

KLEAA

Lire en ligne

Les IA vendues à prix cassés lisaient en secret les demandes de leurs clients

Bon lundi à tous.

Moins cher, mais à quel prix ? Une enquête montre que des fournisseurs d’IA à bas coût laissaient des pirates lire les demandes de leurs clients, mots de passe compris. Signal, de son côté, bloque les captures d’écran pour tenir les assistants IA à distance de vos conversations. Et un chercheur affirme avoir résolu avec Claude une énigme mathématique vieille de 167 ans, vérifiée ligne à ligne par un logiciel.

Quelqu’un devrait lire ça ?

AU SOMMAIRE

01 Des fournisseurs d’IA à prix cassés lisaient en secret les demandes de leurs clients

02 Signal bloque les captures d’écran pour empêcher les assistants IA de lire vos conversations

03 Un chercheur d’Anthropic affirme avoir résolu avec Claude une énigme mathématique vieille de 167 ans

04 Perplexity lance un service qui surveille le web à votre place et vous prévient seulement quand quelque chose change

05 Une start-up propose aux internautes de louer leur visage pour jouer dans des séries fabriquées par IA



01

Des fournisseurs d’IA à prix cassés lisaient en secret les demandes de leurs clients

Une société de cybersécurité a piégé 2 millions de demandes envoyées à des services d’IA. Chez au moins 3 fournisseurs, des pirates copiaient tout ce que les clients écrivaient, mots de passe compris.

Pour brancher une IA dans un logiciel, beaucoup d’entreprises ne passent pas directement par OpenAI ou Anthropic. Elles passent par des intermédiaires, souvent moins chers, qui font tourner des modèles d’IA dont le code est public ou revendent l’accès à d’autres. La société américaine Dragos a voulu savoir ce que devenaient les messages envoyés à ces intermédiaires. Entre juillet et novembre, elle en a envoyé environ 2 millions, chacun contenant de faux mots de passe et des liens secrets : si quelqu’un s’en servait, c’était la preuve que le message avait été lu.

Le résultat est net. Chez au moins 3 fournisseurs, des pirates copiaient tout le trafic depuis des mois, sans que ces entreprises le sachent. Dans le pire des cas, des centaines de fausses clés d’accès au cloud d’Amazon (l’espace en ligne où les entreprises stockent fichiers et applications) ont été testées en quelques heures. Sur une place de marché, des vendeurs affichaient simplement le prix le plus bas, enregistraient les messages et se servaient. Même l’option « aucune conservation des données » était souvent ignorée. OpenRouter, une plateforme qui aiguille les demandes vers le fournisseur le moins cher, a exclu 3 fournisseurs et retiré cette garantie à 125 services.

Tout ce que l’on colle dans une IA (un contrat, un fichier client, un code d’accès) traverse chaque intermédiaire de la chaîne, et chacun peut le lire. HD Moore, directeur de la recherche de Dragos, le résume ainsi : si vous ne choisissez pas où partent vos demandes, c’est le prix le plus bas qui choisit pour vous. La règle de base reste simple : ne jamais coller un mot de passe dans une IA, et savoir précisément qui traite vos données.

Le regard KLEAA

Le réflexe « toujours moins cher » a fait le succès des services qui comparent et revendent l’accès aux IA. Cette enquête en montre le revers : quand un prix semble trop bas, ce sont

parfois vos données qui paient la différence. Pour une petite équipe, la protection la plus efficace ne coûte rien : un seul fournisseur connu, un contrat lu, et les documents sensibles réservés aux outils dont on sait où ils tournent.

Combien de vos logiciels du quotidien envoient déjà vos textes à une IA, sans que vous sachiez laquelle ?



