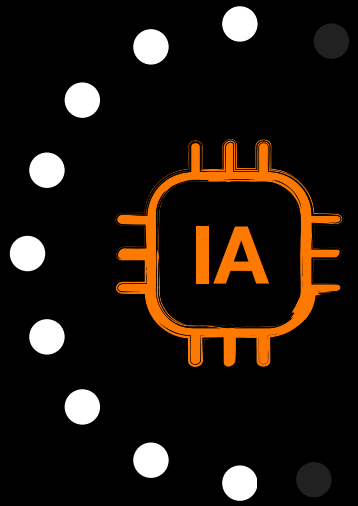
Business

Livre blanc

Réseaux, IA et souveraineté : moderniser pour rester compétitif

En 2025, les réseaux d'entreprise ne sont plus de simples canaux de données : ils deviennent essentiels à la survie des organisations. L'intelligence artificielle (IA) transforme les opérations et fait exploser les besoins réseaux.



Selon les prévisions :

+ 50% du trafic de données en entreprise sera lié à l'IA d'ici 2026, contre 15% en 2021.

En 2025, le trafic IA devrait atteindre 39 exaoctets, puis doubler l'année suivante.

source : AI Network Traffic Forecast, 2022–30, Omdia

Face à ces volumes massifs et souvent imprévisibles, les entreprises françaises — industrielles comme de services — doivent garantir sécurité, faible latence et résilience.

Pourtant, la préparation fait défaut, seulement :

49%

des organisations estiment leurs réseaux de centres de données prêts pour l'IA.

Et la préparation du réseau étendu est encore moindre. En France, une croissance économique faible (0,6% prévue en 2025), une dette élevée et des mesures d'austérité compliquent les arbitrages d'investissement. Les dirigeants se retrouvent donc devant un choix difficile : retarder les mises à niveau, au risque d'obsolescence, ou investir pour sécuriser l'avenir. source : EMA AI Networking Survey 2025

Les défis de la transformation des réseaux

La modernisation est complexe, particulièrement pour les entreprises françaises qui reposent encore sur des architectures MPLS* ou VPN traditionnelles. Parmi les principaux obstacles :

- Intégration : migrer vers de nouvelles architectures comporte des risques d'interruption difficiles à accepter dans des environnements critiques. Des contrats existants, souvent de longue durée, rendent le changement risqué.

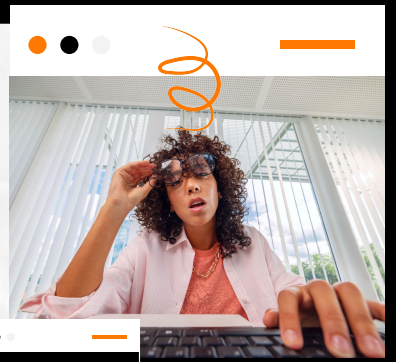
- Pressions économiques : dans un contexte budgétaire contraint, les coûts initiaux du SD-WAN sont un frein, notamment face à une forte concurrence sur les prix.

*__MPLS :__ Multiprotocol Label Switching

- Barrières à l'engagement : inertie organisationnelle, scepticisme, crainte d'enfermement fournisseur et courbe d'apprentissage ralentissent l'adoption.
Le besoin de support local ou d'une portée mondiale est soulevé, tandis que la pression tarifaire reste forte.

Ces enjeux s'ajoutent aux impératifs de conformité **(RGPD)*** et à la gestion d'équipes hybrides, plaçant les responsables techniques dans une position délicate.

*RGPD : Règlement général sur la protection des données



Chapitre 1

SD-WAN : une réponse clé pour supporter l'IA générative

L'IA générative sollicite fortement les réseaux : analyses en temps réel, volumes distribués et exigences de latence faible imposent une connectivité rapide, fiable et sécurisée. Aujourd'hui, moins de la moitié des organisations disposent d'une infrastructure adaptée pour soutenir les déploiements de **GenAI*.** Le **SD-WAN*** apparaît comme une solution-clé : il constitue une surcouche logicielle qui oriente intelligemment le trafic entre liens publics et privés, optimisant coûts, performances et sécurité.

