NumSpot
Cloud. Européen. Citoyen.

Le partenaire cloud souverain et de confiance des secteurs stratégiques et sensibles

Garantir les plus hauts standards de sécurité pour assurer la protection de leurs données et celles des citoyens.

Pourquoi faire le choix d'un cloud souverain et de confiance SecNumCloud pour faire tourner ses solutions d'IA ?

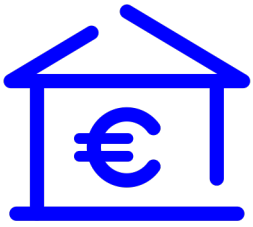
Résumé

- Pour qu'une IA soit considérée comme de confiance, elle doit assurer le respect de la vie privée, la gouvernance des données et surtout la **robustesse technique** et la **sécurité**.
- Le **cloud souverain et de confiance** répond idéalement aux exigences des pratiques à la pointe de la **cybersécurité** pour limiter la vulnérabilité, a fortiori celle induite par la généralisation des technologies de l'IA.
- Pour ce faire, le recours à un cloud offre différents **avantages essentiels** d'adaptabilité et de taille, pour faire face et répondre aux besoins des modèles d'IA, pouvant être très fluctuants.
- La **qualification SecNumCloud**, par ses différents bénéfices, répond aux plus hauts standards de cybersécurité pour permettre aux entreprises de faire notamment tourner leurs modèles d'IA sur des **données non anonymisées**.

Pour qu'une IA apporte de la valeur ajoutée dans quel que domaine qu'il soit, il est nécessaire qu'elle soit de **confiance**.

La Commission Européenne a défini 7 principes qui doivent être respectés pour qu'une IA soit considérée comme telle. Parmi ces principes, on trouve entre autres le respect de la vie privée, la gouvernance des données et aussi et surtout la **robustesse technique et la sécurité**.

Le cloud, une solution par construction à privilégier pour que les IA soient performantes, pourquoi ?



Un des leviers de performance de l'intelligence artificielle tient dans le fait que plus il y a de données d'entrainement, plus le modèle progresse et devient précis et pertinent. Et la production de données ne cesse de s'accélérer : ainsi chaque seconde, ce sont 7 mégabytes de données qui sont créées pour chaque personne, avec pour conséquence une quantité globale de données qui atteindra 181 zettaoctets en 2025 contre 2 zettaoctets en 2010.

> Le cloud, une solution élastique

Héberger et faire travailler des volumes de données considérables n'est pas ou peu compatibles avec des hébergements on-premise (hébergement des ressources en interne), d'autant plus que le travail des IA nécessite des ressources non-linéaires. Des volumes de ressources très conséquents peuvent en effet s'avérer nécessaires mais à certains moments seulement.
Par rapport au stockage de données traditionnel sur site, les environnements cloud prennent en charge d'**énormes volumes de données**, et cela **sans cloisonnement** ni **accès différé**.
Le mode on-premise n'est donc pas véritablement adapté, car il suppose de s'équiper de beaucoup de ressources qui resteront inemployées sur de longues périodes.

> Le cloud, une solution experte pour la cybersécurité

Le modèle on-premise impose beaucoup de contraintes en matière de maintien des systèmes au sens large. Le non-maintien de ses solutions d'hébergement (dernières mises à jour non implémentées...) augmente considérablement la vulnérabilité de l'hébergement. Le cloud permet de bénéficier de **ressources expertes** à la pointe des pratiques en matière de **cybersécurité** et assurent entre autres les mises à jour des systèmes à chaque nouvelle version.
Les ressources pas assez nombreuses ou expertes font souvent défaut aux organisations qui gèrent leurs ressources IT en propre, ce qui crée des vulnérabilités qui fragilisent les organisations et les exposent donc de façon plus importante aux cyberattaques.

Le cloud souverain et de confiance, un levier majeur pour la sécurité des données, pourquoi ?

Tout d'abord, il faut être conscient que la généralisation des technologies autour de l'IA va introduire de nouveaux risques de sécurité. D'une part en raison non seulement de l'augmentation de la surface d'attaque mais aussi d'autre part du fait de leurs vulnérabilités intrinsèques (attaques par empoisonnement, attaques adverses...).
Le premier défi est donc de sécuriser les intelligences artificielles, mais aussi les **données** qu'elles ingèrent et produisent.

- **Le cloud souverain et de confiance, une solution à l'état de l'art en matière de sécurité et de confidentialité des données sensibles.**

  Pour bénéficier du plein potentiel des modèles d'IA, il est indispensable de les faire tourner sur des **données non anonymisées**. Les acteurs des secteurs stratégiques et sensibles ont pour la plupart renoncé à cela pour des risques de confidentialité des données. En effet, le choix de cloud non souverain et de confiance les expose aux lois extraterritoriales et donc potentiellement à la fuite des données.

- **Le cloud souverain et de confiance SecNumCloud apporte ainsi un triple bénéfice aux organisations :**

  - Une immunité aux lois extraterritoriales
  - Le bénéfice du plus haut niveau de sécurité via la qualification SecNumCloud décerné par l'ANSSI dont les niveaux d'exigence en matière de critères de sécurité sont extrêmement élevés, preuve en est que les sociétés qui peuvent se prévaloir de l'afficher sont très peu nombreuses.
  - L'opportunité de pouvoir faire tourner les modèles sur des données non anonymisées

L'IA également un levier de sécurité pour le cloud

On l'aura compris, le choix du cloud pour faire tourner ses IA présente de très **nombreux avantages**. Il y a un autre aspect de l'IA dont on parle beaucoup moins, c'est l'IA comme **accélérateur de sécurité**.

En effet, parmi ses nombreux bénéfices, l'IA révolutionne aussi la **cybersécurité** en améliorant par exemple les capacités d'authentification, de sécurisation des données, de détection des menaces, d'analyse de code, d'orchestration, de réponse à incident etc.

L'IA peut donc se révéler un réel adjoint du RSSI en apportant par exemple une aide précieuse dans la priorisation des alertes de sécurité quotidiennes. Il n'est pas rare que le nombre de vulnérabilités quotidienne atteigne un chiffre tourant autour des 50, les outils à base d'IA permettent ainsi d'identifier celles sur lesquelles une vigilance et une analyse plus approfondies doivent être apportées.

À propos de NumSpot

NumSpot est un acteur du cloud souverain et de confiance. Né de la volonté de 4 entreprises françaises de premier plan des secteurs public et privé (Banque des Territoires, Docaposte, Dassault Systèmes et Bouygues Télécom), NumSpot propose une offre de cloud indépendant, souverain et robuste adossé au IaaS d'OUTSCALE qualifié SecNumCloud. NumSpot est un cloud réversible et transparent, basé principalement sur l'open source et des solutions européennes. L'offre NumSpot s'adresse prioritairement aux secteurs confrontés à une forte sensibilité des données (secteur public, santé, services financiers et assurance, OIV et OSE) en France et en Europe, et à la recherche d'une solution souveraine et de confiance en accord avec les règlementations RGPD et européennes. NumSpot fait ainsi le choix d'œuvrer pour l'intérêt général en proposant un véritable pacte de confiance entre un fournisseur de cloud, ses clients et les citoyens européens.

Suivez-nous @NumSpot @NumSpotCloud