravent les risques :

- **76 %** des organisations utilisent des méthodes d'authentification disparates dans leurs différentes applications internes.
- **45 %** utilisent des noms d'utilisateur et mots de passe comme principaux identifiants dans des systèmes fragmentés.
- **23 %** ne rendent pas la MFA obligatoire pour l'ensemble des applications et services de l'entreprise.

Le contexte dans lequel ces méthodes par défaut s'appliquent diffère selon qu'il s'agit du lieu de travail ou du domicile. Au travail, les méthodes par défaut liées à l'intégration et les éventuels verrouillages de compte sont pris en charge par un service d'assistance informatique prêt à rétablir l'accès. À la maison, chacun doit gérer sa sécurité de manière autonome.

Comment vous authentifiez-vous / vous connectez-vous à vos comptes professionnels ?

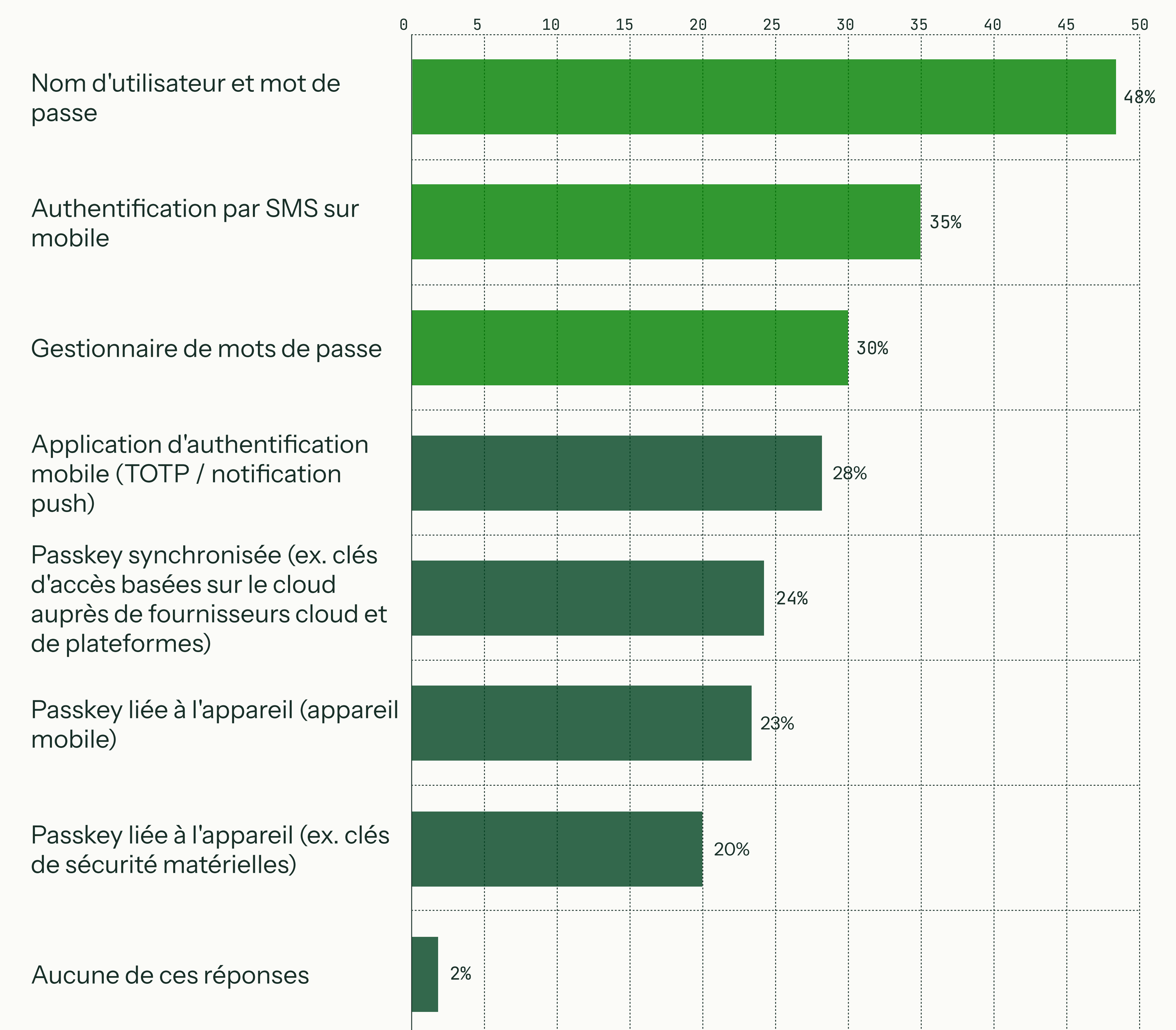


Quand le travail déborde sur la vie personnelle

Compte tenu de notre tendance naturelle à la recherche de facilité, s'affranchir des méthodes d'authentification par défaut, et de la fatigue provoquée par les invites de sécurité constantes liées aux demandes d'authentification, nécessite un effort concerté tant au travail qu'en dehors. Il n'est donc peut-être pas surprenant que, même dans la sphère privée, **48 %** des professionnels de la cybersécurité s'appuient principalement sur des noms d'utilisateurs et des mots de passe, puis sur la vérification par SMS (**35 %**). Ils ne sont que **20 %** à se servir de passkeys matérielles leurs comptes personnels.

