



IA : la mise au point

L'infrastructure réseau indispensable pour réussir le déploiement et la monétisation de l'IA en entreprise

verizon
business

Explorez les promesses et les enjeux de l'IA en entreprise

1. **L'adoption de l'IA requiert un examen objectif de votre réseau**
2. **Résister au raz de marée** : comment gérer l'afflux massif de données IA ?
3. **Industrialiser l'immédiat** : comment concrétiser des cas d'usage IA en temps réel ?
4. **Rester aux commandes** : comment garder le contrôle à l'ère de l'IA ?
5. **Sécuriser le système** : comment se protéger dans un monde dominé par l'IA ?
6. **Checklist** : votre infrastructure réseau est-elle prête pour l'IA ?
7. **Votre plateforme pour la nouvelle ère de la connectivité d'entreprise** : Verizon Business met une expérience et une expertise inégalées au service du réseau pour en libérer tout le potentiel



L'adoption de l'IA requiert un examen objectif de votre réseau

Côté pile, la révolution de l'IA a accéléré de nombreux aspects du travail. Mais, côté face, elle a aussi fait monter la pression. Par exemple, combien de temps avez-vous pour lire cet article ? Sûrement très peu. Surtout si vous cherchez à suivre le rythme d'un secteur en rapide mutation.

Les entreprises n'ont pas autant investi dans les nouvelles technologies depuis les années 2000. Rien qu'en 2025, les leaders de la tech ont misé environ 400 milliards \$ sur l'IA¹ pour donner vie à une panoplie de nouveaux cas d'usage, des robotaxis à la détection automatisée des fraudes.

Ici, c'est un acteur majeur de l'industrie européenne qui a recours à un agent d'ingénierie pour améliorer son efficacité jusqu'à 50 %². Là, une compagnie d'assurance qui confie plus d'un million d'interactions clients chaque année à un chatbot³.

Incontestablement, l'IA suscite beaucoup d'engouement et d'optimisme. Toutefois, elle s'accompagne aussi de risques graves et de problèmes techniques à surmonter. Verizon aide les entreprises à s'adapter à cette nouvelle donne. Une expérience qui nous a permis de voir que, bien souvent, des capacités réseau et une connectivité insuffisantes constituaient des obstacles majeurs au progrès.

La plupart du temps, l'infrastructure censée permettre l'exploitation de l'IA avancée, des grands modèles de langage (LLM) et du machine learning (ML) n'est tout simplement pas à la hauteur. Malgré la définition d'une stratégie IA, rares sont les entreprises qui disposent d'un réseau capable de concrétiser leurs objectifs d'industrialisation.

C'est tout l'enjeu de ce livre blanc.

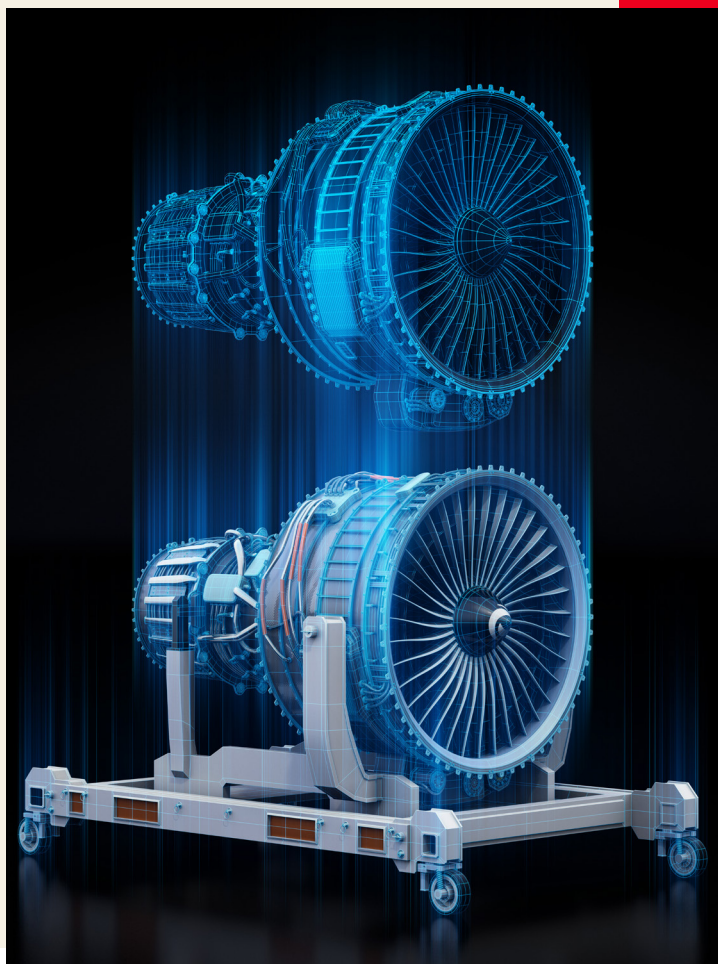
Chez Verizon, nous savons que la réussite de vos initiatives d'IA dépend de votre réseau. IA agentique en soutien de vos équipes internes, vision par ordinateur, solutions augmentées par IA pour vos clients... Quel que soit le projet, une avalanche de trafic de données vous attend. Toutes ces innovations reposent sur un réseau performant, le rouage invisible mais essentiel au succès de l'IA.

