

Checklist d'audit – Combattre la fraude sans créer de frictions

Vos contrôles de sécurité protègent-ils le chiffre d'affaires ou freinent-ils les clients ?

Attirer des clients vers votre vitrine est déjà un défi. Bloquer des acheteurs légitimes au moment du paiement avec des CAPTCHA intrusifs, des refus injustifiés et des obstacles de connexion inattendus est source de frustration et coûte cher.

La plupart des équipes de direction suivent de près les coûts liés aux rétrofacturations, mais rares sont celles qui évaluent les pertes de chiffre d'affaires invisibles dues aux refus injustifiés et aux points de friction de sécurité qui nuisent à la conversion.

Utilisez cette checklist pour examiner la configuration actuelle de la lutte contre la fraude et de la gestion de l'identité. Cela vous aidera à identifier où des barrières de sécurité rigides freinent les ventes et où une threat intelligence simple et moderne peut bloquer la fraude discrètement en arrière-plan.

Instructions : cochez chaque case correspondant à votre configuration actuelle. Si vous n'êtes pas certain ou si vous savez que vous vous appuyez sur une règle statique et générale, laissez la case décochée et considérez-la comme une lacune à combler.

1. Défense contre les bots et sécurité périmétrique

- ☐ Filtrez-vous le trafic automatisé des bots et les scripts de credential stuffing à la périphérie avant qu'ils n'atteignent votre espace de connexion ou vos API ?
- ☐ Les vrais clients peuvent-ils finaliser leur achat sans être interrompus par des CAPTCHA intrusifs sous forme d'images ou d'énigmes ?
- ☐ Utilisez-vous la limitation de débit au niveau de l'edge et le filtrage basé sur la réputation des adresses IP pour bloquer automatiquement les attaques par force brute ?
- ☐ Votre protection anti-bot est-elle suffisamment intelligente pour bloquer les scripts malveillants sans ralentir les personnes effectuant des achats légitimes lors de ventes à forte demande ?

2. Sécurité des identifiants et prévention de l'usurpation de compte

- ☐ Vérifiez-vous automatiquement les mots de passe soumis par l'utilisateur par rapport à des bases de données d'identifiants compromis en temps réel afin de bloquer les connexions compromises ?
- ☐ Proposez-vous des passkeys biométriques (Touch ID, Face ID, Windows Hello) afin d'éliminer totalement la vulnérabilité liée aux mots de passe ?
- ☐ Les utilisateurs peuvent-ils réinitialiser en toute sécurité des comptes compromis sans être bloqués dans des boucles de réinitialisation par e-mail lentes et contraignantes lors du paiement ?
- ☐ Utilisez-vous des recherches par hachage cryptographique (comme la k-anonymisation) afin que les identifiants sensibles des utilisateurs ne soient jamais exposés lors des vérifications de brèches ?

3. Télémétrie des risques contextuels

- ☐ Votre système évalue-t-il les signaux contextuels (tels que l’empreinte de l’appareil, la posture du navigateur et la réputation de l’adresse IP) en moins de 50 millisecondes ?
- ☐ Pouvez-vous détecter des anomalies de déplacement impossible, comme une connexion à Chicago suivie quelques minutes plus tard d’une requête API depuis Francfort ?
- ☐ Plus de 90 % de vos utilisateurs légitimes à faible risque franchissent-ils les étapes de la connexion et de la finalisation d’achat sans aucune demande ou vérification de sécurité ?
- ☐ Les tokens de session sont-ils émis de manière silencieuse en arrière-plan une fois que le risque contextuel est confirmé comme faible ?

4. Vérification adaptative et sécurité renforcée

- ☐ Les contrôles de sécurité supplémentaires (comme l’authentification multifacteur) se déclenchent-ils uniquement lorsque le score de risque d’une session augmente réellement ?
- ☐ Les achats récurrents à faible risque effectués sur des appareils reconnus peuvent-ils être validés sans imposer d’étapes de vérification supplémentaires ?
- ☐ Réservez-vous l’authentification renforcée aux actions à haut risque, telles que la mise à jour des adresses de livraison ou l’échange de points de fidélité de grande valeur ?
- ☐ Proposez-vous des options de vérification fluides par notification push ou biométrie, plutôt que de vous reposer uniquement sur des codes à usage unique envoyés par SMS avec un délai ?

