



Une approche pragmatique pour répondre aux exigences de souveraineté des données et de résilience de Microsoft 365

La bataille pour la souveraineté des données s'intensifie dans un contexte de sensibilité croissante des données, d'incertitudes géopolitiques et de l'omniprésence des SaaS dans les opérations numériques.

Naviguer dans l'art du possible pour respecter les exigences de souveraineté.



Archana Venkatraman
 Senior Research Director,
 Cloud Data Management, IDC Europe

La résilience et la souveraineté des données deviennent non négociables

La souveraineté des données n'est plus optionnelle pour la conformité. Au contraire, elle est maintenant au cœur de la confiance numérique et de la gestion des risques.

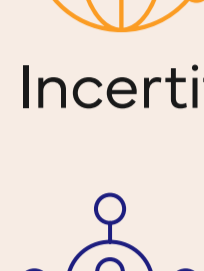
La souveraineté des données et les changements éventuels liés au cloud ont été cités comme les plus grandes préoccupations pour 2026.



Voici les raisons de cette attention accrue :



Augmentation de la valeur et de la sensibilité des données



Incertaines géopolitiques

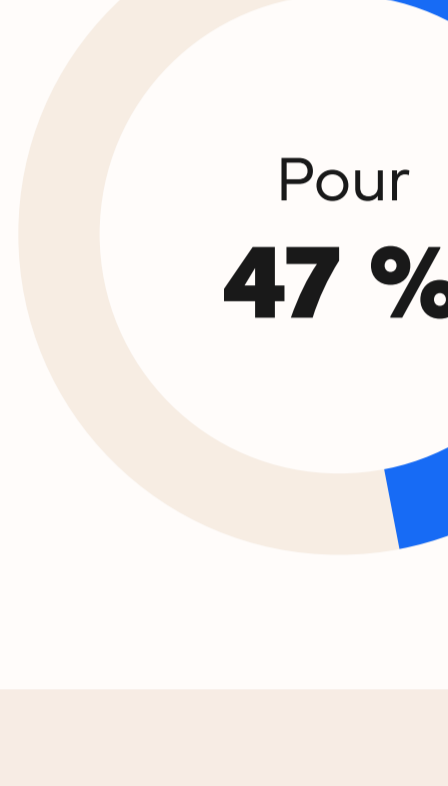


Forte dépendance à l'égard de plateformes tierces pour les opérations commerciales numériques

Source : enquête Future Enterprise Resiliency and Spending Survey, Wave 5 publiée par IDC en juin 2025

Les risques liés à la souveraineté et à la résilience s'étendent à l'ensemble des environnements en cloud, en particulier les SaaS.

Comparativement aux applications IaaS et PaaS, les applications SaaS dominent les environnements numériques. Par conséquent, leur rôle en tant que principal dépositaire de données commerciales sensibles et vitales ne peut plus être ignoré.



des entreprises, c'est dans les environnements SaaS que les données d'entreprise augmentent le plus ou le moins rapidement.



des équipes d'assistance informatique



des équipes de cybersécurité

admettent que c'est dans l'environnement Microsoft 365 qu'elles sont le plus préoccupées par la perte de données, la suppression accidentelle, l'absence de récupération ou les échecs d'audit.

Source : enquête EMEA Cloud Survey, publiée par IDC en 2024 ; enquête CloudOps Survey, publiée par IDC en 2024

S'affranchir de la pensée unique : Une action centrée sur la résilience est essentielle pour rendre les contrôles de données pratiques

La souveraineté présente de multiples facettes et est complexe, ce qui nécessite une approche pragmatique et axée sur la résilience ; le premier obstacle à surmonter est la pensée de facto.

6 organisations sur 10 s'appuient encore sur les mécanismes natifs de protection des données de Microsoft 365.

Pourcentage de répondants : ■ EMEA ■ Total

Catégorie	EMEA (%)	Total (%)
Logiciels tiers	18,7 %	19,2 %
Protection fournie par le fournisseur de SaaS	62,8 %	61,7 %
Pas de protection des données	5,6 %	6,6 %
Ne l'utilisent pas	12,9 %	12,5 %

Cela entraîne des risques tels que la perte de données en raison de caractéristiques de conservation des données par défaut, inflexibles et limitées, ainsi que des capacités de récupération des données rigides en cas de crise.