Dans cet article, nous verrons en détail les répercussions de l'IA sur différentes facettes de l'infrastructure réseau. Nous avons également dressé une checklist pour vous aider à cerner vos difficultés pour les résoudre avant qu'elles ne freinent vos ambitions. Par ailleurs, des experts vous révèlent comment les entreprises à travers le monde saisissent les opportunités offertes par l'IA.

¹The Wall Street Journal, [Big Tech's \\$400 Billion AI Spending Spree Just Got Wall Street's Blessing](#), 2025

²Siemens, [Siemens brings AI to the physical world with Eigen Engineering Agent](#), 2026

³Matthieu Caillat pour AXA Group Operations, [AI at AXA: Leading the future of insurance with responsibility and innovation](#), 2026



Résister au raz de marée

Comment gérer l'afflux massif de données IA ?

Pour vivre, l'IA a besoin de données. Sans elles, les LLM ne pourraient rien générer, les agents ne trouveraient pas et ne réaliseraient pas la suite logique d'un processus, et la personnalisation de masse resterait un procédé extrêmement lent, voire impossible. Mais aujourd'hui, nous faisons face à un véritable tsunami de données.

Vous vous demandez peut-être : « Comment absorber et traiter l'explosion de flux de données requise par les opérations pilotées par IA ? » Pour répondre à cette question, voyons comment certains acteurs du retail et de l'industrie ont réussi à exploiter les données.

Les opérations augmentées par IA sont gourmandes en données

L'IA accélère le développement de toutes sortes de processus métiers, de la production au service client et plus encore.

Les acteurs de l'industrie, par exemple, se sentent de plus en plus à l'aise et compétents vis-à-vis des jumeaux numériques boostés à l'IA, des modèles digitaux de produits ou systèmes du monde réel qui peuvent être ajustés et testés dans le cadre de simulations sans affecter la version physique. Ces outils les aident à améliorer leur business intelligence et leur maintenance prédictive, tout en réduisant les coûts et les interruptions liées à la déclaration, la conformité et la gestion des risques.



Les industriels utilisent depuis longtemps le machine learning pour mieux comprendre leur data. La nouveauté, c'est qu'avec les LLM, ils peuvent désormais interroger directement leurs propres données et obtenir une réponse. »

Christoffer Sundgren

Senior Principal – Business Strategy Manufacturing,
Verizon Business

Avec un jumeau numérique augmenté par IA, on peut ordonner à un modèle d'identifier des problèmes qui seraient imperceptibles autrement. Ce genre d'autodiagnostic par un double des équipements de production offre certes un gain de temps considérable, mais il génère aussi une demande de données colossale.

Par exemple, un fabricant automobile européen photographie les produits sur la chaîne d'assemblage avec un flux vidéo haute définition, un processus entièrement surveillé par un système IA⁴. Si cette mesure lui permet apparemment d'améliorer la qualité, elle s'accompagne néanmoins d'une surcharge de données conséquente : une heure de vidéo 4K peut nécessiter jusqu'à 45 Go de stockage.

Dans le retail aussi, l'adoption de l'IA entraîne une avalanche de données. Concrètement, certains l'utilisent pour optimiser la gestion des stocks et s'assurer que les bons produits sont mis en rayon. Mais cet équilibre est facilement menacé par les variabilités du secteur.

James Hughes, de Verizon Business, a lui-même constaté l'impact sur l'infrastructure réseau des fluctuations saisonnières et de la complexité des besoins.

Les retailers et les industriels doivent s'équiper d'un nouveau socle réseau pour prendre en charge des volumes de données colossaux tout en restant flexibles. L'entraînement des modèles propriétaires implique de provisionner une bande passante data encore plus conséquente, potentiellement, de plusieurs dizaines de gigaoctets plusieurs fois par semaine. Le tout, avec une disponibilité constante.



Il existe des milliers voire des centaines de milliers de capteurs dans une usine et toutes ces données affluent en même temps. »

Colin Wilson

Enterprise Architect, Verizon Business

Quelques heures d'interruption peuvent être tolérées lorsqu'une intervention humaine est possible. En revanche, pour les systèmes d'IA, la coupure se révélerait dévastatrice, notamment pour des opérations agentiques à vitesse machine. Les systèmes de gestion des identités et des accès (IAM) doivent rester constamment connectés pour repousser les cybermenaces dopées à l'IA.

