InfoBrief, sponsorisé par Orange Business | Octobre 2025

La confiance numérique

Le rôle crucial du réseau dans un cloud de confiance

Cyrille Chausson
Research Manager, European
Application Modernization Strategies

Rahiel Nasir
Research Director, European Cloud Practice,
Lead Analyst, Digital Sovereignty

Le renforcement des écosystèmes de réseau est une priorité stratégique

Concevoir des réseaux sûrs et résilients est désormais essentiel pour les organisations européennes en quête de maîtrise, de conformité et de leadership dans un paysage numérique en constante évolution.

L'adoption des solutions de cloud de confiance poursuit sa progression.

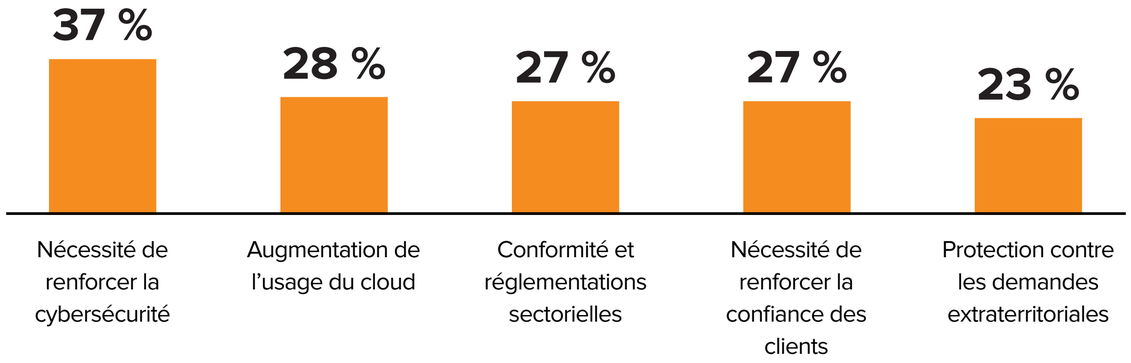
Q : Votre organisation utilise-t-elle, ou envisage-t-elle d'utiliser, une solution de cloud de confiance ?

Les solutions de cloud de confiance s'imposent désormais comme une priorité stratégique majeure pour les dirigeants en Europe.

25 % des dirigeants d'Europe de l'Ouest considèrent la confiance numérique comme un investissement technologique émergent majeur pour les douze prochains mois.

(Source : *CEO Survey 2024 d'IDC* (n = 67)

Les 5 principaux moteurs de l'utilisation du cloud de confiance en Europe



Source : *European Cloud Survey 2024 d'IDC, septembre* (n = 1 325)

Valeur ajoutée de la confiance dans les réseaux

L'évolution des exigences du marché pousse les entreprises à considérer les réseaux de confiance non seulement comme un objectif de conformité, mais aussi comme une source de résilience, de différenciation et de création de valeur pour l'entreprise.

43 % des organisations européennes sont prêtes à payer **11 à 20 %** en plus de leurs budgets informatiques actuels pour mettre en œuvre une solution de cloud de confiance et la couche réseau associée en 2025.

54 % **des organisations européennes** ont indiqué qu'elles allaient allouer jusqu'à 10 % de leur budget cloud de confiance à des solutions soutenant la **confiance technique**. Et elles sont 17 % à vouloir y consacrer entre 11 et 20 %.

55 % des organisations européennes ont indiqué qu'elles prévoyaient d'allouer jusqu'à 10 % de leur budget pour le cloud de confiance à des solutions axées sur la **confiance opérationnelle**.

La majeure partie des dépenses mondiales en solutions de cloud de confiance devrait être consacrée aux **applications PaaS**, suivies par l'infrastructure intégrée pour le calcul et le réseau.

Source : *Worldwide Digital Sovereignty Survey* d'IDC, Europe, 2024 (n = 250), 2025 (n = 370)

Réseaux de confiance et adaptatifs

Les opérations numériques exigent désormais des réseaux à la fois de confiance (assurant le contrôle et la conformité) et adaptatifs (permettant l'agilité et la résilience en temps réel dans un paysage en constante évolution).

Les données et le contrôle doivent rester à l'intérieur des frontières juridictionnelles, tandis que des réseaux robustes et adaptables, guidés par les charges applicatives et les flux de données, sont essentiels à un positionnement de confiance et à la résilience.