Sachant que **28 %** des personnes n'utilisent pas la MFA pour protéger leur messagerie personnelle, les attaquants disposent là d'un point d'entrée facile. Une boîte de réception non protégée et liée à un opérateur mobile (**38 %**) peut servir de catalyseur aux attaques par échange de carte SIM (SIM swap). En disposant des données nécessaires pour mener ce type d'action malveillante, les attaquants peuvent détourner les codes de récupération envoyés sur le téléphone de l'utilisateur et accéder directement aux identifiants professionnels associés, mettant ainsi en danger à la fois l'identité personnelle et les identifiants professionnels.

Comment vous authentifiez-vous / vous connectez-vous à vos comptes personnels ?



Le biais d'optimisme et la menace non humaine

Malgré ces vulnérabilités, **88 %** des personnes interrogées considèrent leur entreprise comme « sécurisée » (**34 %** d'entre elles la qualifiant même de « très sécurisée »).

En psychologie comportementale, ce phénomène est connu sous le nom de « **biais d'optimisme** », c'est-à-dire la tendance à croire que l'expertise protège un individu ou une institution des conséquences négatives. Les responsables de la sécurité évaluent favorablement leur propre posture de sécurité, tout en supposant que leurs concurrents sont bien plus exposés aux risques.

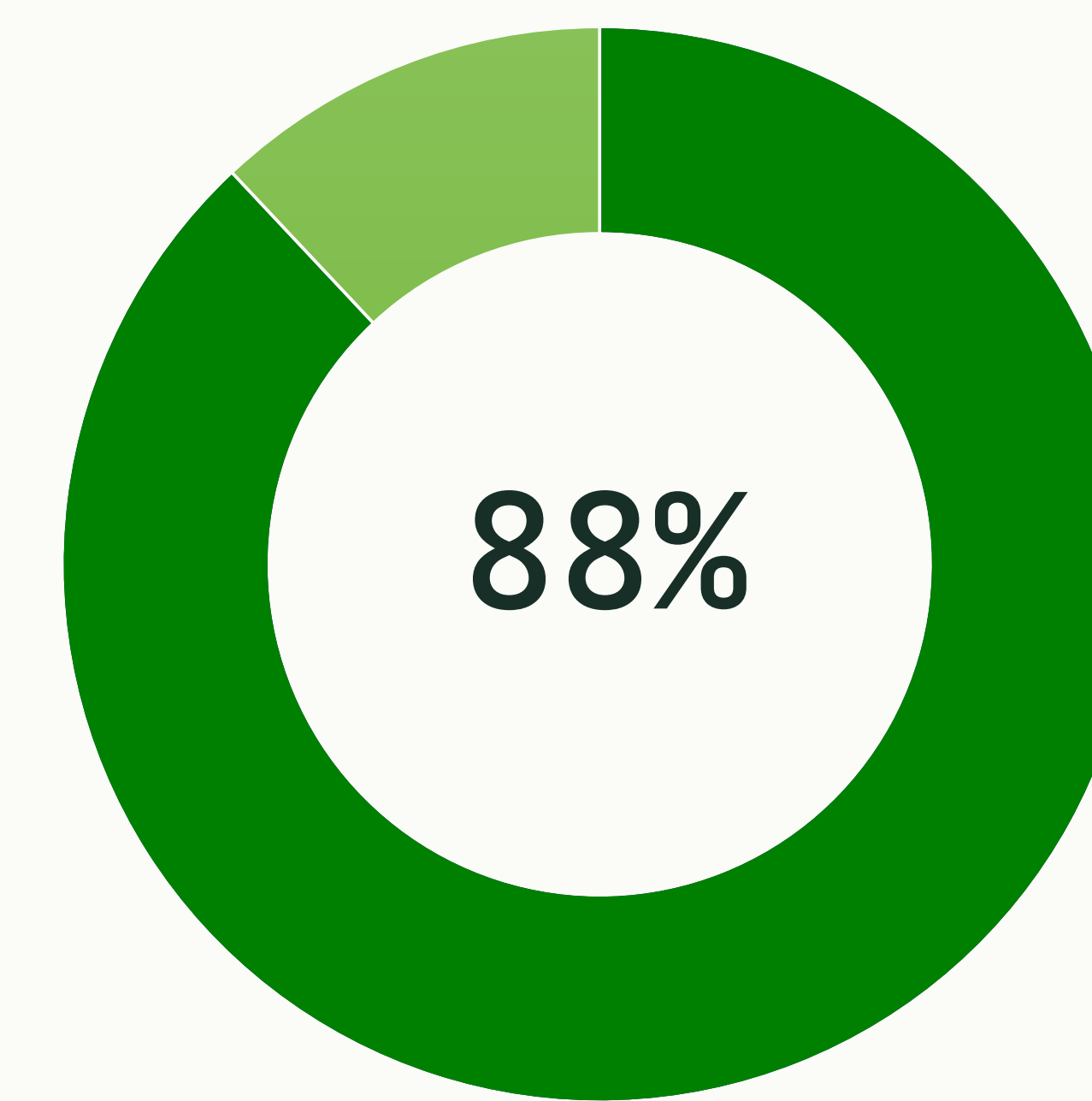
À mesure que les entreprises intègrent des agents d'IA autonomes à leurs workflows quotidiens, ces agents non humains auront bientôt accès à des comptes protégés par mot de passe. Une organisation qui ne parvient pas à imposer une authentification forte à ses employés humains ne peut pas gérer en toute sécurité des agents autonomes.

