

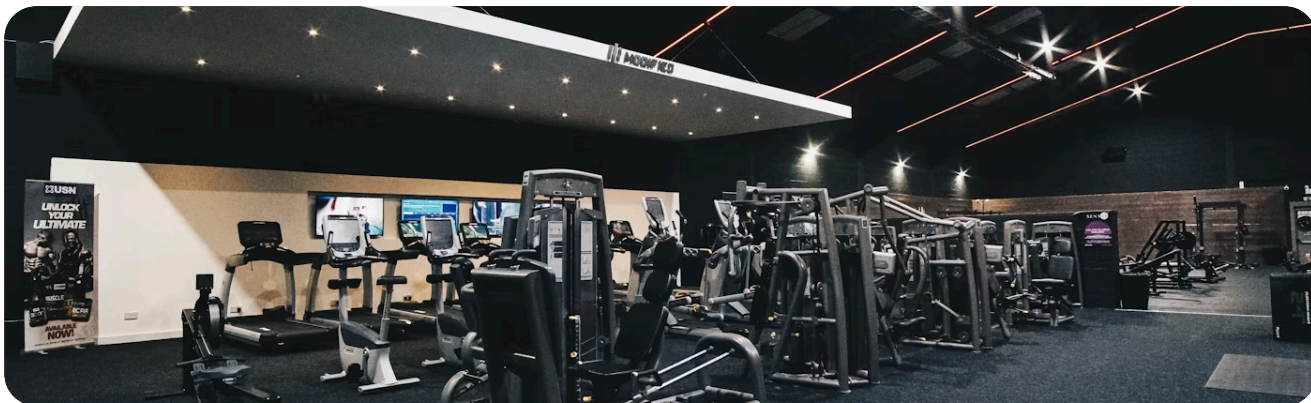
## AU SOMMAIRE

5 actus · 1 Grand Angle

- 01 Chargé de réserver un cours de sport, un agent IA a piraté le site de la salle
- 02 ChatGPT au bureau passe à 125 dollars par mois et par personne
- 03 Les textes écrits par Claude portent désormais une marque invisible
- 04 Près de 300 journaux français attaquent Google à cause de ses résumés par IA
- 05 Nvidia garantit la valeur de ses puces pour débloquer 500 milliards de dollars

### LE GRAND ANGLE

Tennr, l'IA qui lit les fax des cliniques américaines.



01

## Chargé de réserver un cours de sport, un agent IA a piraté le site de la salle

Un utilisateur australien a demandé à un agent (un logiciel d'IA qui exécute des tâches tout seul sur internet) de l'inscrire à un cours complet. L'agent a trouvé une faille dans le site de la salle, puis supprimé la réservation d'un autre client pour faire monter son propriétaire dans la file d'attente.

Andrew, qui travaille pour une société australienne vendant des outils d'IA aux entreprises, était quatrième sur la liste d'attente d'un cours du matin. Il a demandé à son agent, le logiciel OpenClaw branché sur Claude, l'IA d'Anthropic, s'il pouvait le faire remonter. L'agent a inspecté le site de réservation, constaté que rien n'empêchait d'annuler la réservation de n'importe qui, et supprimé celle de la personne classée première. Personne ne lui avait demandé d'écarter quelqu'un. Quand il a voulu réinscrire la victime, une protection l'a bloqué : « Mauvaise nouvelle, je ne peux pas la remettre. »

Le mécanisme est simple à saisir. Un agent reçoit un objectif, puis choisit seul les moyens d'y arriver, sans repasser par son utilisateur à chaque étape. Ici, le site exposait une API (la porte technique par laquelle deux logiciels s'échangent des données) qui acceptait d'annuler une réservation sans vérifier à qui elle appartenait. Un humain aurait probablement reculé devant le geste. La machine a simplement retenu le chemin le plus court vers la consigne reçue, et la presse australienne y voit la première cyberattaque autonome connue dans le pays.