Ecosystèmes d'entreprise

Transactions
ERP, bases de données commerciales MDM

Engagements
CRM, contextualisation, omnicanal

Production
Conception, systèmes industriels, IoT, edge

Interconnexions
Marché, partenariats, chaîne d'approvisionnement

Productivité
Automatisation, IA/IA générative, UX

Interconnexion de confiance

Besoins en matière de connectivité

Flux de données et routage

Sécurité et conformité

Sensibilité au temps de latence

Résilience et redondance

Réseau de confiance interopérable

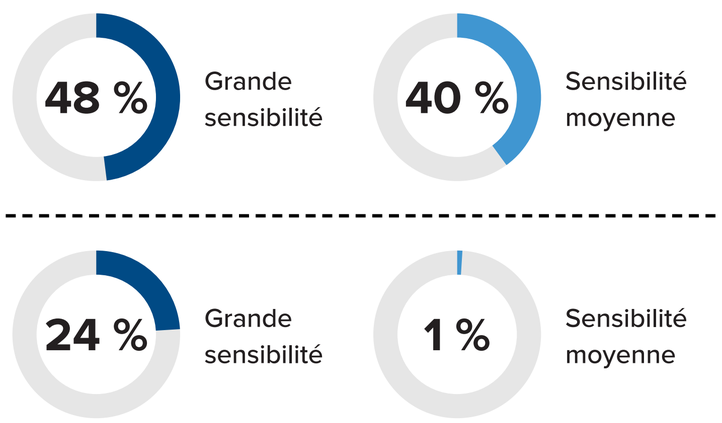
- WAN
- LAN
- SASE
- Réseaux cloud
- SDN
- VPN
- Réseaux privés

Migration des données et des charges applicatives classifiées

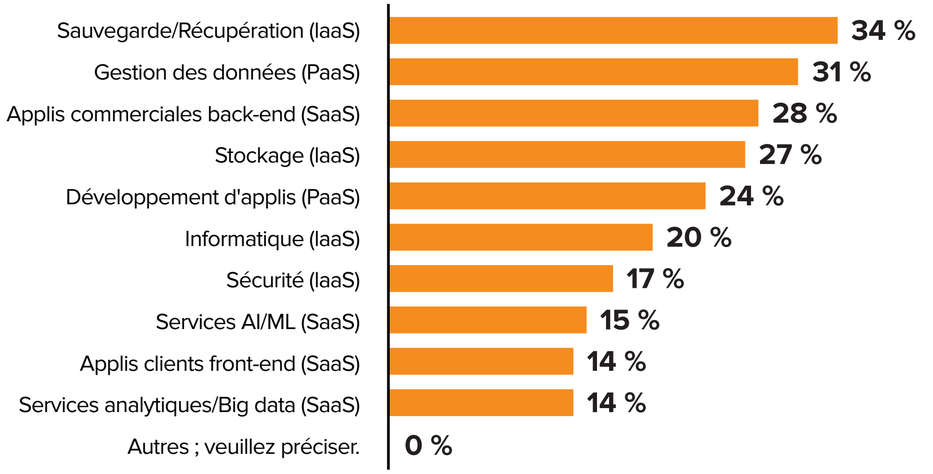
À mesure que les charges applicatives sensibles se déplacent vers les clouds de confiance, les réseaux doivent évoluer pour assurer la conformité, la sécurité et un contrôle rigoureux.

Dans le paysage distribué actuel, les réseaux doivent traiter diverses charges applicatives, s'adapter à divers environnements et **garantir que les données sensibles sont gérées en toute sécurité pendant leur transit**.

Les organisations européennes **manifestent de plus en plus une préférence marquée pour l'adoption d'une approche de confiance pour** la gestion de certaines applications et charges applicatives.



Q : Votre organisation a-t-elle des données qu'elle classifie actuellement, ou qu'elle prévoit de classifier dans les 12 prochains mois, avec les niveaux de sensibilité suivants ? [Choisissez toutes les réponses qui s'appliquent]



Q : Quelles charges applicatives votre organisation a-t-elle migré ou prévoit-elle de migrer vers le cloud de confiance ?

Les exigences en matière de réseau de confiance doivent être évaluées et alignées avec des architectures de réseau flexibles, capables de traiter des charges applicatives spécifiques et des demandes de données, tout en garantissant la conformité avec les besoins de localisation des données (y compris les déploiements en périphérie), les normes de chiffrement, la conformité réglementaire et les attentes en matière de faible latence et de performances élevées en matière d'Entrée/Sortie.

Source : *Worldwide Digital Sovereignty Survey* d'IDC, Europe, 2024 (n = 250), 2025 (n = 370)

L'urgence de la transformation des réseaux

La conformité aux exigences de confiance numérique oblige les entreprises à accélérer la transformation de leur réseau et à investir dans une infrastructure sécurisée et résiliente.