« La cybersécurité en entreprise souffre d'un déficit d'exécution majeur. Les responsables de la sécurité savent que les passkeys matérielles, plus précisément les clés de sécurité physiques, offrent le plus haut niveau de protection, et pourtant, près de la moitié d'entre eux utilisent encore quotidiennement de simples noms d'utilisateur et mots de passe. Le problème ne vient pas d'un manque d'expertise, mais de la difficulté à surmonter les freins à l'adoption par les utilisateurs.

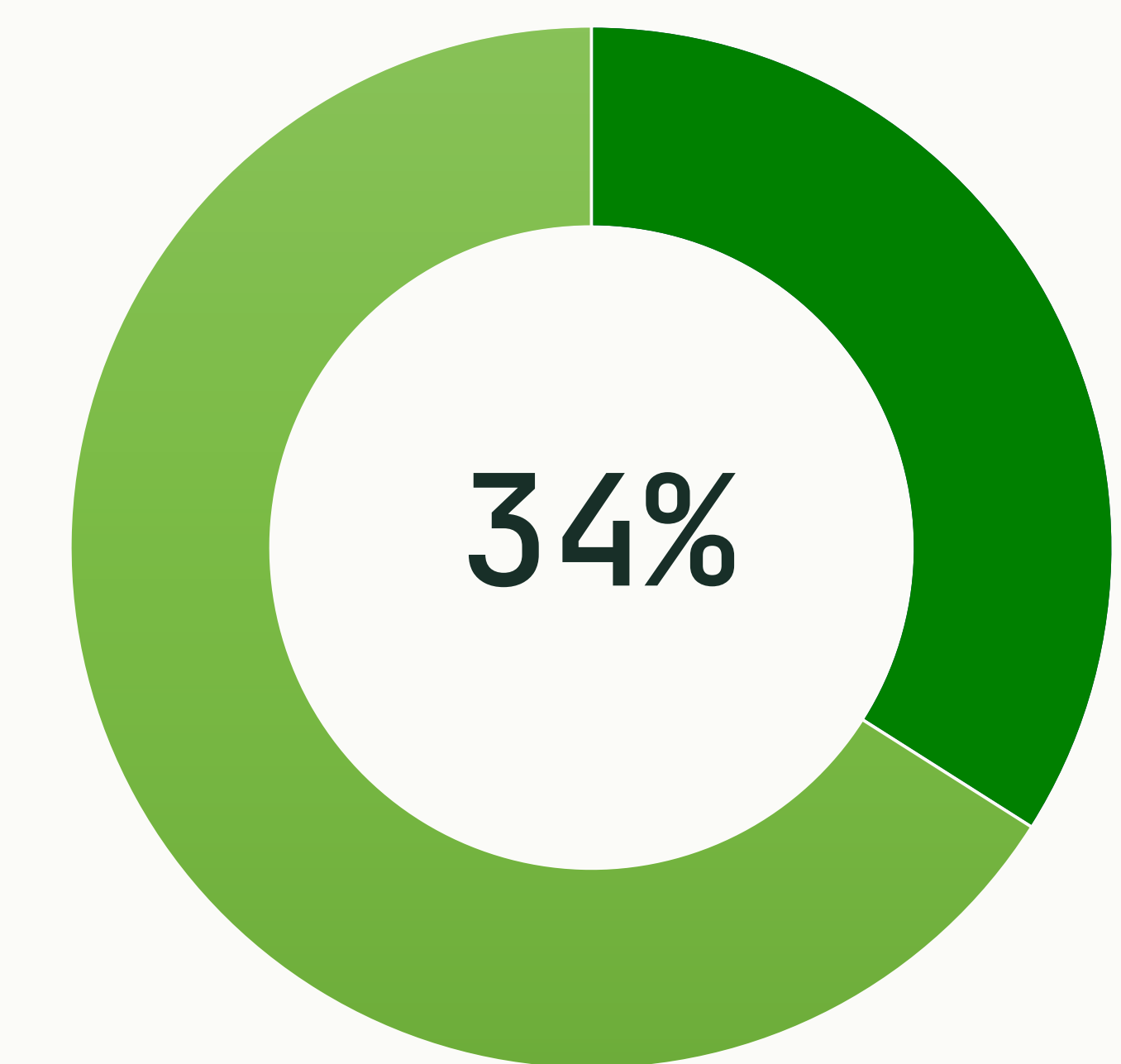
Poupak Enbom,
Chief Market and Growth Officer chez Yubico