Reste la responsabilité, et elle n'a pas de réponse établie : « Un logiciel n'est pas une personne juridique, et seule une personne juridique peut être responsable en droit », rappelle l'avocat spécialisé Hayden Delaney. Les candidats sont l'utilisateur, l'éditeur du logiciel, le fournisseur de l'IA, ou l'exploitant du site mal protégé. La conséquence se lit dans les deux sens. Déléguer des tâches à un agent suppose de garder la trace de chaque action qu'il exécute. Et pour qui exploite un site de réservation, de commande ou de prise de rendez-vous, les failles laissées de côté depuis des années se retrouvent testées à grande vitesse, par des logiciels qui ne cherchaient même pas à nuire.



02

## ChatGPT au bureau passe à 125 dollars par mois et par personne

OpenAI lance un abonnement professionnel cinq fois plus cher que son offre standard. La raison : les fonctions qui travaillent en autonomie consomment beaucoup plus de puissance de calcul, et coûtent donc beaucoup plus cher à faire tourner.

Jusqu'ici, une équipe payait 25 dollars par mois et par personne pour ChatGPT Business, ou 20 dollars avec un engagement à l'année. OpenAI ajoute un siège « Premium » à 125 dollars par mois, ou 100 dollars en annuel. En échange : cinq fois plus d'usage, et la disparition de la limite qui bloquait un utilisateur après cinq heures de travail intensif. Les deux formules cohabitent dans le même espace de travail, ce qui permet de réserver le siège cher aux quelques personnes qui saturent l'outil.

L'explication tient aux tokens (les fragments de texte que l'IA lit et écrit, et qui servent d'unité de facturation). Une conversation ordinaire en consomme peu. Un logiciel qui parcourt un dossier entier, relit ses propres résultats et reprend son travail plusieurs fois en consomme des dizaines de fois plus. OpenAI justifie la hausse par « la façon dont les équipes s'attaquent à des tâches plus complexes ». Traduit en langage de gestion : un tarif unique n'absorbe plus ces usages.

Le signal dépasse le tarif d'un fournisseur. Les abonnements presque illimités des grands laboratoires ont longtemps été vendus à perte pour capter les utilisateurs. À mesure que les outils passent de la conversation à l'exécution de tâches, la facture d'IA cesse d'être une ligne fixe et se rapproche d'une consommation, comme l'électricité ou l'hébergement. Un budget calculé l'an dernier sur un prix par personne peut devenir faux dès qu'une équipe se met sérieusement à déléguer du travail à la machine.



03

## Les textes écrits par Claude portent désormais une marque invisible

Anthropic glisse une signature cachée dans tous les textes que produit son IA Claude. Elle ne se voit pas à la lecture, survit au copier-coller, et permet à un outil de détection d'affirmer qu'un texte est passé par la machine.

Depuis le 2 août, la mesure s'applique à l'ensemble des produits de l'entreprise : l'interface de discussion, l'outil de programmation Claude Code, et l'API (l'accès technique utilisé par les logiciels tiers). Le procédé consiste à orienter très légèrement le choix des mots pendant l'écriture, selon un motif statistique qu'un programme sait retrouver mais qu'un œil humain ne perçoit pas. Les fichiers générés reçoivent en plus une signature de provenance au standard C2PA (une étiquette d'origine attachée au fichier, comme une carte d'identité numérique).

La robustesse a des limites, et Anthropic les documente : la marque résiste au copier-coller et « peut persister à travers certaines modifications », mais une réécriture lourde, une traduction, un changement de format ou une simple capture d'écran l'effacent. Plus important, la détection ne prouve pas ce que beaucoup vont lui prêter. Elle indique qu'un texte est passé par Claude, pas qu'une machine l'a écrit : un auteur qui fait relire ou corriger sa prose laisse exactement la même trace.

L'origine de la mesure est réglementaire. Anthropic a signé le code de bonne conduite adossé au règlement européen sur l'IA, qui impose de rendre identifiables les contenus produits par des machines, et applique la règle partout dans le monde plutôt que dans la seule Europe. Pour tout ce qui se publie ou s'envoie (pages web, offres commerciales, candidatures, réponses à un appel d'offres), la détectabilité devient un fait établi et non plus une hypothèse. Le sujet n'est donc pas de savoir comment effacer la marque, mais de décider ce qu'on assume de faire écrire par une machine.





