2023

Examen des menaces visant l'espace de connexion de vos clients – et leurs tenants et aboutissants

The State of Secure Identity Report

okta

Sommaire

Avant-propos :

une authentification client plus sûre

La cadence des innovations et l'accès étendu à l'information ont totalement bouleversé la demande en solutions d'identité au cours de la dernière décennie. L'identité constitue désormais le principal point d'entrée de sécurité en entreprise, tant pour les applications axées collaborateurs que pour celles axées clients. Pendant ce temps, les attaques visant l'identité se sont multipliées et complexifiées. Dans ce contexte, la détection et la protection contre ces types d'attaques sont devenues des considérations critiques. Chez Okta, nous tenons à occuper une place de premier plan dans la lutte contre les attaques prenant l'identité pour cible. Cette mission implique non seulement de proposer des produits d'identité de pointe, mais aussi de rehausser les standards du marché en matière de sécurité et proposer de bonnes pratiques à nos clients.

La sécurisation de l'espace de connexion représente l'une des étapes les plus cruciales de ce parcours. L'espace de connexion s'appuie sur l'**authentification**, une fonction essentielle des services de **gestion des identités et des accès clients (CIAM)** pour confirmer l'**identité numérique**, à savoir une série d'attributs définissant un utilisateur donné (ou une **entité** non humaine, comme un terminal ou un système spécifique) dans le contexte d'une application.

Malheureusement, les utilisateurs légitimes ne sont pas les seuls à s'intéresser à ce qui se cache derrière l'espace de connexion. Pour les acteurs malveillants qui pénètrent par effraction, l'opération peut rapporter gros, et plusieurs facteurs économiques ont conduit à l'émergence d'un véritable écosystème de technologies, services et autres ressources qui facilitent de telles **intrusions**.

Tous secteurs confondus, on observe une accélération soutenue des attaques contre les entreprises, des plus petites aux plus grandes. À l'heure où les cybercriminels redoublent d'efforts et ne lésinent pas sur les moyens, notamment en tirant parti des outils d'intelligence artificielle qui transforment la société et les entreprises, protéger l'espace de connexion exige plus que jamais des défenses renforcées.

Pour ne rien arranger, les entreprises ont généralement besoin de portails clients B2C (business-to-consumer) ou B2B (business-to-business) accessibles depuis un réseau internet public. Enfin, l'expérience d'authentification doit être suffisamment visible pour inspirer confiance au client, mais suffisamment fluide pour ne pas causer de désagréments inutiles.

Pendant de nombreuses années, l'authentification du client reposait essentiellement sur un facteur de connaissance, souvent un mot de passe, censé n'être connu que de l'utilisateur légitime et du fournisseur de l'application. Mais ce postulat est constamment infirmé : la connaissance peut être volée ou apprise (p. ex. via l'**Open Source Intelligence**). Les mots de passe, en particulier, sont problématiques, et tant les fournisseurs d'applications que les services CIAM dont ils dépendent doivent inciter les clients à utiliser des facteurs d'authentification plus sûrs. Idéalement, ils devraient également les encourager à utiliser **l'authentification multifacteur (MFA)**.

Jusqu'il y a peu, on pouvait raisonnablement faire valoir qu'il était (quasi) impossible de satisfaire simultanément les deux impératifs que sont l'authentification sécurisée et l'expérience utilisateur – l'un ou l'autre étant inévitablement sacrifié – et que le MFA était trop compliqué pour que son adoption s'étende, surtout dans un contexte B2C.

Mais avec la généralisation des **passkeys**, et surtout des **passkeys synchronisées**, ces arguments ne sont plus défendables. Nous sommes même convaincus que l'avènement des passkeys synchronisées sera un jour considéré comme un jalon majeur de la protection des **identités clients**. De plus, même en faisant abstraction de leurs avantages en termes de sécurité, les passkeys ont démontré qu'elles offraient une expérience utilisateur pratique et familière bien supérieure à celle d'autres approches.

Et ce n'est pas trop tôt. Aujourd'hui, les identités numériques contrôlent l'accès à un nombre croissant d'applications et de services. À ce titre, elles ont des répercussions considérables sur de nombreux aspects de la vie moderne. Cet impact ne fera que grandir à l'avenir : l'authentification, l'**autorisation** et le CIAM en général deviendront des éléments essentiels au maintien de la confiance, de la sécurité et de la confidentialité. En conséquence, le CIAM joue également un rôle charnière dans l'accessibilité et c'est aux responsables de l'identité qu'il revient de déterminer si ce rôle tendra à combler ou à creuser le fossé numérique.

Dans cette troisième édition de notre rapport « The State of Secure Identity » annuel, nous avons voulu sensibiliser davantage les lecteurs aux menaces posées à l'identité client et aux mesures défensives à appliquer pour les neutraliser. Cette année, nous avons quelque peu remanié la structure du rapport qui se présente désormais sous la forme d'un parcours en trois étapes :

- Avant l'espace de connexion – celui-ci devant être accessible, certes, mais pas à tout le monde.
- Au niveau de l'espace de connexion – où la bataille de l'identité fait rage chaque jour.
- Après l'espace de connexion – parce que la sécurisation de l'accès ne s'arrête pas au moment où l'utilisateur a passé la porte.

Merci de vous joindre à nous pour ce périple.

Shiven Ramji
President, Customer Identity Cloud, Okta

Résumé

La gestion des identités et des accès clients (CIAM) représente un segment unique du marché plus large constitué par les solutions de gestion des identités et des accès (IAM). En effet, les applications orientées clients sont confrontées à un paysage de menaces en constante évolution et doivent offrir une expérience à la fois conviviale et hautement confidentielle et sécurisée.

Le présent rapport montre que la fraude à l'inscription, le credential stuffing et le contournement de l'authentification multifacteur (MFA) sont des menaces qui ciblent chaque jour la grande majorité des espaces de connexion client.

Résumé

L’espace de connexion, une aubaine pour les cybercriminels

Ce rapport révèle qu’entre le 1er janvier 2023 et le 30 juin 2023 :

13,9 % des tentatives d’enregistrement de compte répondaient aux critères d’une tentative de fraude à l’inscription tels que définis par la solution Okta Customer Identity Cloud, opérée par Auth0 :

- Parmi les 10 secteurs les plus représentés dans la plateforme, quatre se démarquent en raison du nombre particulièrement important d’inscriptions frauduleuses dont ils sont la cible : les services financiers (28,8 %), les médias (28,4 %), l’industrie (25,1 %), et le secteur des logiciels/SaaS/technologies (24 %).
- Un pic de 10 millions de tentatives d’inscription frauduleuse en une seule journée a été enregistré par la plateforme.
- Le 15 avril, plus de 64 % des tentatives d’enregistrement de compte ont été identifiées comme frauduleuses.

24,3 % des tentatives de connexion répondaient aux critères d’une attaque par credential stuffing tels que définis par la solution Customer Identity Cloud :

- Parmi 10 secteurs les plus représentés dans la plateforme, plusieurs secteurs ont enregistré un nombre plus important d’attaques par credential stuffing : le commerce de détail/e-commerce (51,3 %), les médias (42,3 %), les solutions logicielles/SaaS/technologiques (32,1 %) et les services financiers (30,3 %).
- Un pic de 27 millions de tentatives de credential stuffing en une seule journée a été enregistré par la plateforme.
- Le 1er janvier, plus de 46 % des tentatives de connexion ont été attribuées à des attaques par credential stuffing.

12,7 % des tentatives d’authentification MFA répondaient aux critères d’une attaque malveillante (p. ex. une tentative de contournement du MFA) tels que définis par la solution Customer Identity Cloud :

- Parmi les 10 secteurs les plus représentés dans la plateforme, les médias (12,8 %), les services financiers (10,9 %) l’industrie (7,8 %) et les solutions logicielles/SaaS/technologiques (6,4 %) ont été confrontés à la proportion la plus élevée de tentatives de contournement du MFA.
- Un pic de 750 000 incidents de contournement du MFA en un jour a été enregistré par la plateforme.
- Le 11 juin, les tentatives de contournement du MFA représentaient plus de 30 % de toutes les tentatives d’authentification multifacteur.

Le secteur d’activité d’une entreprise n’est pas le seul facteur influençant les menaces dont il fait l’objet. Par exemple, les petites et grandes entreprises semblent être davantage ciblées par des tentatives d’inscription frauduleuse, de credential stuffing et de contournement du MFA que les organisations de taille moyenne. On peut raisonnablement en déduire que les cybercriminels considèrent les grandes entreprises comme des cibles de plus grande valeur, et les petites comme des proies plus faciles.

Même la région dont elles proviennent a une influence : les entreprises basées dans la région Asie-Pacifique (APAC) sont de loin les plus ciblées par des tentatives d’inscription frauduleuse, tandis que celles du continent américain (AMER) sont confrontées à un nombre plus élevé d’attaques par credential stuffing.

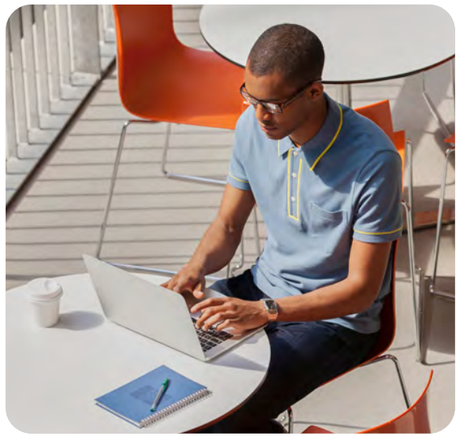
		Tentatives d’inscription frauduleuse[1]		Tentatives de credential stuffing[2]		Tentatives de contournement du MFA[3]	
		Taux	Classement	Taux	Classement	Taux	Classement
	Globalement (toutes technologies confondues)	13,9 %	—	24,3 %	—	12,7 %	—
10 secteurs les plus représentés	Publicité/marketing	1,0 %	10	16,7 %	6	3,4 %	9
	Services financiers	28,8 %	1	30,3 %	4	10,9 %	2
	Agroalimentaire/ restauration/hôtellerie	9,0 %	8	11,4 %	8	5,5 %	5
	Santé	6,3 %	9	16,1 %	7	4,6 %	7
	Industrie	25,1 %	3	17,7 %	5	7,8 %	3
	Médias	28,4 %	2	42,3 %	2	12,8 %	1
	Services professionnels	13,4 %	5	7,2 %	10	4,5 %	8
	Commerce de détail/e-commerce	9,3 %	7	51,3 %	1	5,0 %	6
	Logiciels/SaaS/ technologies	24,0 %	4	32,1 %	3	6,4 %	4
	Voyage/transport	9,7 %	6	7,2 %	9	2,9 %	10
Taille de l’entreprise	Grandes entreprises	19,9 %	1	39,4 %	1	9,5 %	2
	Moyennes entreprises	12,6 %	3	20,1 %	3	9,0 %	3
	Petites entreprises	19,4 %	2	30,9 %	2	20,3 %	1
Siège de l’entreprise	AMER	9,4 %	2	28,0 %	1	12,0 %	1[4]
	APAC	27,9 %	1	13,3 %	3	11,0 %	2
	EMEA	8,1 %	3	20,2 %	2	7,6 %	3

Tableau 1. Récapitulatif des taux d’attaques déterminés par la plateforme Customer Identity Cloud (du 1er janvier 2023 au 30 juin 2023)

[1] Proportion du nombre total de tentatives d’inscription
[2] Proportion du nombre total de tentatives d’authentification par mot de passe
[3] Proportion du nombre total de MFA
[4] Consultez la section Méthodologie pour savoir pourquoi les trois régions sont inférieures à la moyenne mondiale

Résumé

Protéger et satisfaire les clients grâce au CIAM



Si une solution de gestion des identités collaborateurs peut accepter un nombre relativement plus élevé de **points de friction** et souvent compter sur une base d'utilisateurs mieux formés à la sécurité, une solution CIAM ne dispose pas des mêmes atouts et doit s'appuyer sur des techniques de sécurité plus subtiles pour atteindre une posture de sécurité robuste et résiliente, tout en préservant l'aspect pratique et convivial de l'expérience utilisateur.

Comme les attentes des clients sont de plus en plus élevées et que le paysage des menaces ne cesse d'évoluer, ces techniques doivent être continuellement adaptées pour bénéficier du meilleur compromis entre expérience utilisateur, sécurité et confidentialité – un équilibre qui lui-même fluctue selon la tolérance au risque et le profil de risque de chaque entreprise.

Mise en œuvre de défenses multiniveaux

Les contrôles de base (dont la limitation du débit, le blocage des adresses IP suspectes et la détection des mots de passe compromis) constituent autant de mesures de défense nécessaires, mais ne suffisent pas.

De même, la mise en œuvre de politiques efficaces en matière de mots de passe (mots de passe forts, processus de réinitialisation sécurisée, etc.) et de bonnes pratiques de gestion de sessions (exclusion des tokens des URL, génération de nouveaux tokens et aléatoires après la connexion, etc.) sont indispensables, mais ne représentent qu'une partie de la solution.

De la même façon que les cybercriminels investissent dans divers outils pour contourner les mesures de sécurité en place, les services CIAM et les fournisseurs d'applications doivent également accroître leurs investissements dans des défenses de nouvelle génération.

Par exemple, l'outil Bot Detection avec Okta AI a démontré sa capacité à détecter près de 80 % des bots ciblant les systèmes d'authentification. Il est important de souligner que ces fonctionnalités défensives ont été implémentées sans créer de points de friction inutiles pour les utilisateurs. En entraînant et en adaptant continuellement l'IA au cœur de la fonction Bot Detection, il est possible d'éviter dans la plupart des cas l'affichage d'un CAPTCHA aux utilisateurs, afin de leur offrir une expérience qui n'a rien perdu en fluidité.

De plus, l'expérience a démontré que l'efficacité de cet outil a un effet dissuasif non négligeable : en trois mois, certains de nos plus grands clients ont vu chuter leur moyenne de trafic de bots de près de 90 % après avoir activé la fonction Attack Protection, ce qui laisse penser que les cybercriminels préfèrent s'en prendre à des cibles plus faciles.

Authentification renforcée

Nous n'insisterons jamais assez sur le potentiel des passkeys pour renforcer l'authentification des clients par rapport aux connexions basées sur les mots de passe. Les mots de passe sont à l'origine de nombreuses menaces basées sur l'identité et les passkeys représentent un pas en avant important qui devrait permettre de reléguer les mots de passe à un rôle mineur dans la sécurisation des connexions :

- En particulier, les passkeys synchronisées offrent une authentification forte à la fois familière et pratique, qui convient parfaitement au consommateur lambda, très sensible aux points de friction. (En fait, depuis le 10 octobre 2023, Google propose une passkey comme option par défaut pour la connexion aux comptes Google personnels.)
- Les **passkeys liées au terminal** constituent un excellent choix pour les marchés B2B et d'autres applications clients exigeant l'authentification renforcée offerte par les clés de sécurité et les authentificateurs certifiés **FIDO**.

Le MFA en général continue aussi de jouer un rôle majeur dans le renforcement de l'authentification des clients. Par le passé, les entreprises orientées clients hésitaient à introduire et à imposer le MFA, craignant que des points de friction supplémentaires n'entravent les conversions. Toutefois, ces objections n'ont plus de raison d'être, et ce, depuis quelques années déjà.

- **Le MFA adaptatif** permet aux fournisseurs d'applications de limiter les demandes MFA supplémentaires aux connexions risquées, où le niveau de risque constitue un critère important des signaux d'attaque.
- **L'authentification renforcée** permet aux fournisseurs d'applications de donner accès à des ressources à faible risque via un mécanisme d'authentification relativement plus faible (p. ex un mot de passe) et de limiter l'authentification renforcée (p. ex le MFA) aux cas où un utilisateur souhaite accéder à une ressource plus sensible.

Mais n'oublions pas que les cybercriminels investissent eux aussi davantage de ressources dans les mécanismes de contournement des facteurs MFA relativement plus faibles. Il est donc capital que les fournisseurs d'applications proposent à leurs clients des authentificateurs basés sur la possession ou la biométrie.

Développer ou acheter ?

Le développement d'une telle solution CIAM multiniveau représente un projet de grande envergure que peu d'entreprises ont les moyens de mener à bien. Quoi qu'il en soit, ces différents niveaux de protection et technologies sont nécessaires pour offrir une expérience client pratique et sécurisée qui protège aussi la confidentialité.

Pour la plupart des entreprises, une solution CIAM agile, qui intègre la sécurité dans sa conception, constitue l'approche la plus efficace : elle leur permet d'adapter la gestion des identités et des accès clients et de l'optimiser constamment, sans devoir faire appel à des ressources qui seraient mieux employées au développement des compétences clés de l'entreprise.

Une solution d'authentification tierce peut faire toute la différence

Une récente enquête mondiale menée auprès d'équipes de développement a mis en évidence l'intérêt d'intégrer l'authentification tierce aux applications SaaS.

Basée sur 675 réponses de professionnels du monde entier, l'enquête a révélé ce qui suit :

- **La fonction d'authentification se classe en troisième position des processus les plus chronophages en termes de gestion et maintenance**, juste derrière les fonctions de stockage et gestion des données, et l'automatisation et les outils DevOps.
- **L'authentification tierce réduit le délai de lancement plus que tout autre composant SaaS :** 88 % des entreprises qui utilisent une plateforme SaaS tierce pour l'authentification ont réduit leurs délais de lancement l'année dernière.

Pour en savoir plus, lisez notre rapport Le point sur l'adoption des services SaaS par les équipes de développement. ■

Introduction à la protection des identités clients

La sécurisation des identités clients doit être une priorité absolue pour tout fournisseur d'applications ou de services, pour une raison évidente : un grand nombre d'acteurs malveillants veulent accéder à ce qui se cache derrière votre espace de connexion et sont prêts à déployer des efforts considérables pour arriver à leurs fins.

Dans cette troisième édition de notre rapport « The State of Secure Identity » annuel, nous avons tenu à sensibiliser les lecteurs à diverses considérations :

- Les menaces posées à l'identité client
- Les techniques actuellement disponibles qui peuvent être superposées pour ériger des défenses robustes et fiables

Pour ce faire, nous examinerons les schémas d'attaque les plus courants et redoutables, ainsi que les tendances générales qui façonnent le paysage des menaces de demain.

Dans la mesure du possible, nous fournirons des données provenant d'Okta Customer Identity Cloud opéré par Auth0 (qui fournit des fonctionnalités CIAM à plusieurs milliers d'entreprises de toutes tailles) pour illustrer la prévalence et l'impact des menaces ciblant l'identité.

Mais avant d'entrer dans les détails, il convient de s'attarder un instant sur le contexte unique de l'identité client, en particulier :

- La nécessité d'offrir des expériences pratiques et sécurisées
- Le rôle essentiel de la gestion des identités et des accès clients (CIAM)
- L'évolution permanente des mécanismes d'authentification
- Le double tranchant de l'intelligence artificielle (IA)

Introduction à la protection des identités clients

Les clients attendent des expériences sûres et pratiques

Pour toute entreprise servant ses clients via un canal numérique, il est essentiel de minimiser les points de friction inhérents à chaque interaction. Concrètement, il s'agit de limiter le nombre de clics nécessaires, de concevoir des interfaces utilisateurs intuitives, de réduire la latence et d'offrir une expérience utilisateur cohérente et pratique sur l'ensemble des canaux (tels que les sites web et les applications).

Pour protéger leurs services et leurs clients légitimes, les entreprises doivent également mettre en œuvre des mesures de sécurité capables de résister à un large éventail d'attaques ciblant l'identité. Dans un scénario idéal d'implémentation de l'identité, le nombre de points de frictions serait infini pour les cybercriminels, et pratiquement nul pour les utilisateurs authentiques – mais pas entièrement, car un point de friction opportun et adapté permet de renforcer la confiance.

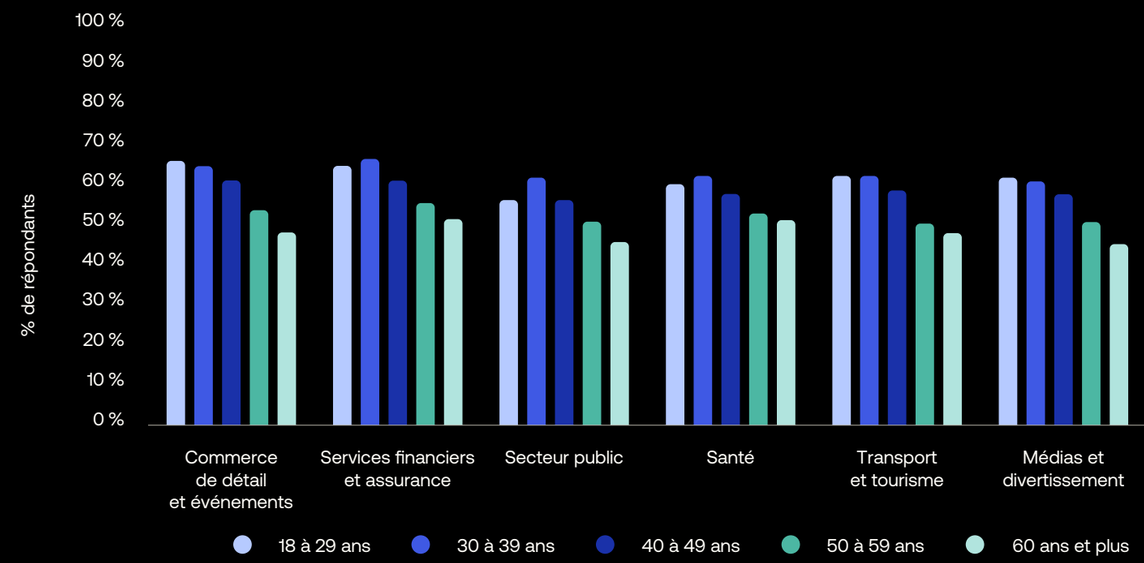
Bien qu'il s'agisse d'un objectif louable, le monde réel nécessite souvent des compromis. Par exemple, le déploiement d'un mécanisme permettant de détecter et de bloquer les attaques de bots à grande échelle peut accroître la résilience globale d'une application, mais au détriment d'un certain nombre d'utilisateurs humains invités à répondre à une vérification de sécurité.

Une fois déployé, le mécanisme peut être affiné en fonction d'informations opérationnelles afin de trouver le bon équilibre entre sécurité et commodité. Dans la pratique, cet équilibre variera d'une application à l'autre, d'une entreprise à l'autre et d'un secteur à l'autre, car chaque combinaison de clientèle, de paysage des menaces et de préférences de sécurité est unique. Pour compliquer encore les choses, l'équilibre peut fluctuer au fil du temps, à mesure que les cybercriminels adaptent leurs tactiques, techniques et procédures (TTP) et choisissent de nouvelles cibles, et que les souhaits des clients évoluent.

Cependant, les entreprises qui se mobilisent pour trouver cet équilibre peuvent en tirer des bénéfices considérables. Par exemple, le rapport d'Okta Customer Identity Trends Report 2023, qui s'appuie sur une enquête mondiale menée auprès de 21 512 consommateurs de 14 pays, a révélé que près de 60 % des personnes interrogées seraient plus susceptibles de faire appel à une marque dont les services offrent un processus de connexion simple, fluide et sécurisé (figure 1). C'est particulièrement le cas des groupes démographiques plus jeunes, qui sont extrêmement convoités.

Figure 1. Les consommateurs sont plus susceptibles de faire appel à une marque en ligne s'ils savent que l'expérience de connexion est simple, fluide et sécurisée.

Les graphiques représentent l'ensemble des réponses « Très susceptible » et « Plutôt susceptible ».



Introduction à la protection des identités clients

Le rôle du CIAM dans la sécurisation des identités et des applications

Un mécanisme de détection des bots tel que celui décrit ci-dessus n'est qu'un élément parmi d'autres de la pile de sécurité de l'identité, tout comme la protection des identités n'est qu'un aspect de la gestion des identités et des accès clients (CIAM).

Les solutions CIAM modernes sont conçues pour aider les entreprises à trouver le juste équilibre entre commodité, respect de la confidentialité et sécurité pour chaque type d'utilisateur souhaitant accéder à leurs services ou applications. Elles permettent également aux entreprises de faire évoluer en permanence l'expérience utilisateur, de réduire le nombre de sollicitations de l'équipe d'ingénierie concernant les fonctionnalités liées à l'identité (ce qui lui permet de se concentrer sur les fonctionnalités principales) et de répondre efficacement aux exigences réglementaires, contractuelles et de certification.