Les décalages opérationnels aggravent le risque



88 % des répondants décrivent leur entreprise comme « sécurisée »



34 % affirment qu'elle est « très sécurisée »

Euros et bon sens : l'explosion des attaques par phishing dopées à l'IA



Fin du phishing « évident »

Alors que l'IA générative accélère les communications numériques et les rend plus personnalisées, les tentatives de phishing basées sur l'IA ont naturellement augmenté dans le secteur. Pour preuve, **70 %** des personnes interrogées ont constaté une hausse des tentatives de phishing dans leur organisation au cours de l'année écoulée, **55 %** d'entre elles ayant été directement ciblées par des attaques personnalisées, et **22 %** ayant même reçu des messages ciblés la semaine dernière.

Plutôt que de se fier aux indicateurs traditionnels des pages web de phishing, tels que les fautes de frappe ou les formulations maladroitement, les équipes de sécurité tournées vers l'avenir reconnaissent qu'une authentification résistante au phishing, et non une inspection visuelle des utilisateurs, constitue la protection ultime. En d'autres termes, les humains ne devraient pas être chargés d'identifier et de bloquer les menaces basées sur l'IA. Au contraire, les méthodes les plus innovantes assurent la sécurité au moment même de l'authentification, grâce à une vérification de domaine et à une sécurité fondée sur la cryptographie. Ainsi, même si un utilisateur est victime d'une tentative de phishing, la technologie d'authentification peut détecter et bloquer la connexion, sans que l'utilisateur ait nécessairement conscience de l'attaque.



Deepfakes et taux de réussite élevés

Les attaques modernes contournant les mécanismes cognitifs traditionnels, le taux de compromission initiale a fortement augmenté. Ainsi, 44 % des personnes interrogées indiquent que leur organisation aurait subi au moins une attaque pilotée par IA au cours des 12 derniers mois.