***GenAI :** l'IA générative
***SD-WAN :** Software-Defined Wide Area Network.

Quelques éléments contextuels :

78% des organisations utilisent l'IA dans au moins une fonction métier contre 55% en 2023.

source : McKinsey Global Survey on AI, 2025

Une enquête montre que :

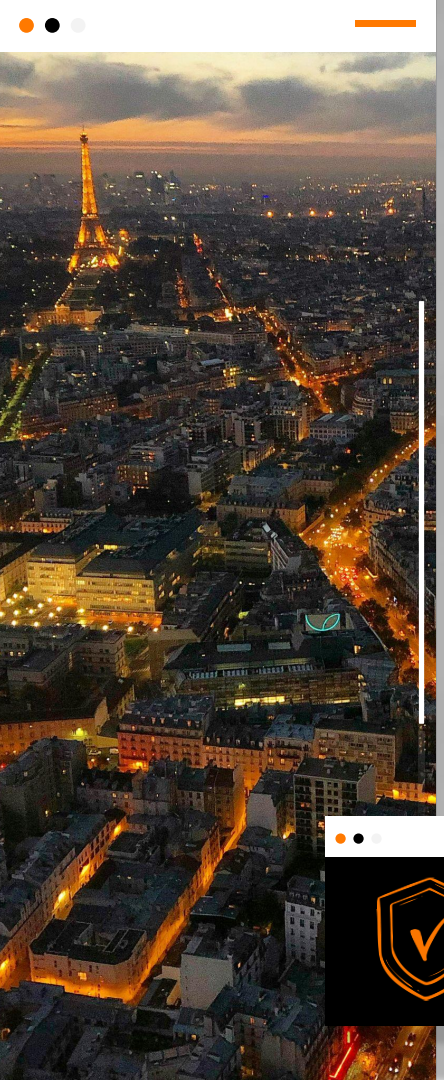
84%

des dirigeants considèrent la cybersécurité comme priorité pour les usages d'IA générative et …

96%

estiment devoir réévaluer leur posture de cybersécurité face à ces nouveaux usages

source : IBM Institute for Business Value



En France, le SD-WAN dépasse le cadre d'un simple confort opérationnel : **il est une assurance de viabilité.**

Dans l'industrie, il sécurise l'IoT en usine pour surveiller les chaînes de production et prévenir les pannes ; dans les services, il optimise les insights clients pilotés par l'IA comme dans les banques où il facilite l'analyse en temps réel des données clients pour personnaliser les offres ; dans les universités et écoles en ligne, il soutient les campus connectés pour supporter des milliers d'utilisateurs simultanés.

Retarder son adoption peut coûter cher : des inefficacités ou des failles peuvent faire monter les coûts à long terme jusqu'à 50 % de plus. Le marché européen du SD-WAN managé atteindra 1,40 milliard d'euros en 2025, avec une croissance annuelle de 24,7% jusqu'en 2030*.

source : Mordor Intelligence

Pourquoi le SD-WAN change la donne ?

Les réseaux traditionnels, rigides et coûteux, peinent à absorber les flux massifs générés par l'IA, entraînant pics de latence et vulnérabilités. Le SD-WAN apporte des réponses concrètes :

Optimisation dynamique : il priorise les flux IA critiques (entraînement de modèles, inférence en temps réel), réduisant la latence de 30 à 50% par rapport aux réseaux MPLS classiques, tout en combinant la fiabilité du MPLS et l'accessibilité d'Internet pour multiplier la bande passante disponible sans surcoût.

Sécurité intégrée : via des politiques zero-trust et une segmentation fine, il protège contre les menaces accrues par l'IA (deepfakes, attaques automatisées). Associé à SASE, il renforce la protection des données en transit.

Visibilité centralisée : une gestion centralisée simplifie l'exploitation multi-sites, essentielle pour les industriels exportateurs.

Le SD-WAN offre la flexibilité nécessaire pour accéder aux données, qu'elles résident dans des clouds publics, privés ou à l'Edge. Avec une adoption généralisée d'architectures hybrides en Europe, il orchestre les connexions entre AWS, Azure, Google Cloud, clouds privés et environnements edge, garantissant des performances optimales pour les workloads IA. Sa scalabilité permet d'ajouter sites ou clouds en quelques clics, sans investissements matériels lourds.