En termes d'identité, les trois principales fonctionnalités d'un CIAM efficace sont l'authentification, l'autorisation et la gestion des identités :

- **L'authentification** vérifie l'identité des utilisateurs qui se connectent aux comptes concernés.
- **L'autorisation** permet d'octroyer à un utilisateur le bon niveau d'accès à une application et/ou à des ressources.
- **La gestion des identités**, lorsqu'elle est complète et bien conçue, permet aux administrateurs de mettre à jour les autorisations d'accès des utilisateurs et d'implémenter des politiques de sécurité. Elle permet également aux clients de gérer (dans les limites des cas d'usage concernés et des réglementations en vigueur) leurs propres identités, données et préférences.

Bien que la définition de base du CIAM reste la même au sens propre, ce à quoi ce terme renvoie (cas d'usage spécifiques, composants fonctionnels mis en jeu, organisations concernées, etc.) a évolué, en particulier au cours des dernières années.

Aujourd'hui, le CIAM répond à de nombreux besoins :

- **Clients particuliers –** Dans le cadre de la vente aux particuliers, l'implémentation réussie d'un CIAM vous permet de proposer des promotions et recommandations hautement personnalisées et capables de générer des recettes supplémentaires, mais aussi d'apporter une valeur ajoutée à vos clients, accompagnée d'une expérience utilisateur pratique sur l'ensemble de vos canaux numériques.
- **Clients professionnels –** Un très grand nombre d'entreprises s'appuient principalement sur des applications SaaS B2B (business-to-business) pour soutenir leurs activités. Toutefois, au sein de chaque entreprise, chaque type d'utilisateur a besoin d'un niveau d'accès spécifique aux différentes ressources. Leur proposer une expérience simple et sécurisée implique donc de gérer de façon précise les identités et les droits d'accès. Le CIAM offre une solution idéale à ces difficultés en permettant aux clients d'applications SaaS B2B de gérer eux-mêmes leurs identités.
- **Autres acteurs, partenaires et parties prenantes connues –** Dans le cas des applications SaaS et grand public, les clients gèrent eux-mêmes leur identité. Il existe toutefois de nombreuses situations dans lesquelles il est nécessaire que l'identité soit gérée par l'entreprise qui propose le service concerné. Afin de répondre aux cas d'usage dans lesquels les identités des clients sont connues et administrées par un fournisseur de services, le CIAM propose tous les outils dont les entreprises ont besoin pour gérer la création, la maintenance et la fin de vie des comptes clients.

Dans le contexte de la gestion des identités collaborateurs, les administrateurs peuvent imposer des contrôles avec (comparativement) un peu moins d'égards pour l'expérience utilisateur. Dans le cadre de la gestion des identités clients, la nécessité de minimiser, ou du moins de gérer soigneusement les points de friction engendre un certain nombre défis, en particulier liés à l'authentification.

Introduction à la protection des identités clients

Adapter l'authentification sécurisée pour répondre au désir de simplicité

Bien que l'approche Zero Trust représente une évolution majeure en matière de gestion des identités collaborateurs, le CIAM a quant à lui toujours fonctionné sur un modèle sans confiance. Dans presque tous les cas d'usage CIAM purs, ni le fournisseur d'application ni le fournisseur d'identité ne contrôlent les terminaux à partir desquels les utilisateurs accèdent au service.

Pour établir une confiance suffisante pour permettre une interaction ou une transaction, c'est-à-dire accorder un certain niveau d'accès, les flux d'identité exigent de chaque utilisateur qu'il présente un ou plusieurs facteurs d'authentification :

- **Connaissance –** Une information que l'utilisateur connaît, telle qu'un mot de passe ou une question de sécurité
- **Possession –** Un élément que l'utilisateur possède, tel qu'un téléphone ou accès à un compte de messagerie.
- **Inhérence –** Une caractéristique propre à l'utilisateur, correspondant à un attribut biométrique tel qu'une empreinte digitale, un visage ou un profil vocal. Dans la plupart des cas, le terminal atteste que la personne qui tente de s'authentifier est la même que celle qui a initialement configuré ce type d'authentification.

Cependant, ce qui n'était au départ qu'une simple page ou boîte de dialogue de connexion remplie par des humains a radicalement changé au fil des ans :

- **Complexification des mots de passe –** Comme les cybercriminels ont appris à deviner les mots de passe faibles et à tirer parti de la tendance trop fréquente à réutiliser les mots de passe, les exigences en matière de complexité ont évolué. Les mots de passe sont de plus en plus longs et doivent souvent comporter à la fois des caractères spéciaux, des chiffres et des combinaisons de lettres majuscules et minuscules.
- **Développement de la gestion des mots de passe –** Les utilisateurs sont contraints d'utiliser des mots de passe plus nombreux et complexes, ce qui a favorisé l'adoption de gestionnaires de mots de passe, qu'ils soient implémentés dans un navigateur ou dans une application distincte.
- **Importance croissante du MFA –** Face à la multiplication des attaques de **phishing** et à l'apparition d'énormes bases en ligne contenant des extractions de mots de passe, l'authentification multifacteur (MFA) a fait des adeptes en tant que protection efficace contre l'**usurpation de compte (ATO)**.

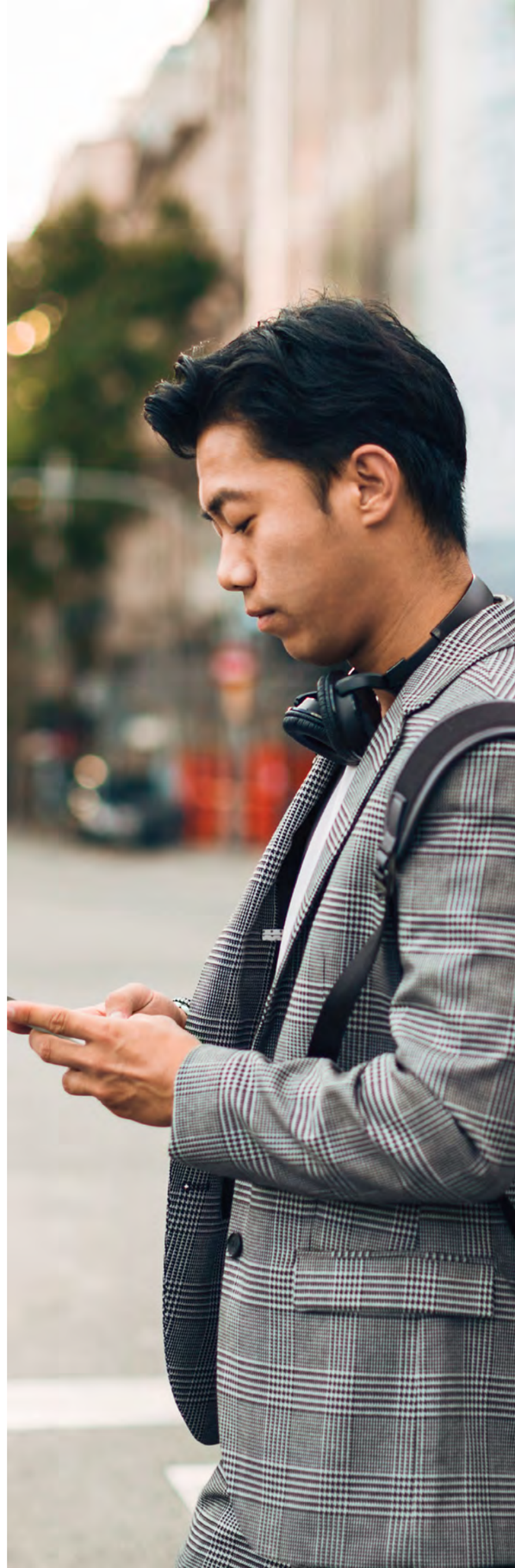
Malheureusement, les frictions associées aux techniques MFA traditionnelles ont entravé leur adoption. Par ailleurs, de nombreuses techniques MFA plus anciennes sont aujourd'hui menacées dans la mesure où les cybercriminels disposent de moyens peu coûteux de contourner cet obstacle important à grande échelle.

En réponse à l'évolution des techniques d'authentification et des TTP des cybercriminels, les solutions CIAM ont introduit de nouvelles couches de protection des identités afin de contrer un large éventail de cyberattaques automatisées qui non seulement coûtent cher aux entreprises, mais menacent également la confidentialité des clients.

Les mesures de sécurité modernes, telles que le MFA adaptatif et l'authentification renforcée, sont conçues pour ne créer des frictions que lorsque le niveau de risque le justifie, se rapprochant ainsi de plus en plus de la solution idéale. Pour décider dans quels cas précis une vérification de sécurité est nécessaire, c'est-à-dire pour maintenir un équilibre optimal entre sécurité et commodité, les solutions CIAM modernes s'appuient sur des systèmes intelligents qui analysent les signaux de risque et d'autres données contextuelles (comme le niveau d'accès demandé) pour évaluer le risque, sélectionner le type de demande d'authentification approprié, etc.

En fait, l'intelligence artificielle (IA) est depuis longtemps intégrée aux systèmes d'identité, et son importance ne va sans aucun doute qu'aller croissant. En effet, au-delà de la sécurité, l'IA peut par exemple être utilisée pour optimiser les expériences clients.

Cependant, si l'IA offre de nombreux avantages, elle n'est en définitive qu'un outil supplémentaire qui peut être utilisé à bon ou à mauvais escient.



Introduction à la protection des identités clients

L'IA facilite les attaques ciblant l'identité à grande échelle

À un niveau élémentaire, l'intelligence artificielle (IA) peut être considérée comme une décision prise par un ordinateur et dont « l'intelligence » la rend impossible à distinguer d'une décision humaine, indépendamment de la manière dont la décision est prise.

L'idée de départ remonte à 1943, bien avant l'invention de l'ordinateur à mémoire numérique, lorsque le logicien Walter Pitts et le neuroscientifique Warren McCulloch tentèrent de créer une représentation mathématique des neurones d'un cerveau humain.

Depuis les années 1960, l'intelligence artificielle a évolué pour englober de très nombreux algorithmes capables d'effectuer diverses tâches. L'une d'elles est la détection et reconnaissance de modèles, généralement appelée machine learning, ou apprentissage automatique. Le domaine du machine learning a progressé de manière spectaculaire au cours des 15 dernières années grâce aux progrès réalisés dans la construction et la manipulation des réseaux neuronaux. Grâce à des ordinateurs plus puissants que jamais, les réseaux neuronaux peuvent gagner en « profondeur », ce qui a permis l'émergence du deep learning, ou apprentissage profond, plus pratique et économique.

Cependant, l'évolution de l'IA qui a le plus marqué les esprits, certains dirons même secoué le grand public, est l'apparition et les progrès rapides de l'IA générative, principalement grâce à des avancées remarquables dans les grands modèles de langage (LLM).

Soudain, la rédaction en prose et la création d'images complexes (et réalistes, si tel est le but recherché) ne sont plus l'apanage des seuls humains. De plus, comme les LLM maîtrisent bien l'écriture, y compris la programmation, et que beaucoup de choses sont aujourd'hui contrôlées par logiciel, ils sont à l'origine de percées et d'avancées inattendues dans un grand nombre de domaines.

Dans le contexte de la protection des identités, les progrès de l'IA rendent le paysage des menaces plus dangereux à plusieurs égards. Par exemple, l'IA peut :

- **Accentuer la dangerosité des attaques ciblant l'identité existantes de faible qualité, mais forte intensité –** Le credential stuffing, les inscriptions frauduleuses, la fraude aux SMS et d'autres attaques peuvent devenir plus difficiles à détecter et plus efficaces ou dévastatrices.
- **Favoriser l'apparition de tout nouveaux types d'attaques ciblant l'identité –** Certaines nouvelles attaques seront anticipées par les équipes de sécurité ou découvertes à l'avance par les chercheurs, mais d'autres ne deviendront apparentes que lorsqu'elles seront identifiées sur le terrain. (Il s'agit là du problème des « inconnues inconnues ».)
- **Contourner certaines mesures de sécurité existantes –** Les outils basés sur l'IA ont déjà démontré leur capacité à résoudre les CAPTCHA et à tromper les systèmes biométriques vocaux à l'aide de deepfakes.

Par ailleurs, les capacités de codage et de création de scripts de l'IA générative permettent aux cybercriminels de lancer plus facilement des attaques quel que soit leur niveau de compétence (notamment en programmation), ce qui pourrait attirer davantage de prétendants dans l'écosystème de la cybercriminalité et améliorer leur efficacité opérationnelle.

Attaques personnalisées efficaces à grande échelle

La nouvelle menace la plus dangereuse pour l'identité réside peut-être dans le fait que l'IA permet le **spear phishing** à grande échelle. Considérons un exemple de processus d'attaque plausible :

1. Un cybercriminel choisit une entreprise à cibler.
2. Le cybercriminel utilise des techniques **OSINT (Open Source Intelligence)** pour compiler la liste des collaborateurs de l'entreprise.
3. Le cybercriminel introduit cette liste dans une API de recherche sociale (de nombreuses options sont disponibles), qui renvoie ensuite une liste de comptes de réseaux sociaux associés à chaque collaborateur.
4. Le cybercriminel filtre la liste par programmation afin d'identifier les collaborateurs disposant des comptes de réseaux sociaux ouverts et actifs, puis examine chacun d'entre eux pour identifier qui l'utilisateur suit, quels messages il aime, ce qu'il publie, quand il est actif, etc. Le cybercriminel peut même effectuer une analyse des sentiments par thème pour élaborer des profils psychologiques hautement personnalisés, qu'il peut mettre à jour au fil du temps.
5. Le cybercriminel suit chaque collaborateur sur les applications sociales disponibles et se met à interagir avec lui de manière tout à fait anodine (par exemple, en aimant et en repartageant des publications, en ajoutant des commentaires, etc.) afin de créer un lien.
6. Le cybercriminel surveille l'actualité et les tendances du moment pour trouver une occasion d'entrer en contact avec chaque collaborateur sur le plan personnel.
7. Le cybercriminel rédige un e-mail (ou un message direct, quelle que soit la plateforme) et contacte chaque collaborateur ciblé.
8. Si la cible répond, la conversation peut se poursuivre jusqu'à ce que la confiance établie soit suffisante pour que le cybercriminel puisse formuler une demande avec une forte probabilité d'être bien accueilli.

Jusqu'il y a peu, l'exécution de ce type de chaîne d'attaque représentait une entreprise fastidieuse et coûteuse car elle devait être effectuée manuellement. Aujourd'hui, elle peut être presque entièrement automatisée et exécutée à grande échelle, permettant ainsi de cibler personnellement des milliers de collaborateurs au sein de nombreuses entreprises à moindres frais.

Renforcement des défenses

Heureusement, si l'IA aidera sans aucun doute les cybercriminels, elle permettra aussi de doper les capacités des équipes de sécurité. Par exemple, l'IA peut être utilisée aux fins suivantes :

- **Renforcement de la sécurité des applications dès la conception –** Tout comme les cybercriminels, les fournisseurs d'applications peuvent utiliser l'IA pour détecter les vulnérabilités et les failles de sécurité, et ainsi renforcer la sécurité des logiciels et des systèmes avant même leur publication.
- **Amélioration de la détection automatique des menaces –** L'analyse contextuelle et comportementale est déjà capable d'éclairer les évaluations des risques intelligentes et de détecter les menaces avancées ciblant l'identité, et les progrès de l'IA ne feront qu'améliorer la capacité à exécuter ces fonctions et à en introduire de nouvelles.
- **Réduction des risques –** Qu'il s'agisse d'automatiser les mesures de défense (telles que les actions de confinement ou le blocage des activités malveillantes) ou d'associer une série d'actions recommandées à une alerte, l'IA offrira une aide précieuse pour la réduction des risques et la réponse proactive aux attaques.

Le décor étant planté, commençons notre exploration de l'espace de connexion, et au-delà. ■

Partie 1 : avant l’espace de connexion

Ces défenses initiales ont pour but d’empêcher toute entité illégitime (être humain ou machine/système) d’accéder à l’interface de connexion.

Plus tôt une entité malveillante peut être bloquée, mieux c’est, car cela réduit les coûts de calcul et limite les actions de reconnaissance que le cybercriminel peut effectuer (par exemple, en recevant et en analysant les messages d’erreur).

À cette fin, un certain nombre de mesures de défense sont implémentées à différents niveaux de l’infrastructure d’identités :

- Les **défenses d’hébergement**, qui sont appliquées par le fournisseur d’hébergement (p. ex. Microsoft Azure, Amazon Web Services) ou au niveau de la couche d’hébergement (p. ex. Cloudflare)
- Les **défenses de plateforme**, qui s’appliquent à l’ensemble de la plateforme CIAM (p. ex. Okta Customer Identity Cloud)
- Les **défenses d’application**, qui s’appliquent à une seule application CIAM (p. ex. une solution interne ou autonome)

Partie 1 : avant l'espace de connexion

Les défenses de la couche hébergement sont en première ligne

Les fournisseurs d'hébergement proposent un certain nombre de fonctionnalités de sécurité destinées à empêcher l'utilisation abusive des services qu'ils hébergent, telles que :

- **Neutralisation des attaques DDoS –** Les protections permettent à votre application CIAM de rester accessible aux utilisateurs légitimes, même face à des attaques de grande ampleur (en particulier au niveau de la couche TCP/UDP).
- **Gestion des bots –** Une première couche de filtrage des bots repose généralement sur une combinaison d'analyses comportementales, de threat intelligence et de boucles de feedback.
- **Limitation du débit –** Des contrôles permettent de se protéger contre les attaques DoS, les stratégies de force brute et l'utilisation abusive des API en imposant des restrictions sur la vitesse à laquelle une entité particulière peut accéder à la plateforme/application CIAM.

Partie 1 : avant l'espace de connexion

Les défenses de la couche plateforme et application profitent de l'effet de réseau

S'étalant sur un spectre allant du tactique au stratégique, ces défenses sont plus efficaces lorsqu'elles sont utilisées en combinaison et personnalisées pour répondre à des besoins spécifiques.

Elles bénéficient aussi énormément des effets de réseau. Une plateforme CIAM fournissant des services de gestion des identités clients à plusieurs centaines ou milliers d'entreprises peut collecter infiniment plus de données de threat intelligence qu'une application CIAM isolée, au profit de chaque entreprise connectée à la plateforme. Par exemple, les adresses IP observées lors de l'attaque d'un tenant peuvent être bloquées pour tous les tenants.

Limitation du débit

La limitation du débit est un outil utile pour contrer les attaques par force brute de grande envergure en imposant des restrictions sur la vitesse à laquelle une entité particulière peut interagir avec la plateforme CIAM dans son ensemble, ou avec l'application CIAM d'entreprises individuelles.

Dans les deux cas, lorsqu'une entité dépasse un seuil prescrit (p. ex. un nombre maximum de tentatives en une heure), des mesures de sécurité peuvent être déclenchées :

- Demande d'authentification (p. ex. CAPTCHA)
- Interdiction d'accéder à l'interface de connexion jusqu'à l'expiration d'un certain délai défini

Par ailleurs, la limitation du débit est également efficace pour limiter l'impact des attaques DDoS qui ciblent le service d'identité. Pour les sites et services dont les fonctionnalités sont protégées par un mécanisme de connexion, la saturation du service d'authentification entraîne le même résultat que n'importe quel autre type d'attaque DoS : empêcher les clients légitimes d'utiliser le service.

Blocage des adresses IP suspectes

Le blocage des adresses IP suspectes pour les empêcher d'accéder aux services connectés à Internet est utilisé depuis des décennies et reste utile aujourd'hui, à condition que ses limites soient reconnues.

L'approche est simple :

- Des facteurs particuliers sont utilisés pour déterminer si une adresse IP peut être considérée comme fiable.
- Les adresses qui n'atteignent pas un seuil de confiance prescrit se voient refuser l'accès à l'application.

La même technique générale peut être appliquée aux numéros de téléphone, aux adresses e-mail (p. ex. certaines applications n'autorisent que les utilisateurs de services e-mail payants à s'inscrire) et à d'autres variables.

Pour faciliter ce filtrage, de nombreuses entreprises s'abonnent à des services de threat intelligence, d'autres tiennent une liste interne de réputations basées sur leurs propres observations directes, et d'autres encore combinent ces approches.

Détection des bots

Le trafic généré par les bots entrave les flux d'identité à toutes les étapes du parcours utilisateur. Outre le désagrément majeur occasionné, il a également un coût caché. À titre d'exemple, la plateforme Customer Identity Cloud reçoit chaque mois plusieurs milliards de demandes de connexion provenant de bots, ce qui équivaut potentiellement à plusieurs millions de dollars de frais de calcul supportés par les fournisseurs d'applications simplement pour traiter ce trafic fallacieux.

En analysant diverses sources de données et observations, il est possible de déterminer avec un haut degré de certitude si une tentative de connexion émane d'un bot.

Le cas échéant, la demande peut être bloquée ou ignorée d'emblée, ou l'entité peut être invitée à répondre à une demande d'authentification, telle qu'un CAPTCHA.

Utiliser des machines pour combattre les machines

Composant essentiel de l'extension Attack Protection pour Customer Identity Cloud, la fonctionnalité Bot Detection neutralise les attaques de script (p. ex. le credential stuffing, la prédiction de mot de passe, le password spray) contre les applications natives, les flux **passwordless** et les pages de connexion personnalisées.

En analysant plus de 60 sources de données (tels que des événements passés associés à une adresse IP, l'historique des connexions récentes, les données de réputation des adresses IP et une série d'autres facteurs), Bot Detection prédit quand une demande d'identité est susceptible de provenir d'un bot. Au-delà d'un certain seuil de prédiction/confiance, le flux d'authentification présente une contre-mesure, telle qu'un CAPTCHA.

Bot Detection est un excellent exemple de la façon dont l'IA peut améliorer les techniques antérieures :

- La première version, introduite en février 2021, était basée sur des règles et permettait de détecter 18 % des bots.
- La deuxième version, lancée en août 2021, utilisait le machine learning pour l'analyse comportementale. Cette approche optimisée par l'IA a plus que doublé l'efficacité, enregistrant un taux de détection de 45 % des bots.
- La version la plus récente, lancée en juin 2022, détecte 79 % des bots, soit la meilleure performance à ce jour, en dépit du fait que les cybercriminels ne cessent d'affiner leurs propres techniques.

Il est important de souligner que ces fonctionnalités défensives optimisées ont été implémentées sans créer de points de friction inutiles pour les utilisateurs. En entraînant et en adaptant continuellement l'IA au cœur de la fonction Bot Detection, il est possible d'éviter dans la plupart des cas l'affichage d'un CAPTCHA aux utilisateurs.

De plus, une étude interne détaillée examinant les effets avant/après de Bot Detection a révélé un fort effet dissuasif :

- En moyenne, les clients de l'étude qui ont activé Bot Detection ont constaté une réduction du trafic malveillant de plus de 40 %.
- Certains clients de grande taille ont constaté une baisse de plus de 90 % du trafic de bots.

Ces résultats suggèrent que les cybercriminels préfèrent éviter de cibler les entreprises qui disposent de défenses de pointe. ■

Partie 2 : à l’espace de connexion

Les entités qui parviennent jusqu’à l’espace de connexion ont déjà franchi une série d’obstacles conçus pour bloquer les cybercriminels. À ce stade, l’utilisateur légitime peut exécuter deux actions :

- Créer un compte
- Se connecter à un compte existant

Comme nous le verrons, les cybercriminels ciblent régulièrement les deux services.

Partie 2 : à l'espace de connexion

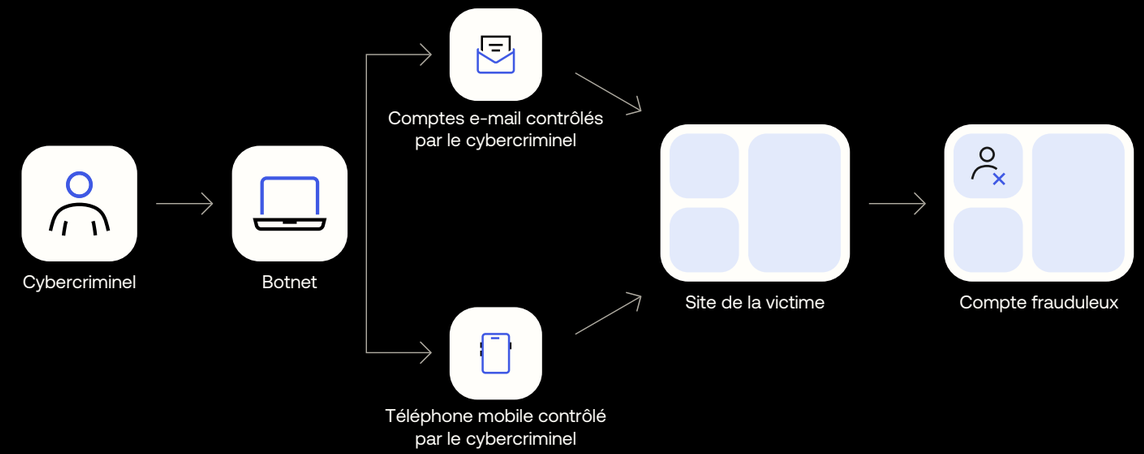
Les offres spéciales à l'inscription attirent les acteurs malveillants

Le moyen le plus simple pour un utilisateur malveillant d'accéder aux privilèges, aux services et aux informations se trouvant derrière l'espace de connexion est de créer des comptes frauduleux qui seront sous son contrôle dès le premier jour.