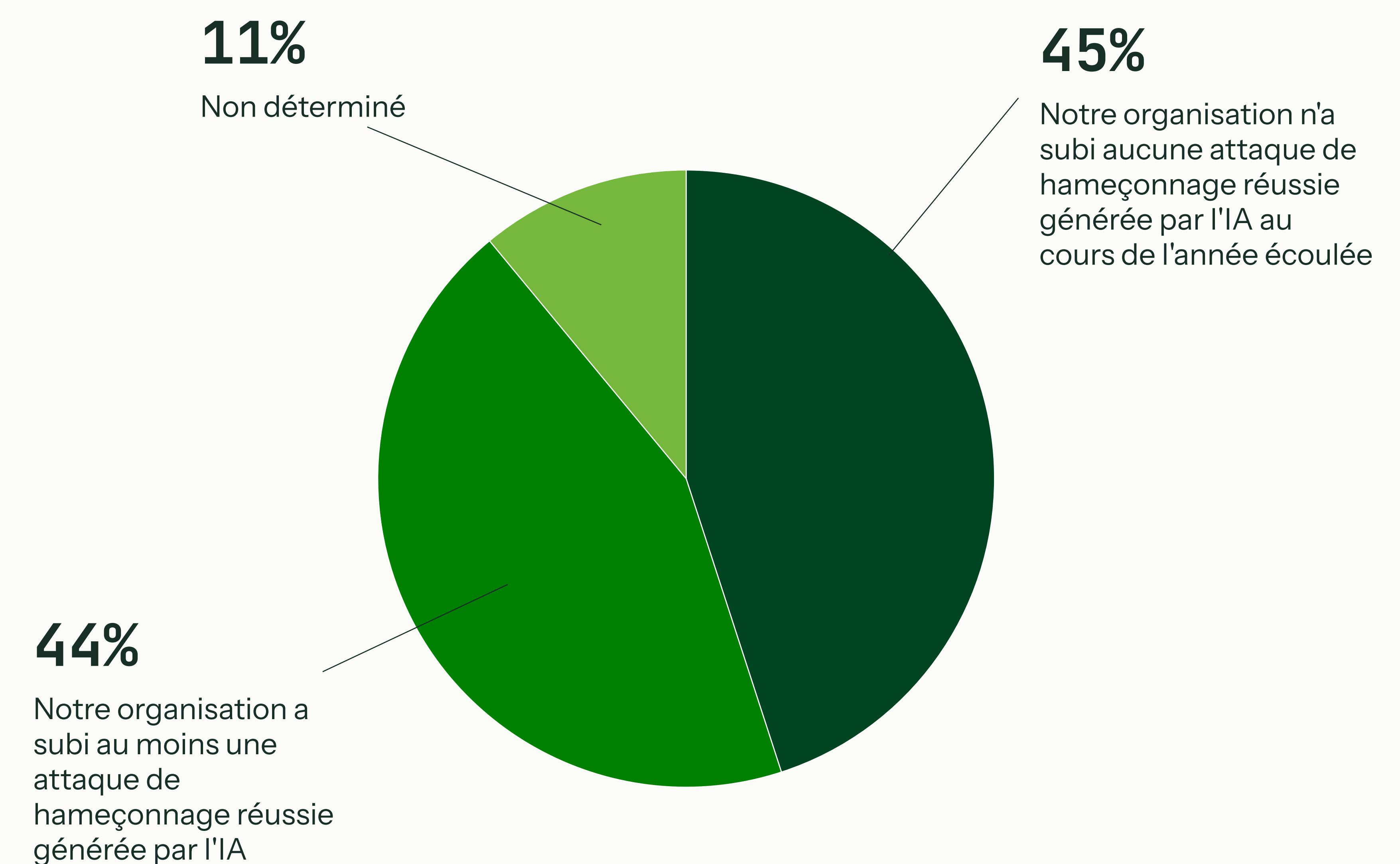
Le clonage vocal et les médias synthétiques permettent désormais aux cybercriminels de se faire passer pour des collègues de confiance à partir d'un minimum de contenu source :

- **43 %** ont signalé des vidéos suspectes, des messages vocaux ou des usurpations par téléphone visant des dirigeants ou des clients.
- **29 %** ont été directement ciblés par des communications utilisant des « deepfakes ».

Le rapport Okta intitulé « 2026 AI Agents at Work » décrit une seconde voie d'accès à ces mêmes organisations. Plus de la moitié des professionnels interrogés (52 %) déclarent utiliser des outils d'IA non approuvés sur leur lieu de travail, et près d'un quart d'entre eux le font régulièrement. Les contenus les plus fréquemment partagés par ceux qui utilisent des outils non approuvés sont les messages internes et les e-mails (54 %), les informations relatives aux ressources humaines (45 %) et les documents confidentiels de l'entreprise, notamment les données financières et les contrats (39 %).



Laquelle des affirmations suivantes est vraie concernant le succès des attaques de hameçonnage (phishing) générées par l'intelligence artificielle (IA) dans votre organisation au cours de l'année écoulée ?



Saurez-vous repérer le bot ? (Spoiler : les experts n’y sont pas parvenus)

Les entreprises comptent depuis longtemps sur leurs employés pour faire office de « pare-feu humain » et détecter les anomalies. Pour tester ce mécanisme de défense, nous avons présenté deux messages à des responsables de la sécurité : l’un rédigé par un humain, l’autre généré par une IA, et nous leur avons demandé d’en identifier la source.

E-mail rédigé par un humain

Bonjour [NOM],

Notre manuel du chercheur / guide de l'employé a été mis à jour afin d'intégrer les modifications pour 2027. Plusieurs sections ont été ajoutées. Veuillez consulter l'intégralité du document mis à jour et en accuser réception d'ici le 1er novembre 2026.

Action requise – À effectuer avant le 1er novembre 2026

Veuillez vous connecter à l'intranet de notre entreprise et consulter la notification dans la section « À faire ». Ce document, ainsi que l'ensemble de nos politiques, sont accessibles sur notre page d'accueil.

Nous vous remercions par avance pour votre collaboration qui permet à notre entreprise de rester en conformité.

Cordialement,
Votre équipe RH

Les résultats révèlent que **la détection humaine ne constitue plus une mesure de sécurité viable** :

- Seuls **36 %** des professionnels de la sécurité ont correctement identifié la question rédigée par un humain, **54 %** ont pensé que le message avait été rédigé par une IA et **10 %** n'étaient pas sûrs.
- **39 %** des répondants n'ont pas non plus réussi à reconnaître la question générée par l'IA.

