IDC PERSPECTIVE

Protection des données pour Microsoft Office 365 : négliger la sauvegarde et la restauration compromet la résilience, la continuité des activités et la productivité de l'entreprise

Archana Venkatraman

SYNOPSIS

Synopsis : La stratégie de protection des données pour Microsoft Office 365

Ce document IDC Perspective présente le point de vue d'IDC sur les stratégies de protection des données pour Microsoft Office 365 (O365). La solution Office 365 est de plus en plus utilisée dans le contexte post-pandémique actuel où les entreprises adoptent rapidement des outils software-as-a-service (SaaS) pour la bureautique et le travail collaboratif dans une logique de productivité, de résilience numérique et de continuité des activités. Office 365 occupe donc une place centrale dans l'entreprise ; il est donc impératif d'y appliquer une politique de protection de données pour en garantir la sécurité, la conformité et la restauration. Sans cela, l'entreprise s'expose à des risques.

Principaux éléments à retenir

- L'utilisation de la solution O365 (ou Microsoft 365) s'étend au-delà de la messagerie électronique et concerne de plus en plus Teams, SharePoint, OneNote, OneDrive, etc. L'utilisation croissante des produits O365 entraîne une augmentation des volumes de données dans l'environnement SaaS.
- Seulement 23 % des entreprises interrogées par IDC ont indiqué qu'elles utilisaient une solution tierce de sauvegarde pour leurs environnements O365. Les entreprises les plus avancées dans le processus de transformation numérique sont plus susceptibles de disposer d'une solution dédiée à la protection des données des environnements O365 que les entreprises à la traîne dans ce domaine.
- Sans stratégie de protection des données dédiée, les entreprises s'exposent à de nombreux risques, tels que des attaques par ransomware, des effacements de données accidentels ou d'autres pertes de données, des défauts de conformité, des failles dans la rétention des données et une dépendance vis-à-vis des environnements SaaS.

Mesures recommandées

- Lorsque les entreprises choisissent d'utiliser des services cloud, elles doivent bien comprendre ce qu'implique le « principe de la responsabilité partagée ».
- Placez la sauvegarde des environnements O365 en tête de vos priorités afin de garantir la résilience et la continuité de vos activités.
- Exploitez les fonctions natives du prestataire SaaS, ainsi que les mécanismes de sécurité mis en place au niveau de l'infrastructure. Mais n'oubliez pas de renforcer cette sécurité de base à l'aide d'une solution tierce de protection des données permettant de minimiser les risques liés à l'utilisation des solutions SaaS.
- Assurez-vous que votre stratégie de protection des données s'applique à toutes les données hébergées dans l'ensemble des environnements IT, y compris votre datacenter, les environnements multicloud, les environnements SaaS, ainsi que les platform-as-a-service (PaaS).

Source : IDC, 2020

Décembre 2020, IDC N° EUR147031720

VUE D'ENSEMBLE DE LA SITUATION

Les applications SaaS telles que Microsoft 365 (et les anciennes versions d'Office 365) sont considérées comme essentielles pour moderniser l'expérience des employés, intégrer de nouveaux outils collaboratifs et créer un environnement de travail numérique. Pendant la pandémie de COVID-19, les outils de messagerie électronique et collaboratifs des applications SaaS ont été largement utilisés pour le travail à distance. L'analyse des derniers résultats financiers (1er trimestre 2021) de Microsoft montre que l'entreprise a connu une croissance rapide de son chiffre d'affaires grâce aux activités de cloud computing. Les revenus générés par Office 365 ont notamment augmenté de 21 %.

Au cours une enquête récente d'IDC conduite auprès d'utilisateurs finaux, plus de 77 % des entreprises interrogées ont affirmé qu'elles utilisaient Microsoft Office 365. Selon l'enquête d'IDC de novembre 2020 intitulée *European Software Survey*, au moins 90 % des entreprises des pays économiquement avancés, tels que le Royaume-Uni, utilisent O365.

O365 : au-delà de la messagerie électronique

L'environnement Microsoft Office englobe de nombreuses applications de productivité et collaboratives, telles que Microsoft Exchange, Teams, OneDrive, OneNote et SharePoint. Avec plus de 115 millions d'utilisateurs quotidiens (selon un billet de blog de Microsoft publié le 16 novembre 2020), Teams devient un outil incontournable pour le travail collaboratif à distance. Les entreprises cherchent à l'utiliser comme une plateforme permettant de créer des applications et des services spécifiques.