Il existe un certain nombre de motivations potentielles pour agir de la sorte, par exemple :

- **Obtenir un accès inéquitable à quelque chose de rare**, tel qu'un arrivage de baskets en édition limitée, des billets de concert, de nouvelles consoles de jeux vidéo en pénurie, etc.
- **Bénéficier de récompenses ou d'offres spéciales associées à la création d'un compte**, notamment des cartes-cadeaux, des tokens de cryptomonnaie, etc.
- **Lancer des campagnes de spam, de désinformation ou de cyberactivisme** qui utilisent des comptes pour participer à des fils de commentaires ou pour amplifier des messages
- **Commettre une fraude à l'identité synthétique**, qui utilise souvent les services financiers et les comptes de services d'utilité publique
- **Revendre des comptes** à des parties intéressées
- **Nuire à la capacité du fournisseur d'application à fournir des services** en épuisant l'espace de noms des utilisateurs potentiels et en empêchant ainsi les utilisateurs légitimes de s'inscrire
- **Optimiser les attaques d'usurpation de compte (ATO)** en utilisant les comptes frauduleux pour manipuler soigneusement les taux de réussite et d'échec des connexions afin de contourner les mesures de sécurité automatisées

Figure 2. Anatomie des attaques par inscription frauduleuse



Les inscriptions frauduleuses ciblent principalement les entreprises qui opèrent dans un contexte B2C, en particulier dans le cas où un utilisateur peut créer un compte gratuitement et sans aucune condition préalable (telle qu'une preuve d'achat).

Les inscriptions frauduleuses peuvent créer des problèmes importants et entraîner des dépenses inutiles, surtout lorsque les attaques sont menées à grande échelle.

Premièrement, les utilisateurs malveillants peuvent porter préjudice à l'expérience des utilisateurs légitimes (p. ex. en raflant des produits très demandés), ce qui entraîne le mécontentement des clients et une atteinte à la réputation de l'entreprise. En outre, ils consomment des ressources et peuvent abuser de leur accès pour attaquer directement l'entreprise ou lui nuire.

Deuxièmement, dans la mesure où l'un des principaux objectifs des entreprises B2C est de transformer les prospects en nouveaux clients, des flux de conversion entiers sont souvent optimisés en fonction des données analytiques qui montrent comment les utilisateurs interagissent avec le service. Les inscriptions frauduleuses polluent ces données, ce qui complique considérablement les activités d'analyse commerciale et peut nécessiter des projets de nettoyage onéreux.

Malheureusement, comme les entreprises B2C (en particulier) dépendent tellement de la maximisation des taux de conversion, la tentation est grande de minimiser les frictions au cours du processus d'enregistrement. Cependant, la réduction des frictions pour les utilisateurs légitimes élimine également les obstacles pour les utilisateurs malintentionnés.

Le cybercriminel peut chercher à ne créer qu'un nombre relativement restreint de comptes frauduleux ou utiliser un botnet pour automatiser la création d'un grand nombre de comptes (plusieurs milliers, voire millions). Dans ce dernier cas, l'opération peut être facilitée par des listes de noms d'utilisateur courants.

Une augmentation soudaine du nombre d'échecs d'inscription (ou du taux d'échec des inscriptions) est un très bon indicateur et suggère que votre application fait l'objet d'une attaque. Dans ce cas, un examen approfondi du trafic d'inscription est recommandé pour voir si des seuils ou des règles doivent être modifiés.

Observations globales

La figure 3 présente une vue globale (c'est-à-dire à l'échelle de la technologie) des tentatives d'inscription frauduleuse sur 30 mois. Dès le premier coup d'œil, deux caractéristiques majeures se dégagent :

1. Les inscriptions frauduleuses constituent un véritable fléau pour les services d'inscription client.
2. Le volume des inscriptions frauduleuses (et, par conséquent, leur « contribution » au nombre total de tentatives d'inscription) varie considérablement d'un jour à l'autre.

Deux tendances importantes sont légèrement moins évidentes.

Tout d'abord, la proportion journalière maximale d'inscriptions frauduleuses a diminué au cours de cette même période :

- En 2021, les tentatives d'inscription frauduleuse représentaient fréquemment (93 fois) la majorité du nombre total de tentatives d'inscription d'un jour donné, et à 19 reprises, les tentatives d'inscription frauduleuse ont représenté plus de 70 % des tentatives d'inscription du jour.
- En 2022, les tentatives d'inscription frauduleuse n'ont représenté plus de 60 % des tentatives d'inscription qu'à 5 occasions.
- Au cours du premier semestre 2023, les tentatives d'inscription frauduleuse n'ont dépassé 50 % que lors d'une seule journée (le 15 avril).

Ensuite, la proportion du nombre total de tentatives d'inscription attribuées à des inscriptions frauduleuses a diminué de manière significative au cours de cette période de 30 mois :

- En 2021, 31,8 % des tentatives d'inscription avaient été identifiées comme frauduleuses.
- En 2002, cette proportion était tombée à 18,6 %.
- Au premier semestre 2023, elle a chuté à 13,9 %.

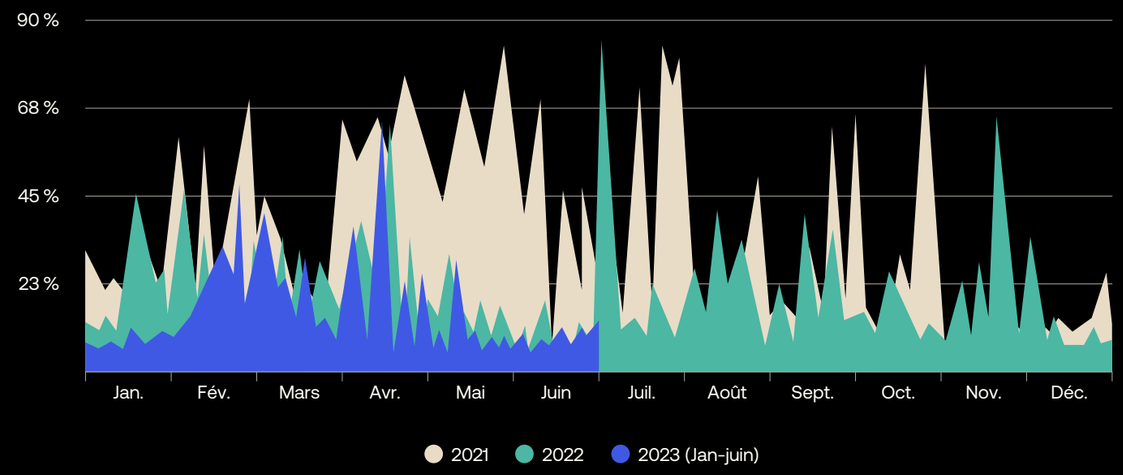
Nous pensons que la raison principale de ces tendances positives réside dans l'amélioration continue des défenses multiniveau de la technologie, plutôt qu'une réduction majeure du nombre de tentatives de création de comptes frauduleux par les cybercriminels (nous reviendrons sous peu sur cette hypothèse).

Il est également important de reconnaître que seules les inscriptions les plus manifestement suspectes atteignent les seuils requis pour être considérées comme frauduleuses. Par ailleurs, une fois qu'une entité a été identifiée comme l'auteur d'une tentative de fraude à l'inscription, de nombreux tenants implémentent des contrôles qui empêchent les tentatives d'inscription malveillantes. Dans ce cas, ces tentatives n'ont même pas l'occasion d'être comptabilisées ou enregistrées en tant qu'événements d'inscription frauduleuse.

En outre (au risque de nous répéter, mais le point est vraiment important), pour pouvoir accéder à l'écran de connexion, les cybercriminels doivent avoir franchi un certain nombre de défenses au niveau des couches hébergement, plateforme et application.

Pour ces raisons, les pourcentages mentionnés ci-dessus et indiqués dans les figures ci-dessous doivent être considérés comme le minimum absolu. En réalité, un service d'inscription dépourvu de couches successives de défenses efficaces risque fort d'être inondé, voire complètement submergé, par des enregistrements de comptes automatisés.

Figure 3. Les inscriptions frauduleuses sont une menace constante, mais constituent une part décroissante du nombre total de tentatives d'inscription dans Customer Identity Cloud grâce aux optimisations apportées à notre suite de produits.



Analyse par secteur

Une inspection plus approfondie des données sous-jacentes révèle que les tentatives d'inscription frauduleuse sont réparties de façon inégale.

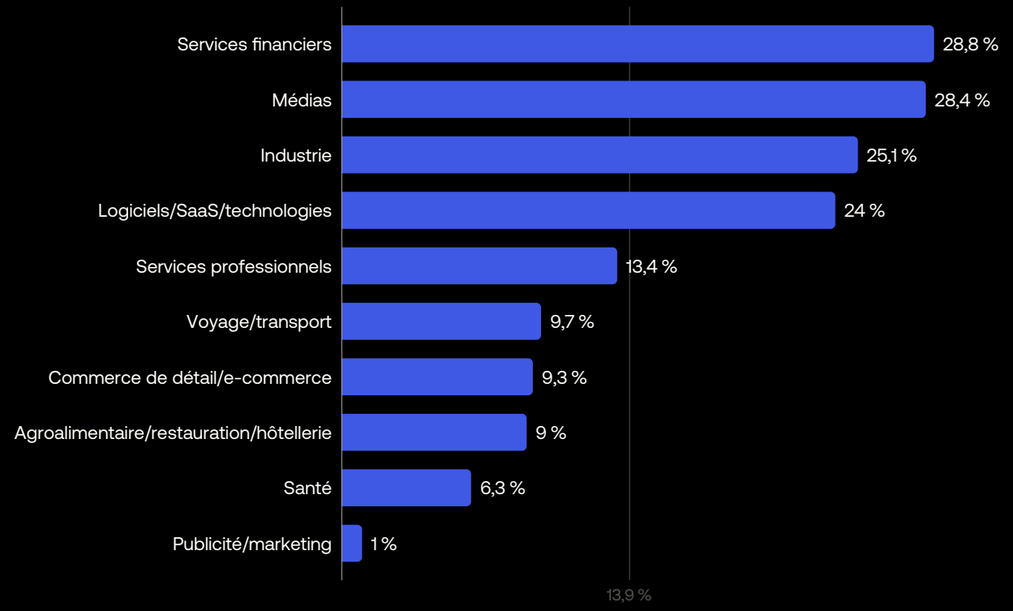
Parmi les 10 secteurs les plus représentés dans Customer Identity Cloud, les services financiers (28,8 %), les médias (28,4 %) l'industrie (25,1 %) et les solutions logicielles/SaaS/technologiques (24,0 %) ont tous été confrontés à des proportions de tentatives d'inscription frauduleuse supérieures à la moyenne (figure 4).

Pourquoi les comptes de ces secteurs sont-ils si prisés par les cybercriminels ? Il n'existe aucun moyen pratique de le savoir avec certitude, et les réponses peuvent être nombreuses et variées, mais voici quelques explications possibles :

- Les fournisseurs et établissements de services financiers offrent souvent des primes de bienvenue et d'autres avantages (p. ex. des points de voyage, des taux d'intérêt plus bas) lors de l'ouverture d'un nouveau compte, et tout ce qui a une valeur monétaire est attrayant pour les cybercriminels. Les comptes peuvent également être utilisés pour faciliter le blanchiment d'argent et comme première étape d'une fraude à l'identité synthétique.
- Les médias proposent souvent des forums de commentaires, si bien que le contrôle de comptes permet de diffuser de la désinformation, des messages de haine, de la propagande, des liens de spam et d'autres contenus malveillants auprès d'un large public.
- Les entreprises du secteur de l'industrie sont très ciblées par les cybercriminels, car toute interruption de la production les incite à répondre aux demandes de rançon. Il est donc possible qu'au moins certains comptes frauduleux soient créés dans le cadre de chaînes d'attaque plus longues. En outre, les fabricants qui pratiquent la vente directe aux consommateurs peuvent offrir un accès spécial à des séries limitées, incitant ainsi les revendeurs potentiels à créer une multitude de comptes.
- Un grand nombre de services logiciels/SaaS/technologiques appliquent un modèle freemium qui soumet un ou plusieurs facteurs à un plafond (p. ex. le nombre d'heures d'utilisation, le volume de stockage, les ressources de calcul disponibles, etc.). Certains comptes frauduleux constituent peut-être une tentative de contournement de ces restrictions.

Remarque : des informations contextuelles supplémentaires éclairant l'analyse par secteur sont disponibles dans l'annexe C.

Figure 4. Les secteurs des services financiers et des médias sont confrontés à une proportion de tentatives d'inscription frauduleuse supérieure à la moyenne.



Curieusement, les grandes et les petites entreprises semblent être confrontées à une proportion significativement plus élevée de tentatives d'inscription frauduleuse que leurs homologues de taille moyenne (figure 5).

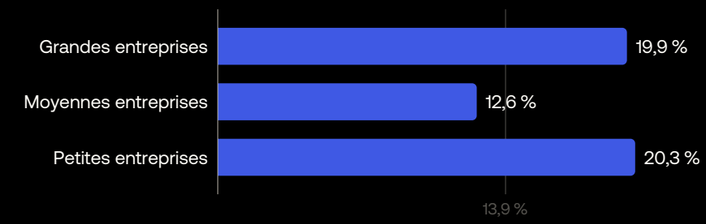
Les cybercriminels suivent les mêmes incitants économiques que les entreprises légitimes et cherchent à maximiser leurs profits. Les observations suggèrent donc que la valeur attendue de la fraude à l'inscription contre les grandes et les petites entreprises est supérieure à celle attendue des entreprises de taille moyenne.

Nous pouvons supposer que les cybercriminels peuvent raisonnablement s'attendre à ce que les grandes entreprises soient bien défendues (c'est-à-dire qu'ils ont relativement moins de chances de réussir), mais que le gain d'une attaque réussie est suffisamment élevé pour que le retour sur investissement justifie l'effort.

Les petites entreprises peuvent présenter la situation inverse : un gain plus faible par attaque, mais un taux de réussite suffisamment élevé pour que l'attaque vaille la peine.

Remarque : des informations contextuelles supplémentaires éclairant l'analyse par taille d'entreprise sont disponibles dans l'annexe D.

Figure 5. Les inscriptions frauduleuses semblent particulièrement fréquentes dans les grandes et les petites entreprises.

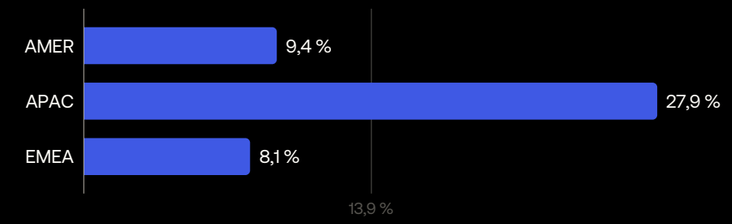


De même, de nouvelles différences apparaissent lorsque l'on agrège les données en fonction de la région où l'entreprise est basée (figure 6). Les entreprises basées sur le continent américain (AMER) (9,4 %) et dans la région EMEA (8,1 %) enregistrent des proportions comparativement beaucoup plus faibles de tentatives d'inscription frauduleuse, par rapport aux entreprises basées dans la région APAC (27,9 %).

Une telle disparité de départ entre la région Asie-Pacifique et les autres régions peut être le symptôme d'une approche moins mature de la protection des identités, qui se manifeste par l'implémentation d'un nombre réduit de produits et fonctionnalités de sécurité dans le vivier d'enregistrement de compte.

Remarque : des informations contextuelles supplémentaires éclairant l'analyse par région sont disponibles dans l'annexe E.

Figure 6. La proportion de tentatives d'inscription frauduleuse est beaucoup plus élevée dans les entreprises de la région APAC que dans celles du continent américain (AMER) ou de la région EMEA.



Mesures de défense

Outre les couches défensives en place avant l'accès à l'espace de connexion, il existe plusieurs autres approches pouvant être appliquées pour réduire les inscriptions frauduleuses :

- **Règles et actions préalables à l'inscription** (p. ex. demande d'authentification, demande d'informations supplémentaires) afin de réduire davantage les risques qu'un nouvel utilisateur s'avère illégitime
- **Authentification sociale** pour externaliser la prévention des inscriptions frauduleuses
- **Vérification des identités** lorsque le risque est perçu comme particulièrement élevé
- **Validation des informations de contact** (adresse e-mail, numéro de téléphone, etc.), par exemple au moyen d'un code d'accès à usage unique (OTP) ou d'un **magic link**

Il est essentiel que les renseignements obtenus à partir des inscriptions qui échouent, quelle que soit la raison, soient réintégrés dans l'évaluation de threat intelligence globale. Par exemple, une adresse IP qui tente d'enregistrer un nombre prédéterminé de comptes dans un laps de temps donné et échoue (p. ex. 10 tentatives en une heure), doit être considérée comme risquée. La désignation « risquée » conduira à filtrer les tentatives de connexion de cette adresse IP au niveau de la plateforme ou de l'application (c'est-à-dire avant l'espace de connexion).

Cependant, à l'exception de l'authentification sociale, chacune des approches mentionnées ci-dessus introduit des points de friction supplémentaires dans le processus d'inscription. Il faut donc veiller à trouver le bon équilibre.

En outre, les entreprises doivent être conscientes que les cybercriminels ont commencé à utiliser les méthodes de validation par SMS et par appel de façon abusive, comme expliqué ci-contre.

Pleins feux sur deux menaces : fraude aux SMS et fraude au numéro surtaxé

La disponibilité universelle des SMS en fait un canal attrayant pour les flux d'identité. Par exemple, un grand nombre de sites proposent des flux d'inscription qui intègrent ou autorisent uniquement l'inscription par SMS (p. ex. Toast, Uber), et le SMS est un mécanisme populaire pour l'inscription et les demandes MFA (p. ex. **OTP** et magic link).

Malheureusement, les cybercriminels exploitent les champs de formulaire pour inciter les fournisseurs d'applications à envoyer des SMS ou des appels téléphoniques à des numéros surtaxés, ce qui leur permet d'empocher une partie des recettes.

Dans les deux cas, c'est l'entreprise dont l'application est exploitée qui supporte les coûts, qui peuvent être importants. Ainsi, en février 2023, Elon Musk a affirmé que Twitter perdait 60 millions de dollars par an à cause de « SMS d'authentification à deux facteurs frauduleux ».

Comme pour les autres attaques examinées dans ce rapport, les cybercriminels ont découvert des tactiques permettant de réduire le risque de détection. Par exemple, ils peuvent :

- alterner les numéros de téléphone pour éviter de dépasser les limites fixées pour chaque numéro individuel ;
- procéder avec discrétion, en étendant l'attaque sur plusieurs jours, semaines ou mois (en fait, aussi longtemps que possible avant de se faire prendre).

Comme de nombreuses entreprises ont recours aux SMS pour l'inscription et l'authentification des utilisateurs, il n'est pas envisageable de désactiver purement et simplement ce canal. Néanmoins, l'infrastructure d'identités doit intégrer un moyen très intelligent de prévenir ou neutraliser la fraude téléphonique.

Authentification sociale

L'authentification sociale offre aux utilisateurs finaux une fonction d'**authentification unique (SSO)**. En utilisant les identifiants existants d'un fournisseur de réseau social tel que Facebook, Twitter ou Google, l'utilisateur peut facilement s'inscrire (puis se connecter) à un service tiers au lieu de créer un nouveau compte.

En plus d'offrir aux utilisateurs finaux une expérience pratique, l'authentification sociale peut contribuer à lutter contre la fraude à l'inscription, *à condition que le fournisseur de la connexion ait implémenté des mesures de sécurité robustes au niveau des inscriptions*.

Le problème, c'est que les services varient à cet égard, obligeant ainsi les fournisseurs d'applications à identifier eux-mêmes les tiers dignes de confiance.

L'authentification sociale offre également d'autres avantages potentiels aux fournisseurs d'applications, notamment :

- **Augmentation des inscriptions –** Un grand nombre d'utilisateurs préfèrent réutiliser un compte existant plutôt que d'en créer un nouveau.
- **Vérification de l'adresse e-mail –** Le fournisseur du réseau social est responsable de la vérification de l'adresse e-mail de l'utilisateur. Si le fournisseur partage cette information, vous obtiendrez des adresses e-mail valides plutôt que les adresses factices souvent utilisées pour s'inscrire dans les applications web. Le fournisseur de réseau social gère également le processus de récupération du mot de passe.
- **Possibilités de personnalisation accrues –** Les fournisseurs de réseaux sociaux peuvent vous communiquer des informations supplémentaires que les utilisateurs ont accepté de partager (localisation, centres d'intérêt, date d'anniversaire et autres), que vous pouvez utiliser pour améliorer vos services.
- **Expérience de retour en un clic –** Une fois que les utilisateurs se seront inscrits à votre application via l'authentification sociale, leur retour sera très simple, dans la mesure où ils seront probablement déjà connectés au réseau social et qu'un seul clic suffira pour se connecter à votre application.

Vérification des identités

L'une des idées fausses les plus répandues concernant le CIAM est que l'authentification et la vérification de l'identité sont équivalentes. Or, si l'authentification (p. ex. une connexion à l'aide d'un nom d'utilisateur et d'un mot de passe) démontre qu'un utilisateur possède les identifiants correspondant à un compte particulier, elle ne prouve pas que l'utilisateur est bien celui qu'il prétend être. C'est ici qu'entre en jeu la vérification des identités.

La vérification des identités met en œuvre des contrôles supplémentaires pour créer un degré de confiance élevé dans l'identité de vos candidats à l'inscription.

Dans le contexte du CIAM, il est essentiel que les solutions de vérification des identités soient évolutives en termes de charge, car le CIAM nécessite généralement des workflows en temps réel pour faire face aux pics associés aux variations saisonnières et aux programmes promotionnels. Heureusement, au cours des dernières années, un certain nombre de techniques automatisées de vérification des identités ont été développées pour répondre aux exigences réelles de l'inscription des clients :

- **L'authentification basée sur la connaissance (KBA)**, qui s'appuie sur ce qu'un utilisateur, et idéalement lui seul, connaît
- **La numérisation et validation croisée de documents**, qui utilise une pièce d'identité avec photo fiable (p. ex. un passeport ou un permis de conduire) pour vérifier que l'identité revendiquée par un utilisateur correspond à son identité réelle
- **La vérification de l'opérateur téléphonique**, qui tire parti du fait que l'identité de l'utilisateur a déjà été confirmée lorsqu'il s'est abonné à un service téléphonique

Partie 2 : à l'espace de connexion

La réutilisation des identifiants favorise l'usurpation de compte

Si les inscriptions frauduleuses représentent (au minimum) un désagrément coûteux, l'usurpation de compte constitue une menace plus importante pour la sécurité et la confidentialité.

Dans un contexte B2C, les cybercriminels peuvent avoir accès à des ressources (p. ex. des points de fidélité), à des privilèges (p. ex. la possibilité d'effectuer des achats, en particulier de produits dont la disponibilité est limitée) et à des informations démographiques et d'identification personnelle de grande valeur.

Dans un contexte B2B, un cybercriminel qui réussit à détourner un compte utilisateur peut l'utiliser pour accéder à des données très sensibles, provoquant ainsi une brèche assortie de lourdes sanctions réglementaires et contractuelles pour l'entreprise ciblée.

Bien que certaines tentatives d'usurpation de compte ciblent des personnes (nous examinerons certaines approches dans la 3e partie), la plupart sont des attaques par force brute (p. ex. T1110) ayant recours à une ou plusieurs des techniques suivantes :

- **Credential stuffing** (p. ex. T1110.004) – Un cybercriminel essaie des identifiants connus (c'est-à-dire provenant d'une brèche ou d'une extraction de mots de passe) sur d'autres sites et services.
- **Password spray** (p. ex. T1110.003) – Un cybercriminel essaie une liste relativement restreinte des mots de passe les plus courants sur de nombreux comptes différents.
- **Prédiction de mot de passe** (p. ex. T1110.001) – Une approche un peu plus grossière dans laquelle un cybercriminel essaie de nombreux mots de passe sur un certain nombre de comptes.