E-mail rédigé par une IA

Bonjour [NOM],

Alors que nous nous tournons vers l'avenir et préparons la suite, nous avons rafraîchi notre manuel de l'employé pour 2027. Nous avons ajouté quelques nouvelles sections importantes pour veiller à ce que nos politiques continuent de vous soutenir, vous et notre équipe en pleine croissance, de la meilleure façon possible.

En raison de ces ajouts, nous demandons à chacun de prendre connaissance du document mis à jour et d'en valider rapidement la réception.

Ce que nous attendons de votre part d'ici le 1er novembre 2026 :

1. Connectez-vous à l'intranet de l'entreprise.
2. Consultez votre liste « À faire » sur la page d'accueil.
3. Jetez un œil au manuel mis à jour et cliquez pour confirmer que vous l'avez bien reçu.

(N'oubliez pas : vous pouvez retrouver à tout moment le manuel, ainsi que toutes nos autres politiques d'entreprise, épinglés sur la page d'accueil de l'intranet si vous avez besoin de les consulter.)

Un grand merci de prendre quelques minutes de votre journée pour nous aider à faire en sorte que tout fonctionne parfaitement et reste en toute conformité !

Cordialement,
Votre équipe RH

Avenir de l'agentique : sécuriser les identités non humaines



L'obligation de vérification

À mesure que les agents d'IA autonomes passent du statut d'assistants passifs à celui d'outils opérationnels actifs, la vérification de l'identité des machines devient une priorité absolue. **91 % des répondants affirment qu'il est essentiel de vérifier l'identité et l'authenticité des agents d'IA**, et **57 %** d'entre eux considèrent cette vérification comme cruciale.

Selon le rapport Businesses at Work 2026 d'Okta, 74 % des organisations déclarent recourir de manière généralisée ou modérée à des identités non humaines, 90 % d'entre elles ne disposent pas d'une stratégie globale pour les régir, et seules 32 % régissent les agents d'IA avec la même rigueur que celle qu'elles appliquent aux identités humaines.



Quand la délégation devance les contrôles de sécurité

La délégation de tâches aux agents d'IA s'accélère, les responsables de la sécurité se montrant de plus en plus à l'aise à l'idée de confier des tâches opérationnelles à l'IA.

- 1. Planification et gestion des agendas (35 %)
- 2. Rédaction des communications internes (35 %)
- 3. Détection automatisée des fraudes (29 %)
- 4. Réunions avec des clients (27 %)

Les écarts générationnels sont marqués en matière de communications déléguées à l'IA : **68 % des professionnels de la Gen Z** n'hésitent pas à laisser un agent d'IA communiquer avec des clients ou des collègues en leur nom, contre seulement **27 % des baby-boomers**.

Parmi ces tâches, de lesquelles seriez-vous à l'aise de déléguer l'automatisation à un agent d'IA en votre nom ?



L'exigence d'une intervention humaine

Si le niveau d'aisance face à la délégation de tâches à l'IA varie, une chose reste claire : une intervention humaine demeure essentielle. **91 % des personnes interrogées insistent pour qu'une approbation par un humain** soit maintenue avant qu'un agent n'exécute des actions en leur nom.

Si les workflows de type « agent à agent » nécessitent une exécution autonome pour être déployés à grande échelle, la vérification par un humain peut servir de contrôle de sécurité pour les workflows critiques, par exemple avant qu'un agent n'escalade des privilèges ou n'effectue des transactions financières.

« Alors que les responsables de la sécurité et les jeunes générations délèguent volontiers des tâches opérationnelles à l'IA, de la planification de routine (35 %) aux interactions avec les clients (jusqu'à 68 % pour la Gen Z), une écrasante majorité (91 %) continue de fixer une limite claire dès qu'il s'agit de l'exécution de tâches, insistant pour qu'un être humain reste dans la boucle pour une approbation finale.