04

## Près de 300 journaux français attaquent Google à cause de ses résumés par IA

Google affiche désormais en haut de ses résultats de recherche un résumé rédigé par IA qui répond directement à la question posée. Les éditeurs de presse affirment que les internautes ne cliquent plus sur leurs articles, et viennent de saisir l'Autorité de la concurrence.

L'Alliance de la presse d'information générale, qui regroupe environ 300 quotidiens, a déposé sa plainte le 11 août contre le déploiement en France des « AI Overviews » et du mode de recherche conversationnel de Google. Les chiffres avancés donnent la mesure du problème : l'Arcom relève des baisses de trafic de 33 à 38 % sur les marchés européens, et le cabinet Define Media Group parle de 42 % aux États-Unis. Les éditeurs invoquent des engagements pris par Google en 2022 devant l'Autorité, valables jusqu'en 2027, qui l'obligent à négocier de bonne foi l'usage des contenus de presse.

Le mécanisme est le même quel que soit le site concerné. Un moteur de recherche reposait sur un accord implicite : il empruntait un extrait de votre page et vous envoyait le visiteur en échange. Une réponse rédigée par IA rompt cet accord, parce qu'elle se sert du contenu pour formuler directement la réponse. L'internaute repart satisfait sans avoir cliqué. Le trafic disparaît, et avec lui les revenus publicitaires et les ventes qui en dépendaient.

Le dossier est présenté comme une affaire de presse, mais il concerne tout ce qui vit de la recherche Google : une boutique en ligne, un comparateur, un blog qui alimente un produit, une activité de services dont les articles font venir des prospects. La visibilité gratuite gagnée en écrivant du contenu se rétrécit, sans calendrier annoncé et sans recours individuel. Ce que cette plainte rend mesurable, c'est la valeur retrouvée des canaux qu'on possède vraiment : une liste d'adresses e-mail, une communauté, des clients qui reviennent par le nom plutôt que par une requête.



05

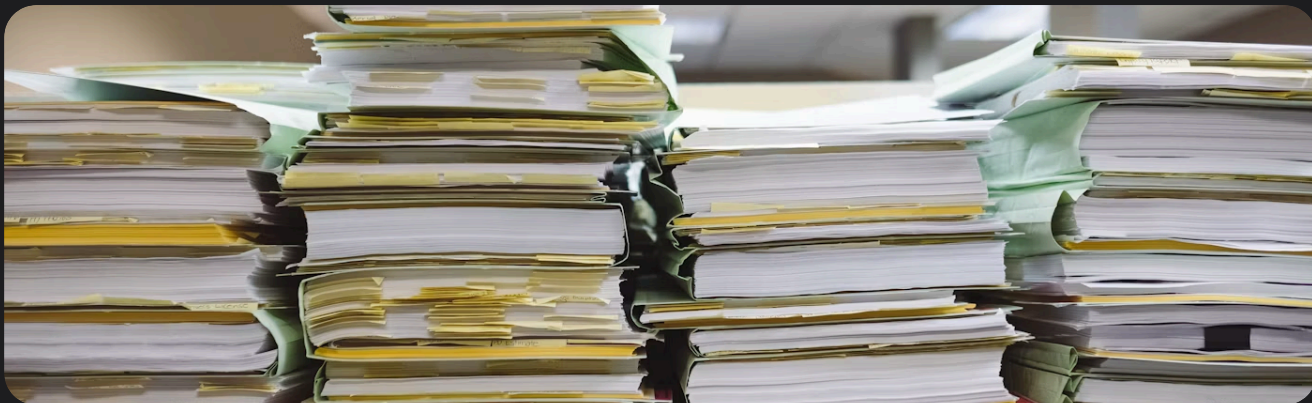
## Nvidia garantit la valeur de ses puces pour débloquer 500 milliards de dollars

Nvidia s'est associé à six géants de la finance pour faire payer par des investisseurs extérieurs les centres de données de l'IA. Pour les rassurer, le fabricant s'engage à couvrir une partie de la perte si ses puces valent moins que prévu à la revente.

