White Paper

Souveraineté des données à l'ère du cloud : une approche centrée sur la résilience

Sponsorisé par : Veeam

Archana Venkatraman
Décembre 2025

LE POINT DE VUE D'IDC

Parmi les sujets technologiques qui occupent au moins autant l'espace que l'IA aujourd'hui, la souveraineté des données s'impose. Pour près d'un quart des organisations, elle prime désormais sur l'innovation.

À l'ère où les données sont le nouvel or noir, les lois extraterritoriales, les tensions géopolitiques et la dépendance au cloud créent des risques inédits. La souveraineté devient alors une priorité stratégique pour garantir contrôle et autonomie.

La souveraineté n'est plus une simple question de conformité : elle est le socle de la confiance numérique et le cœur d'une nouvelle approche de gestion des risques.

Pourquoi accorder une telle importance à la souveraineté et peut-on atteindre de tels objectifs ?

Du monde VUCA au monde BANI : une nouvelle réalité

La terminologie de la transformation a évolué : de volatile, incertain, complexe et ambigu (VUCA) pendant la pandémie, à fragile, anxieux, non linéaire et incompréhensible (BANI) en 2025. Cette dernière description reflète la normalisation des chocs de marché et des vagues d'innovation; des chocs difficiles à comprendre et encore plus difficiles à anticiper.

Dans ce contexte, la souveraineté des données s'est élevée au rang de pilier de la gestion des risques.

DANS CE LIVRE BLANC

L'objectif de ce document est d'explorer les impératifs de souveraineté des données, notamment dans les environnements SaaS comme Microsoft 365. Il présente également les préoccupations des utilisateurs finaux et les raisons de l'accent mis sur la souveraineté. Enfin, des étapes concrètes sont proposées pour relever ces défis, en adoptant une approche double, centrée sur la résilience et la conformité.

Décembre 2025, IDC US53943725

APERÇU DE LA SITUATION

Les préoccupations relatives à la souveraineté sont multiples. Les entreprises cherchent avant tout à atténuer les risques géopolitiques : exposition aux demandes d'accès de gouvernements étrangers (CLOUD Act…), ou interruption de service par "lockout" technologique en cas de litige international. Elles doivent aussi respecter des exigences réglementaires strictes (RGPD, Data Act, AI Act…), qui mettent l'accent sur la localisation, la portabilité et le contrôle des données.

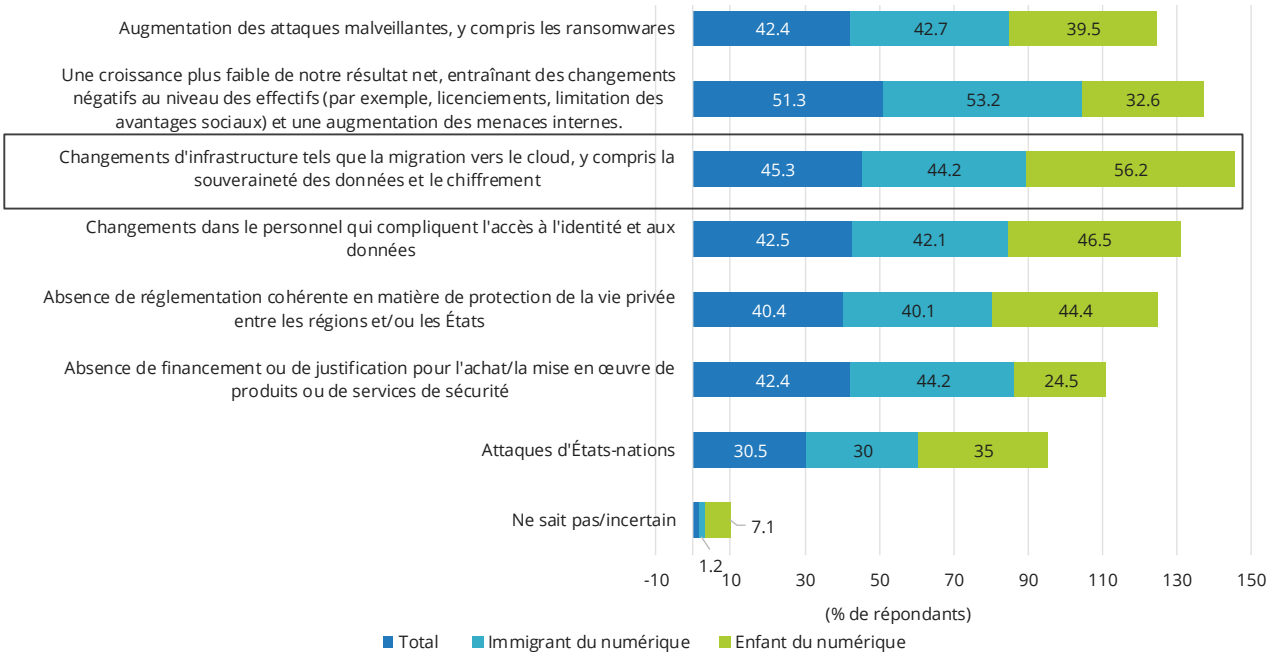
Il est intéressant de noter que les organisations ayant une plus grande maturité numérique sont plus sensibles aux risques liés aux données. Comme le montre la figure 1, la souveraineté des données et les potentielles évolutions du cloud figurent parmi les plus grandes préoccupations pour 2026, selon l'enquête *Future Enterprise Resiliency and Spending (FERS)Survey* d'IDC, publiée en juin 2025.