Une forte dépendance à l'égard des données natives signifie également que les organisations n'ont pas un accès flexible à leurs données et, plus important encore, qu'elles n'ont pas un contrôle total sur les informations nécessaires à la continuité, à la souveraineté et à la conformité.

Source : enquête Cloud Data Logistics and Protection Survey, publiée par IDC en août 2025

La valeur des technologies de protection des données, de sécurité et de résilience et le fossé grandissant entre les natifs du numérique et les adeptes.

La croissance rapide des données dans les SaaS, tels que Microsoft 365, souligne l'importance d'assurer le contrôle et l'autonomie stratégique des actifs de données.

87% des natifs du numérique (77 % de toutes les organisations) s'engagent à investir davantage dans la protection des données SaaS.

Les organisations considèrent la classification et la protection des données comme deux domaines qu'il est « extrêmement important » d'aborder dans un avenir proche.



Cependant, **62%** des organisations s'appuient encore sur les fonctionnalités de protection des données natives ou par défaut de Microsoft 365, ce qui augmente considérablement les risques.

La sécurité, le risque et la conformité restent des domaines technologiques qui sont non seulement à l'abri des réductions budgétaires, malgré les incertitudes macroéconomiques, mais qui connaîtront même des « augmentations budgétaires importantes » en 2025 et au-delà.



Source : enquête CloudOps Survey, publiée par IDC en 2024 ; enquête Future of Enterprise Resiliency and Spending Survey, publiée par IDC en décembre 2024

Souveraineté des données et principes de conception de la résilience de Microsoft 365

Un environnement Microsoft 365 souverain est un ensemble de choix architecturaux et de cadres juridiques.

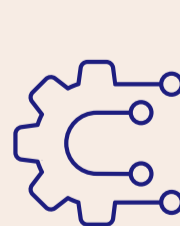
Les organisations doivent mettre en place une stratégie de données résiliente qui inclut la surveillance réglementaire. Elles doivent documenter leurs processus, en commençant par la conformité réglementaire. Elles doivent, la documentation des rôles et des responsabilités et leurs politiques en matière de risques.

La stratégie de la souveraineté technique doit couvrir les trois **pilliers de la souveraineté des données** :



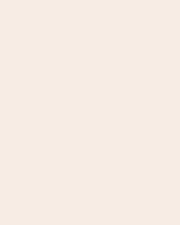
Juridiction légale :

Veiller à la clarté de la gouvernance des données de sauvegarde, des contrôles d'accès et du chiffrement.



Résidence des données :

Assurer le choix et la flexibilité de l'endroit où les données de sauvegarde sont stockées, et contrôler le mouvement des données et les audits de données. Veiller à ce que les métadonnées soient traitées avec sensibilité.

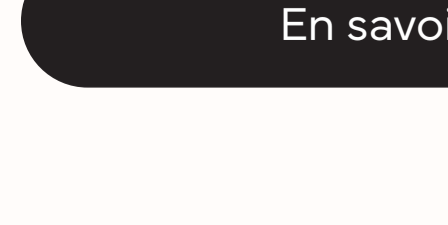


Autonomie opérationnelle :

Vérifier le contrôle nécessaire pour la cyber-résilience et la conformité réglementaire avec des caractéristiques telles que l'immutabilité des données, la traçabilité des journaux d'audit et la séparation logique. Il est essentiel pour l'intégrité opérationnelle et la continuité des activités de se concentrer davantage sur la récupération grâce à des mécanismes tels que la récupération granulaire, un délai de récupération plus rapide et une couverture complète de la succession de Microsoft 365.

Ligne de source : IDC Research, 2025

Message du sponsor



Veeam est le leader mondial de la résilience des données, garantissant une continuité d'activité sans compromis.

Avec un vaste réseau de partenaires dans le monde entier, Veeam assure une protection des données résiliente et une reprise d'activité sans faille, quel que soit l'endroit où se déroule l'activité. Veeam Data Cloud pour Microsoft 365 et Entra ID offre la solution de sauvegarde SaaS la plus complète et la plus moderne du marché pour lutter contre les cybermenaces et les pertes de données d'aujourd'hui. Protect Exchange, SharePoint, OneDrive, Teams et Entra ID au sein d'une seule et même solution.

En savoir plus