Microsoft place Teams au centre de ses innovations pour O365 en apportant les améliorations suivantes :

- Rapprochement de Power Platform
- Possibilité pour les utilisateurs de créer, partager et suivre des données directement au sein de l'outil
- Mise à disposition d'outils de développement (tels que Microsoft Teams Toolkit pour Visual Studio et Visual Studio Code) pour commencer à développer des applications Teams.

Teams est utilisée partout. Selon le rapport financier de Microsoft du 4ème trimestre 2020, plus de 1 800 entreprises comptent plus de 10 000 utilisateurs de Teams et plus de 70 entreprises en comptent au moins 100 000. Dans le secteur des soins de santé, l'application est de plus en plus utilisée. Par exemple, le NHS au Royaume-Uni a choisi Microsoft 365 dont les outils de productivité et collaboratifs sont utilisés par 1,2 million d'employés afin d'améliorer l'expérience des patients. En outre, le nombre d'utilisateurs de Microsoft 365 E5 a plus que doublé en une année.

L'accroissement des usages d'O365 provoque une augmentation du volume de données généré.

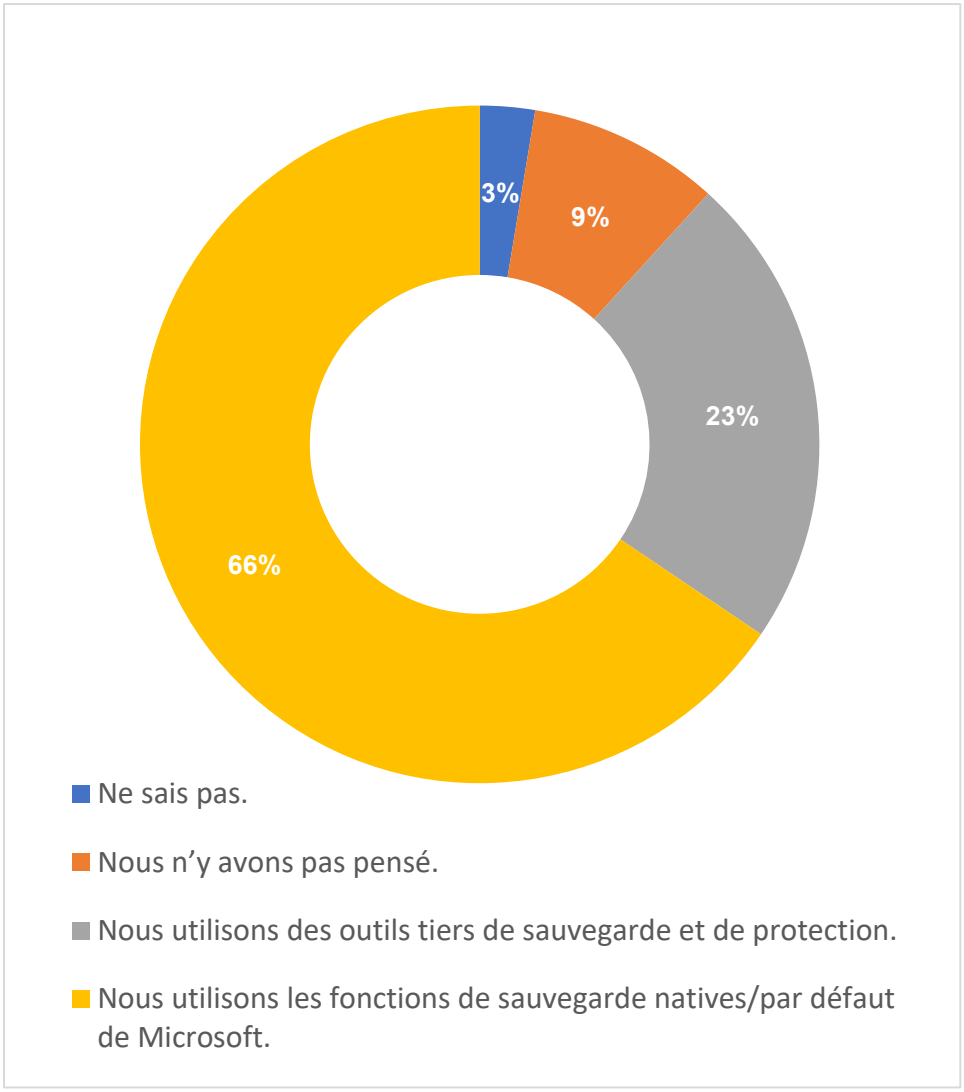
La mise en place d'une protection des données dédiée est souvent le fruit d'une réflexion après-coup

Tandis qu'O365 devient le centre de productivité de l'entreprise, la stratégie de protection des données dédiée à l'environnement O365 s'inscrit aujourd'hui encore dans une réflexion après-coup, comme le montre le Graphique 1.