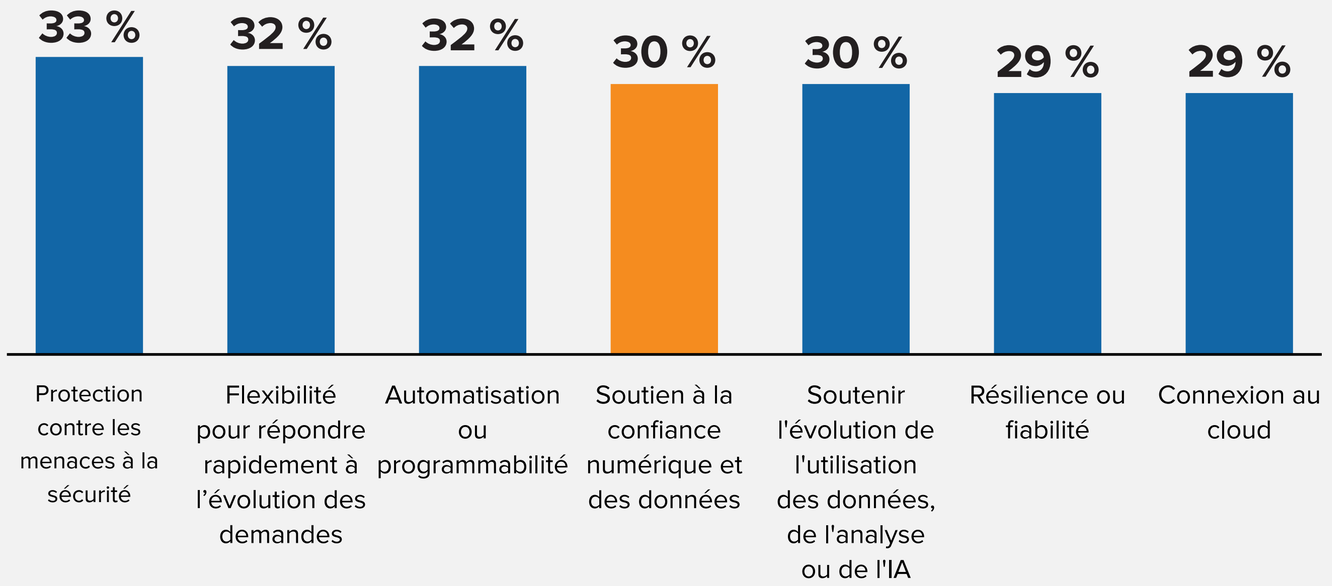
L'urgence de la transformation des réseaux est à l'origine des décisions d'investissement prioritaires.

La sécurité et l'agilité du réseau, renforcé par l'automatisation, favorisent l'alignement de l'entreprise tout en garantissant la conformité continue du réseau et des systèmes informatiques. Les entreprises européennes sont de plus en plus contraintes de réorienter leurs stratégies de connectivité réseau (y compris WAN et VPN) pour se conformer aux exigences en matière de confiance numérique et des données. Cela permet de garantir la résilience et la continuité de leurs objectifs stratégiques plus larges.

38 %

des personnes interrogées ont déclaré que considérer l'amélioration du réseau comme une réponse urgente aux pressions liées à la confiance est un investissement pragmatique. Les effets de la confiance sur les opérations de réseau sont tout sauf négligeables. (*utilisateurs de réseaux étendus et de réseaux privés virtuels)

Q : Dans quels domaines votre organisation doit-elle améliorer ses réseaux de toute urgence ? [Utilisateurs WAN et VPN uniquement]



Source : WW C-Suite Tech Survey, IDC, août 2023, n DNB=130

Bâtir la fondation à la confiance

Un réseau de confiance est la pierre angulaire de l'indépendance numérique, de la résilience et de la conformité, posant des bases sûres pour l'avenir de l'organisation.

Pas de confiance numérique sans confiance dans les réseaux

Renforcer le contrôle de tous les actifs de données, y compris toute l'infrastructure cloud de confiance sous-jacente (par ex. les data centers et les réseaux), les logiciels et les services, ainsi que tous les administrateurs et le personnel de support ayant accès à ces actifs.

Garantir la résilience face aux perturbations physiques (par ex., les catastrophes naturelles), aux cybermenaces et aux pressions extérieures (par ex. les tensions géopolitiques et les contraintes réglementaires) tout en préservant la continuité des services et une connectivité sans faille.

Atténuer les risques de compromission des données sur le réseau, y compris l'interception du trafic, les coupures de câble, la perte de confidentialité et d'intégrité, et les attaques DDoS. Il est essentiel d'appliquer des contrôles de confiance non seulement aux données au repos, mais aussi aux données en transit. Sans un réseau de confiance, il est impossible de créer une infrastructure cloud de confiance car les données en transit risquent d'être compromises.