80%

des entreprises européennes adoptant des architectures hybrides

Source : EdgeDelta, 2024

L'intégration de l'IA dans le SD-WAN permet également d'automatiser des configurations orientées business et d'optimiser les connexions hybrides (on-site et cloud).

Un cas d'usage Orange Business : une grande entreprise industrielle a réduit de 40% ses temps de déploiement IA en connectant ses usines et son datacenter cloud via SD-WAN, améliorant ses prévisions logistiques en temps réel.

Dans un monde marqué par l'incertitude économique, les cybermenaces et les tensions géopolitiques, le SD-WAN n'est pas seulement une évolution technologique, c'est un levier stratégique pour transformer l'IA en un avantage compétitif. En garantissant **performance**, **sécurité**, **résilience** et **efficacité économique**, il répond directement aux priorités de modernisation des réseaux des entreprises françaises.

< Retour

Thomas Sourdon note l'usage actif d'API publiques pour progresser vers un réseau « basé sur l'intention », où IA, **ML*** et orchestration configurent le réseau selon des objectifs commerciaux.

ML* : Machine Learning

Thomas Sourdon

« En parallèle, nous exploitons activement des API publiques pour progresser vers l'objectif d'un réseau basé sur l'intention. Cela permettra à terme aux équipes réseau d'utiliser l'IA, le machine learning et l'orchestration réseau pour configurer les réseaux en fonction des objectifs commerciaux. »

>>

Source : Orange Business, 2024

Chapitre 2

SASE et IA : Duo indispensable pour la sécurité et résilience

Les modèles d'IA consomment des flux massifs distribués entre clouds publics, environnements on-premise, API tierces et objets connectés. Cette distribution accroît les vulnérabilités, les coûts et l'impact des incidents : le coût moyen d'une violation de données approche plusieurs millions de dollars, et les attaques visant les infrastructures critiques ont augmenté.

+20%

d'attaques cyber en 2024 selon l'ANSSI… et la tendance ne faiblit pas en 2025.

source : ANSSI

10,5 billions de dollars

c'est ce que le cybercrime pourrait coûter au monde en 2025.

source : Cybersecurity Ventures, édition 2025

Dans ce contexte, la sécurité ne peut rester un artefact ajouté après coup ; elle doit être intégrée à l'architecture réseau.
Il faut un modèle cloud-native, distribué et identitaire : SASE.

SASE : (Secure Access Service Edge), l'ossature d'une connectivité sécurisée

John Kindervag (créateur du Zero Trust) a décrit **SASE** comme « l'évolution pratique du Zero Trust, sécurisant chaque extrémité dans un monde piloté par l'IA ». Anupam Upadhyaya, vice-président Prisma SASE chez Palo Alto Networks « Le SASE basé sur l'IA permet une gestion autonome du réseau, grâce à des analyses prédictives et à l'identification et au traitement proactifs des problèmes potentiels avant qu'ils n'affectent les performances. »

source : Mordor Intelligence

Le SASE combine réseau et sécurité dans une plateforme cloud-native : SD-WAN, SWG (secure web gateway), FWaaS (firewall as a service) et ZTNA (zero trust network access). L'objectif est d'offrir une expérience homogène pour tous les usages (utilisateurs, sites, IoT, cloud) via des PoP (points de présence) globaux et des politiques identitaires.

Pour l'IA, SASE apporte plusieurs bénéfices :

- Chemins optimisés vers les services cloud, réduisant la latence.
- Suppression des backhauls coûteux et des itinéraires détournés pour des équipes distribuées.
- Inspection approfondie, prévention des fuites et chiffrement, garantissant l'intégrité des données en transit et au repos.

Le SD-WAN améliore la performance mais peut introduire des vulnérabilités : le SASE répond à ces risques en intégrant la sécurité au sein du SD-WAN, automatisant la détection des menaces et réduisant les erreurs humaines.