À cette sensibilité accrue et ce contexte géopolitique s'ajoute une dépendance grandissante aux cloud publics, particulièrement chez les digital-native, dont l'activité s'appuie fortement sur des environnements SaaS.

FIGURE 1

Principales préoccupations en matière de sécurité ou de protection de la vie privée

Q. Dans le contexte géopolitique et économique actuel, quel est le problème de sécurité ou de protection de la vie privée qui vous préoccupe le plus pour l'année prochaine ? (Premier, deuxième et troisième rangs combinés)



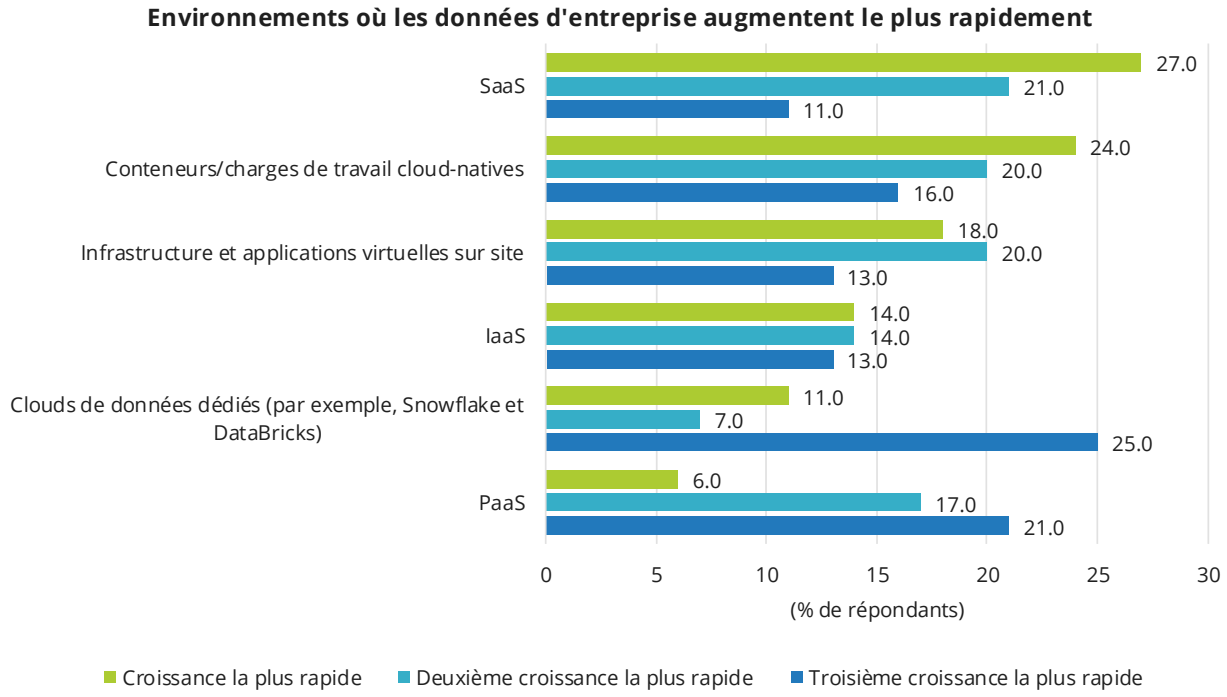
n = 885 (digital native n = 76, autres = 809)