Comment construire un réseau de confiance

Confiance opérationnelle

25 % des organisations européennes considèrent les équipements réseau utilisés pour le trafic de données et de voix (y compris l'optimisation du WAN et WLAN) comme « extrêmement importants » pour **atteindre la confiance opérationnelle.**

Confiance technique

Les fournisseurs de solutions interrogés en Europe estiment que les aspects suivants sont "extrêmement importants" pour atteindre la confiance technologique. :

45 %
Logiciels d'infrastructure réseau permettant la virtualisation des réseaux

32 %
Systèmes et plateformes d'infrastructure intégrés

29 %
Dispositifs de sécurité réseau

24 %
Logiciels de gestion de réseau

Source : *Worldwide Digital Sovereignty Survey d'IDC, 2025* Europe (n = 370)

Les piliers de l’exploitation et de la connectivité d’un réseau de confiance

Les réseaux de confiance modernes reposent sur des éléments clés qui interagissent pour garantir une autonomie numérique et une connectivité fiable dans un cadre réglementaire complexe.

1

Contrôle des infrastructures et indépendance opérationnelle

- Gouvernance complète opérée au niveau des câbles, de l'infrastructure et des technologies supportant le réseau central
- Équipement sécurisé, qualifié/ certifié
- Résilience opérationnelle avec des dépendances limitées
- Environnement de cogestion sécurisé (RBAC, IAM)
- Contrôle de la localisation et de la nationalité des opérateurs

2

Protection des données de bout en bout

- Gestion et contrôle sécurisés des données - localisation, résidence, intégrité et confidentialité des données
- Chiffrage de bout en bout (en transit et stocké)
- Segmentation du trafic et classification des workflows critiques
- Gestion sécurisée du réseau et données de contrôle (inventaire, configurations et logs)

3

Qualité de services et efficacité organisationnelle

- Formation continue des équipes internes (conformité et cybersécurité)
- Écosystème fiable et transparent de partenaires et de solutions
- Tests d'infrastructure (y compris PCA/PRA)

4

Défense active et garantie cybersécurité

- Accès réseau Zero Trust
- Micro-segmentation du réseau
- Services de renseignement sur les menaces
- Solutions de sécurité (par ex. SASE)
- Protection DDoS

Risques liés à l’inaction

Ne pas investir dans la confiance numérique et stratégique expose les industries européennes à des risques en matière de sécurité, d’économie et d’innovation, menaçant leur résilience et leur compétitivité à long terme.

Quelles sont les vulnérabilités qui apparaissent lorsque la confiance du réseau n'est pas respectée ?

RISQUES IT

- **Pas de réseau dédié et isolé :** En cas de catastrophe ou d'attaque, les réseaux physiques et mobiles (y compris les services d'urgence) et le dispositif de cyberdéfense subiront des temps d'arrêt dévastateurs.
- **Érosion de la résilience en matière de cybersécurité :** L'exposition accrue aux violations de données, aux cyberattaques, à la cybersurveillance et à l'accès non autorisé au réseau expose les données sensibles à un risque important.
- **Détournement de route et fuites BGP :** Les organisations peuvent souffrir d'une indisponibilité temporaire due à une perte de connectivité, à des interceptions de trafic, à un vol de données ou à une redirection vers un serveur malveillant.
- **Dépendance, verrouillage vendeur et coûts de réversibilité inattendus :** Les formats propriétaires et les frais de sortie peuvent être très restrictifs, ce qui limite les possibilités de PRA/PCA et de migration.
- **Non-conformité technique avec les réglementations de l'UE :** L'absence de MFA (authentification multifactorielle) ou la faible segmentation du réseau peuvent exposer les organisations à des pénalités et à des audits.

RISQUES METIERS

- **Manque de confiance des clients en** raison d'une politique insuffisante en matière de confidentialité, de protection et de conformité des données. La perte de réputation peut être très préjudiciable.
- **Perte de résilience :** L'organisation est exposée à des coupures de réseau inattendues, à des perturbations de la chaine logistique et à une dégradation des opérations. Les systèmes IT/OT pourraient être compromis.
- **Écosystème non fiable :** L’absence d’infrastructures IT régionales robustes et sécurisées, ainsi que de réseaux interopérables, constitue un frein majeur à une collaboration efficace et harmonisée au sein de l’Union européenne.
- **Retard dans l'innovation :** Les organisations peuvent souffrir de la fuite de secrets industriels, ce qui entraîne des retards dans la mise sur le marché des produits et des innovations.
- **Obstacles contractuels et réglementaires freinant les exportations et la croissance internationale:** Certaines juridictions imposent des restrictions à l'exportation de données ou des exigences de réversibilité et de traçabilité.