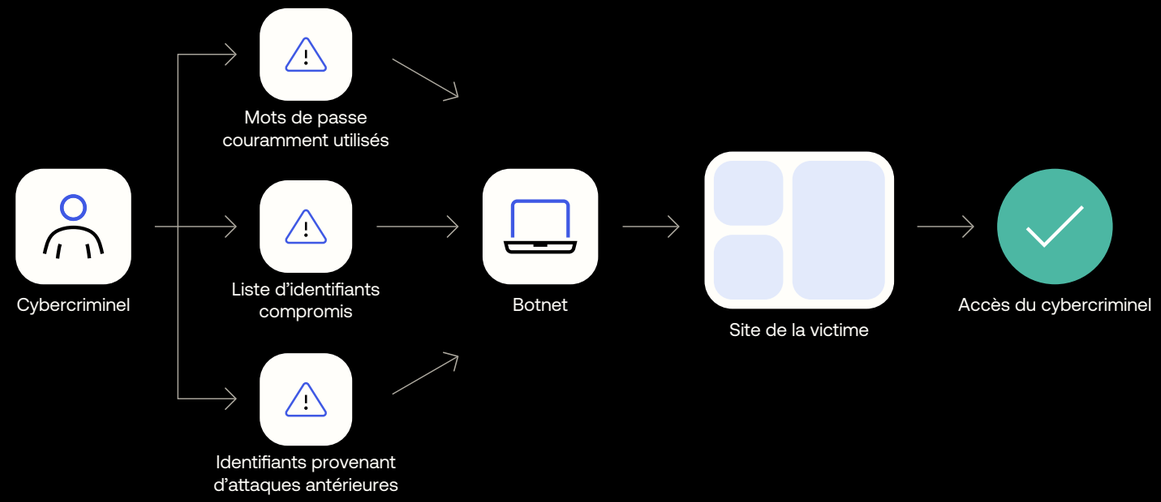
Il convient de noter que si elles sont exécutées à une échelle suffisante, chacune de ces attaques peut avoir pour effet, intentionnel ou non, de ralentir l'authentification pour les utilisateurs légitimes ou de rendre le service d'authentification complètement indisponible.

Ces trois approches reposent sur les mauvaises habitudes des utilisateurs en matière de mots de passe (mots de passe simples, réutilisation des mots de passe) – un problème courant qui facilite considérablement ces attaques et en réduit le coût. Par exemple, un petit nombre d'optimisations, notamment l'utilisation de listes de mots de passe compromis et de dictionnaires de mots fréquemment utilisés dans ces mots de passe, peuvent améliorer considérablement la probabilité de tomber sur le bon mot de passe (ou, plus précisément, d'essayer un mot de passe dont la valeur de hachage est identique à celle du mot de passe correct).

Parmi les trois attaques décrites ci-dessus, le credential stuffing est la plus efficace (du point de vue du cybercriminel) et la plus dangereuse (du point de vue du fournisseur d'application et de ses clients), parce que c'est la plus précise. En utilisant des paires nom d'utilisateur/mot de passe connues, un cybercriminel a moins de probabilités de déclencher les mécanismes de détection automatique.

Malheureusement, les obstacles au lancement de telles attaques sont très limités, et les cybercriminels emploient un certain nombre de tactiques pour tenter de contourner les défenses. Ainsi, certains d'entre eux intercalent dans le flux de connexion des identifiants valides connus, parfois associés aux comptes frauduleux qu'ils contrôlent, afin de limiter le taux d'échec.

Figure 7. Anatomie des attaques par credential stuffing



Pour les cybercriminels plus sophistiqués, les attaques par credential stuffing sont attrayantes, car leur coût marginal est quasiment nul. Prenons l'exemple d'une chaîne de frappe (kill chain) étendue à partir de la figure 7, où l'acteur malveillant utilise un service cybercriminel pour lancer une campagne de phishing afin d'obtenir des identifiants. L'attaquant sait que les identifiants extraits sont actifs au moment de leur collecte, ce qui lui permet de lancer une attaque par credential stuffing avec un taux de réussite présumé élevé. Dans ce scénario, il suffit de modifier quelques paramètres d'un script pour cibler des entreprises ou services différents.

Outre l'usurpation de compte, le credential stuffing est souvent utilisé pour l'étape intermédiaire de découverte/validation de comptes. Par exemple, un cybercriminel peut prendre une large base d'identifiants volés, la mettre à l'essai sur un service particulier, puis vendre à prix fort une liste d'identifiants validés.

Observations globales

La figure 8 montre une vue sur 30 mois des tentatives de credential stuffing relevées dans Customer Identity Cloud. Comme pour les tentatives d'inscription frauduleuse, une rapide analyse visuelle suggère que la proportion des tentatives de connexion imputables au credential stuffing a considérablement diminué au cours de cette période, et c'est effectivement le cas :

- En 2021, 42,8 % des tentatives de connexion ont été attribuées au credential stuffing. (Comme pour les tentatives d'inscription frauduleuse, les critères à remplir pour recevoir cette dénomination sont très stricts et les tentatives supplémentaires ne sont pas consignées.)
- En 2022, la proportion était de 33,4 %.
- Au premier semestre 2023, elle a chuté pour tomber à 24,3 %.

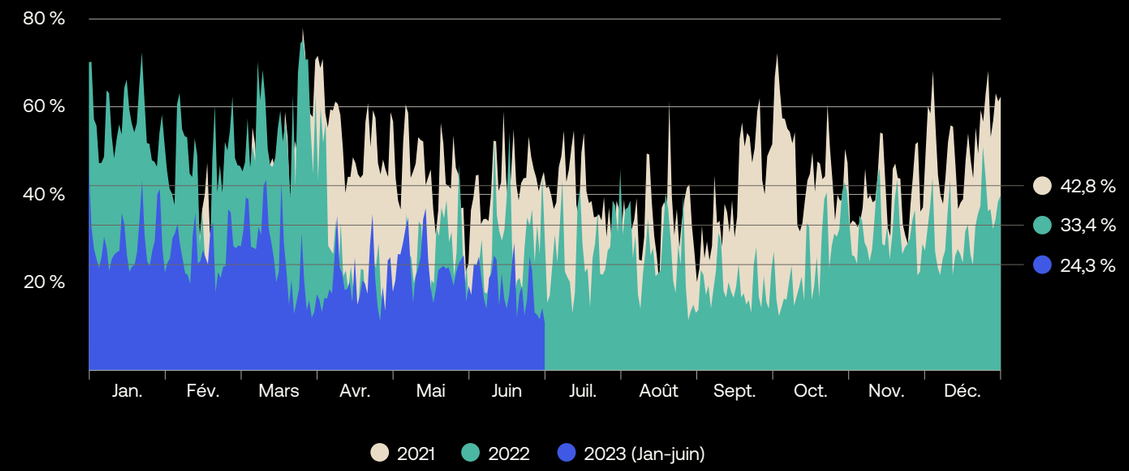
Une inspection plus approfondie révèle qu'un important changement s'est produit en avril 2022 :

- Entre le 1er janvier 2021 et le 31 mars 2022, le credential stuffing représentait 47,3 % des tentatives de connexion.
- Entre le 1er mai 2022 et le 30 juin 2023, seulement 24,6 % des tentatives de connexion remplissaient les critères du credential stuffing.

Que s'est-il donc passé en avril 2022 ? En résumé, au cours des deux premières semaines du mois, l'ordre dans lequel les couches de défense de Customer Identity Cloud filtraient le trafic des attaques a été modifié, avec l'application de Bot Detection plus tôt.

Nous pensons que ce seul changement est responsable de la réduction spectaculaire et durable du credential stuffing et d'autres attaques par force brute contre l'espace de connexion, mais aussi de la plupart des améliorations constatées dans l'analyse de la figure 3 (relative aux tentatives d'inscription frauduleuse). Cette observation souligne l'importance de disposer de plusieurs couches de défense et d'optimiser l'organisation de ces couches.

Figure 8. La proportion des tentatives d'inscription attribuées au credential stuffing a diminué de manière significative en 2023. Les améliorations apportées à la fonctionnalité Bot Detection de Customer Identity Cloud pourraient être à l'origine de ce déclin.



Analyse par secteur

La segmentation des observations par secteur d'activité (figure 9) souligne à quel point le credential stuffing est particulièrement problématique pour certains secteurs.

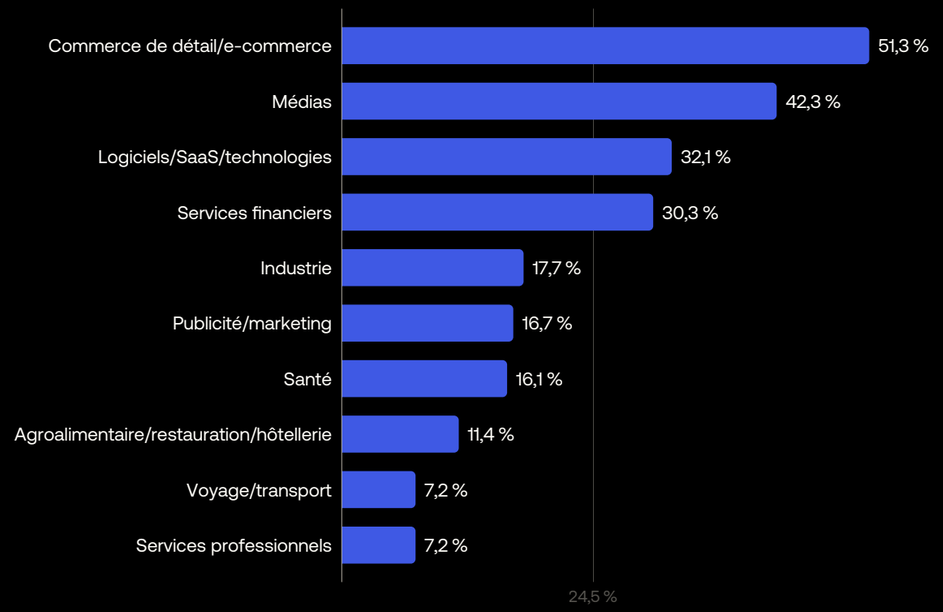
Dans le secteur du commerce de détail/e-commerce, plus de la moitié (51,3 %) des tentatives de connexion sont imputables au credential stuffing. Il est évident que les cybercriminels sont attirés par de tels comptes, que ce soit pour voler des points de fidélité, obtenir un accès inéquitable à des ressources limitées, effectuer des achats avec l'argent de quelqu'un d'autre, mettre la main sur des informations de paiement ou toute autre raison.

Le secteur des médias subit également une proportion très importante des tentatives de credential stuffing (42,3 %), probablement pour les raisons citées précédemment.

Le secteur des logiciels/SaaS/technologies enregistre la troisième proportion la plus élevée (32,1 %). Dans ce cas, il est possible que les acteurs malveillants cherchent à exploiter les comptes afin d'accéder à des informations sensibles et de les exfiltrer, que ce soit pour les utiliser directement ou dans le cadre d'une attaque de plus grande envergure. Par exemple, une tentative de phishing semblera plus convaincante si elle fait référence à des informations de projet uniquement accessibles à un service de confiance.

Enfin, le secteur des services financiers enregistre également une proportion d'attaques de credential stuffing plus élevée que la moyenne. Ici, un acteur malveillant pourrait avoir de nombreuses motivations, notamment voler des données personnelles pour les vendre ou les utiliser dans le cadre de fraudes à l'identité synthétique, ou commettre des fraudes financières (p. ex. initier des transactions et des transferts).

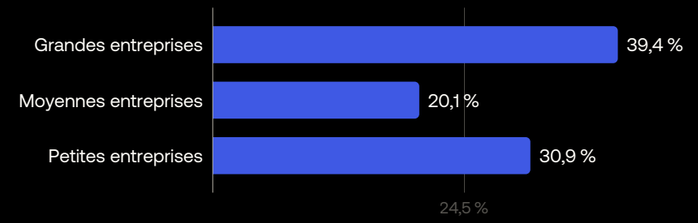
Figure 9. Les entreprises de commerce de détail/e-commerce doivent faire face à une proportion extrêmement élevée de tentatives de credential stuffing, soit près du double de la moyenne tous secteurs confondus.



Comme pour les tentatives d'inscription frauduleuse, nous constatons que les petites et les grandes entreprises sont la cible d'un nombre de tentatives de credential stuffing proportionnellement plus élevé que les moyennes entreprises (figure 10).

Cette observation corrobore la théorie suggérée précédemment, selon laquelle les grandes et les petites entreprises fournissent le retour sur investissement le plus élevé aux cybercriminels, contrairement aux moyennes entreprises.

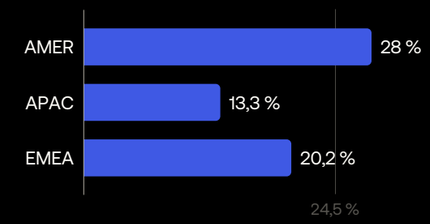
Figure 10. Les petites et grandes entreprises semblent être des cibles plus attrayantes que les moyennes, sans doute parce que les cybercriminels estiment que le retour sur investissement est plus favorable.



Comme le montre la figure 11, les entreprises dont le siège social est établi sur le continent américain (AMER) subissent une proportion plus élevée de tentatives de credential stuffing (28 %) par rapport aux entreprises basées dans la région APAC (13,3 %) ou EMEA (20,2 %).

Un nombre disproportionné d'entreprises mondiales des secteurs du commerce de détail/e-commerce, des médias, des logiciels/SaaS/technologies et des services financiers sont basées sur le continent américain. Il est possible que cette concentration explique en partie la proportion plus élevée de tentatives de credential stuffing observée dans l'ensemble de données, en raison de la taille des entreprises et de leur notoriété aux yeux des cybercriminels.

Figure 11. La proportion de tentatives de credential stuffing est plus élevée dans les entreprises du continent américain (AMER) que dans celles des régions APAC et EMEA.



Les mots de passe sont source de problèmes

Lorsqu'un titulaire de compte réutilise les mêmes mots de passe (ou des mots de passe similaires) sur plusieurs sites, cela crée un effet boule de neige, où une seule paire d'identifiants peut être utilisée pour compromettre plusieurs applications.

Soyons réalistes, il n'y a pas de raison de croire que les utilisateurs vont collectivement et spontanément modifier leurs habitudes en matière de mots de passe. Ainsi, le rapport Customer Identity Trends Report 2023 d'Okta a révélé ce qui suit :

- 33 % des répondants indiquent ressentir de la frustration lorsqu'ils doivent créer un mot de passe respectant un certain nombre de critères.
- 25 % éprouvent de la frustration lorsqu'ils doivent créer un mot de passe pour chaque service en ligne.

Pour ne rien arranger, les comptes actifs ne représentent généralement qu'une petite partie du nombre total de comptes d'un utilisateur. De nombreux autres sont oubliés ou non gérés. La moindre compromission de l'un de ces services négligés peut fournir à un cybercriminel un énorme volume d'identifiants utilisateurs et les données personnelles associées.

Par ailleurs, les cybercriminels sont passés maîtres dans l'art d'utiliser ces informations à grande échelle pour compromettre des comptes que les clients détiennent auprès d'autres marques. Par exemple, le rapport Data Breach Investigations Report (DBIR) 2023 de Verizon a révélé que 86 % des brèches constatées au niveau des applications web ont recours à l'utilisation d'identifiants volés. Qui plus est, les identifiants et les informations personnelles (qui peuvent être vendus, mais également exploités dans des flux de récupération de mot de passe) sont les données les plus couramment exfiltrées, ce qui alimente constamment le cycle d'attaques.

L'avenir doit être, et sera, différent.

Du point de vue des utilisateurs, l'expérience de connexion traditionnelle deviendra une rare exception, et les mots de passe seront une méthode d'authentification de dernier recours. À mesure que la dépendance aux mots de passe s'estompera, disparaîtra également toute une catégorie d'attaques ciblant l'identité.

Pour en savoir plus sur cet avenir prometteur, et découvrir ce que vous pouvez mettre en place dès aujourd'hui, consultez l'eBook Authentication after passwords: Maximizing conversions (and enhancing security) in the age of convenience.

Mesures de défense

Une fois encore, en plus des mesures de défense déjà appliquées, un certain nombre de techniques supplémentaires peuvent contribuer à prévenir l'usurpation de compte (ATO).

Il existe deux approches simples :

- **Déplacement impossible –** Cette approche consiste à détecter les tentatives de connexion d'un « utilisateur » à partir d'un emplacement géographique impossible à rejoindre dans le délai écoulé depuis la dernière connexion réussie.
- **Authentification sociale –** En plus de simplifier les inscriptions, l'authentification sociale renforce la sécurité, car un utilisateur est plus susceptible de déployer des efforts pour protéger ses comptes de réseaux sociaux.

Des techniques plus avancées incluent la détection des mots de passe compromis, l'implémentation de politiques efficaces de gestion des mots de passe (notamment de réinitialisation) et – pour une authentification la plus sécurisée possible – l'application d'un MFA fort.

La défense la plus « simple » et la plus efficace contre l'usurpation de compte (ATO) basée sur les mots de passe consiste sans doute à abandonner les mots de passe, une perspective qui a gagné en réalisme lorsqu'Apple, Google et Microsoft se sont engagés à prendre en charge une norme courante de connexion sans mot de passe.

Passkeys

Les passkeys sont des authentifiants FIDO détectables par les navigateurs ou incorporés au sein d'applications natives ou des clés de sécurité pour une authentification sans mot de passe. Basées sur les normes de l'Alliance FIDO et du World Wide Web Consortium (W3C), les passkeys remplacent les mots de passe par des paires de clés cryptographiques et peuvent être utilisées de façon similaire aux méthodes de déverrouillage des terminaux mobiles – généralement par biométrie ou par saisie d'un code d'accès.

Les passkeys se présentent sous deux formes : les passkeys liées au terminal et les **passkeys synchronisées**.

Chaque passkey liée au terminal est associée à un équipement unique, qui sert de facteur de possession. Les passkeys liées au terminal peuvent être utilisées sur des authentificateurs et clés de sécurité certifiés FIDO, y compris ceux ayant obtenu une certification de sécurité.

Les passkeys liées au terminal sont disponibles depuis quelques années, mais certains des aspects qui contribuent à une authentification forte (c'est-à-dire associée à un seul terminal) limitent leur adoption par le plus grand nombre.

Les passkeys synchronisées, quant à elles, sont synchronisées entre les différents terminaux d'un utilisateur via un service cloud, tel qu'un écosystème de système d'exploitation ou un gestionnaire de mots de passe. Cela crée une expérience utilisateur très familière pour les utilisateurs, condition nécessaire pour une adoption généralisée, en particulier auprès du grand public.

Lorsqu'un utilisateur souhaite se connecter, le site ou le service lui demande s'il veut utiliser sa passkey. Pour ce faire, il suffit à l'utilisateur de s'authentifier sur son terminal, par exemple via la biométrie, un code PIN ou un schéma à dessiner.

Du point de vue du site ou du service, la passkey valide un facteur de possession (c'est-à-dire un terminal autorisé à utiliser la passkey synchronisée) et soit un facteur d'inhérence (en cas d'utilisation de la biométrie), soit un facteur de connaissance (en cas d'utilisation du code d'accès du terminal). Par conséquent, les passkeys synchronisées augmentent considérablement la sécurité des comptes pour la majorité des utilisateurs, ce qui contribue à réduire l'usurpation de compte (ATO) basée sur les mots de passe.

Introduction aux passkeys

L'adoption massive des passkeys par les utilisateurs représenterait un grand pas en avant dans la lutte contre le phishing, l'usurpation de compte et autres menaces ciblant l'identité.

Pour en savoir plus, consultez le livre blanc Introduction aux passkeys – Comment l'authentification FIDO résistante au phishing améliore les expériences utilisateurs et prévient le piratage de comptes.

Détection des mots de passe compromis

Un aspect déplorable, mais bien réel, du paysage actuel des menaces est qu'il existe des marketplaces entières à l'intention des cybercriminels. Par exemple, les cybercriminels peuvent facilement acheter d'énormes listes d'identifiants compromis.

Les risques associés aux identifiants compromis peuvent être gérés dans une certaine mesure en utilisant ces mêmes listes d'identifiants de façon défensive, pour détecter l'utilisation de mots de passe révélés par une compromission. En cas de détection, un fournisseur d'application peut avertir l'utilisateur et suggérer, voire exiger une mesure d'atténuation des risques (p. ex. modifier le mot de passe ou appliquer un facteur MFA fort).

Heureusement, les gestionnaires de mots de passe dédiés et les fonctionnalités intégrées aux navigateurs et aux systèmes d'exploitation facilitent la création, le stockage sécurisé et l'utilisation de mots de passe plus longs et plus complexes par les utilisateurs, ce qui élimine certaines raisons fondamentales pour lesquelles ils choisissent et réutilisent des mots de passe faibles. En outre, ces mêmes solutions avertissent souvent les utilisateurs en cas de divulgation de leurs identifiants lors de brèches, ce qui accroît la connaissance des risques.

Espérons que le recours aux mots de passe compromis et la menace qu'ils présentent diminueront suite à ces efforts.

Combler les lacunes avec Credential Guard

Il est important de reconnaître qu'il existe souvent un long délai entre le moment où des identifiants compromis deviennent disponibles sur des marketplaces cybercriminelles et le moment où ils apparaissent dans des flux de threat intelligence, ce qui laisse suffisamment de temps aux acteurs malveillants pour les exploiter.

Credential Guard comble ces lacunes grâce à une équipe d'experts qui infiltre les communautés cybercriminelles pour avoir accès à des données exposées dès qu'une brèche se produit. Vous pouvez ainsi mieux protéger vos utilisateurs et sécuriser vos applications en réinitialisant plus tôt les mots de passe compromis.

Pour en savoir plus, consultez l'article de blog Detect Breached Passwords Faster with Auth0 Credential Guard.

Politiques de mots de passe efficaces

Outre l'implémentation de la détection des mots de passe compromis, certains moyens simples mais efficaces permettent de renforcer la sécurité des identités :

- Exiger des utilisateurs qu'ils créent des mots de passe forts
- Empêcher les utilisateurs de revenir à un mot de passe déjà utilisé dans cette application (c'est-à-dire prévenir la rotation des mots de passe)
- Implémenter un processus fort de réinitialisation des mots de passe

La réinitialisation des mots de passe est une nécessité pour toutes les applications, mais si votre processus complique la vie de vos clients, vous leur donnez une raison d'arrêter d'utiliser votre service.

Pour vous fournir un peu de contexte, voici ce que le rapport Customer Identity Trends Report 2023 d'Okta a mis en lumière :

- 63 % des répondants ont confié qu'au moins une fois par mois, ils sont dans l'incapacité de se connecter à un compte car ils ont oublié leur nom d'utilisateur ou mot de passe.
- 24 % rencontrent ce problème au moins une fois par semaine.
- 6 % le rencontrent au moins une fois par jour.

Si la réinitialisation d'un mot de passe est généralement possible, les clients, en particulier dans les environnements B2C, peuvent décider que le processus n'en vaut pas la peine. Vous perdrez alors des conversions et des utilisateurs. Seulement 52 % des répondants ont déclaré avoir toujours accès à l'ensemble de leurs comptes.

Des processus efficaces de réinitialisation des mots de passe remplissent deux fonctions :

1. **Ils limitent les frictions pour le client –** Votre client ne devrait pas mettre plus d'une minute à réinitialiser son mot de passe, et le processus ne doit demander que des informations que les clients se sentent à l'aise de saisir, par exemple des adresses e-mail.
2. **Ils garantissent la protection des informations du client –** Par exemple, en offrant des protections contre des situations comme l'échec répété de plusieurs tentatives de connexion et en envoyant des informations uniquement via des canaux sécurisés.

L'e-mail est le plus souvent utilisé pour la réinitialisation des mots de passe, car il satisfait deux de ces critères : il limite les points de friction, car la saisie d'une adresse e-mail est simple et rapide pour un client, et il protège ses informations (en partant du principe que seul le client a accès à sa boîte de réception).

Une seule erreur dans la réinitialisation des mots de passe peut gâcher toute l'expérience de votre client avec votre produit. Ces erreurs prennent souvent la forme des éléments suivants :

- **Questions de sécurité –** Les informations statiques (votre ancienne école, le nom de jeune fille de votre mère, et même le nom de votre animal de compagnie) sont facilement accessibles via OSINT.
- **Mots de passe en texte clair –** Plutôt que de réinitialiser le mot de passe, certains sites renvoient le mot de passe d'origine au client, ce qui constitue une vulnérabilité majeure. Pour qu'un mot de passe puisse être envoyé en texte clair, il doit être stocké en texte clair, ce qui accroît les risques d'attaque.
- **Messages d'erreur –** Lorsqu'une application indique si une adresse e-mail est enregistrée ou non, un acteur malveillant pourrait déterminer si un client possède un compte, ce qui lui fournit une information supplémentaire à utiliser contre votre client.
- **Demande d'informations inutiles –** Un équilibre doit être trouvé entre sécurité et simplicité d'utilisation. Demander aux clients une pièce d'identité avec photo est une pratique sûre, mais son effet global sur l'expérience client est négatif.