Source : *Future Enterprise Resiliency and Spending Survey, Wave 5,* IDC, juin 2025

Les entreprises constatent une accélération de la croissance des données dans leurs environnements numériques, en particulier dans le SaaS (voir figure 2). Pour 47 % d'entre elles, ces environnements figurent en tête ou en deuxième position des zones où les données progressent le plus rapidement. Étant donné que des applications comme Microsoft 365 et Salesforce représentent la plus grande part du marché cloud, devant l'IaaS et le PaaS, leur rôle critique pour l'entreprise est indéniable.

FIGURE 2

La croissance des données s'accélère dans tous les environnements, en particulier dans le SaaS



n = 1 431

Source : *EMEA CloudOps Survey,* IDC, 2024

Dans leurs conversations avec IDC, les responsables IT et métiers indiquent souvent que Microsoft 365 est au cœur des préoccupations en matière de souveraineté des données, en raison de son utilisation généralisée pour les données de collaboration et de communication sensibles.

Dans ce contexte, les dépenses de protection des données ne sont plus un simple “assurance” passive : elles deviennent stratégiques pour la résilience, l’atténuation des risques de souveraineté et la continuité d’activité. Cela est particulièrement vrai pour les digital native.

> IDC observe que 77 % de toutes les organisations et 87 % des digital native prévoient d'augmenter leurs budgets de protection des données SaaS. En outre, les organisations considèrent la classification et la protection des données comme deux domaines « extrêmement importants » pour leur organisation en 2025 et 2026.

Définir et comprendre la souveraineté des données

Une souveraineté numérique totale semble illusoire compte tenu de la nature interconnectée de l’économie numérique et de la complexité des chaînes d’approvisionnement technologiques.

Toutefois, IDC estime que reconnaître l’impossibilité de l’isolement absolu ne diminue pas l’impératif de souveraineté ni l’exposition aux risques. Cela invite au contraire à une approche pragmatique pour sortir de l’impasse.

Cette approche s’articule autour de plusieurs impératifs : bâtir une autonomie stratégique, établir un contrôle et une résilience des données, des infrastructures critiques et de l’activité commerciale.

Ce changement subtil mais essentiel assume la réalité d’une dépendance numérique mondiale, tout en donnant aux organisations les moyens d’atténuer les risques, de protéger la propriété intellectuelle, de renforcer la résilience et d’assurer la continuité d’activité malgré un environnement géopolitique et réglementaire mouvant.

Trois leviers sont essentiels : clarifier la responsabilité partagée, évaluer l’appétence au risque, et structurer une stratégie par étapes.

La résilience comme levier d’action principal

Quatre perspectives permettent de décortiquer la complexité de la souveraineté et d’en faire un enjeu de résilience :

- **Données :** résidence, chiffrement, mécanismes de contrôle d’accès.
- **Juridique :** pouvoirs de lockout, obligations contractuelles, injonctions judiciaires.
- **Opérationnelle :** cyber-résilience, conformité, administration courante, gestion des incidents, sauvegarde et restauration.
- **Technique :** environnements isolés (air-gap), continuité d’activité, capacité d’accès et de migration/exit.