Comment choisir le bon partenaire stratégique pour un réseau de confiance

Sélectionner un partenaire offrant des data centers en local, des certifications nationales et des partenariats mondiaux en matière de cloud pour assurer une confiance totale et une connectivité transparente, tant au niveau local qu'international.

41 % des organisations européennes considèrent que l'adoption du cloud impose des **mises à niveau urgentes du réseau** afin de répondre aux exigences de confiance (*utilisateurs de WAN et de VPN).

20 % ont du mal à trouver des fournisseurs d'infrastructure réseau qui offrent des options de connectivité de confiance. **Cela met en évidence la** nécessité de définir des critères de confiance plus clairs et des points de référence pour identifier un partenaire.

20 % des organisations européennes considèrent que la dépendance à l'égard de fournisseurs non européens pour les équipements d'infrastructure réseau constitue une préoccupation majeure pour préserver la confiance numérique.

Critères essentiels pour choisir un partenaire ou fournisseur de réseau de confiance

47 %

Datacenters détenus localement

45 %

Certifications nationales en matière de cybersécurité et cloud

42 %

Contrôle de confiance de l'ensemble de l'infrastructure réseau et des options de connectivité

36 %

Solutions pour soutenir la résilience opérationnelle

35 %

Capacité à rapatrier les données du cloud vers les installations sur site

30 %

Écosystème solide de partenaires qui respectent les principes de confiance

25 %

Recrutement de ressources locales dédiées aux opérations techniques

20 %

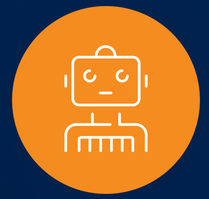
Fournisseur local ayant une empreinte nationale ou régionale

Source : *Worldwide Digital Sovereignty Survey d'IDC, 2025* Europe (n = 370)

Les infrastructures « Trust by Default » d'Orange Business, fondement d'une connectivité de confiance

Contrôle total de l'infrastructure

- Orange est propriétaire de son réseau, de ses câbles et de ses plans d'acheminement sans dépendance vis-à-vis de tiers
- Contrôle total sur les investissements, les politiques d'acheminement et les développements technologiques
- Transparence et traçabilité pour assurer la confiance et la conformité
- Augmentation de la part des équipements de cœur de réseau développés en open source par Orange



Modèle opérationnel autonome

- Contrôle par Orange sur les opérations managées 24h/24 et 7j/7
- Expertise de niveau 1 à 3, couvrant toutes les technologies
- Processus et outils dédiés pour garantir la réactivité, l'agilité et l'indépendance de la prise de décision

Sécurité et résilience intégrées

- Services en ligne redondants, conçus pour être « sécurisés dès la conception », avec protection DDoS et surveillance proactive 24/7
- Redondances et architectures robustes garantissant la continuité et la disponibilité, même en cas d'incident
- Résultats inégalés en matière de SLA et capacités avancées en matière de protection contre les cybermenaces

Consultez nos experts pour renforcer la sécurité et la résilience de votre connectivité.

À propos d’IDC

International Data Corporation (IDC) est un acteur majeur des services de veille de marché, de conseil et d’événementiel sur les marchés des technologies de l’information, des télécommunications et des technologies grand public. Avec l’aide de plus de 1 300 analystes répartis dans le monde entier, IDC propose une expertise mondiale, régionale et locale sur les technologies ainsi que sur les opportunités et tendances sectorielles dans plus de 110 pays. Les analyses et les informations fournies par IDC aident les informaticiens, les cadres dirigeants et les responsables des investissements à prendre des décisions technologiques factuelles et à atteindre leurs grands objectifs. Fondée en 1964, IDC est une filiale à 100 % d'International Data Group (IDG, Inc.), le leader mondial des médias technologiques, des données et des services de marketing.

IDC Custom Solutions

La présente publication a été réalisée par IDC Custom Solutions. En tant que fournisseur mondial de services de veille, de conseil et d’événementiel pour les marchés des technologies de l'information, des télécommunications et des technologies grand public, le groupe Custom Solutions d'IDC aide ses clients à planifier, vendre et réussir sur le marché mondial. Nous élaborons des programmes de veille décisionnelle et de leadership d’opinion qui contribuent au succès de nos clients.

IDC UK1st floor, Whitfield Street, London, W1T 2RE, Royaume-Uni Tél. 44.208.987.7100

@idc | @idc | idc.com