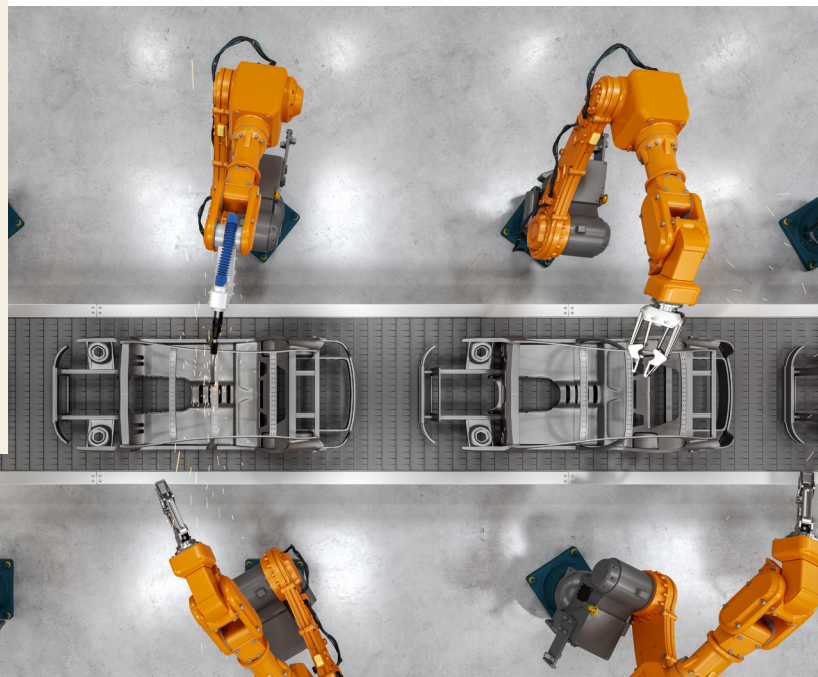
À l'heure où l'IA agentique intègre de plus en plus de workflows, ces besoins ne feront qu'augmenter.



Les outils IA ne seront pas les seuls éléments du réseau. Il y aura aussi toutes les autres applications que les retailers voudront exécuter, comme les assistants virtuels ou les outils de paiement. Et tout cela demandera de la bande passante. »

James Hughes

CTO Retail, Verizon Business



⁴ Groupe BMW, [This is how DIGITAL the BMW iFACTORY is](#), 2023

Les agents IA traitent davantage de données, de diverses manières

Outre nos modes de travail, l'IA agentique promet de révolutionner nos approches de l'infrastructure réseau. Ces systèmes intelligents pilotés par IA exécutent des workflows de bout en bout grâce à une variété d'outils et d'API. L'objectif : prendre des décisions en temps réel au service d'objectifs précis, le tout avec une intervention humaine minimale.

Pour reprendre l'expression de Christoffer Sundgren, les workflows agentiques se résument à « des machines qui communiquent entre elles ». Désormais, les entreprises combinent plusieurs agents pour construire des workflows solides et efficaces. Notons toutefois que les machines ne se parlent pas tout à fait de la même façon que nous. Elles s'envoient des informations à une vitesse fulgurante, ce qui génère d'importants volumes de trafic et encore plus de données par seconde que nous, humains, ne pourrions le faire.

Cette évolution implique de repenser notre conception des réseaux, qui ne suivent plus l'axe « nord-sud » traditionnel mais sont bien plus horizontaux. Les machines transmettant des informations aux datacenters et aux systèmes d'entreprise avant même qu'elles soient livrées, l'heure est venue d'imaginer les capacités selon un axe « est-ouest ».

Pour un fonctionnement optimal, les agents IA ont besoin d'un accès permanent aux données. Ils doivent aussi opérer au plus près de la périphérie réseau pour garantir une latence minimale. Or, cela nécessite d'augmenter

massivement les flux data, l'utilisation des tokens et la bande passante du réseau. Autre impératif : une infrastructure en mesure de sous-tendre l'accès en temps réel aux données.

Aujourd'hui, la priorité des entreprises devrait concerner le développement d'une architecture réseau capable de supporter un volume aussi colossal de données.



Les entreprises ont tout un maillage de données à un endroit, leurs utilisateurs à un autre, et des workloads ou LLM encore ailleurs, ce qui fait peser une demande colossale sur le réseau.

Colin Wilson

Enterprise Architect, Verizon Business

Auto-évaluation : votre réseau est-il scalable ?