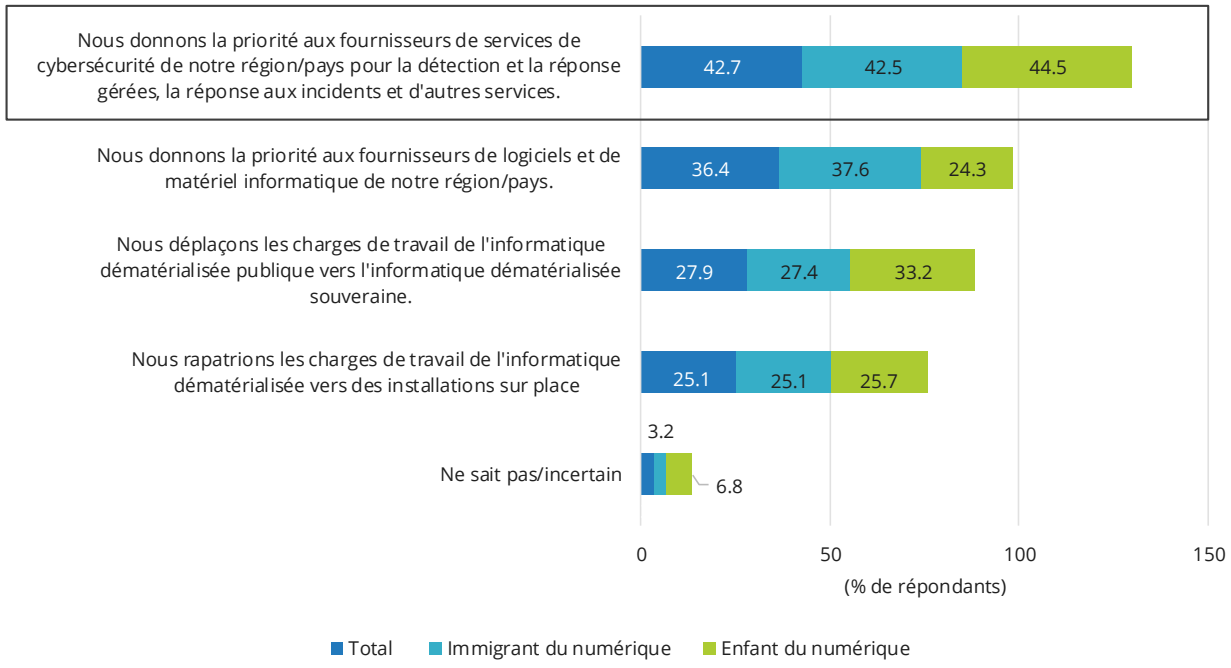
Ainsi détaillée et décortiquée, il devient clair que la souveraineté des données peut et doit être construite par couches, en capitalisant sur les mécanismes existants de conformité et d'atténuation des risques. Les digital natives ont parfaitement intégré ces mécanismes à leur fonctionnement.

Il n'y a pas de rapatriement massif, à l'heure actuelle, des environnements SaaS ou de cloud publics (voir la figure 3). Les organisations, surtout les digital native, comprennent le potentiel de ces technologies pour réaliser leurs ambitions en matière d'innovation. Leur réponse aux risques potentiels consiste donc plutôt à renforcer leurs environnements cloud et SaaS via des services et technologies centrés sur la résilience.

FIGURE 3

Comment les organisations adaptent-elles leurs stratégies de résilience à la lumière des incertitudes géopolitiques ?

Q. Lequel des énoncés suivants décrit la manière dont les incertitudes géopolitiques actuelles touchent vos plans de sécurité/résilience pour l'année en cours ?



n = 885 (digital native n = 76, autres = 809)

Source : *Future Enterprise Resiliency and Spending Survey, Wave 5,* IDC, juin 2025

La sécurité, le risque et la conformité restent des domaines "immunisés" contre les coupes budgétaires en période d'incertitude macroéconomique, et devraient enregistrer des hausses significatives en 2025 et au-delà, comme l'ont indiqué les responsables IT interrogés dans l'enquête d'IDC *Future Enterprise Resiliency and Spending Survey* de décembre 2024.