5. Refus injustifiés et gouvernance des revenus

- ☐ Vos responsables et votre équipe de gestion des risques mesurent-ils activement les taux de refus injustifiés en parallèle des métriques traditionnelles de rétrofacturation pour fraude ?
- ☐ Votre taux de refus injustifiés est-il suivi et maintenu en dessous de la moyenne de référence du secteur, fixée à 1,5 % ?
- ☐ Les clients récurrents, dont l’identité a été vérifiée, sont-ils automatiquement exemptés des contrôles antifraude renforcés en fonction de leur historique d’identité ?
- ☐ Votre système d’identité transmet-il en temps réel le contexte utilisateur et la télémétrie de risque directement en aval vers les moteurs de paiement et de détection de la fraude ?

6. Gestion des frictions propres à chaque secteur

- ☐ **Commerce de détail et e-commerce** : les personnes prêtes à acheter peuvent-elles finaliser leur achat facilement, sans être contraintes de créer un compte ou de passer par des vérifications répétitives ?
- ☐ **Streaming et médias** : les utilisateurs peuvent-ils rester connectés sur les Smart TV et les appareils mobiles sans être confrontés à des demandes de réauthentification fréquentes ?
- ☐ **Fintech et iGaming** : les utilisateurs peuvent-ils effectuer des inscriptions instantanées ou des transferts de faible montant sans être ralentis par des vérifications initiales trop lourdes ?
- ☐ **Voyages et fidélisation** : les points de fidélité client, cartes cadeaux et miles VIP sont-ils protégés contre le credential stuffing sans nuire à l’expérience quotidienne des clients ?

7. Préparation aux agents d’IA et aux transactions automatisées

- ☐ Votre architecture de sécurité peut-elle faire la différence entre des bots de scraping malveillants et des agents d’IA délégués par des clients légitimes pour leurs achats ?
- ☐ Votre système peut-il accorder à des assistants d’IA des tokens à durée de vie limitée et à périmètre d’autorisation restreint (en utilisant OAuth 2.0 Token Exchange) sans exposer les identifiants des utilisateurs ?
- ☐ Appliquez-vous des limites de dépenses granulaires et des restrictions d’actions sur les transactions d’IA automatisées ?
- ☐ Les clients peuvent-ils facilement consulter, gérer ou révoquer les autorisations accordées à leurs assistants d’achat personnels pilotés par l’IA ?

Calculer votre score

Additionnez vos cases cochées pour évaluer la situation de votre configuration client et sécurité :

24 à 28 cases cochées

Optimisé

Votre configuration bloque la fraude discrètement en arrière-plan tout en laissant le passage en caisse entièrement ouvert aux acheteurs légitimes.

16 à 23 cases cochées

Solide, mais perte de chiffre d'affaires

Vos défenses principales sont efficaces, mais des obstacles de sécurité statiques et des refus injustifiés vous font probablement perdre des ventes.

Moins de 16 cases cochées

Risque élevé pour la conversion

Des contrôles de sécurité obsolètes et une friction généralisée poussent les acheteurs vers la concurrence et pénalisent les véritables clients.

Vous voulez éliminer les obstacles lors du paiement sans augmenter les risques ?

L'évaluation de vos dispositifs de lutte contre la fraude n'est qu'un point de départ. Résoudre les refus injustifiés et les abandons de connexion n'exige pas de remplacer votre pile technologique ni de relâcher vos exigences en matière de sécurité. En évaluant discrètement le risque contextuel en arrière-plan, vous pouvez bloquer la fraude automatisée en temps réel, tout en maintenant un processus de paiement rapide et accessible aux acheteurs légitimes.

Réservez une session de cadrage de 30 minutes avec un architecte en solutions Auth0 pour examiner les résultats de votre checklist, évaluer votre configuration de sécurité actuelle et élaborer un plan sur mesure afin d'éliminer les refus injustifiés et de protéger le chiffre d'affaires.