Synergie IA + SASE

Les plateformes SASE modernes intègrent des moteurs d'IA capables de détecter en temps réel anomalies et menaces, d'orchestrer des réponses proactives, de prioriser dynamiquement le trafic critique et de prévoir les dégradations de performance. En retour, le SASE protège l'accès aux modèles, aux ensembles de données et aux processus d'opérations d'apprentissage automatique (MLOps, Machine Learning Operations) en utilisant une authentification forte (ZTNA, Zero Trust Network Access), une segmentation fine et des outils de prévention des fuites de données et de sécurité des applications cloud (DLP/CASB, Data Loss Prevention/Cloud Access Security Broker).

L'intégration de SASE peut susciter des réticences (complexité, coûts initiaux, manque de compétences), mais la migration peut être progressive et s'appuyer sur des intégrateurs proposant des solutions managées, permettant de conserver certains investissements existants et de consolider les fonctions de sécurité en une plateforme unique. D'autant plus que les bénéfices sont avérés.

À titre d'illustrations : Dans la finance, le SASE utilise l'IA pour repérer les fraudes en temps réel sur les transactions en ligne, protégeant les données clients ; Dans le retail, l'IA associée au SASE améliore la sécurité distante en permettant un accès flexible et sécurisé depuis n'importe où pour les employés, en appliquant des politiques zero trust à grande échelle.

Source : Zscaler, Inc.

Le SASE est un impératif plutôt qu'une option, et une condition de mise en œuvre sûre et résiliente de l'IA. En alignant réseau, sécurité et gouvernance, cette architecture offre une fondation capable de protéger les actifs stratégiques, d'assurer la continuité d'activité et de permettre le déploiement de projets d'IA dans un cadre maîtrisé.

Chapitre 3

Observabilité : le sixième sens à l'ère de l'IA

« Ce qui n'est pas mesuré n'existe pas. » La maxime de Niels Bohr n'a jamais été aussi d'actualité. Face à l'accélération des volumes de données liée à l'IA générative et à la dépendance au cloud, le monitoring traditionnel montre ses limites. L'observabilité, renforcée par l'AIOps, devient la clé pour gérer efficacement les infrastructures hybrides et distribuées.

Le trafic vers les plateformes d'outils IA a bondi de :

+50% passant de **7 milliards** de visites en février 2024 à **10,53 mds** en janvier 2025.

Cela souligne la surcharge des réseaux et le besoin d'observabilité en temps réel pour gérer ces flux.

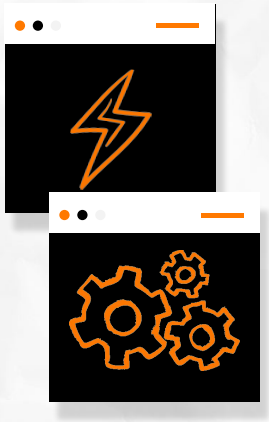
Source : Étude Menlo Security, via Infosecurity Magazine

Beaucoup de DSI reconnaissent l'importance de l'observabilité (77%), mais près de la moitié manquent de clarté sur ses apports concrets (47%) - livre blanc "L'Observabilité IT : élément clé pour une transformation digitale réussie", publié par **Pierre Audoin Consultants.** Source : Sitsi Pacanalyst, 2023.

Pourtant, l'observabilité ne se confond pas avec le simple monitoring et ses apports sont tangibles : elle cherche à comprendre l'état interne d'un système à partir de ses sorties. Ses trois piliers — métriques, traces et logs — doivent être complétés par la fraîcheur des données, le profilage et, surtout, le contexte métier. Ce n'est pas la collecte seule, mais la corrélation et l'enrichissement contextuel qui transforment des données brutes en intelligence opérationnelle.

Le périmètre couvert inclut le réseau et le transport (eBPF, NetFlow/IPFIX, streaming telemetry), les infrastructures et le cloud, les applications et microservices (OpenTelemetry), les postes de travail et l'expérience utilisateur.

Ainsi, un incident devient une histoire lisible : origine de la dégradation, dépendances impactées, conséquences business et actions de remédiation recommandées.