1. Avons-nous de la visibilité sur le volume de données supplémentaire généré par nos opérations IA actuelles et futures, provenant notamment des capteurs, flux vidéos et outils agentiques ?
2. Notre infrastructure réseau peut-elle s'adapter au pic de demande et à la charge de base liés à l'exécution simultanée de plusieurs outils IA ?
3. Avons-nous mappé l'emplacement de nos données, nos utilisateurs et nos workloads IA ? Avons-nous évalué si notre réseau peut déplacer les informations efficacement entre ces points ?
4. Avons-nous une stratégie d'architecture réseau capable de prendre en charge le trafic de données est-ouest requis par les agents IA ?
5. Savons-nous bien quels équipements sont connectés et quels droits d'accès leur sont octroyés, afin de limiter notre surface d'attaque ?
6. Avons-nous tiré les leçons de la « dette technique » ? Sommes-nous certains que l'intégralité de nos appareils et systèmes sont bien contrôlés et gérés ? Cela nous permettrait, le moment venu, de les décommissionner en toute sécurité, avec l'assurance que les dispositifs critiques continueront de fonctionner.

Industrialiser l'immédiat

Comment concrétiser des cas d'usage IA en temps réel ?

L'IA évolue à une vitesse sans précédent. Elle promet des solutions instantanées et des actions en temps réel. Le problème, c'est que cette rapidité dépend entièrement du réseau sous-jacent.

Prenons l'exemple des véhicules autonomes. Les voitures sans chauffeur doivent opérer dans un univers complexe en 3D en toute sécurité. Pour cela, chacun des 40 et quelques capteurs qui permettent la conduite automatisée doivent absorber jusqu'à 50 points de données différents par milliseconde, puis prendre des décisions en temps réel⁵.

Or, ces véhicules orchestrent jusqu'à 200 capteurs différents indispensables à leur fonctionnement. Attendre simplement à un feu rouge se transforme donc en véritable épreuve de calcul intensif. Ils n'ont pas le temps d'échanger des signaux avec le cloud. Le raisonnement doit avoir lieu au niveau du véhicule lui-même, directement à la périphérie.

Dans la finance, l'IA en temps réel sert à détecter la fraude dès qu'elle est commise afin de contrer la menace grandissante du clonage de voix et des attaques de phishing dopées à l'IA. Les modèles peuvent être entraînés à identifier en continu activités suspectes et risques, en s'appuyant sur une reconnaissance avancée des schémas et une scalabilité élevée. Le but : détecter ce qui échappe à la vigilance humaine⁶.

Certains retailers vont même jusqu'à mettre cette technologie au service des clients, leur offrant la possibilité d'essayer des articles virtuellement depuis chez eux, avec leur appareil mobile. Cependant, comme l'explique James Hughes, cette fonctionnalité peut peser lourd sur le réseau.



La majorité de cette activité retail sera consommée sur un appareil mobile et pilotée, voire générée par IA. Mais ces appareils doivent se connecter à l'environnement retail. Il faut une infrastructure suffisamment robuste et une priorisation des applications optimisée

pour assurer cette fonctionnalité. De plus, les workloads doivent être réalisés d'une manière spécifique pour servir l'IA en temps réel. »

James Hughes
CTO Retail, Verizon Business

La course à l'IA a déjà commencé. Or, cette technologie s'accompagne de défis et d'opportunités, auxquels les entreprises doivent se préparer.

⁵ Automotive World, Le moteur caché des voitures autonomes : les données chronologiques et l'IA, 2024

⁶ IBM, Détection de la fraude bancaire par IA, 2025



Pourquoi certaines applications IA doivent rester à la périphérie

Pour chacun de ces cas d'usage, l'IA doit opérer au cœur même de l'action. Autrement dit, une architecture cloud ne conviendrait pas ici, les utilisateurs ne pouvant simplement pas attendre que les informations fassent un aller-retour vers un datacenter distant.

Un réseau compatible avec l'Edge Computing pourrait servir de trait d'union entre de simples requêtes adressées aux LLM et des opérations entièrement automatisées.

Christoffer Sundgren de Verizon Business aide les industriels à construire des réseaux pensés pour ces

nouveaux enjeux. Il souligne que les industriels voulant adopter l'IA en temps réel ont besoin d'un réseau à faible latence, de même que des liaisons montantes cloud traditionnelles pour l'entraînement et la mise à jour des modèles.

En outre, la disponibilité reste essentielle : la défaillance d'un simple composant ne doit ni ralentir les opérations ni compromettre la sécurité. L'Edge AI doit aider à limiter ce risque en dispersant le traitement des données, de sorte que le dysfonctionnement d'un maillon de la chaîne n'entraîne pas l'arrêt total des activités.

Auto-évaluation : votre réseau prend-il en charge les applications en temps réel ?