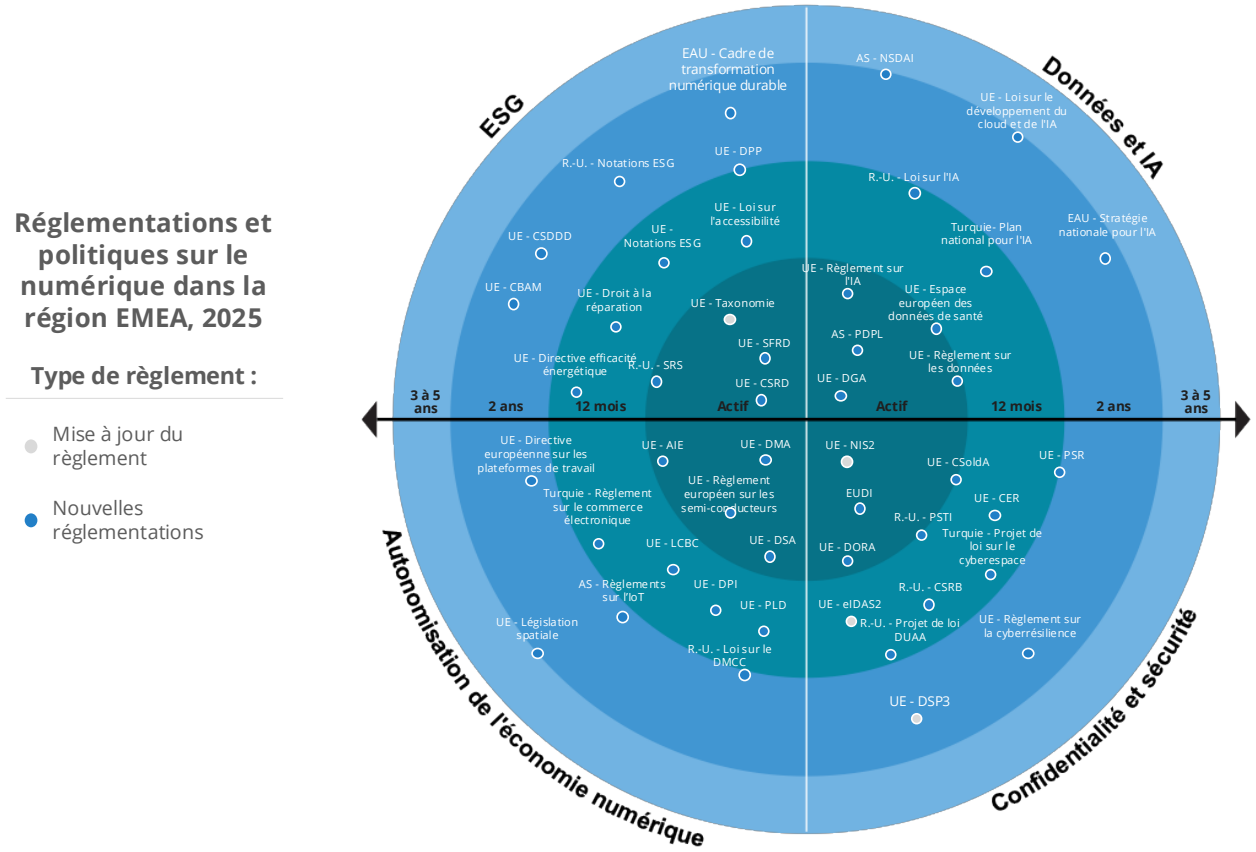
Les deux autres domaines à l'abri des coupes budgétaires sont l'IA et l'automatisation, ainsi que la modernisation de l'infrastructure.

Mais en cette période instable, le retour sur investissement en matière de sécurité est essentiel. IDC estime que la conformité peut servir de guide aux entreprises pour orienter leurs investissements en matière de sécurité au bon endroit, en fonction de leurs lacunes en matière de risques.

L'environnement réglementaire est extrêmement complexe et il existe une multitude de nouvelles réglementations auxquelles il faut se conformer (voir la figure 4). IDC estime que la voie à suivre consiste à se concentrer sur l'orientation et le mandat plutôt que sur les détails : résilience, atténuation des risques tiers, déclaration obligatoire des violations, tests continus et capacités de restauration.

FIGURE 4

Aperçu des réglementations en évolution et émergentes



Source : *EMEA Digital Regulations and Policies Research*, IDC, 2025

PERSPECTIVES ET RECOMMANDATIONS

La première action à mener est une checklist de résilience des données Microsoft 365 couvrant la stratégie data, la transformation RH et des processus, et les contrôles techniques. Cette approche “by design” intègre portabilité et contrôle.