Authentification multifacteur (MFA) forte

Protéger des comptes grâce à l'application du MFA permet de réduire considérablement le temps, les efforts et le coût de correction des usurpations de compte.

Toutefois, en pratique, l'efficacité du MFA en tant que mesure de défense contre cette menace est limitée par deux facteurs :

1. Les faibles taux d'adoption par les fournisseurs d'application et faibles taux d'utilisation par les clients
2. L'utilisation de facteurs secondaires qui peuvent être contournés par les cybercriminels

Bien qu'une analyse approfondie de l'adoption, de l'inscription et de l'utilisation du MFA dépasse la portée de ce rapport, nous pouvons utiliser les données disponibles pour éclairer quelque peu le sujet.

Par exemple, dans l'ensemble complet de données, le ratio entre les événements d'authentification avec mot de passe et les tentatives MFA valides avoisine 41 ; en d'autres mots, pour chaque tentative MFA valide, on compte environ 41 authentifications avec mot de passe.

Nous pouvons utiliser ce même ratio pour déterminer et comparer les taux relatifs d'utilisation du MFA par secteur d'activité (figure 12).

Cela révèle que seuls trois des 10 secteurs les plus représentés semblent présenter une utilisation du MFA plus élevée que la moyenne, c'est-à-dire un ratio plus faible entre les authentifications avec mot de passe et les tentatives MFA valides.

Dans le secteur des services financiers, nous observons 12 authentifications avec mot de passe pour chaque événement MFA valide. Le ratio du secteur industriel (24) est deux fois plus élevé que celui des services financiers, mais reste considérablement plus faible que celui des services professionnels (37).

Nous pouvons également constater que trois des secteurs les plus représentés – agroalimentaire/restauration/hôtellerie (137), médias (155) et publicité/marketing (400) – présentent des ratios extrêmement élevés, ce qui indique un manque relatif d'utilisation du MFA.

Pour satisfaire notre curiosité, nous nous sommes également intéressés aux autres secteurs en dehors des 10 les plus représentés, et en avons découvert cinq autres dont les ratios sont plus faibles que la moyenne (figure 13). Trois secteurs – les services juridiques (4), les télécommunications (6) et le secteur public (6) – font figure d'exception. Étant donné que les trois travaillent avec des données sensibles ou des infrastructures importantes, il est réjouissant d'observer une utilisation plus intensive du MFA.

Bien que le ratio examiné ci-dessus ne soit qu'une variable proxy, il suggère fortement que certains secteurs d'activité s'appuient plus que d'autres sur le MFA. En effet, ceux qui travaillent avec des données ou des systèmes sensibles semblent y avoir davantage recours.

Toutefois, face au renforcement général des défenses d'identité et à la lente progression du MFA, les acteurs malveillants se concentrent sur le contournement de ces défenses (figure 14).

Figure 12. Les secteurs fortement réglementés présentent généralement des taux d'adoption du MFA plus élevés, avec les services financiers et la santé proches ou inférieurs à la moyenne (parmi les 10 secteurs les plus représentés dans notre ensemble de données).

Rapport entre le nombre total d'authentifications par mot de passe et le nombre de tentatives MFA valides (10 secteurs d'activité les plus représentés, 2023)

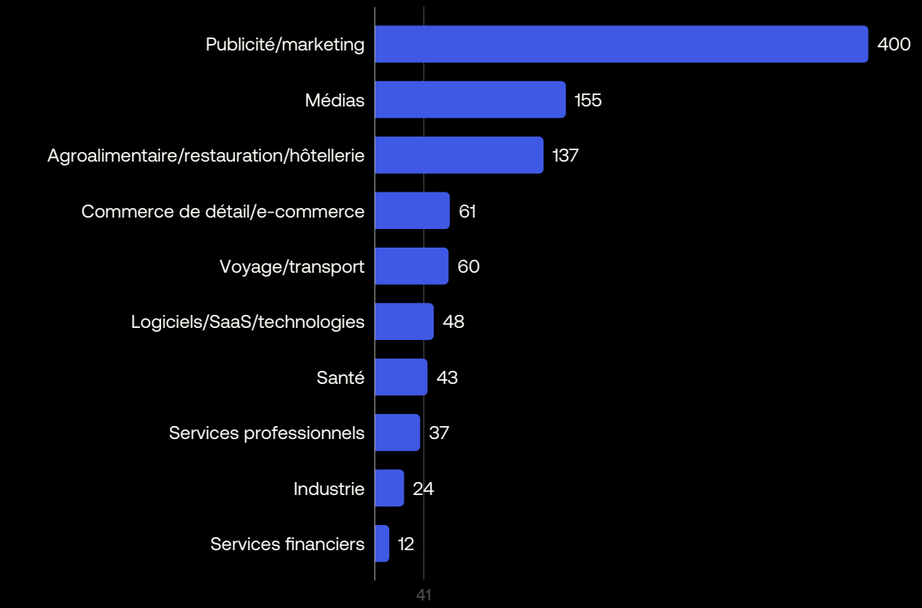


Figure 13. En dehors des 10 secteurs les plus représentés, 5 autres secteurs présentent des rapports supérieurs à la moyenne entre les tentatives MFA valides et le nombre total d'authentifications par mot de passe.

Rapport entre le nombre total d'authentifications par mot de passe et le nombre de tentatives MFA valides (autres secteurs d'activité notables, 2023)

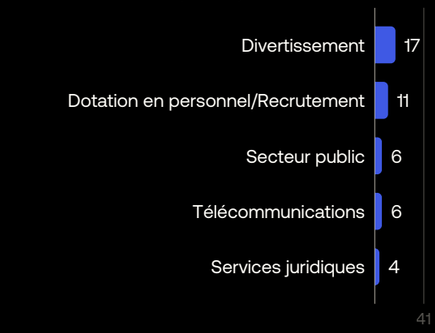
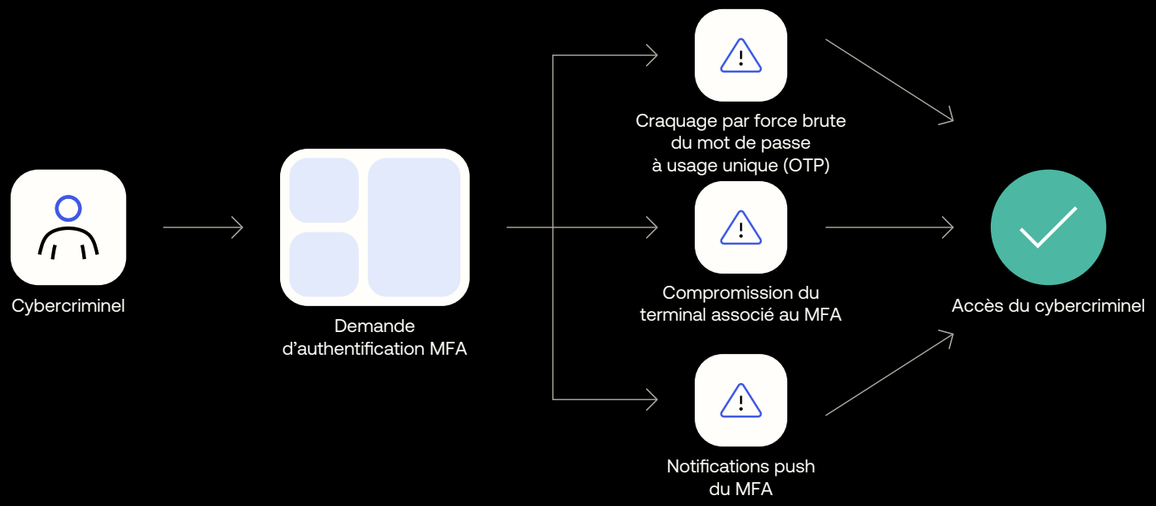


Figure 14. Anatomie des techniques courantes de contournement du MFA



Par exemple, plusieurs outils sont désormais disponibles pour faciliter les attaques contre certains des facteurs secondaires relativement plus faibles, en particulier les mots de passe à usage unique envoyés par SMS. Le vecteur d'attaque le plus courant consiste à appliquer une force brute pour engendrer une **fatigue MFA** en vue de piéger l'utilisateur ou de le contraindre à répondre à la demande MFA même s'il ne l'a pas initiée. En répondant à cette demande, l'utilisateur autoriserait involontairement l'acteur malveillant à se connecter.

Par ailleurs, les cybercriminels ont recours à l'**échange de carte SIM** et/ou au **social engineering** pour contourner les défenses MFA.

Dans une attaque par échange de carte SIM, le cybercriminel convainc l'opérateur mobile de l'utilisateur cible de transférer le numéro mobile de l'utilisateur vers une carte SIM en possession de l'acteur malveillant. Les cybercriminels peuvent avoir recours au social engineering (p. ex. piéger un agent du service d'assistance), faire appel à un utilisateur interne malveillant ou commettre une compromission (c'est-à-dire accéder aux services administratifs de l'opérateur) pour échanger la carte SIM.

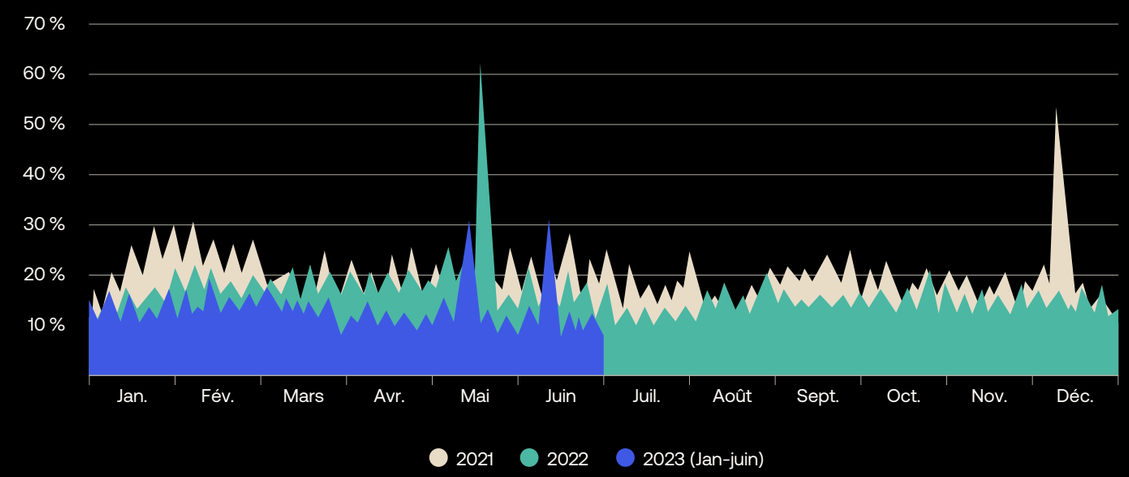
Une fois la carte SIM échangée, tout facteur MFA reposant sur le numéro de téléphone (mot de passe à usage unique envoyé par SMS, magic link envoyé par SMS, mot de passe à usage unique transmis via un appel vocal, etc.) peut désormais être fourni par l'acteur malveillant.

Les cybercriminels peuvent également employer des tactiques de social engineering directement contre le fournisseur d'application. Par exemple, un acteur malveillant disposant de quelques informations personnelles (souvent disponibles à l'achat ou acquises via OSINT) pourrait essayer de convaincre un agent du service d'assistance de modifier les détails du compte. Le cybercriminel peut même contacter directement les utilisateurs afin de les inciter à désactiver certaines protections du compte.

Malheureusement, le coût de l'exécution de campagnes de social engineering continue à chuter. Cette diminution s'explique par une plus grande efficacité (IA, automatisation, etc.), par les brèches majeures et les sites de dépôt de données bien fournis, et par la propension de nombreux utilisateurs à divulguer des informations en ligne (p. ex. sur les réseaux sociaux).

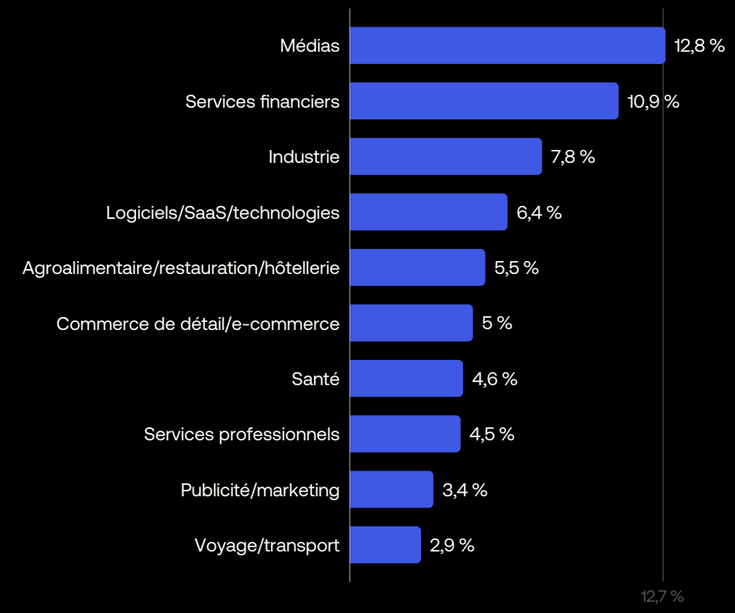
Pour toutes ces raisons, le contournement du MFA est un risque bien réel pour les entreprises et leurs clients. Ainsi, au cours des six premiers mois de l'année 2023 (figure 15), 12,7 % des tentatives MFA remplissaient les critères de contournement du MFA. Si cette proportion est en baisse par rapport à 2022 (15,5 %) et à 2021 (18,1 %), cette diminution est probablement imputable à un changement de tactiques plutôt qu'à un recul de la menace elle-même.

Figure 15. Le contournement du MFA chute comparé à 2021 et 2022, mais reste une technique appréciée des cybercriminels dès lors que le coût d'exécution du social engineering continue à baisser.



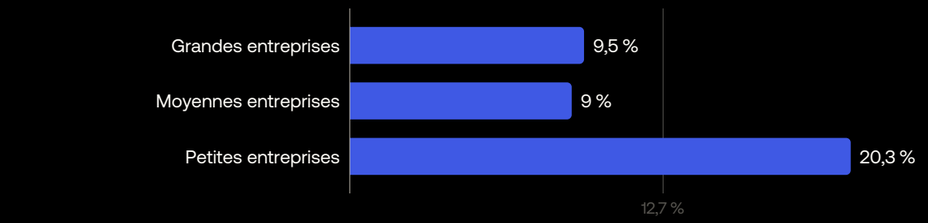
Il est intéressant de noter qu'un seul des 10 secteurs les plus représentés a enregistré une proportion plus élevée que la moyenne de tentatives de contournement du MFA (figure 16) : le secteur des médias, avec 12,8 % (juste au-dessus de la moyenne). La moyenne globale est dopée par le secteur public (29,9 %) et le secteur du divertissement (28,6 %), ainsi que par les clients auxquels nous n'avons attribué aucun secteur d'activité spécifique.

Figure 16. La bonne nouvelle ? Certains secteurs connaissent toujours des proportions moyennes ou inférieures à la moyenne de tentatives de contournement du MFA. Le secteur Voyage/Transport est en tête (parmi les 10 secteurs les plus représentés dans notre ensemble de données).



La menace semble particulièrement présente dans les petites entreprises (figure 17), où plus d'un cinquième (20,3 %) des tentatives de MFA remplissent les critères requis pour être considérées comme des tentatives de contournement du MFA.

Figure 17. Les petites entreprises semblent subir une proportion de tentatives de contournement du MFA plus élevée que les entreprises moyennes ou grandes.



Compte tenu de l'évolution rapide et dangereuse du paysage des menaces, lors de l'implémentation du MFA, il est essentiel que la solution :

- **Soit implémentée correctement –** Sans cela, les lacunes et les solutions de contournement (visant par exemple à prendre en charge l'authentification héritée ou permettant aux administrateurs de contourner le MFA) seront exploitées.
- **Utilise des facteurs secondaires forts –** Les techniques de contournement du MFA ciblent généralement des facteurs plus anciens (p. ex. ceux privilégiant les SMS), et les attaques par force brute continuent à se concentrer sur des authentificateurs basés sur la connaissance. L'utilisation d'authentificateurs basés sur la possession ou de facteurs biométriques peut donc considérablement réduire le risque d'aboutissement d'une attaque par force brute.

Comme précédemment mentionné, les technologies efficaces dans les applications grand public doivent établir un équilibre entre sécurité et facilité d'utilisation, alors que les méthodes d'authentification plus anciennes nécessitaient souvent de choisir entre ces deux caractéristiques.

Cependant, ce compromis se transforme progressivement en faux choix :

- Le **MFA adaptatif** est une politique MFA flexible et extensible qui permet de prévenir l'usurpation de compte (ATO) sans augmenter les frictions pour les vrais utilisateurs. Pour ce faire, il évalue le risque potentiel pendant chaque transaction de connexion, puis invite l'utilisateur à procéder à une vérification supplémentaire uniquement si nécessaire.
- **Les nouvelles méthodes MFA sont sûres et pratiques –** Les méthodes MFA basées sur la biométrie intégrée aux terminaux via **WebAuthn** (p. ex. Apple Face ID, Apple Touch ID ou Windows Hello) ou les clés de sécurité WebAuthn (p. ex. YubiKey, Feitian ou Titan) offrent à la fois une sécurité renforcée (les cybercriminels détestent WebAuthn) et une facilité d'utilisation optimale, ce qui rapproche l'authentification de la solution idéale présentée dans l'introduction de ce rapport.

S'il reste peu probable que les particuliers adoptent des clés de sécurité dédiées, les fonctionnalités biométriques deviennent de plus en plus courantes sur les terminaux abordables. Permettre aux utilisateurs de s'authentifier à l'aide de la biométrie de leur terminal présente deux avantages :

- Cette approche réduit considérablement les points de friction pendant la demande d'authentification, ce qui augmente la rétention des utilisateurs et les revenus.
- Elle renforce la sécurité, étant donné que le flux ne peut pas être ciblé par le phishing d'acteurs malveillants. ■

Partie 3 : après l’espace de connexion

La protection des identités clients – ainsi que les droits et privilèges en rapport avec celle-ci – ne s’arrête pas à l’étape d’authentification. Elle doit, au contraire, être maintenue pendant toute la session de l’utilisateur.

Partie 3 : après l'espace de connexion

Les cybercriminels convoitent encore plus les tokens de session dans un monde sans mot de passe

Après l'authentification d'un utilisateur dans une application, le navigateur stocke un cookie web. Ce dernier contient un token de session, à savoir un bloc de données généré par l'application, qui assure le suivi d'un utilisateur connecté et lui évite d'avoir à se reconnecter jusqu'à l'expiration de la session ou sa déconnexion.

Si un cybercriminel vole un cookie de session et l'injecte dans son navigateur, il peut souvent accéder à la même session que l'utilisateur légitime aussi longtemps que la session reste active – cette durée dépendant du fournisseur de l'application.

Il existe plusieurs moyens d'intercepter un token de session :

- **Attaques côté client** (p. ex. T1539, T1185) – Plusieurs méthodes permettent d'extraire un token de session de l'application client, dont les scripts intersites (XSS), les JavaScript malveillants ou encore les malwares. Ainsi, la plupart des familles de malwares courantes en circulation aujourd'hui incluent des modules espions baptisés « infostealer » qui ont la capacité d'extraire les cookies.
- **Attaques de phishing Adversary-in-the-middle (AiTM)** (p. ex. T1557, T1566, T1539) – Les cybercriminels utilisent le social engineering pour rediriger les utilisateurs vers un site web malveillant configuré comme un serveur proxy HTTP inverse, qui relaie les demandes entre l'utilisateur ciblé et une application web usurpée. Si un utilisateur est amené à se connecter à l'application web légitime via l'un de ces sites malveillants, le cybercriminel peut alors accéder aux identifiants de l'utilisateur et au token de session renvoyé au navigateur. Le cybercriminel peut également accéder au trafic réseau (éventuellement via un point d'accès malveillant) pour observer et voler le token de session.

Même si le détournement de session peut parfois prendre la forme d'une opération de plus grande envergure, il est généralement utilisé dans le cadre d'une attaque ciblée contre des utilisateurs spécifiques d'une entreprise présentant une grande valeur.

Toutefois, avec l'adoption croissante de l'authentification sans mot de passe, nous pensons que les cybercriminels vont désormais concentrer leurs efforts sur les tactiques, techniques et procédures (TTP) de détournement de session.

Mise en vente des tokens de session

La plupart des tokens volés sont ensuite vendus sur des marketplaces cybercriminelles, ce qui permet aux cybercriminels cherchant à compromettre un compte d'une entreprise spécifique de simplement acheter le token qui les intéresse – souvent pour quelques dizaines de dollars.

Comme expliqué ci-après, une solution possible pour limiter le risque consiste à réduire la durée maximale des sessions. Si cette mesure n'a aucun effet lorsqu'un utilisateur est directement ciblé par des tactiques de social engineering, elle est très efficace en revanche pour neutraliser les infostealers, en raison du délai généralement observé entre la collecte des tokens (et des identifiants) et leur publication sur un marché clandestin.

Mesures de défense

Pour améliorer la sécurité des sessions et les protéger contre le détournement, plusieurs solutions sont possibles :

- Évitez d'ajouter les tokens de session aux URL.
- Utilisez un gestionnaire de sessions sécurisées côté serveur, capable de générer un nouveau token de session aléatoire après la connexion.
- Stockez les tokens de session dans un emplacement sécurisé et révoquez-les après la déconnexion.
- Raccourcissez la durée maximale des sessions.

De façon plus générale, les fournisseurs d'applications devraient également envisager l'implémentation d'un mécanisme de réauthentification des utilisateurs lorsque les circonstances l'exigent, comme nous le verrons ci-après.

Bonnes pratiques de gestion des sessions d'application

Lorsqu'elle fait intervenir un fournisseur d'identités (IdP), la gestion des sessions d'application peut poser bien des difficultés et certaines des solutions disponibles dans le marché sont souvent incomplètes.

Pour en savoir plus, lisez l'article de blog Best Practices for Application Session Management.

Authentification renforcée

Comme nous l'avons mentionné à plusieurs reprises, il est essentiel de trouver le juste compromis entre sécurité et facilité d'utilisation pour créer une expérience utilisateur de qualité.

Renforcer l'authentification permet aux fournisseurs d'applications de trouver ce juste équilibre, dans ce cas-ci en adaptant les demandes d'identité supplémentaires à l'importance de la ressource et au niveau de risque associé en cas d'exposition.

Avec cette approche progressive, les utilisateurs (ou ceux tentant d'usurper leur identité) peuvent accéder à certaines ressources avec un jeu d'identifiants donné, mais seront invités à fournir des informations supplémentaires (via une demande MFA, par exemple) si les ressources sollicitées sont plus sensibles.

L'inconvénient d'une authentification renforcée réside dans la difficulté de sa mise en œuvre. En effet, une implémentation efficace exige une attention et une planification rigoureuses.

Authentification continue

Répondre correctement à une première demande d'authentification n'est pas une raison suffisante pour octroyer un accès à long terme.

En surveillant continuellement certains signaux (p. ex. l'emplacement d'un utilisateur, le terminal et les applications utilisés, les schémas d'utilisation, l'heure, le comportement de saisie, etc.) le système d'authentification vérifie simplement, chaque fois que nécessaire, si le degré de confiance reste suffisamment élevé pour accepter de prolonger l'accès de l'utilisateur.

Cette « authentification continue » est extrêmement performante, car elle améliore à la fois la sécurité et l'expérience utilisateur. Qui plus est, sa fiabilité est bien supérieure à celle que peut offrir un simple mot de passe.

Cela étant, l'implémentation de l'authentification continue dans le contexte de l'identité client exige un consentement éclairé – et sans doute continu – de la part des utilisateurs, en plus d'une méthode quelconque de suivi des terminaux. Compte tenu de ces exigences, les solutions d'authentification restent de fait limitées aux scénarios B2B et à certains cas d'usage B2C sensibles, tels que les services financiers et de santé. ■

Optimiser la sécurité et l'expérience client grâce au CIAM

Mettre en place un CIAM performant – c'est-à-dire l'implémenter de façon évolutive pour satisfaire simultanément les impératifs de sécurité, de confidentialité et de fluidité de l'expérience utilisateur – est un défi de taille pour toutes les entreprises :

- Dans la mesure où le CIAM se situe au cœur des systèmes orientés client (constituant une source pour les analyses de marché et jouant un rôle dans les efforts d'acquisition, de conversion et de rétention des clients), il s'aligne avec les équipes marketing et expérience client.
- Parallèlement, le CIAM joue un rôle important en matière de sécurité et de confidentialité, ce qui le place inévitablement dans la sphère des RSSI, DSI et autres responsables.
- Enfin, le CIAM reste intrinsèquement un ensemble de solutions technologiques, ce qui en fait le domaine des équipes IT, voire des directeurs techniques (lorsqu'il est, à juste titre, considéré comme un facteur de transformation digitale).