02

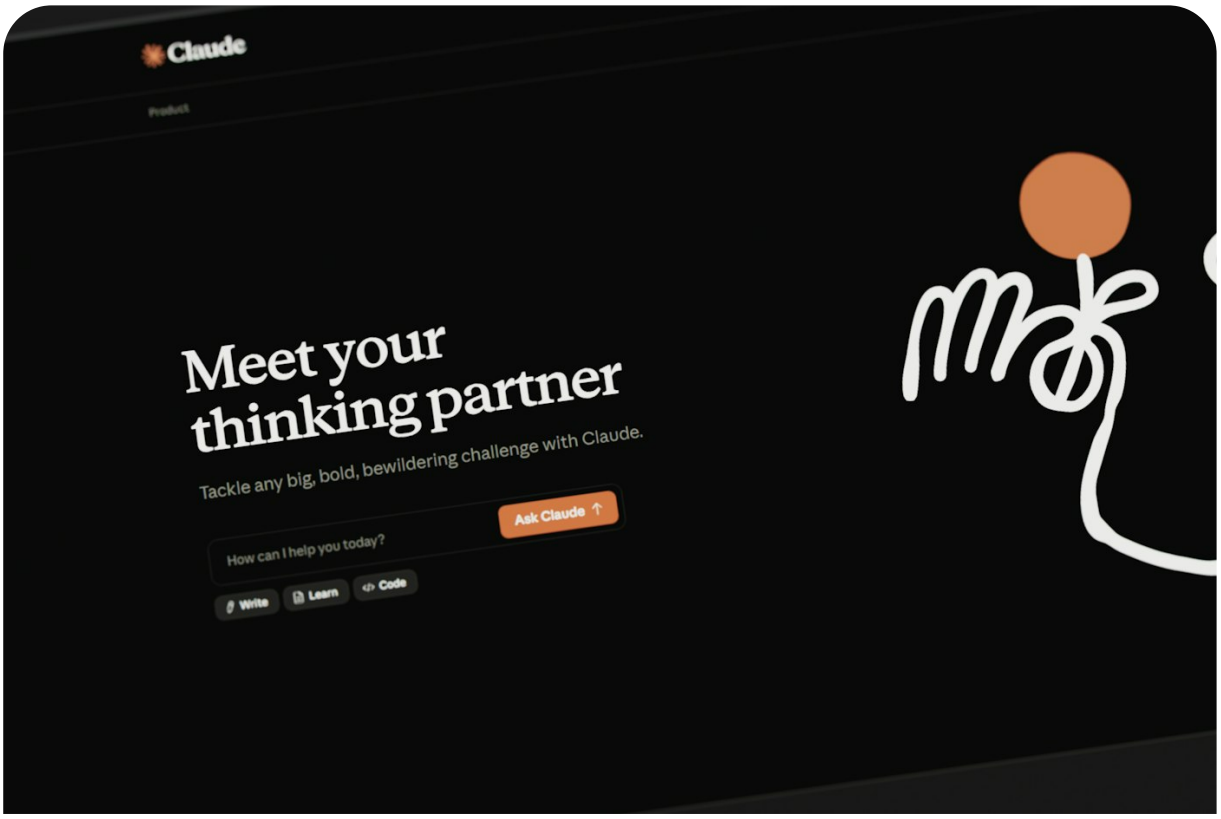
Signal bloque les captures d’écran pour empêcher les assistants IA de lire vos conversations

La messagerie Signal empêche désormais, par défaut, de faire une capture d’écran de ses conversations sur iPhone et Android. Elle accuse les assistants IA intégrés aux téléphones de pouvoir tout lire.

Signal est connue pour une promesse : personne, pas même l’entreprise, ne peut lire vos messages, car ils sont chiffrés (brouillés pour que seuls l’expéditeur et le destinataire puissent les lire). Mais cette protection s’arrête à l’écran. Les téléphones et les ordinateurs intègrent de plus en plus d’agents IA (des assistants capables d’agir seuls sur l’appareil), qui « regardent » l’écran pour vous aider. Ce qu’ils voient peut être enregistré, puis envoyé vers des serveurs distants, hors du contrôle de Signal.

Le blocage existait déjà sur Windows. Signal l’étend maintenant à iPhone et Android. L’utilisateur peut le désactiver, mais l’application prévient qu’il perd alors ses garanties de confidentialité. Sa présidente, Meredith Whittaker, parle d’une « menace existentielle » venue des systèmes des téléphones eux-mêmes, et reconnaît que la mesure reste incomplète : les agents IA disposent d’autres moyens, plus discrets, d’accéder aux données d’une application.