La stratégie de contrôle technique doit couvrir les trois piliers de la souveraineté des données :

- **La compétence juridique** *permet de clarifier les lois applicables aux données de sauvegarde et aux accès aux données.* La possibilité de gérer les clés de chiffrement offre un niveau de sécurité supplémentaire contre les injonctions provenant de l’étranger.
- **La résidence des données** *garantit le choix et la flexibilité de l'endroit où les données de sauvegarde sont stockées et permet de contrôler les mouvements et les audits des données.* Cependant, stocker la sauvegarde sur le même environnement cloud peut annuler l’indépendance. Idéalement, il faut stocker aussi les métadonnées (noms de fichiers, informations utilisateurs) dans le périmètre souverain défini.
- **L'autonomie opérationnelle** *permet de vérifier que la plateforme de protection des données offre le contrôle nécessaire à la cyber-résilience et à la conformité réglementaire.* L’immuabilité des sauvegardes (avec journaux d’audit traçables) est centrale contre les ransomwares et menaces internes. Les sauvegardes doivent être séparées (domaine et identifiants distincts) pour éviter une propagation depuis Microsoft 365. D'autres mécanismes incluent la restauration granulaire, un délai de restauration plus rapide (OTR) et l'étendue de la couverture (Exchange, SharePoint, OneDrive, Teams et les configurations Azure/Entra ID). Il est essentiel que *toutes* les données soient sauvegardées et sécurisées et que les équipes IT puissent restaurer l'ensemble de la structure opérationnelle avec un minimum d'interruptions.

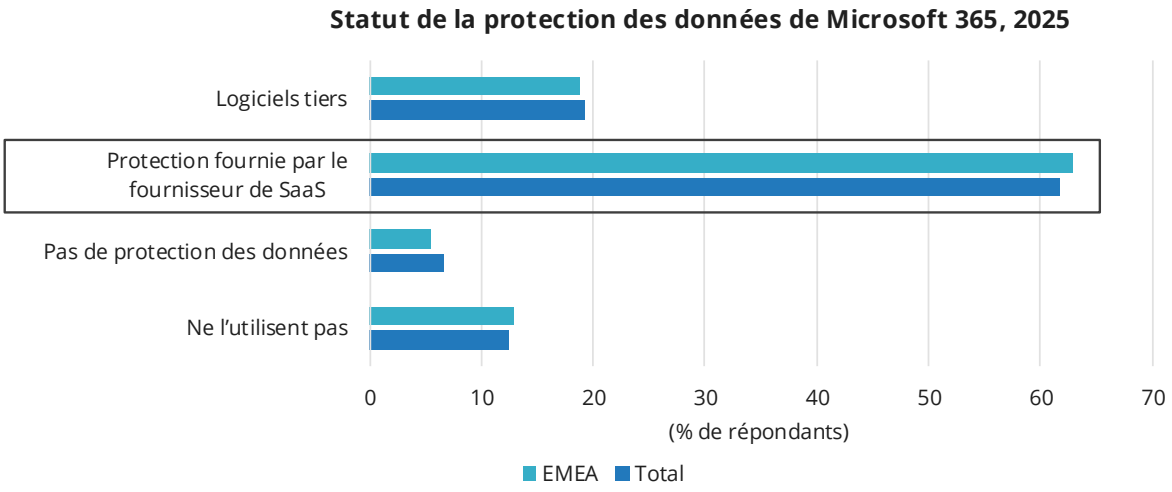
DEFIS ET OPPORTUNITES

Bien que la souveraineté des données fasse l'objet d'une attention accrue, rares sont les organisations qui joignent le geste à la parole. En fait, de nombreuses organisations sont confrontées à des risques considérables en matière de conformité, de continuité des activités, de résilience et de souveraineté, car elles n'ont pas intégré de stratégies élémentaires d'atténuation des risques, telles que la sauvegarde Microsoft 365.

Comme le montre la figure 5, un nombre important d'organisations continuent de s'appuyer sur des stratégies de protection des données natives de Microsoft 365, selon l'enquête *Cloud Data Logistics and Protection Survey*, IDC, août 2025.