Pour trouver un juste équilibre entre sécurité et expérience client, tous les responsables concernés doivent collaborer dans l'implémentation du CIAM en tenant compte des cas d'usage, des types de clients, des types de données, des risques propres au secteur et de la tolérance au risque.

Protection des identités clients

Bloquer les attaques sophistiquées d'usurpation d'identité actuelles et perturber les modèles économiques des cybercriminels, tout en préservant la qualité de l'expérience des utilisateurs légitimes, est uniquement possible en combinant plusieurs outils de sécurité, opérant à différents niveaux, en une posture défensive cohérente.

L'achat, l'intégration, la configuration de chaque outil individuel, sans compter leur monitoring, optimisation et orchestration continus, exigent des compétences en pénurie, demandent une attention soutenue en termes opérationnels et sollicitent fortement les ressources de l'entreprise qui seraient mieux employées à développer des compétences clés.

Pour toutes ces raisons et d'autres encore, une solution CIAM de pointe, agile, avec une architecture de défense en profondeur et où la sécurité est intégrée dès la conception, est une approche bien plus efficace pour sécuriser les identités que ne l'est l'autre option, à savoir le développement et la gestion d'un système de gestion des identités en interne.

Dix bonnes pratiques de gestion des identités clients

Que vous ayez décidé de développer votre propre solution en interne ou de vous en remettre à un fournisseur IDaaS (Identity-as-a-Service), ces quelques recommandations pourraient vous être utiles :

- **Utilisez des messages d'erreur génériques –** Des messages détaillés peuvent faciliter la tâche aux cybercriminels en fournissant des informations sur les utilisateurs existant dans le système. Laissez les cybercriminels dans le flou en affichant des messages d'erreur génériques.
- **Implémentez la gestion de sessions sécurisées –** Utilisez un gestionnaire de sessions sécurisées côté serveur, capable de générer un nouvel ID de session après la connexion. N'insérez pas les ID de session dans l'URL et veillez à ce qu'ils soient stockés dans un emplacement sécurisé et révoqués après la déconnexion.
- **Ne livrez pas vos produits avec des identifiants par défaut –** Les identifiants administrateur par défaut représentent un vecteur d'attaque majeur car de nombreuses entreprises ne les changent pas. S'il peut sembler pratique de provisionner de nouveaux terminaux et utilisateurs avec des identifiants par défaut, il est de loin préférable d'utiliser des technologies telles que OpenID Connect, d'adopter l'authentification sans mot de passe ou d'imposer aux utilisateurs la définition d'un mot de passe à la première connexion.
- **Ne stockez pas les mots de passe en texte clair –** Si les mots de passe conservés dans votre base de données sont véritablement illisibles, ils n'ont aucune valeur pour les cybercriminels. Le chiffrement fait de votre entreprise une cible bien moins attrayante, mais il doit être correctement implémenté.

Ensuite, pensez à mettre en place des mesures de défense élémentaires :

- **Limitez le nombre d'échecs de connexion –** Les attaques par force brute, comme le credential stuffing, donnent lieu à un nombre important d'échecs pour une seule connexion réussie. L'identification de ce type de comportement permet de détecter des attaques et de déclencher l'application de contre-mesures.
- **Imposez l'utilisation de mots de passe forts –** De nombreuses attaques par force brute aboutissent lorsque les mots de passe sont trop faibles ou courants. Exigez des mots de passe d'une certaine longueur, complexité et rotation, sur la base des recommandations du NIST ou d'autres politiques basées sur des preuves.
- **Détectez l'utilisation de mots de passe compromis –** De nombreux utilisateurs réemploient des mots de passe similaires, voire identiques, sur de nombreux sites. Par conséquent, la compromission d'un site ou service peut en impacter bien d'autres. Obligez les utilisateurs à modifier des identifiants compromis.

Enfin, adoptez des mécanismes d'authentification renforcée :

- **Encouragez l'utilisation des passkeys –** Les passkeys offrent une authentification plus robuste et les passkeys synchronisées contribuent à une expérience utilisateur fluide, nécessaire à la généralisation de leur adoption auprès des consommateurs.
- **Proposez un MFA fort –** Lors du déploiement du MFA, privilégiez les authentificateurs et les méthodes basées sur WebAuthn. Si vous avez déjà implémenté le MFA depuis un certain temps, pensez à migrer les utilisateurs existants vers ces facteurs d'authentification secondaires plus forts et oubliez les approches d'ancienne génération.
- **Adoptez le MFA adaptatif et renforcez l'authentification –** Pour les entreprises soucieuses d'éviter des points de friction supplémentaires, ces techniques permettent de trouver un plus juste compromis entre sécurité et expérience utilisateur.

Découvrez Auth0 by Okta pour en savoir plus sur la gestion des identités ■

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.

Auth0 est une technologie fondamentale d'Okta et de sa ligne de produits phares, Okta Customer Identity Cloud. Pour en savoir davantage et créer un compte gratuit, les développeurs peuvent se rendre sur le site Auth0.com.

Clause de non-responsabilité

Le présent document et toute recommandation qu'il propose ne constituent pas des conseils juridiques, commerciaux ou en matière de confidentialité, sécurité ou conformité. Le contenu de ce document revêt un caractère purement informatif et pourrait ne pas refléter les normes de sécurité, de confidentialité et les réglementations les plus récentes, ou tous les problèmes pertinents. Pour obtenir de tels conseils, il vous revient de vous adresser à votre conseiller juridique ou à tout autre conseiller professionnel en matière de sécurité, confidentialité ou conformité, 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 ne formule aucune déclaration, garantie ou autre assurance concernant le contenu de ce document. Pour en savoir plus sur les assurances contractuelles d'Okta à ses clients, rendez-vous à cette adresse okta.com/agreements.

Tous les produits, fonctions et fonctionnalités mentionnés ici qui ne sont pas encore disponibles pourraient être distribués plus tard qu'aux dates annoncées ou annulés. Les roadmaps produits ne représentent en rien un engagement, une obligation ou une promesse d'offre de produit ou fonctionnalité, et les clients ne doivent pas se baser sur ces plans pour prendre leur décision d'achat.

Postface

Prochaine étape, l'autorisation

Il ne fait aucun doute que l'importance des identités numériques ne fera que croître au cours des mois, années et décennies à venir. Par conséquent, la capacité à bien gérer et sécuriser les identités clients constituera le socle de la plupart des interactions numériques.

Comme nous l'avons vu, les menaces contre l'identité client se généralisent, évoluent en continu et gagnent en sophistication, ce qui signifie que les services CIAM doivent continuellement anticiper, réagir et s'adapter.

Ainsi, nous nous attendons à ce que l'adoption croissante des passkeys contraigne les cybercriminels à se concentrer sur des TTP post-authentification, d'où l'importance croissante de mesures telles que la gestion sécurisée des sessions, l'authentification renforcée et l'authentification continue.

Mais l'authentification n'est qu'un aspect d'un CIAM. L'autorisation, à savoir la détermination des ressources auxquelles un utilisateur est autorisé à accéder, est tout aussi importante, même si l'on ne lui accorde pas autant d'attention. Avec l'utilisation de l'identité numérique comme moyen de contrôle des droits, des informations, des services et d'autres privilèges, l'autorisation deviendra un élément incontournable des offres personnalisées et un mécanisme de protection majeur contre les intrusions et les compromissions de données qui s'ensuivent.

En définitive, la protection des identités clients consiste à établir et à préserver la confiance qui permet aux personnes et aux entreprises d'interagir au quotidien.

Les enjeux sont considérables, à la hauteur de notre engagement.

Shiven Ramji
President, Customer Identity Cloud, Okta

Annexes

Annexes

Annexe A : Glossaire

Tout au long de ce rapport, nous utilisons une série de termes spécifiques qu'il valait la peine de définir :

- **Authentification multifacteur (MFA, Multi-Factor Authentication) :** méthode d'authentification exigeant plusieurs facteurs, par exemple la biométrie, un mot de passe à usage unique, une application d'authentification, etc.
- **Authentification multifacteur adaptative (Adaptive MFA) :** politique MFA flexible et extensible permettant de protéger les applications contre des acteurs malveillants sans ajouter de points de friction pour les utilisateurs ; une telle approche évalue le risque potentiel associé à chaque connexion, puis demande à l'utilisateur un facteur de vérification supplémentaire dans les cas requis
- **Authentification renforcée :** approche d'authentification destinée à trouver le juste équilibre entre sécurité et friction, en permettant aux utilisateurs d'accéder à certaines ressources avec un seul jeu d'identifiants, mais en leur demandant des identifiants supplémentaire en cas d'accès à des ressources sensibles
- **Authentification sociale :** implémentation de l'authentification unique (SSO) permettant aux utilisateurs de se connecter à plusieurs applications et services au moyen d'un même compte, généralement d'un fournisseur de réseau social
- **Authentification unique (SSO, Single Sign-On) :** solution d'authentification permettant à un utilisateur de se connecter une seule fois et avec une seule identité afin d'accéder par la suite à d'autres systèmes indépendants sans devoir saisir à nouveau des facteurs d'authentification
- **Authentification :** confirmation d'une identité numérique (tel que le mécanisme utilisé par les applications pour identifier les utilisateurs)
- **Autorisation :** processus visant à déterminer les ressources auxquelles peut accéder un utilisateur (par exemple, mécanisme utilisé par les applications pour déterminer ce qu'un utilisateur est autorisé à faire)
- **Échange de carte SIM :** technique permettant à un cybercriminel de prendre le contrôle du numéro de téléphone mobile d'un utilisateur en convainquant l'opérateur mobile de l'utilisateur ciblé de transférer le numéro mobile de l'utilisateur vers une carte SIM en possession de l'acteur malveillant
- **Entité :** objet identifiable et unique qui existe indépendamment des modifications apportées à ses attributs ; dans le contexte du CIAM, il s'agit généralement d'un utilisateur, d'un terminal ou d'une ressource informatique (système ou application)
- **Fatigue MFA :** technique utilisée par un cybercriminel pour inonder un utilisateur de notifications MFA dans l'espoir qu'il les acceptera ou les approuvera, ce qui lui permet d'avoir accès à un compte ou à un service
- **FIDO :** acronyme de Fast Identity Online, souvent utilisé pour désigner l'Alliance FIDO, une association sectorielle ouverte dont la mission consiste à développer et à promouvoir des normes d'authentification pour limiter la dépendance excessive vis-à-vis des mots de passe
- **Friction :** dans le monde numérique, le terme « friction » ou « point de fricton » désigne tout ce qui ralentit les interactions d'un client avec vos services. Pour un utilisateur, ces interactions peuvent inclure (sans s'y limiter) l'inscription à un service, la connexion à un compte existant, la récupération d'informations de compte oubliées et le paiement d'un achat
- **Gestion des identités et des accès clients (CIAM, Customer Identity and Access Management) :** système permettant aux entreprises d'octroyer à leurs utilisateurs finaux un accès à leurs propriétés numériques et régissant la façon dont elles gèrent, collectent, analysent et stockent de façon sécurisée les données de ces utilisateurs
- **Identité client :** regroupe les informations collectées par les marques pour en savoir plus sur leurs clients et établir en toute sécurité une relation de confiance basée sur le consentement, en déterminant qui sont leurs clients et comment ils veulent interagir
- **Identité numérique :** série d'attributs définissant un utilisateur donné dans le contexte d'une application
- **Intrusion :** événement de sécurité (ou série d'événements de sécurité) au cours duquel un utilisateur non autorisé accède à un système ou à une ressource système
- **Magic link :** lien généré par une API d'authentification qui est envoyé à un utilisateur. Lorsqu'il clique sur le lien, l'utilisateur est directement connecté. D'un point de vue fonctionnel, un magic link est similaire au processus au cours duquel un utilisateur reçoit un e-mail avec un mot de passe à usage unique, revient dans l'application et saisit ce mot de passe, à la différence qu'il ne doit pas effectuer ces étapes
- **Mot de passe à usage unique (OTP, One-Time Passcode/Password) :** séquence de caractères numériques ou alphanumériques générée par l'API d'authentification qui authentifie un utilisateur pour une seule connexion ou transaction
- **Open Source Intelligence (OSINT) :** collecte, analyse et distribution d'informations mises à disposition du public et légalement accessibles (conformément au SANS)
- **Passkey liée au terminal :** passkey qui est liée à un équipement spécifique et qui sert de facteur de possession
- **Passkey synchronisée :** passkey qui peut être partagée en toute sécurité par/entre plusieurs terminaux (par exemple au sein d'un écosystème de système d'exploitation ou via un gestionnaire de mots de passe)
- **Passkey :** identifiants FIDO détectables par les navigateurs ou incorporés au sein d'applications natives, ou clés de sécurité pour une authentification sans mot de passe
- **Passwordless :** l'authentification sans mot de passe (passwordless) désigne un mécanisme permettant d'authentifier un utilisateur sans lui demander de saisir un mot de passe
- **Phishing :** technique de social engineering utilisant généralement la ruse, la pression ou une forme quelconque de manipulation pour inciter les utilisateurs à partager des informations sensibles
- **Social engineering :** terme générique incluant toutes les tactiques et techniques visant à inciter une cible à divulguer des informations sensibles ou à effectuer une action pour le compte du cybercriminel
- **Spear phishing :** forme très ciblée de phishing (visant par exemple une personne ou une entreprise) qui inclut souvent des informations présentant un intérêt particulier, dont la cible suppose qu'elles ne sont pas connues du plus grand nombre
- **Usurpation de compte (ATO, Account TakeOver) :** but poursuivi par un cybercriminel lors de la plupart des attaques contre les systèmes de gestion des identités et des accès (IAM), à savoir obtenir un accès à un compte existant d'un utilisateur légitime et le contrôler
- **WebAuthn :** forme abrégée de Web Authentication, standard d'authentification web via une API JavaScript faisant partie de la spécification FIDO

Annexes

Annexe B : Méthodologie

Ce rapport s'appuie sur les données collectées par Okta Customer Identity Cloud, opéré par Auth0, qui fournit des fonctions CIAM à des milliers d'entreprises de toutes tailles, partout dans le monde.

En particulier, le rapport résume les logs d'événements journaliers en numérateurs (p. ex. les événements de connexion frauduleux) et dénominateurs (p. ex. le nombre total d'événements de connexion), ce qui permet de normaliser de façon pertinente les tendances en matière de menaces et de contrôler les changements constants apportés à la composition des clients de Customer Identity Cloud.

Ces données d'événements sont associées, lorsqu'elles existent, à des informations sur le secteur du tenant (sélectionné par ce dernier), sa taille (petite, moyenne ou grande entreprise) et la région où l'entreprise est basée, avant d'être agrégées de façon anonyme.

Comme ce rapport est basé sur de véritables déploiements de production, il recense des activités réelles collectées sur la plateforme Customer Identity Cloud. Il dépend par conséquent des produits et fonctions activés par chaque client (ainsi que leur configuration) et des fonctionnalités de ces produits, susceptibles d'évoluer au fil du temps.

Pour déterminer les 10 secteurs les plus représentés au sein des clients Customer Identity Cloud, nous avons classé chaque secteur en fonction de quatre facteurs, sur les six premiers mois de l'année 2023 :

- Nombre de tenants
- Nombre total d'événements de connexion
- Nombre total d'événements d'authentification par mot de passe
- Nombre total de tentatives MFA

Nous considérons les 10 secteurs présentant le classement moyen le plus élevé comme les secteurs les plus représentés.

L'analyse des sous-groupes dépend d'attributs qui ne sont pas toujours disponibles pour tous les clients/tenants (p. ex. le secteur, la taille et le pays ou région du siège). En d'autres termes, les graphiques affichant une agrégation globale basée sur de tels attributs n'incluront pas tous les tenants. Par exemple, alors que la figure 3 inclut des données de tous les tenants, la figure 6 n'inclut que ceux :

- pour lesquels nous disposons du pays du siège ;
- dont le pays du siège fait partie de l'une des régions représentées (AMER, APAC ou EMEA).

La figure 6 n'inclut donc pas les données des tenants qui n'ont pas précisé le pays du siège de l'entreprise ou dont le pays ne fait pas partie des trois régions.

Dans un cas extrême, l'effet lié au sous-groupe a créé un scénario dans lequel les trois grandes régions du monde présentent une proportion de tentatives de contournement du MFA inférieure à la moyenne (mondiale). L'explication est simple : les clients basés en dehors des trois grandes régions ou pour lesquels nous ne disposons pas des données sur le siège ont été également comptabilisés dans la moyenne mondiale. Dès lors, celle-ci est plus élevée que la moyenne des clients appartenant aux régions AMER, APAC ou EMEA.

Annexes

Annexe C: Tableaux récapitulatifs par secteur

Les sous-sections suivantes offrent un contexte supplémentaire pour les 10 secteurs les plus représentés dans l'ensemble de données 2023 :

Agroalimentaire/restauration/hôtellerie

Inclut la production et la distribution des boissons et produits alimentaires et les services connexes, ainsi que les activités de loisir et l'hébergement (hôtels et restaurants)

Commerce de détail/e-commerce

Inclut les entreprises qui vendent et distribuent des produits et services aux consommateurs via des points de vente physiques ou des plateformes numériques

Industrie

Inclut la production de biens physiques de tous types, allant des produits électroniques grand public aux automobiles

Logiciels/SaaS/technologies

Activités centrées sur le développement, la distribution et le support des logiciels, dont les services SaaS et les technologies

Médias

Inclut les entreprises chargées de créer, distribuer et diffuser du contenu comme les journaux télévisés, les émissions de divertissement et la publicité

Professional Services

Inclut un large éventail de services destinés à répondre aux besoins des entreprises, par exemple des services juridiques, marketing, comptables et de conseil

Publicité/marketing

Dédié à la création, à la promotion et à la diffusion de campagnes destinées à informer et à mobiliser le public pour soutenir des produits et services

Santé

Inclut les prestataires de soins de santé et les organismes qui les prennent en charge (comme les assurances médicales), l'industrie pharmaceutique et les technologies médicales

Services financiers

Inclut des services bancaires, d'assurances et de gestion de patrimoine, ainsi que d'autres services destinés à gérer et à distribuer le capital

Voyage/transport

Inclut les compagnies aériennes et ferroviaires, les hôtels, les agences de voyages et les services connexes spécialisés dans le transport des personnes et des marchandises

Tableau 2. Publicité/marketing

Récapitulatif des tendances en matière de menaces ciblant l'identité pour le secteur de la publicité/marketing

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	1,4 %	1,5 %	1,0 %
Tentatives de credential stuffing	2,7 %	4,9 %	16,9 %
Tentatives de contournement du MFA	17,6 %	4,1 %	3,4 %

Tableau 3. Services financiers

Récapitulatif des tendances en matière de menaces ciblant l'identité pour le secteur des services financiers

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	23,4 %	50,8 %	28,8 %
Tentatives de credential stuffing	46,6 %	41,8 %	30,3 %
Tentatives de contournement du MFA	3,7 %	4,8 %	10,9 %

Figure 18. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises du secteur de la publicité/du marketing

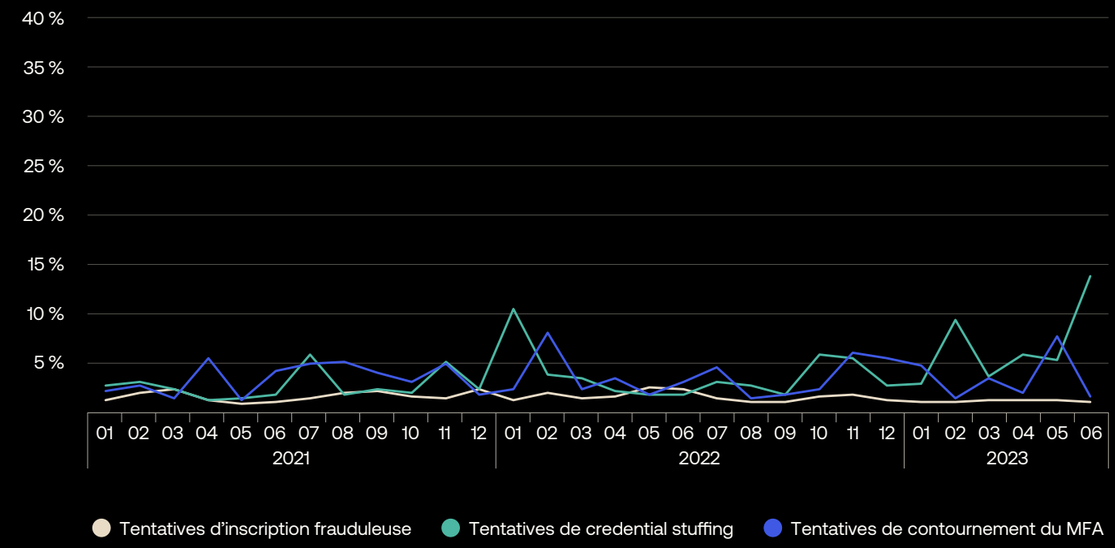


Figure 19. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises du secteur des services financiers

Tableau 4. Agroalimentaire/restauration/hôtellerie

Récapitulatif des tendances en matière de menaces ciblant l'identité pour le secteur de l'agroalimentaire, restauration et hôtellerie

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	3,3 %	17,8 %	9,0 %
Tentatives de credential stuffing	23,6 %	21,5 %	11,4 %
Tentatives de contournement du MFA	8,3 %	9,2 %	5,5 %

Tableau 5. Santé

Récapitulatif des tendances en matière de menaces ciblant l'identité pour le secteur de la santé

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	1,9 %	2,8 %	6,3 %
Tentatives de credential stuffing	4,5 %	3,3 %	16,1 %
Tentatives de contournement du MFA	6,0 %	9,0 %	4,6 %

Figure 20. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises du secteur de l'agroalimentaire/restauration/hôtellerie

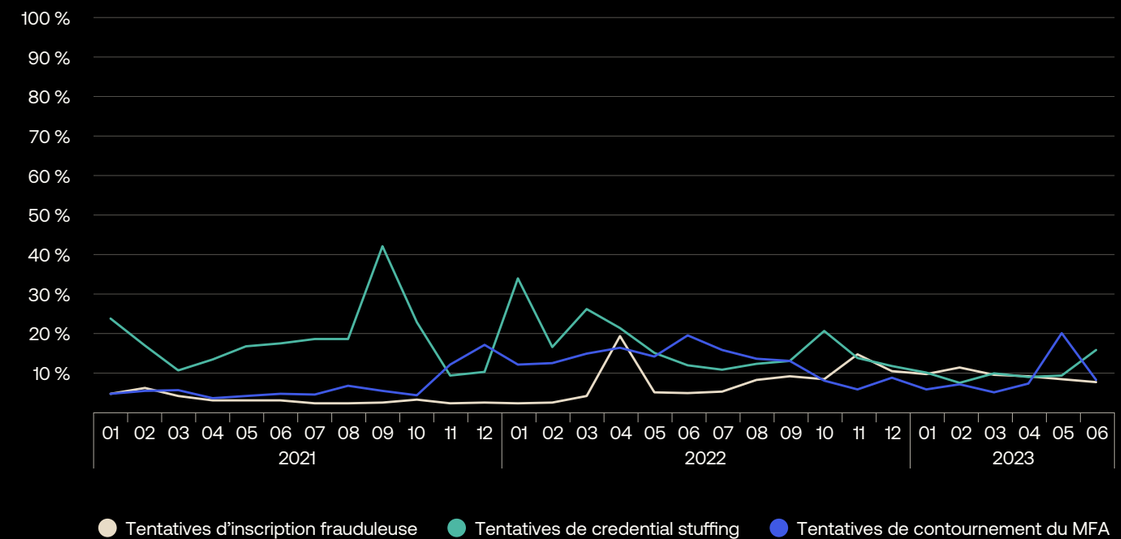


Figure 21. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises du secteur de la santé