1. Parmi nos cas d'usage IA, lesquels nécessitent des réponses en temps réel ? Une forte latence pourrait-elle les rendre irréalisables ou dangereux ?
2. En cas de panne d'un composant, quel est le degré de résilience de notre infrastructure réseau ? Pourrions-nous assurer la continuité de nos opérations IA sans danger ?
3. Quels seraient nos délais de reprise potentiels en cas de composant défaillant ?
4. L'infrastructure priorise-t-elle nos applications et nos workloads de manière à garantir les performances en temps réel, en particulier sur les équipements utilisateurs ou mobiles ?



Rester aux commandes

Comment garder le contrôle à l'ère de l'IA ?



Imaginons que l'on construise un modèle pour la recherche pharmaceutique. On ne voudra pas partager ces données avec n'importe qui. Il faudra absolument les

sécuriser, même si l'on veut exploiter toute l'intelligence de l'IA. »

Colin Wilson

Enterprise Architect, Verizon Business

Quel que soit le secteur, les entreprises ont besoin de visibilité et de contrôles robustes sur leurs données. C'est un fait qu'il est bon de répéter, surtout dans un monde où l'on confie de plus en plus d'informations sensibles aux outils IA. Toutefois, sans contrôle des accès, les entreprises voient non seulement leur compétitivité menacée, mais elles risquent aussi d'enfreindre les réglementations sur la protection des données.

Autre sujet émergent à l'ère de l'IA : la souveraineté. Contrairement à ce que l'on pourrait croire, l'emplacement physique des datacenters est le critère le moins important, selon Satya Nadella, CEO de Microsoft. Pour lui, c'est plutôt le contrôle sur les modèles entraînés sur les données propriétaires qui détermine la « souveraineté IA d'entreprise »⁸.

Le Forum économique mondial propose une autre définition, qui s'applique aux entreprises, même si elle

concerne d'abord les ambitions gouvernementales : « La capacité des économies à façonner, déployer et gouverner les écosystèmes IA dans le respect de leurs propres valeurs, tout en assurant un contrôle, une flexibilité et, in fine, une résilience à la fois stratégique et opérationnelle »⁷.

La souveraineté de l'IA porte sur l'intégralité de la stack, ce qui recouvre aussi bien l'infrastructure, avec les GPU et les réseaux électriques, que la gouvernance, notamment sous forme de cadres juridiques et éthiques. Ainsi, si un État (ou, à moindre échelle, une entreprise) conserve le contrôle opérationnel total de cette stack, alors il sera pleinement souverain de son IA.

Dans ce nouveau monde, le contrôle et la transparence sur les droits de propriété des données sont indispensables pour rester dans la course.

⁷ Contrôleur européen de la protection des données, [TechDispatch #2/2023 - Intelligence artificielle explicable](#), 2024

⁸ The Register, Microsoft CEO: AI sovereignty isn't where it runs, it's who controls it, 2026

Les modèles propriétaires, une réponse à l'inquiétude autour des données

Pour les entreprises réticentes à l'idée de partager des informations avec des LLM publics, la solution la plus évidente est de construire leurs propres modèles.

Dans tous les secteurs, les programmeurs et les équipes IT sont désormais capables de concevoir eux-mêmes des modèles efficaces dans des systèmes isolés. Certaines structures préfèrent utiliser des forks de LLM publics, avec des contrats interdisant la fuite d'informations en dehors des cloisons prévues ou l'entraînement du modèle parent sur celles-ci. D'autres exécutent des outils IA intégralement dans des réseaux locaux, sans la moindre ouverture vers l'extérieur susceptible de faciliter une fuite de données.

Ce contrôle total présente notamment un avantage : le modèle d'IA peut être entraîné sur des informations

d'entreprise et ajusté pour répondre à des besoins précis. Si les vastes jeux de données de LLM grand public, comme ChatGPT ou Claude, s'avèrent pratiques au quotidien, certaines activités nécessitent des connaissances et une expertise qui échappent à ces outils.

Évidemment, l'exploitation et l'entraînement de ces modèles consomment un volume colossal de données. Superposés aux activités réseau habituelles, ils mettraient à rude épreuve les infrastructures même les mieux préparées.

Pour toute entreprise cherchant à développer une IA isolée ou à l'intégrer à ses workflows, il est donc crucial d'évaluer l'adéquation de l'infrastructure réseau et d'investir dans sa modernisation, si nécessaire.



Auto-évaluation : maîtrisez-vous (vraiment) vos données ?