GRAPHIQUE 1

Stratégies de protection des données des environnements O365 dans les entreprises européennes

Q. *Comment votre entreprise protège-t-elle, stocke-t-elle et restaure-t-elle ses données dans les environnements O365 (Exchange, SharePoint, OneDrive, Teams, etc.) ?*



Source : *European Software Survey*, IDC, novembre 2020 (n = 634)

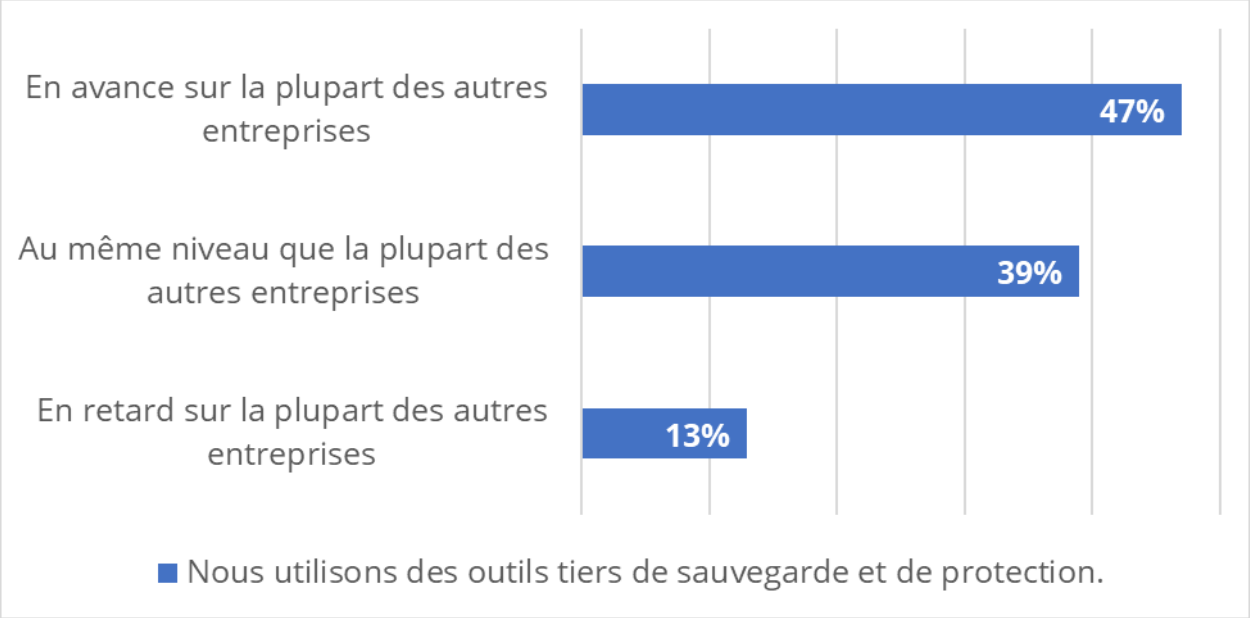
Les résultats de cette enquête montrent que :

- Seulement 23 % des entreprises interrogées par IDC utilisent un service tiers dédié de sauvegarde et de restauration des données pour protéger leur environnement O365/M365.
- 77 % des utilisateurs de M365 et O365 utilisent les fonctionnalités natives de Microsoft ou n'ont pas réfléchi à la protection des données pour leur environnement de messagerie électronique et collaboratif cloud.

Les entreprises les plus avancées dans le processus de transformation numérique sont plus susceptibles d'utiliser des technologies dédiées de protection des données SaaS pour assurer la continuité des activités et la restauration des données, comme le montre le Graphique 3.