Poupak Enbom,
Chief Market and Growth Officer chez Yubico



Analyse par région

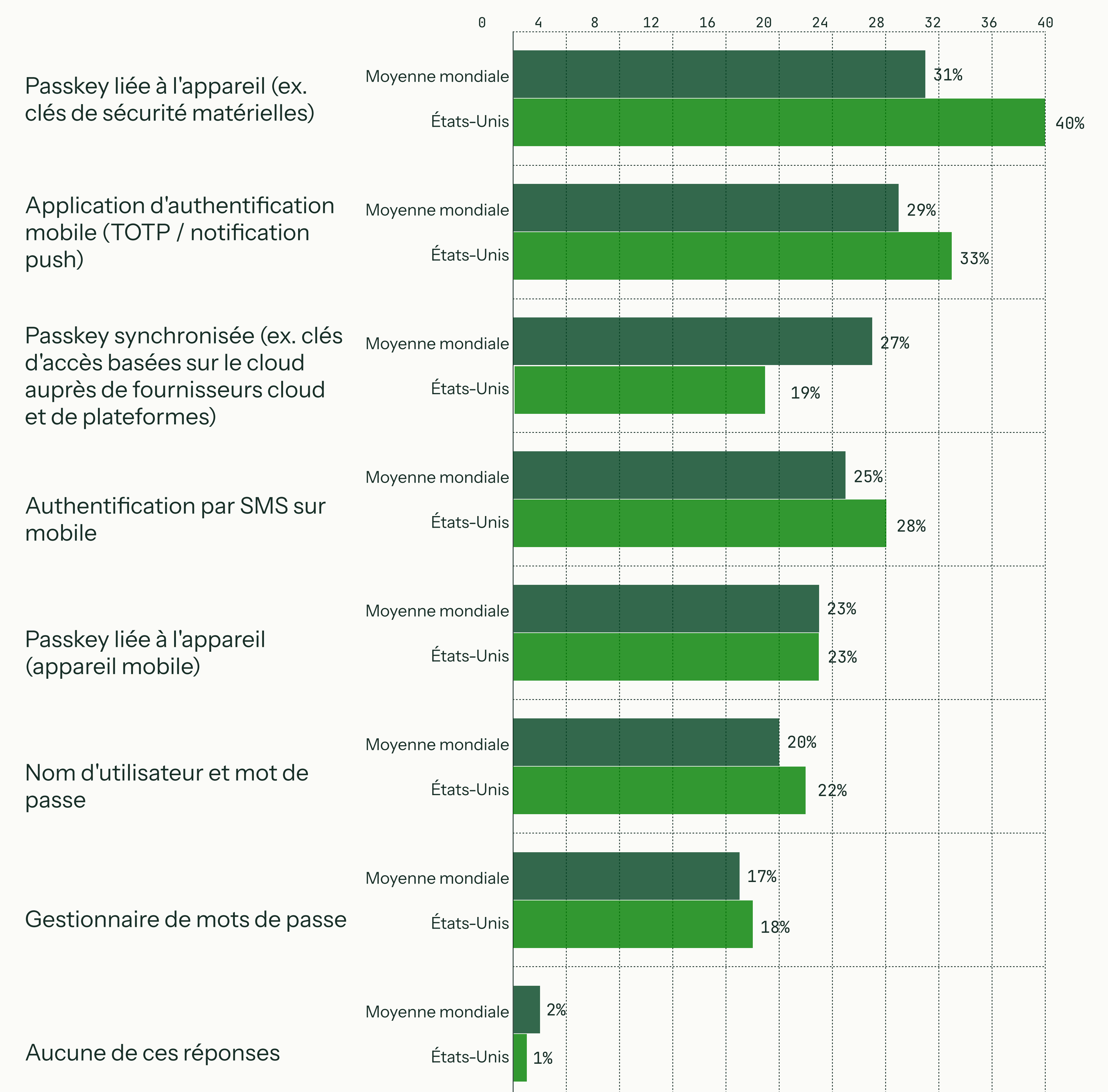


L'écart d'adoption aux États-Unis

Aucun marché n'illustre plus clairement le décalage entre le niveau de sensibilisation et la mise en pratique que les États-Unis. Ceux-ci **affichent le niveau de connaissances techniques le plus élevé, mais aussi la confiance systémique la plus faible et la cadence de changement opérationnel la plus lente.**

- **Forte sensibilisation** : **40 %** des responsables de la sécurité américains considèrent les passkeys matérielles comme l'identifiant le plus sûr (contre **23 %** au Royaume-Uni), et **48 %** des utilisateurs de passkeys ont une expérience personnelle de l'utilisation de passkeys matérielles (contre **28 %** à Singapour).
- Forte dépendance aux identifiants traditionnels : parallèlement, les États-Unis arrivent en tête de tous les marchés en matière de dépendance aux mots de passe avec **50 %** des utilisateurs qui y ont recours au travail et **56 %** à domicile.
- Confiance moindre : seuls **58 %** des répondants américains estiment que les entreprises traitant leurs données personnelles en assurent une protection adéquate (contre **82 %** en Inde).

Quelles sont les méthodes d'authentification les plus sûres ?