1. Notre infrastructure réseau peut-elle absorber la charge générée par l'exécution et l'entraînement d'un modèle IA propriétaire ou isolé en plus des opérations actuelles ?
2. Avons-nous mis en place des contrôles réseau, comme les environnements protégés par air-gap ou la connectivité privée, pour conserver les données sensibles dans les limites approuvées ?
3. Comment protégeons-nous les données en transit entre les nœuds de calcul distribués ?
4. Comment maintenons-nous une latence suffisamment faible pour éviter les réacheminements susceptibles d'envoyer les données dans des territoires qui échappent à notre souveraineté ?
5. Notre infrastructure peut-elle appliquer les critères de souveraineté et s'assurer que les données sont traitées et stockées uniquement dans les bonnes régions ?
6. En cas de compromission d'une partie du réseau, disposons-nous des mécanismes de contrôle appropriés pour bloquer les accès non autorisés à nos systèmes IA et aux données qu'ils exploitent ?
7. Comment restons-nous en conformité avec des réglementations comme le RGPD ou la loi européenne sur l'IA ?

Sécuriser le système

Comment se protéger dans un monde dominé par l'IA ?



Les LLM et les agents IA constituent des outils redoutablement efficaces pour automatiser de nombreuses tâches. Mais leur fonctionnement même étend la surface d'attaque : ils sollicitent des données de réseaux externes et les transfèrent de machine en machine. Plus que jamais, la sécurisation de l'entreprise constitue donc une priorité absolue.

Et pour cause, les agents IA bénéficient d'une autonomie croissante qui leur permet de réaliser des appels d'API, d'interroger les bases de données et même d'exécuter du code. Imaginons qu'un attaquant parvienne à manipuler l'IA

pour la forcer à effectuer des actions malveillantes malgré ses garde-fous (prompt injection). Les conséquences seraient catastrophiques, en particulier dans la finance ou la logistique.

La malveillance n'est pas toujours en cause. Lorsque des collaborateurs expérimentent avec des agents interconnectés et des solutions d'automatisation, ces outils peuvent adopter des comportements imprévisibles, voire préjudiciables. D'où la nécessité de mettre en place de strictes mesures de surveillance et de réduction des risques à chaque étape pour éviter ces dérives.

Garder la main sur les données sensibles est une lourde responsabilité

En matière de sécurité, toute entreprise doit se poser un certain nombre de questions fondamentales :

- Les données clients et de paiement sont-elles totalement à l'abri d'une compromission ?
- Sommes-nous en conformité avec les lois internationales sur le respect de la vie privée ?
- Resterons-nous en conformité et en sécurité si l'IA est exécutée indépendamment sur nos réseaux ?
- Si ce n'est pas le cas, comment pouvons-nous renforcer sa sécurisation et son contrôle ?

Colin Wilson suggère aussi de se demander : « Mes données ont-elles été compromises et envoyées là où elles ne devraient pas être ? Les acteurs cyber peuvent-ils y accéder ? »

« Comment veillons-nous à ce que les données envoyées ne soient pas interceptées et remplacées par des informations fausses, biaisées ou malintentionnées ? »

Si la sécurité de l'IA agentique n'en est qu'à ses balbutiements, il ne fait quasiment aucun doute que la visibilité et les contrôles réseau constituent la première ligne de défense qui alertera les systèmes supérieurs en cas de menace éventuelle.

Le réseau voit tout. Ce moteur invisible qui carbure aux données propulse les processus essentiels. Sa surveillance devrait donc figurer au cœur de toute stratégie de sécurité IA, afin d'identifier et de neutraliser les comportements inhabituels.

La sécurité réseau à l'ère de l'IA repose sur trois piliers incontournables :

- **Le SASE**, ou Secure Access Service Edge, offre aux clients et collaborateurs diverses options d'accès au réseau d'entreprise (sans fil et haut débit inclus) pour se connecter en toute sécurité où qu'ils soient dans le WAN.
- **Les politiques Zero Trust** reposent sur un simple postulat : on ne peut et ne doit faire confiance à aucun utilisateur ni appareil, à l'intérieur comme à l'extérieur du périmètre réseau.

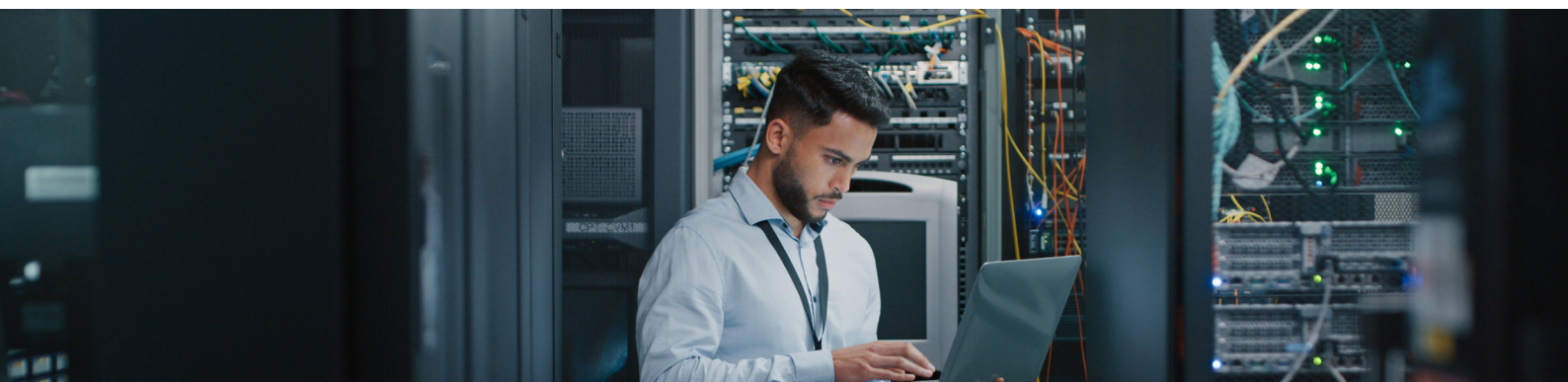
- **La visibilité** occupera une place de plus en plus cruciale à mesure que les réglementations imposeront des systèmes d'IA explicables et transparents.