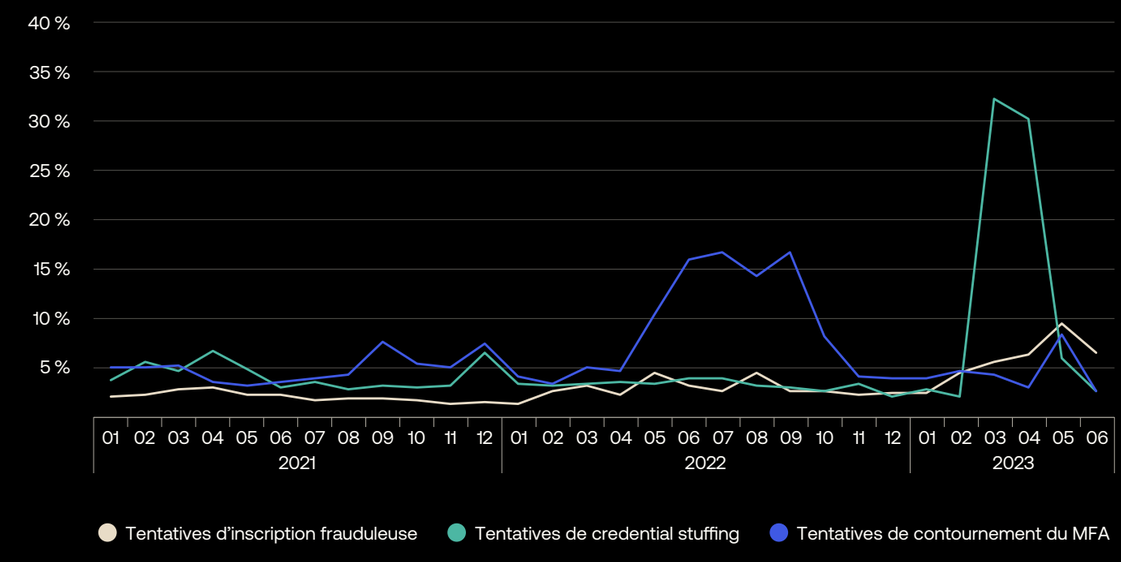


Tableau 6. Industrie

Récapitulatif des tendances en matière de menaces ciblant l'identité pour le secteur de l'industrie

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	14,3 %	17,8 %	25,1 %
Tentatives de credential stuffing	45,9 %	18,4 %	17,7 %
Tentatives de contournement du MFA	6,5 %	10,0 %	7,8 %

Figure 22. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises du secteur de l'industrie

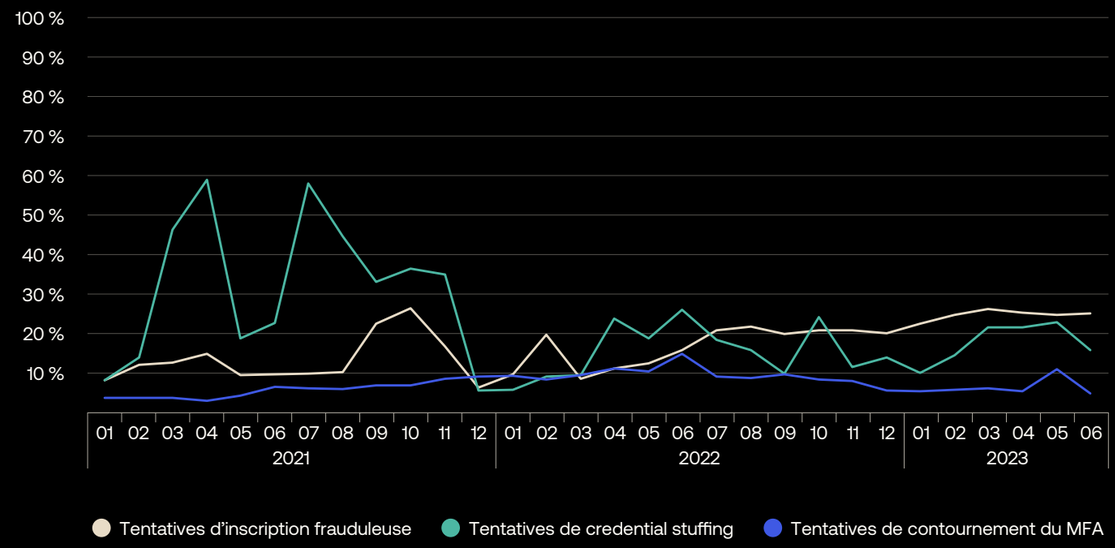


Tableau 7. Médias

Récapitulatif des tendances en matière de menaces ciblant l'identité pour le secteur des médias

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	9,0 %	15,7 %	28,4 %
Tentatives de credential stuffing	22,7 %	17,9 %	42,3 %
Tentatives de contournement du MFA	27,4 %	25,1 %	12,8 %

Figure 23. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises du secteur des médias

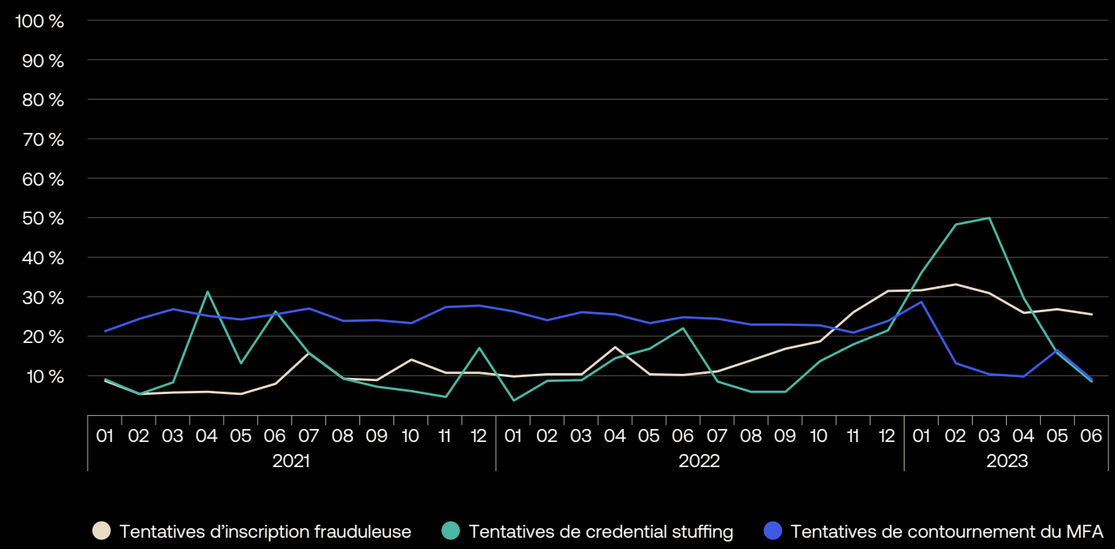


Tableau 8. Services professionnels

Récapitulatif des tendances en matière de menaces ciblant l'identité pour le secteur des services professionnels

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	5,9 %	6,1 %	13,4 %
Tentatives de credential stuffing	7,3 %	4,8 %	7,2 %
Tentatives de contournement du MFA	13,1 %	6,7 %	4,5 %

Tableau 9. Commerce de détail/e-commerce

Récapitulatif des tendances en matière de menaces ciblant l'identité pour le secteur du commerce de détail/e-commerce

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	2,0 %	3,6 %	9,3 %
Tentatives de credential stuffing	55,6 %	56,8 %	51,3 %
Tentatives de contournement du MFA	5,7 %	5,3 %	5,0 %

Figure 24. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises du secteur des services professionnels

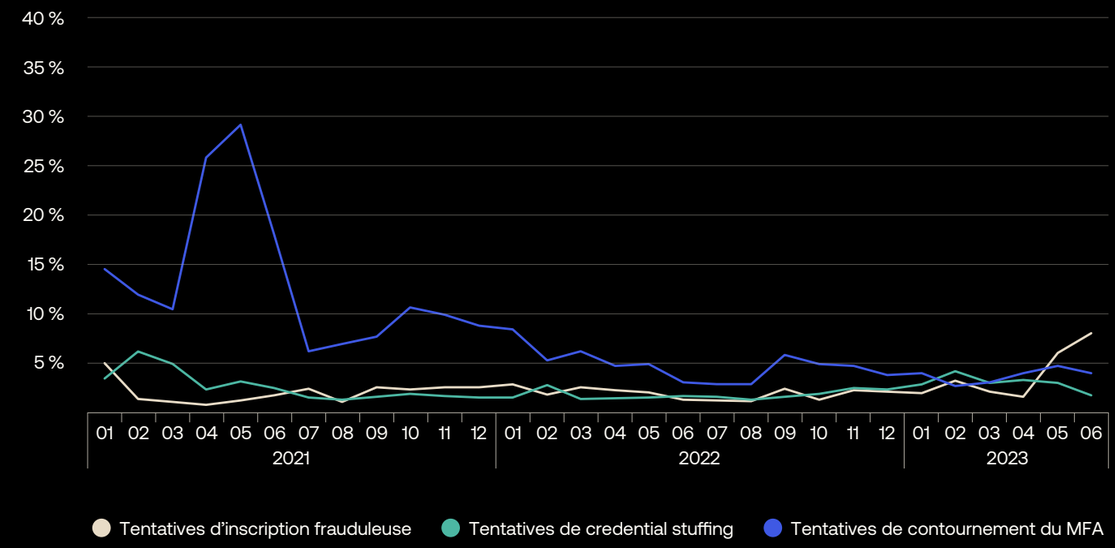


Figure 25. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises du secteur du commerce de détail/e-commerce

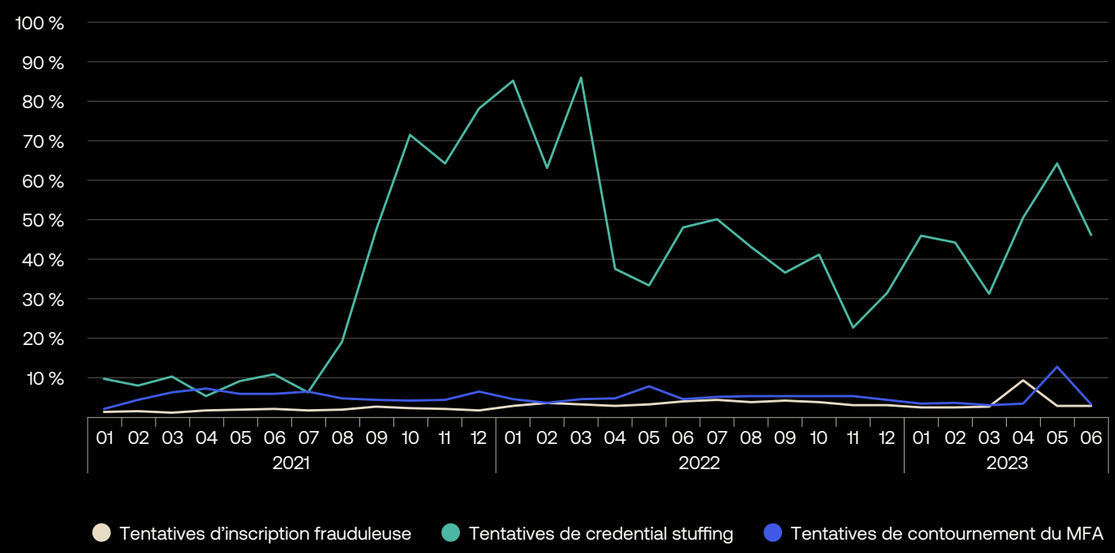


Tableau 10. Logiciels/SaaS/technologies

Récapitulatif des tendances en matière de menaces ciblant l'identité pour le secteur des logiciels/SaaS/technologies

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	54,9 %	26,1 %	24,0 %
Tentatives de credential stuffing	53,6 %	34,5 %	32,1 %
Tentatives de contournement du MFA	37,5 %	21,6 %	6,4 %

Tableau 11. Voyage/transport

Récapitulatif des tendances en matière de menaces ciblant l'identité pour le secteur du voyage/transport

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	5,1 %	13,7 %	9,7 %
Tentatives de credential stuffing	27,4 %	19,0 %	7,2 %
Tentatives de contournement du MFA	6,9 %	3,0 %	2,9 %

Figure 26. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises du secteur des logiciels/SaaS/technologies

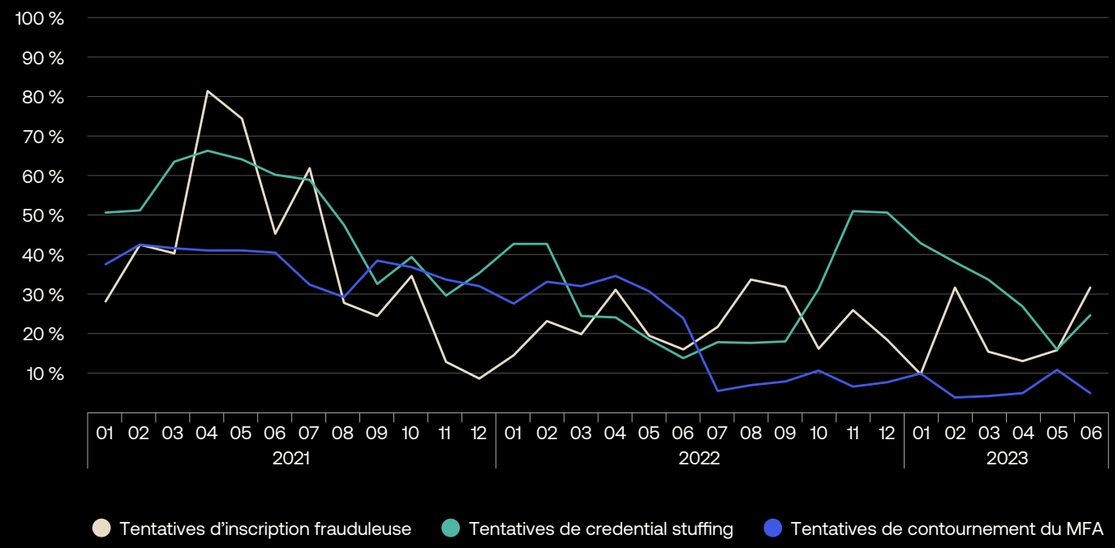
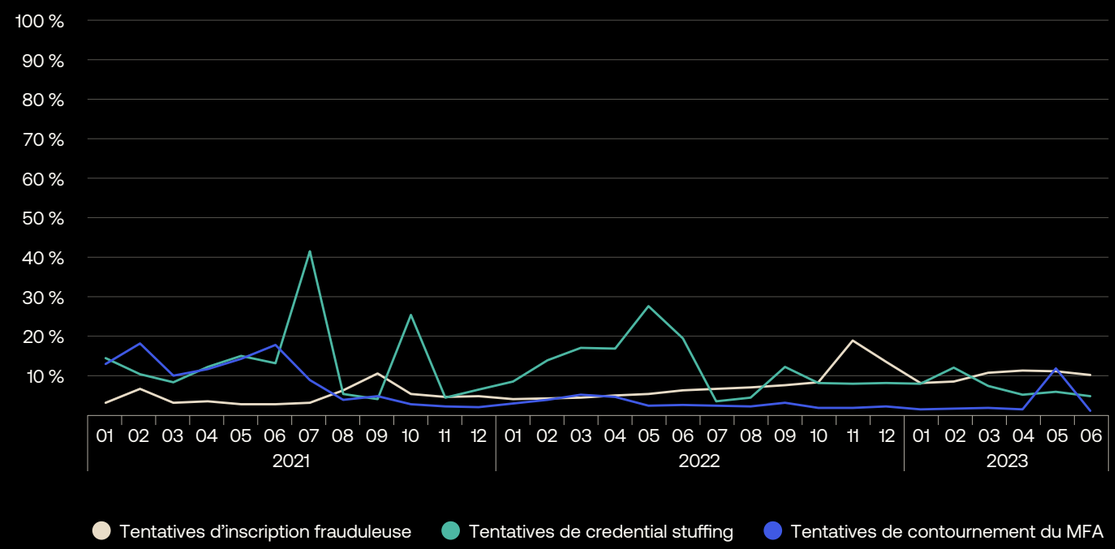


Figure 27. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises du secteur des transports et du tourisme



Annexes

Annexe D : Tableaux récapitulatifs des différents segments d’entreprises

Les sous-sections suivantes offrent un contexte supplémentaire pour les petites, moyennes et grandes entreprises.

Tableau 12. Petites entreprises

Récapitulatif des tendances en matière de menaces ciblant l’identité pour le segment des petites entreprises

	2021	2022	1er sem. 2023
Tentatives d’inscription frauduleuse	65,1 %	44,6 %	19,4 %
Tentatives de credential stuffing	54,0 %	35,7 %	30,9 %
Tentatives de contournement du MFA	9,1 %	25,0 %	20,3 %

Figure 28. Vue quotidienne sur 30 mois des menaces ciblant l’identité dans les petites entreprises

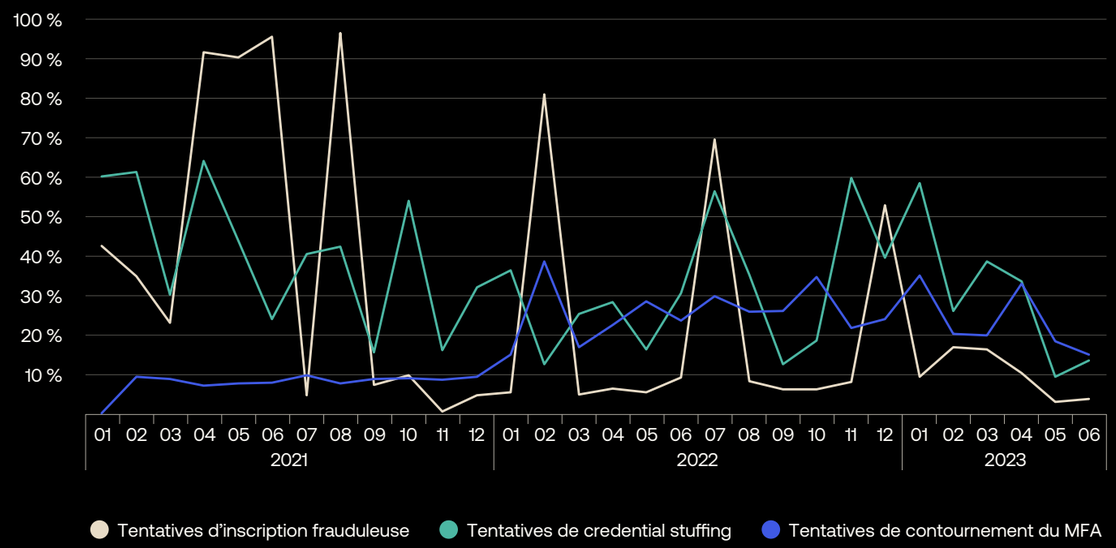


Tableau 13. Moyennes entreprises

Récapitulatif des tendances en matière de menaces ciblant l'identité pour le segment des moyennes entreprises

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	39,9 %	6,0 %	12,6 %
Tentatives de credential stuffing	32,1 %	30,5 %	20,1 %
Tentatives de contournement du MFA	4,4 %	6,2 %	9,0 %

Tableau 14. Grandes entreprises

Récapitulatif des tendances en matière de menaces ciblant l'identité pour le segment des grandes entreprises

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	16,2 %	20,7 %	19,9 %
Tentatives de credential stuffing	50,6 %	44,0 %	39,4 %
Tentatives de contournement du MFA	32,3 %	16,4 %	9,5 %

Figure 29. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises de taille moyenne

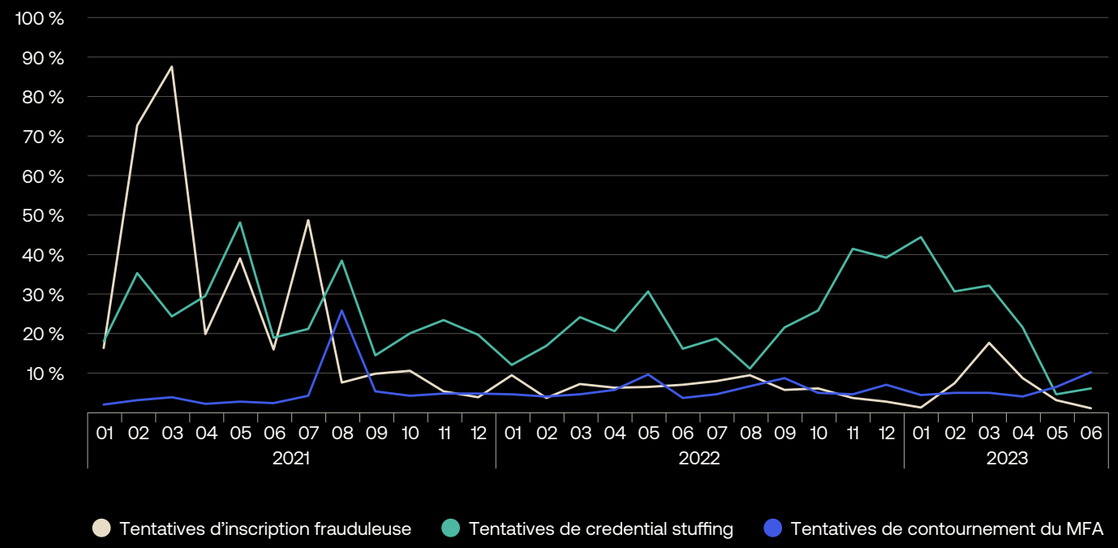
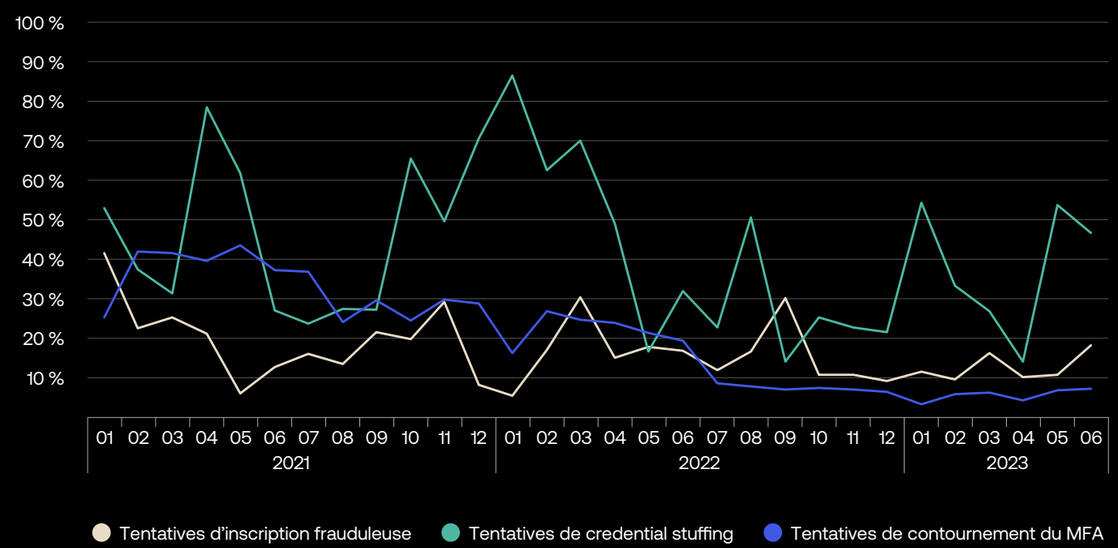


Figure 30. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les grandes entreprises



Annexes

Annexe E : Tableaux récapitulatifs des différentes régions

Les sous-sections suivantes offrent un contexte supplémentaire pour l'analyse par région.

Remarque : à mesure que la portée de l'analyse se réduit, la taille de l'échantillon de données pertinentes aussi, ce qui peut entraîner des fluctuations à court terme plus fréquentes et de plus grande amplitude.

Tableau 15. Continent américain

Peut inclure tous les pays recensés dans la liste de pays de la FAA, l'autorité de l'aviation civile américaine, dénommée Countries in the Western Hemisphere.

Récapitulatif des tendances en matière de menaces ciblant l'identité pour les entreprises basées sur le continent américain

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	35,8 %	14,7 %	9,4 %
Tentatives de credential stuffing	48,1 %	43,8 %	28,0 %
Tentatives de contournement du MFA	6,9 %	11,0 %	12,0 %

Tableau 16. Amérique latine

Pays potentiellement inclus : Argentine, Belize, Bolivie, Brésil, Chili, Colombie, Costa Rica, Équateur, El Salvador, Guyane française, Guatemala, Guyane, Honduras, Mexique, Nicaragua, Panama, Paraguay, Pérou, Suriname, Uruguay et Venezuela.