AIOps : intelligence pour la résilience

L'AIOps combine big data et apprentissage automatique pour automatiser les opérations IT : corrélation d'événements, détection d'anomalies, détermination de causalité. Selon Dynatrace, 72% des organisations ont adopté l'AIOps pour réduire la complexité de leur environnement multicloud. Source : Dynatrace

Les freins à l'adoption de l'observabilité et de l'AIOps restent toutefois réels, mais pas insurmontables : coût des outils (56,8% citent le prix comme barrière), manque de compétences internes (47,5%) et intégration chaotique d'outils hétérogènes.
Source : The State of Observability - Overcoming complexity through AI-driven analytics and automation strategies, Dynatrace 2024

Néanmoins, ces obstacles sont surmontables avec l'appui de partenaires experts, faisant de l'observabilité un atout majeur pour aligner les priorités réseaux, cybersécurité et économiques.

Chapitre 4

Multi-cloud + Edge : l’architecture pour industrialiser l’IA

L’IA exige une plateforme distribuée : le multi-cloud apporte agilité et résilience ; l’Edge garantit latence faible, souveraineté et efficacité. Ensemble, ces deux volets forment l’architecture capable de déployer des modèles IA performants, sécurisés et conformes au RGPD, tout en maîtrisant les coûts et accélérant le time-to-value.

Pourquoi ce duo est stratégique ?

Les usages tendent vers l'instantané : détection d'anomalies en production, analyses vidéo, assistance embarquée exigent des latences < 50 ms. En usine, en santé ou pour l'aide à la conduite, chaque milliseconde compte. L'Edge réduit la latence — parfois à moins de 10 ms — en rapprochant l'inférence des sources de données, tandis que le multi-cloud orchestre l'entraînement des modèles et le stockage à long terme.

Le multi-cloud permet de répartir les charges selon performance et coût : entraînement intensif sur un cloud public optimisé, traitement de données sensibles sur un cloud privé souverain. Exemple : dans **le retail**, l'analyse IoT peut combiner clouds publics pour le traitement massif et clouds privés pour la donnée client ; dans **la finance**, les transactions temps réel peuvent être monitorées sur cloud privé pour les données sensibles et sur cloud public pour les modèles d'anomalie.

Le marché multi-cloud pour l'IA devrait croître

de 25%

en 2025

source : CloudZero, mai 2025

avec **90%**

des entreprises adoptant des stratégies hybrides

source : CloudZero, mai 2025

Le marché de l'Edge computing atteindra

261mds $

Le marché de l'edge computing atteindra

source : IDC via CloudZero, mai 2025

Les enjeux à prendre en compte :

- Complexité de gestion : orchestrer plusieurs clouds et déployer des infrastructures edge sur de nombreux sites nécessite une stratégie et des outils de gouvernance unifiés.

- Sécurité fragmentée : chaque cloud et chaque point edge introduisent des spécificités ; maintenir une posture de sécurité cohérente demande une expertise pointue.

La synergie gagnante

"Le multi-cloud combiné à l'edge crée une solution robuste qui favorise la performance et la scalabilité pour les workflows IA distribués. C'est l'architecture par défaut pour les leaders de demain." - **Brian Hoekelman, VP, Product & Business Development.** Source Otava Channel Futures mai 2025

Le modèle optimal **combine Edge et multi-cloud :**

- L'Edge collecte, filtre et traite les données brutes en temps réel, effectue l'inférence immédiate et retourne les résultats critiques.

- Le multi-cloud prend en charge l'entraînement massif des modèles, l'archivage et l'analyse approfondie.

Cette architecture hybride est aujourd'hui la seule capable de répondre aux exigences modernes de l'IA : inférence ultra-rapide à la périphérie, entraînement massif dans le cloud, tout en garantissant souveraineté et résilience.

Conclusion

Pour les entreprises françaises, moderniser le réseau n’est plus un choix optionnel : **c’est une condition de compétitivité face à l’IA. SD-WAN, SASE, Observabilité/AIOps et une architecture multi-cloud + Edge constituent ensemble, le socle permettant de transformer l’IA en avantage stratégique.**

En garantissant **performance**, **sécurité**, **résilience** et **maîtrise des coûts**, ces briques techniques répondent directement aux priorités de modernisation des réseaux des organisations et préparent les infrastructures aux défis de demain.

Explorons votre contexte (environnements hybrides, flux IA, priorités de sécurité) et identifions des actions à impact.

Évaluation rapide

30 min d'échanges

Recommandations concrètes

Je prends rendez-vous