On ne résout pas les problèmes de sécurité avec une boîte noire, mais avec une culture de la sécurité solidement ancrée dans l'entreprise. La difficulté avec l'IA, c'est qu'il n'y a personne. Cette culture doit donc être pleinement intégrée aux principes organisationnels ou aux modèles, dès la conception. »

Colin Wilson

Enterprise Architect, Verizon Business



Auto-évaluation : votre réseau est-il sécurisé ?

1. L'infrastructure réseau prend-elle en charge le chiffrement en transit ? Pouvons-nous garantir qu'il est impossible d'intercepter ou de manipuler les données pendant leur transfert ?
2. Disposons-nous de l'architecture adéquate pour contrôler et surveiller les flux de données et veiller à ce qu'ils ne passent que par des juridictions qui respectent nos obligations de conformité ?
3. Notre sécurité repose-t-elle sur des principes Zero Trust empêchant tout appareil, utilisateur ou agent IA d'accéder au réseau sans autorisation, et ce, à chaque étape ?
4. Notre réseau nous offre-t-il une visibilité complète sur les flux de données au sein de notre infrastructure, permettant de détecter et de signaler en temps réel toute activité inhabituelle ou non autorisée ?
5. Connaissons-nous toutes les capacités de chaque agent que nous construisons/ exécutons ? À quelles données peut-il accéder ? Où vont les résultats ?
6. Les interactions (internes et externes) entre systèmes agentiques sont-elles modélisées et mappées ? Sommes-nous certains de comprendre les limites des capacités et les risques ?



Le moteur invisible de l'IA

La bonne infrastructure réseau concrétise vos projets d'IA

La réussite d'une initiative IA repose sur un réseau robuste, sécurisé et ultra-performant. À l'ère de l'IA, une bande passante évolutive et une latence extrêmement faible sont indispensables aux infrastructures réseau et de connectivité.

Traditionnellement, l'infrastructure réseau est perçue comme un coût, surtout avec l'augmentation des volumes de données. Pourtant, elle constitue un véritable levier stratégique. L'innovation IA peut ainsi être monétisée, à condition que les charges critiques ne perturbent pas les opérations courantes.

Mais avant de pouvoir en récolter les fruits, il faut s'assurer que le réseau 1) peut absorber la surcharge de données gourmandes en bande passante ; et 2) a une latence assez faible pour répondre rapidement aux besoins de service et de sécurité.

« On ne peut pas déployer un outil de 2026, tel qu'un jumeau numérique, sur une infrastructure réseau de 2005 », explique Christoffer Sundgren.

Et Colin Wilson d'ajouter : « Il faut se demander comment dimensionner le réseau pour supporter toutes ces données qu'on ne peut pas encore exploiter aujourd'hui, mais qu'on voudra utiliser demain ».

Pour vous aider à déterminer vos besoins réseau actuels et futurs, nous avons mis au point une checklist conçue pour les entreprises de toutes tailles et de tous secteurs. Elle met en évidence les implications des initiatives IA pour le réseau et vous guide dans la conception d'une infrastructure à la hauteur des enjeux.

Checklist de préparation du réseau

Votre infrastructure est-elle prête pour l'IA ?