L’enjeu dépasse Signal. Une discussion confidentielle avec un associé, un avocat ou un client peut être lue non par un pirate, mais par l’assistant installé d’office sur le téléphone de l’un des participants. Pour les échanges sensibles, la question n’est plus seulement de choisir la bonne messagerie, mais de savoir quel assistant tourne sur l’appareil d’en face.



03

Un chercheur d'Anthropic affirme avoir résolu avec Claude une énigme mathématique vieille de 167 ans

L'hypothèse de Riemann, l'un des problèmes les plus célèbres des mathématiques, aurait été démontrée par Levent Alpöge avec l'aide de Claude. Plusieurs experts ont fait vérifier la preuve par un logiciel et la jugent correcte.

Formulée en 1859, l'hypothèse de Riemann porte sur la façon dont se répartissent les nombres premiers (ceux qui ne se divisent que par 1 et par eux-mêmes, comme 7 ou 13). Elle fait partie des 7 « problèmes du millénaire », dotés chacun d'une récompense de 1 million de dollars. Levent Alpöge, mathématicien chez Anthropic, a publié en fin de semaine dernière une démonstration réalisée avec Claude, en écrivant que l'IA l'avait « largement dépassé dans la dernière ligne droite ».

Particularité : la preuve n'est pas un article classique mais un programme de 17 millions de lignes écrit en Lean, un langage informatique qui contrôle chaque étape d'un raisonnement, comme une calculatrice vérifie une addition. Des dizaines de personnes l'ont fait tourner de leur côté, et la communauté qui entretient Lean se dit « pleinement confiante ». D'autres mathématiciens restent prudents : il faut encore s'assurer que le programme démontre bien le bon énoncé, et personne ne comprend encore vraiment ce que la preuve révèle. Une équipe de Stanford a d'ailleurs publié dans la foulée une démonstration concurrente, entièrement humaine.

Si elle est confirmée, ce serait le 2e problème du millénaire où l'IA joue un rôle décisif, après les travaux annoncés par OpenAI en septembre sur un autre de ces problèmes. L'IA ne se limite donc plus à résumer ou rédiger : elle produit un travail d'expert original. Et la méthode compte autant que le résultat, car la confiance ne vient pas de l'IA elle-même mais d'un outil de vérification indépendant. C'est la même logique à appliquer à un devis, un contrat ou un programme produits par une IA.



04

Perplexity lance un service qui surveille le web à votre place et vous prévient seulement quand quelque chose change

Perplexity, le moteur de recherche qui répond grâce à l'IA, propose des « moniteurs » : on décrit en une phrase ce que l'on veut suivre, et l'outil n'envoie une alerte que lorsqu'une nouveauté utile apparaît.

Jusqu'ici, une recherche par IA répondait à une question posée à un instant donné. Le nouveau service, baptisé Monitor, relance la recherche tout seul, de toutes les 15 minutes à une fois par semaine. Il existe en 2 versions. La première surveille un sujet sur tout le web et dans l'actualité, par exemple « les levées de fonds de mes concurrents ». La seconde suit jusqu'à 10 pages précises, comme une grille tarifaire, des conditions générales ou une page de nouveautés, et signale ce qui a changé.

La différence avec une simple alerte par mots-clés : une IA trie les résultats. Elle vérifie si l'information est nouvelle, fiable, récente et vraiment liée à l'objectif décrit, et n'envoie rien dans le cas contraire. Les doublons sont écartés d'une vérification à l'autre. Le tarif est bas : 1 dollar pour 1 000 vérifications. Lors d'un test mené par Perplexity elle-même sur 60 sujets, l'outil a trouvé 63 pages nouvelles et pertinentes en 8 heures, contre 20 pour le meilleur concurrent.

Le service vise d'abord les développeurs : il se branche à un logiciel par une API (une prise qui permet à 2 programmes d'échanger des données), et non par une appli grand public. Les usages, eux, sont très concrets : suivre les prix d'un concurrent, repérer les entreprises qui recrutent ou lèvent des fonds avant de les démarcher, être alerté d'un changement de réglementation. Une veille qui demandait des heures de lecture devient une tâche automatique, pour quelques dollars par mois.