FIGURE 5

Importance d'investir dans les éléments fondamentaux de la résilience



n = 832 au total, n = 142 pour l'EMEA

Source : *Cloud Data Logistics and Protection Survey,* IDC, août 2025

Si la sauvegarde native est un bon point de départ, elle n'est pas suffisante. Les entreprises doivent être conscientes des risques encourus :

- Des politiques de conservation par défaut limitées et rigides signifient que les organisations sont susceptibles de perdre des données après seulement 90 jours, ce qui entraîne des pertes de données ou des problèmes de conformité.
- Des capacités limitées en matière de restauration granulaire et plus rapide des données peuvent limiter la capacité des organisations à rebondir rapidement en cas de cyberattaque.

Le contrôle et l'autonomie limités sur les données signifient que les organisations doivent s'en remettre aux politiques et aux stratégies de sécurité du fournisseur SaaS et qu'elles ne disposeront pas d'un accès flexible aux données pour les usages secondaires tels que les tests et le développement, l'analyse, la planification de scénarios ou les tests de restauration.

CONCLUSION

La souveraineté des données ou un « environnement Microsoft 365 souverain » n'est pas un produit unique mais un ensemble de choix architecturaux et de cadres juridiques.

Les organisations doivent établir une stratégie de données résiliente qui inclut la veille réglementaire. Elles doivent transformer leurs processus en commençant par la classification des données, la documentation des rôles et des responsabilités et des politiques de risque de l'organisation. Cela permet de canaliser les investissements de sécurité des données vers les bons domaines et d'obtenir une résilience maximale.

La sauvegarde joue un rôle critique pour assurer la souveraineté Microsoft 365 : elle ajoute une couche de contrôle juridique et opérationnel que l'environnement natif ne garantit pas pleinement.

La stratégie de sauvegarde assure l'autonomie opérationnelle et garantit que l'accès et la gestion des données sont sous le contrôle des clients. Elle permet également aux organisations de choisir et de garantir un emplacement de sauvegarde dans un pays spécifique de l'UE ou du Royaume-Uni pour des raisons de conformité réglementaire.

Une stratégie de protection des données par un tiers permet également de garantir l'immuabilité des données, c'est-à-dire qu'une fois écrites, elles ne peuvent pas être modifiées, écrasées ou supprimées pendant une période de conservation déterminée. L'isolement physique (air-gap) fournit une couche d'isolation logique ou physique du réseau afin de réduire des risques variés (ransomware, malveillance interne, erreur humaine).

La conformité minimale viable ne suffit plus. Face à l'escalade des exigences, les directions IT et métiers doivent architecturer une sécurité des données et une résilience proactives et multicouches.

La souveraineté des données est la clé de votre résilience : déployez des mécanismes opérationnels ciblés et décisifs pour construire une fondation numérique de confiance.

MESSAGE DU SPONSOR

Veeam est le leader mondial de la résilience des données, garantissant une continuité d'activité sans compromis. Veeam vous permet de reprendre la main sur la sécurité de vos données grâce à des solutions de sauvegarde robustes qui protègent vos informations critiques et assurent une restauration rapide en cas de perte.

Veeam Data Cloud pour Microsoft 365 et Entra ID offre la solution de sauvegarde SaaS la plus complète et moderne pour contrer les cybermenaces et les pertes de données. Protégez vos données sur Exchange, SharePoint, OneDrive, Teams et Entra ID — au sein d'une solution unique.

Avec Veeam à vos côtés, protégez vos données et sécurisez vos accès, pour vous concentrer sur l'essentiel : progresser et avancer.

Pour en savoir plus, consultez le site https://www.veeam.com/products/saas/microsoft-office-365-entra-id-backup-service.html.

À PROPOS D'IDC

International Data Corporation (IDC) est le premier fournisseur mondial d'études, de conseils et d'événements pour les marchés des technologies de l'information, des télécommunications et des technologies grand public. Avec plus de 1 300 analystes dans le monde, IDC apporte une expertise globale, régionale et locale dans plus de 110 pays, aidant les professionnels de l'IT, les dirigeants et la communauté financière à prendre des décisions technologiques fondées sur les faits et à atteindre leurs objectifs clés. Fondée en 1964, IDC est une filiale détenue à 100 % par International Data Group (IDG, Inc.).

Siège social mondial :

140 Kendrick Street
Building B
Needham, MA 02494
États-Unis
+1.508.872.8200
Twitter : @IDC
blogs.idc.com
www.idc.com