Besoin métier	Besoin IA	Impact réseau
Opérer à vitesse machine	L'IA interagit avec d'autres systèmes. Elle doit donc opérer rapidement pour réagir en temps réel.	Une latence extrêmement faible pour les communications réseau relève de l'impératif absolu.
Assurer des opérations synchrones en temps réel	Certaines opérations automatisées, comme les véhicules autonomes, requièrent des données synchronisées en temps réel.	Les échanges de données synchrones doivent avoir lieu en périphérie du réseau.
Gérer la croissance exponentielle des données	Les outils IA émergents entraînent une augmentation massive des flux de données et de l'utilisation de jetons.	Une augmentation de la bande passante globale et des capacités est nécessaire pour y faire face.
Unifier les workflows internes	Par nature, les interactions agentiques impliquent par nature des communications entre les systèmes au sein du datacenter.	Le trafic agentique connaît une transformation majeure, passant d'un axe « nord-sud » à « est-ouest ».
Garantir une cybersécurité robuste	Les outils IA élargissent considérablement la surface d'attaque, ce qui nécessite des capacités avancées de détection des menaces.	Les solutions de cybersécurité doivent fonctionner à vitesse machine pour détecter et neutraliser les menaces.
Assurer la continuité des tâches et du contexte	Les outils IA actuels requièrent un accès constant aux données en mémoire pour maintenir le contexte, apprendre et assurer la continuité des tâches exécutées.	Ils ont besoin d'un accès fiable et rapide à une mémoire et un stockage distribués.
Permettre l'IA explicable	Les réglementations de l'UE exigent que les données IA en sortie soient prouvées et explicables, ce qui implique de rendre transparentes les parois de la boîte noire.	Les réseaux devront pouvoir absorber le trafic supplémentaire et sécuriser le stockage des données attribuables dans un souci de conformité.
Maintenir la souveraineté de l'IA	La confidentialité des données, l'alignement éthique et la prévention des fuites de données propriétaires passent par la gouvernance et le contrôle complets de l'utilisation de l'IA.	Des environnements réseau sécurisés et isolés, une IAM robuste et de nouveaux protocoles d'authentification des agents sont nécessaires.
Optimiser les performances	Pour garantir une latence ultra-faible et un accès continu à la mémoire, un déploiement optimal des outils IA s'impose.	Votre réseau doit rapprocher les agents IA et leurs données des points de décision, en périphérie.



Votre plateforme pour la nouvelle ère de la connectivité d'entreprise

Verizon Business met une expérience et une expertise inégalées au service du réseau pour en libérer tout le potentiel

À l'heure où les projets pilotes IA entrent en production, le réseau doit enfin être considéré comme un levier stratégique, et non plus comme un simple poste de dépense.

Pour réussir dans ce nouveau monde, il ne suffit pas d'avoir les meilleurs modèles ou le plus grand jeu de données. La clé ? Une infrastructure capable de transférer les données de manière fiable, sécurisée et rapide vers tous les emplacements, clouds, appareils, capteurs et utilisateurs.

Et pourtant, l'infrastructure reste bien souvent la difficulté numéro un qui empêche les dirigeants d'industrialiser véritablement l'IA. Construits en silos, les environnements d'ancienne génération n'étaient pas pensés pour répondre aux besoins des workloads IA d'aujourd'hui, et encore moins de demain.

Selon les prédictions, la demande en bande passante devrait être multipliée par dix d'ici 2030, notamment sous l'effet de l'IA agentique. Le réseau doit être prêt.

Votre partenaire réseau Tier-1 mondial

Chez Verizon Business, nous sommes mieux placés que quiconque pour vous accompagner face à ces enjeux. Fournisseur Tier-1 dans 180 pays, nous apportons l'étendue, la résilience et les performances exigées par l'IA, de l'usine jusqu'à la périphérie du cloud. En interne

aussi, nous mobilisons l'IA sur plusieurs fronts : optimisation prédictive des réseaux, insights en temps réel pour le service client et prise de décision basée sur les données. Cette approche nous confère une expertise opérationnelle de l'IA, au-delà des seuls concepts théoriques.



Un réseau unique à votre disposition

Aujourd'hui, la plupart des entreprises jonglent avec des dizaines de fournisseurs, de contrats et de réseaux répartis dans plusieurs régions. Une gestion particulièrement ardue, qui les empêche de libérer le véritable potentiel de l'IA.

C'est là que Verizon Business Network as a Service (NaaS) intervient. Connectivité mondiale, liaisons cloud, SASE géré, réseau WAN pensé pour l'IA, sécurité intégrée, conseil, gestion de la DEX... Notre plateforme cloud-first software-defined, entièrement pilotée par Verizon Business, change la donne.

Un seul contrat. Un seul partenaire. Une seule plateforme.

Résilience, Zero Trust, efficacité, visibilité, préparation à l'IA – tels sont les maîtres mots de ce service offrant performances et sécurité uniformes à chaque utilisateur, application et site.

Notre expertise mise à votre service

Nous gérons et déployons des solutions réseau à travers le monde depuis plusieurs décennies, mais nous savons aujourd'hui que l'infrastructure ne fait pas tout. L'important est d'être le partenaire qui vous aide à surmonter les obstacles.

Le potentiel de l'IA est à portée de main. Avec Verizon, votre réseau, ce rouage aussi invisible qu'incontournable, sera prêt.