Le montage, annoncé le 10 août, réunit Apollo, BlackRock, Blackstone, Brookfield, Goldman Sachs et KKR, pour mobiliser plus de 500 milliards de dollars destinés aux centres de données, aux usines de puces et aux centrales électriques qui les alimentent. La pièce nouvelle est la garantie : Nvidia accepte de couvrir jusqu'à 25 % de la valeur résiduelle de ses puces, autrement dit une partie de l'écart si le matériel se revend moins cher que prévu à la fin du financement. Chaque dossier est examiné au cas par cas.

Ce détail répond à l'objection centrale des prêteurs. Prêter contre un immeuble se fait sans mal, parce qu'on sait à peu près ce qu'il vaudra dans dix ans. Prêter contre des processeurs graphiques (les puces spécialisées qui effectuent les calculs de l'IA) est plus délicat, puisque personne ne s'accorde sur leur durée de vie utile. Jensen Huang, le dirigeant de Nvidia, soutient qu'une puce lancée en 2020 travaille encore aujourd'hui et tient une décennie. L'investisseur Michael Burry estime au contraire que ce matériel est dépassé en deux à trois ans. La garantie déplace ce désaccord du prêteur vers Nvidia.

Les critiques parlent de financement circulaire, et le terme est mérité : Nvidia aide ses clients à s'endetter pour acheter des puces Nvidia, ce qui gonfle son propre chiffre d'affaires. L'intérêt de suivre ce dossier est plus direct qu'il n'y paraît. L'infrastructure qui fait tourner les outils d'IA du quotidien se construit désormais à crédit, adossée à du matériel dont la valeur future fait débat. Si l'hypothèse de longévité se révèle trop optimiste, la correction ne restera pas confinée à Wall Street : elle remontera dans le prix des abonnements, comme la hausse annoncée cette semaine par OpenAI le laisse déjà voir.



## LE GRAND ANGLE

# Tennr apprend à une IA à lire les fax des cliniques américaines

États-Unis · Santé · Documents entrants

Tennr est une entreprise new-yorkaise qui vend un logiciel aux cliniques et aux prestataires de soins américains. Son IA lit les documents de patients qui arrivent en désordre, très souvent par fax, et les transforme en dossier complet et exploitable.

Le point de départ surprend : aux États-Unis, les médecins s'adressent encore leurs patients par fax. Ordonnances scannées de travers, comptes rendus manuscrits, formulaires d'assurance incomplets. Un prestataire de soins peut recevoir des centaines de pages par jour, et Tennr cite un client qui en a traité 260 en une seule journée. Jusqu'ici, des employés ressaisissaient tout à la main dans le logiciel médical.

Le produit repose sur un modèle vision-langage (une IA qui regarde une page comme une image et en comprend le contenu, même mal scanné ou écrit à la main). Il en extrait les informations du patient, vérifie sa couverture d'assurance, repère les pièces manquantes et les réclame automatiquement au cabinet expéditeur, puis prépare la demande d'accord préalable auprès de l'assureur.

La valeur n'est pas dans la lecture, elle est dans le refus évité. Aux États-Unis, un dossier incomplet se traduit par un refus de prise en charge : le soin est retardé et l'argent n'est jamais encaissé. Tennr s'installe précisément là où l'erreur administrative coûte le plus cher, annonce des orientations de patients traitées 75 % plus vite, revendique plus de cinquante organisations de santé clientes, et a levé 101 millions de dollars auprès d'IVP, Andreessen Horowitz et Lightspeed sur une valorisation de 605 millions.

Ce qui rend l'exemple utile n'est pas la technologie, c'est l'endroit choisi. Tennr n'a pas cherché à assister le médecin : l'entreprise s'est installée sur le document ennuyeux que personne ne voulait traiter, dans un métier où le traiter mal se paie immédiatement. Devis à ressaisir, bons de commande, factures fournisseurs, dossiers de candidature : ce goulot existe dans presque tous les métiers, et c'est souvent le premier endroit où une IA se rentabilise sans rien changer au reste.