Récapitulatif des tendances en matière de menaces ciblant l'identité pour les entreprises basées en Amérique latine

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	15,8 %	13,7 %	5,7 %
Tentatives de credential stuffing	59,0 %	31,3 %	17,6 %
Tentatives de contournement du MFA	5,0 %	4,8 %	10,7 %

Figure 31. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises basées sur le continent américain

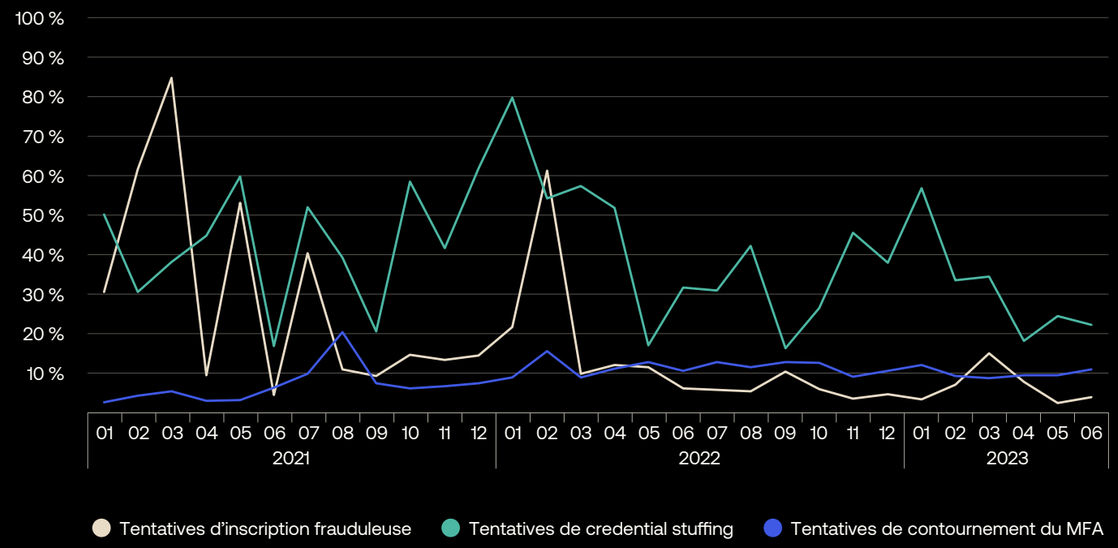


Figure 32. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises basées en Amérique latine

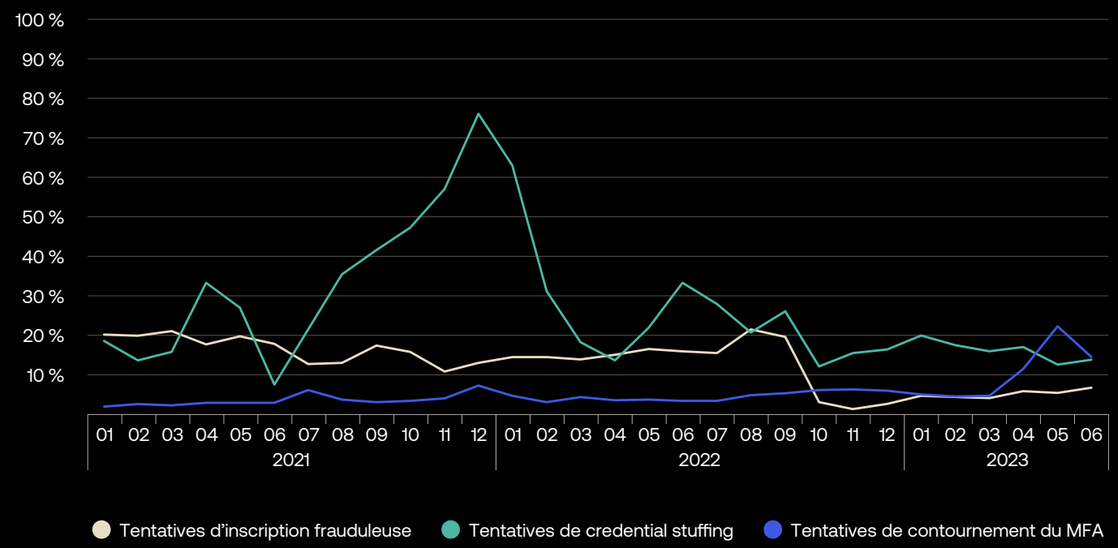


Tableau 17. États-Unis et Canada

Récapitulatif des tendances en matière de menaces ciblant l'identité pour les entreprises basées aux États-Unis ou au Canada

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	37,1 %	14,8 %	9,5 %
Tentatives de credential stuffing	46,1 %	45,1 %	28,5 %
Tentatives de contournement du MFA	7,5 %	14,1 %	12,4 %

Tableau 18. Europe, Moyen-Orient et Afrique

Peut inclure tous les pays recensés dans la liste de pays de la FAA, l'autorité de l'aviation civile américaine, dénommée Countries in Africa, Europe, and the Middle East.

Récapitulatif des tendances en matière de menaces ciblant l'identité pour les entreprises basées en Europe, au Moyen-Orient ou en Afrique

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	18,1 %	20,5 %	8,1 %
Tentatives de credential stuffing	26,4 %	14,1 %	20,2 %
Tentatives de contournement du MFA	34,8 %	20,3 %	7,6 %

Figure 33. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises basées aux États-Unis et au Canada

Figure 34. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises basées en Europe, au Moyen-Orient ou en Afrique

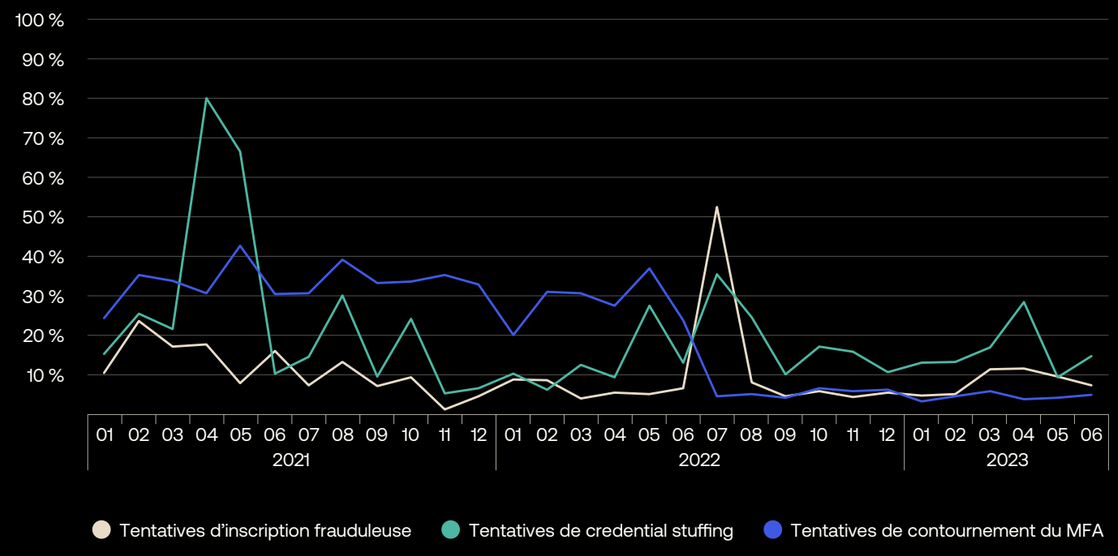


Tableau 19. Pays scandinaves

Pays potentiellement inclus : Danemark, Finlande, Islande, Norvège, Suède et Groenland.

Récapitulatif des tendances en matière de menaces ciblant l'identité pour les entreprises basées dans les pays scandinaves

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	45,4 %	14,9 %	5,2 %
Tentatives de credential stuffing	15,0 %	5,2 %	12,5 %
Tentatives de contournement du MFA	6,0 %	2,9 %	4,1 %

Figure 35. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises basées dans les pays nordiques

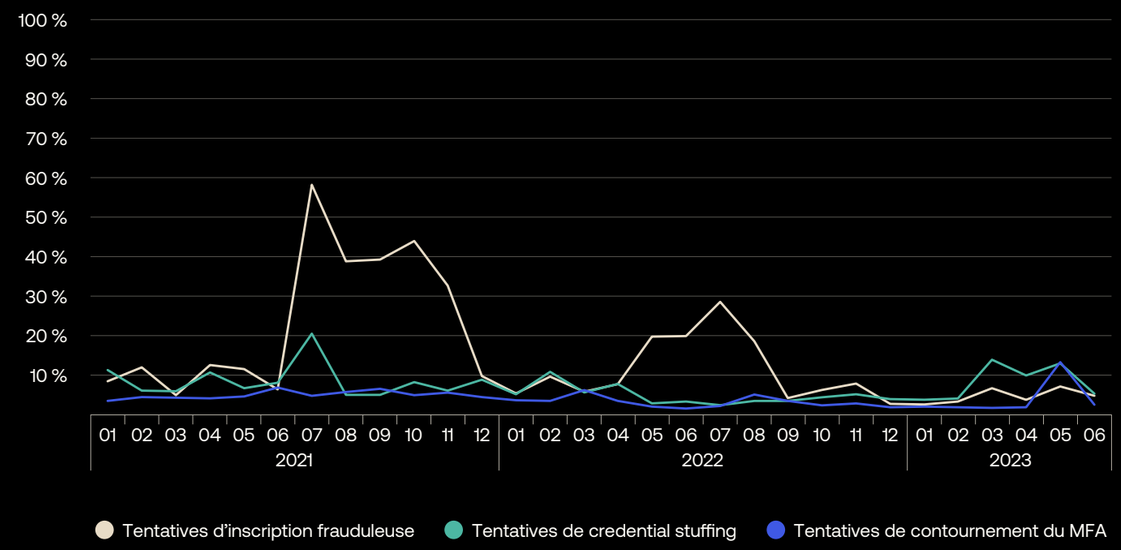


Tableau 20. Europe méridionale

Pays potentiellement inclus : Albanie, Andorre, Bosnie-Herzégovine, Bulgarie, Chypre, Croatie, Espagne, Gibraltar, Grèce, Italie, Kosovo, Macédoine du Nord, Malte, Monténégro, Portugal, Saint-Marin, Serbie, Slovénie, Turquie et le Vatican.

Récapitulatif des tendances en matière de menaces ciblant l'identité pour les entreprises basées en Europe méridionale

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	11,7 %	15,2 %	24,8 %
Tentatives de credential stuffing	18,1 %	14,9 %	10,9 %
Tentatives de contournement du MFA	5,2 %	4,7 %	5,5 %

Figure 36. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises basées en Europe méridionale

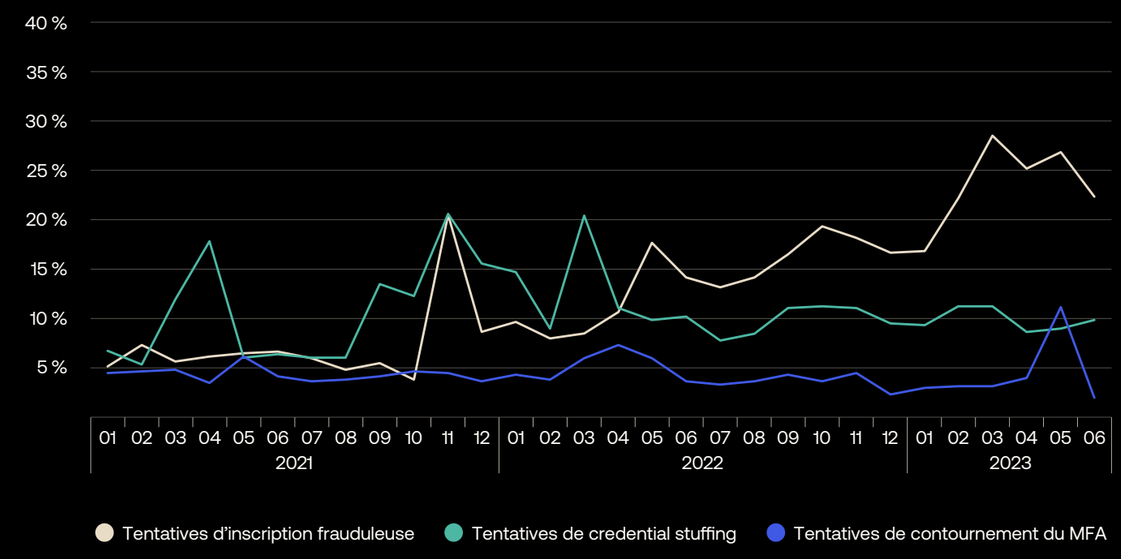


Tableau 21. Royaume-Uni

Pays potentiellement inclus : Angleterre, Écosse, Irlande du Nord et Pays de Galles.

Récapitulatif des tendances en matière de menaces ciblant l'identité pour les entreprises basées au Royaume-Uni

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	5,1 %	11,1 %	13,6 %
Tentatives de credential stuffing	14,5 %	12,9 %	13,3 %
Tentatives de contournement du MFA	1,6 %	2,7 %	4,6 %

Figure 37. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises basées au Royaume-Uni

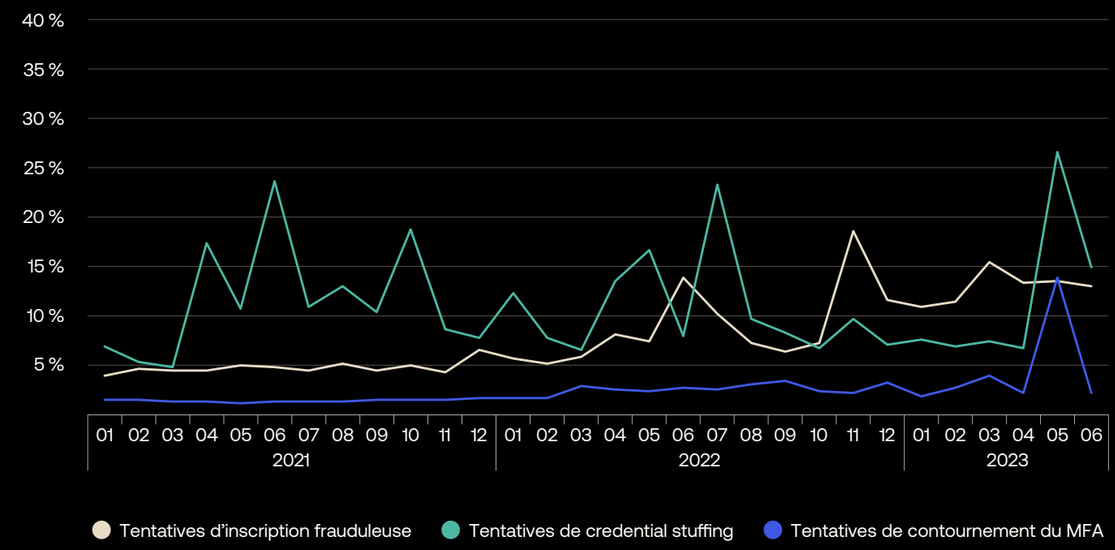


Tableau 22. Europe occidentale

Pays potentiellement inclus : Allemagne, Autriche, Belgique, France, Liechtenstein, Luxembourg, Monaco, Pays-Bas et Suisse.

Récapitulatif des tendances en matière de menaces ciblant l'identité pour les entreprises basées en Europe occidentale

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	14,6 %	28,7 %	5,1 %
Tentatives de credential stuffing	22,7 %	11,2 %	6,3 %
Tentatives de contournement du MFA	10,8 %	11,1 %	14,5 %

Figure 38. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises basées en Europe occidentale

Tableau 23. Asie-Pacifique

Peut inclure tous les pays recensés dans la liste de pays de la FAA, l'autorité de l'aviation civile américaine, dénommée Countries in Asia-Pacific.

Récapitulatif des tendances en matière de menaces ciblant l'identité pour les entreprises basées dans la région Asie-Pacifique

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	52,4 %	28,9 %	27,9 %
Tentatives de credential stuffing	55,0 %	24,3 %	13,3 %
Tentatives de contournement du MFA	6,9 %	10,3 %	11,0 %

Figure 39. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises basées dans la région Asie-Pacifique

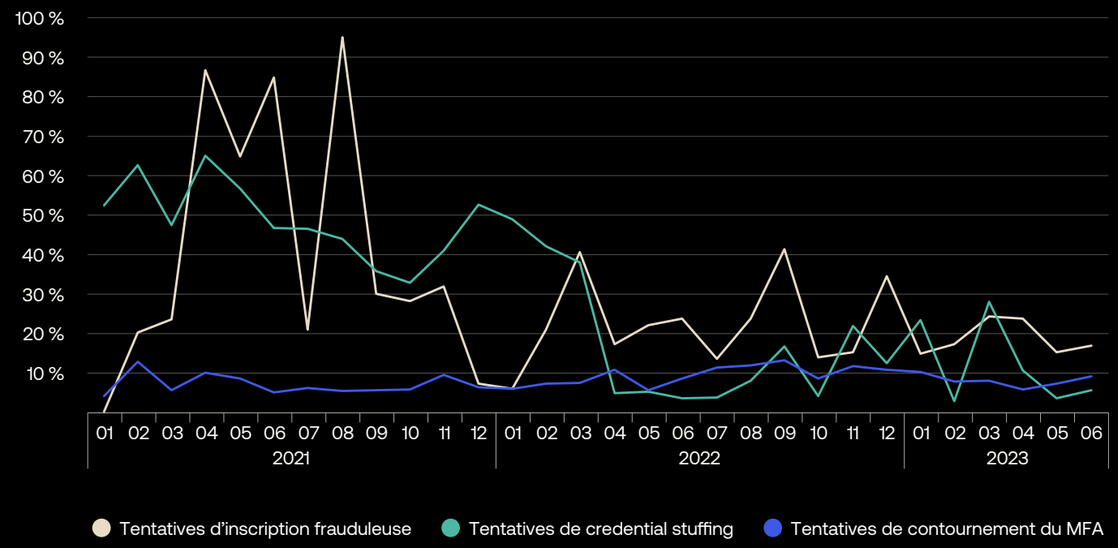


Tableau 24. Japon

Récapitulatif des tendances en matière de menaces ciblant l'identité pour les entreprises basées au Japon

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	16,5 %	33,9 %	43,6 %
Tentatives de credential stuffing	4,1 %	2,7 %	2,4 %
Tentatives de contournement du MFA	25,3 %	16,6 %	21,2 %

Figure 40. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises basées au Japon

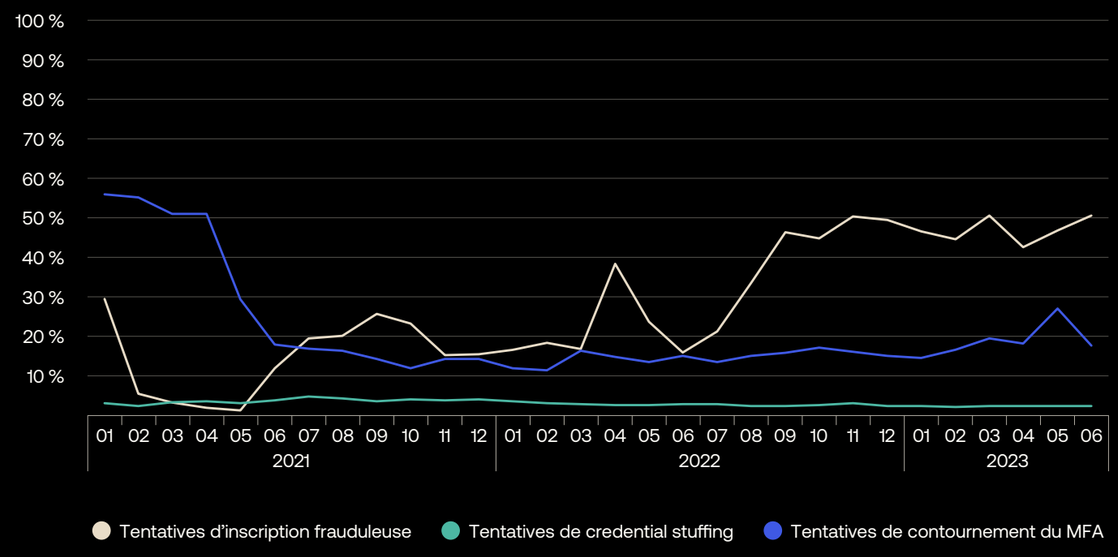


Tableau 25. Australie et Nouvelle-Zélande

Récapitulatif des tendances en matière de menaces ciblant l'identité pour les entreprises basées en Australie ou en Nouvelle-Zélande

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	53,0 %	29,1 %	26,7 %
Tentatives de credential stuffing	57,1 %	26,6 %	14,8 %
Tentatives de contournement du MFA	4,3 %	8,7 %	9,1 %

Tableau 26. Asie du Sud-Est

Pays potentiellement inclus : Brunei, Cambodge, Indonésie, Laos, Malaisie, Myanmar, Philippines, Singapour, Thaïlande, Timor occidental et Vietnam.

Récapitulatif des tendances en matière de menaces ciblant l'identité pour les entreprises basées en Asie du Sud-Est

	2021	2022	1er sem. 2023
Tentatives d'inscription frauduleuse	47,3 %	15,2 %	16,2 %
Tentatives de credential stuffing	73,4 %	55,8 %	24,3 %
Tentatives de contournement du MFA	16,2 %	34,7 %	3,5 %

Figure 41. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises basées en Australie ou Nouvelle-Zélande

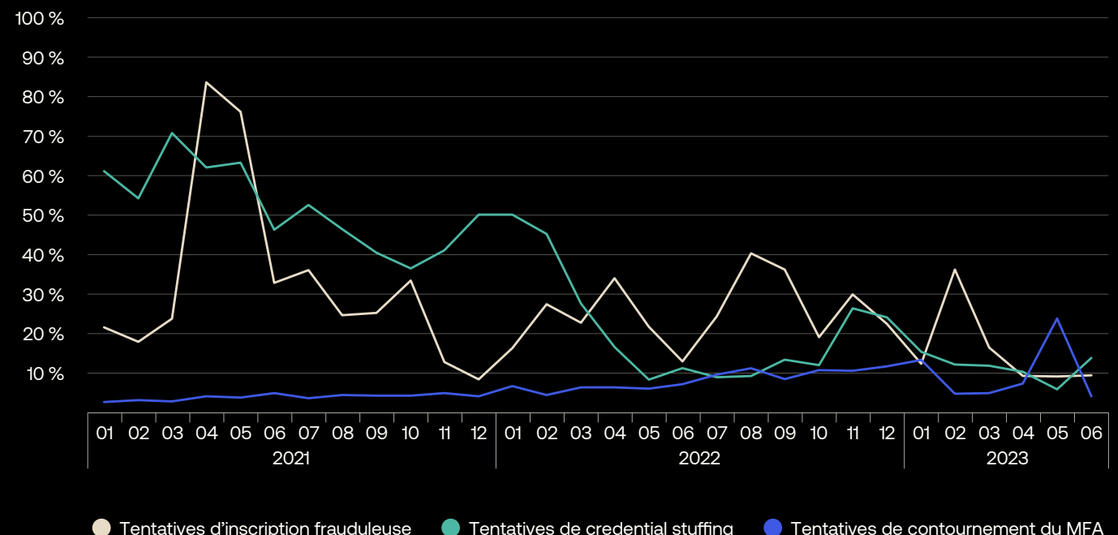
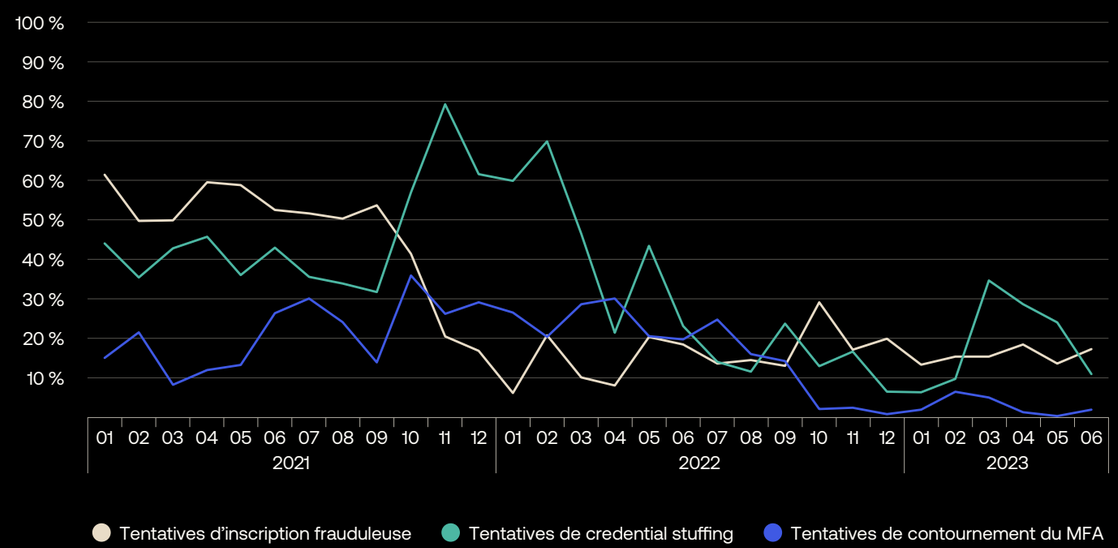


Figure 42. Vue quotidienne sur 30 mois des menaces ciblant l'identité dans les entreprises basées en Asie du Sud-Est



okta

Okta France
Tour Europlaza
20 avenue André Prothin
92400 Courbevoie – France
+33 1 85 64 08 80