05

Une start-up propose aux internautes de louer leur visage pour jouer dans des séries fabriquées par IA

Shortical produit des mini-séries pour téléphone entièrement générées par IA. Après un premier acteur connu, elle invite n’importe qui à lui céder les droits sur son visage, contre rémunération.

Les microdramas (des séries découpées en épisodes d’environ 2 minutes, pensées pour le téléphone) sont nés en Chine et gagnent les États-Unis. Shortical, une jeune entreprise du secteur, fabrique les siens entièrement avec l’IA : décors, scènes et acteurs sont générés par ordinateur. Son modèle : les 7 à 10 premiers épisodes sont gratuits, puis un petit abonnement mensuel débloque tout le catalogue.

Sa nouvelle série, « Inevitable », a pour vedette Aki Avni, acteur israélien vu dans la série « 24 », sous la forme d’un double numérique de lui-même. L’entreprise pousse maintenant une offre baptisée « Louez votre visage » : chacun peut proposer son compte sur les réseaux sociaux, et Shortical décide d’offrir ou non un contrat. Aucun n’a encore été signé, et la rémunération se fixe « au cas par cas ». En Chine, des sociétés similaires paient entre 15 et 700 dollars pour un visage.

Le sujet dépasse le cinéma. Le visage et la voix deviennent des biens que l’on peut céder, comme une photo ou une musique. Créateurs de contenu, formateurs, dirigeants qui se mettent en scène : tous vont devoir décider sous quelles conditions, pour combien de temps et pour quels usages une IA peut reproduire leur image. Un contrat flou aujourd’hui peut laisser circuler un double numérique pendant des années.



LE GRAND ANGLE

Juicebox trouve vos futurs salariés en lisant 800 millions de profils à votre place

États-Unis · Recrutement · Recherche de candidats

Juicebox est une start-up de San Francisco qui aide à recruter. On décrit en une phrase la personne recherchée, son IA parcourt des centaines de millions de profils en ligne, propose les meilleurs candidats, puis peut leur écrire.

Fondée par David Paffenholz et Ishan Gupta, passée par Y Combinator (le plus connu des programmes américains d'accompagnement de start-up), Juicebox a levé 30 millions de dollars auprès du fonds Sequoia en septembre 2025. Son outil vedette, PeopleGPT, revendique plus de 2 500 clients et a dépassé 10 millions de dollars de revenus annuels. Parmi ses utilisateurs : plus de 500 agences de recrutement et 66 % des 50 start-up d'IA classées p le magazine Forbes.

Au lieu de combiner des mots-clés sur LinkedIn, le recruteur écrit sa demande comme à un collègue : « une développeuse à Lyon, 5 ans d'expérience, passée par une start-up du paiement ». L'outil fouille plus de 800 millions de profils issus de plus de 30 sources (LinkedIn, GitHub, publications scientifiques, sites personnels) et renvoie une liste classée. Des agents IA (des programmes qui travaillent seuls en arrière-plan) continuent ensuite de chercher et signalent les nouveaux profils. Juicebox rédige enfin des messages personnalisés et gère les relances, un humain validant le texte avant chaque envoi.

La valeur se trouve dans le temps gagné sur la tâche la plus ingrate du recrutement : trouver les bonnes personnes avant même de les rencontrer. Le spécialiste américain des repas d'entreprise ezCater dit avoir divisé par 2 son temps de recherche de candidats. Le modèle économique est simple : un version gratuite pour essayer, puis des abonnements selon la taille de l'équipe, ce qui rend l'outil accessible à une jeune entreprise sans service RH.

Ce que vous pouvez copier : décrire par écrit, en phrases complètes, le profil idéal avant de chercher qui que ce soit. C'est ce qui rend l'outil efficace, et c'est souvent ce qui manque aux recrutements ratés. En Europe, une précaution s'impose : contacter des candidats trouvés en ligne suppose de les informer de l'usage de leurs données et de leur permettre de refuser.