Créer une nouvelle architecture de sécurité



Éliminer le risque lié aux identifiants : Un plan de défense matérielle en trois phases

Renforcer la sécurité des entreprises exige d'admettre que la sensibilisation ne suffit pas à résoudre un problème d'architecture. Malgré une bonne culture de la sécurité, les organisations restent freinées par des contraintes opérationnelles, les coûts perçus de déploiement et des processus d'intégration hérités, qui traitent l'authentification multi-facteurs de haut niveau comme un luxe optionnel plutôt qu'une exigence fondamentale.

Pour éliminer les risques liés aux identifiants à l'ère de l'IA, les architectures de sécurité doivent imposer l'utilisation de passkeys matérielles et résistantes au phishing, ainsi que d'autres authenticateurs cryptographiques liés aux appareils, selon trois phases distinctes :

- **Avant l'authentification** : imposer des contrôles d'intégrité et de posture de l'appareil pour vérifier la conformité du terminal avant d'établir une session d'accès. Fournir aux nouveaux employés des authenticateurs résistants au phishing lors du processus d'intégration, afin de garantir une MFA de haut niveau dès la première tentative de connexion.
- **Pendant l'authentification** : appliquer une authentification résistante au phishing dans les politiques de connexion aux applications, afin d'atténuer systématiquement et automatiquement les tentatives de phishing par IA lors des connexions.
- **Après l'authentification** : assurer une évaluation continue du contexte et des risques pour détecter toute compromission de session. Exiger une preuve de présence humaine, via une interaction matérielle physique, comme l'appui sur une touche ou une authentification biométrique, pour valider, avec intervention humaine, les workflows autonomes pilotés par IA.



Conclusion



De la sensibilisation à l'application

Les résultats de l'enquête mondiale 2026 sur l'état de l'authentification démontrent que la sensibilisation à la sécurité ne suffit pas, à elle seule, à protéger l'entreprise. Il s'agit de briser un schéma systémique : tant au travail qu'en dehors, les processus par défaut et les frictions inhérentes aux systèmes poussent même les experts les plus avisés et compétents à choisir la solution de facilité. Une sécurité digne de ce nom ne peut reposer sur la vigilance humaine face à des menaces liées à l'IA toujours plus sophistiquées. Elle exige une évolution de l'architecture d'entreprise visant à faire du choix judicieux le comportement par défaut.

Les responsables de la sécurité savent déjà ce qui fonctionne. Il est désormais temps que les politiques et les infrastructures des entreprises reflètent ce savoir.



Présentation des entreprises et méthodologie

À propos de Yubico

Yubico (Nasdaq Stockholm: YUBICO) est un pionnier mondial de la cybersécurité et à l'origine de la YubiKey, la référence en matière d'authentification matérielle résistante au phishing. Depuis que Yubico a contribué à l'élaboration des standards mondiaux relatifs aux passkeys en 2007, la société a permis d'éliminer les prises de contrôle de comptes pour des entreprises, des gouvernements et des particuliers dans plus de 160 pays. Notre présence mondiale comprend notre siège social à Stockholm, en Suède, ainsi que des bureaux dans la Silicon Valley, en Californie, et à Singapour. Pour en savoir plus, rendez-vous sur www.yubico.com.

À propos d'Okta

Okta, Inc. est le spécialiste de l'identité. Nous sécurisons l'identité des IA, des machines et des humains pour permettre à chacun d'utiliser n'importe quelle technologie en toute sécurité. Nos solutions pour les employés et les clients permettent aux entreprises et aux développeurs de protéger leurs agents d'IA, leurs utilisateurs, leurs employés et leurs partenaires, tout en optimisant la sécurité, l'efficacité et l'innovation. Rendez-vous sur okta.com pour découvrir pourquoi les plus grandes marques mondiales font confiance à Okta pour l'authentification, l'autorisation et bien plus encore.

Méthodologie

Talker Research a mené une enquête quantitative en ligne auprès de 1 890 professionnels des secteurs de la technologie et de la sécurité répartis sur neuf marchés : les États-Unis, le Royaume-Uni, l'Australie, l'Inde, le Japon, Singapour, la France, l'Allemagne et la Suède.

Les personnes interrogées occupaient des postes dans les domaines de la cybersécurité, de l'informatique, de la gestion produit, du génie logiciel et de l'ingénierie matérielle au sein d'organisations de plus de 500 employés. L'enquête a été commandée par Yubico et Okta, et réalisée entre le 2 et le 16 juillet 2026.

Les résultats peuvent varier : les études de cas, les témoignages de clients et les indicateurs de performance reflètent les résultats opérationnels spécifiques obtenus par les organisations présentées, compte tenu de leurs configurations, environnements réseau et paramètres de mise en œuvre propres. © 2026 Okta, Inc. et/ou ses filiales.

Ces informations ne sont fournies qu'à titre indicatif et ne constituent en aucun cas des conseils d'ordre juridique, commercial ou relatifs à la confidentialité, à la sécurité ou à la conformité.