GRAPHIQUE 2

Utilisation de services dédiés de protection des données : comparaison entre les leaders du numérique et les entreprises à la traîne dans ce domaine



Source : *European Solutions logicielles Survey*, IDC, novembre 2020 (n = 634)

Du point de vue des secteurs d'activité, seules les entreprises des secteurs de l'assurance, des télécommunications et des prestations de services avaient mis en place une solide stratégie pour la protection des données dans leurs environnements O365/M365.

CONSEILS POUR LES ACHETEURS DE SOLUTIONS TECHNOLOGIQUES

Microsoft améliore en permanence les fonctionnalités et la sécurité de ses environnements O365. Par exemple, de nouvelles fonctionnalités ont été ajoutées, telle que Microsoft Endpoint Data Loss Prevention (DLP), afin d'éviter les pertes de données sur les postes de travail. D'autres fonctionnalités ont également été ajoutées afin de mieux gérer les alertes DLP. Par ailleurs, Microsoft apporte constamment des améliorations à ses SLA, ainsi qu'à la régularité et à la disponibilité de ces mêmes services.

IDC estime que les fonctions natives de sauvegarde et de stockage proposées par défaut dans O365 peuvent servir de point de départ, mais qu'elles ne suffisent pas à répondre à tous les besoins en matière de conformité et de continuité des activités.

Le véritable danger est justement lié au fait que de nombreuses entreprises pensent que ces fonctions natives offrent toutes les garanties de protection dont elles ont besoin. En discutant avec les utilisateurs d'O365, IDC constate que de nombreux utilisateurs confondent les accords de niveau de services (SLA) proposés par Microsoft en matière de disponibilité et les stratégies de sauvegarde. D'autres estiment qu'il n'est pas nécessaire de réfléchir à une stratégie de sauvegarde pour le cloud compte tenu des « caractéristiques propres » à cette technologie.

L'utilisation d'O365 sans système de sauvegarde avancé est risquée

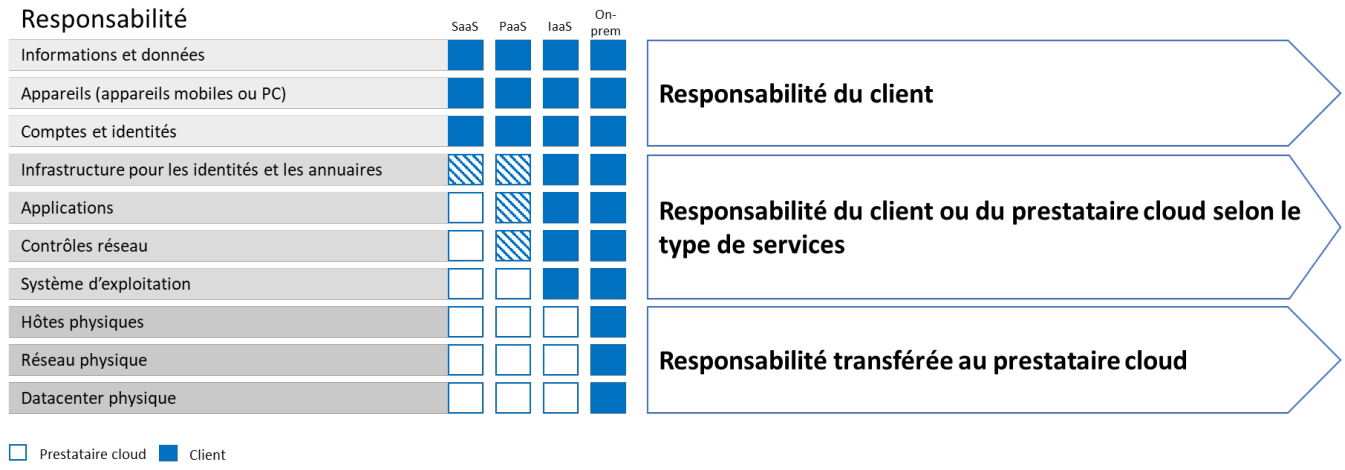
Indépendamment de l'emplacement des données (on-premise ou sur une infrastructure cloud/SaaS, telle que l'environnement 'O365), la protection des données incombe au client ou au propriétaire des données, c'est-à-dire vous.

Le principe de la responsabilité partagée

Les entreprises qui choisissent d'utiliser des services du cloud public doivent parfaitement comprendre le « principe de la responsabilité partagée ». Celui-ci répartit les responsabilités entre le prestataire cloud (le sous-traitant) et l'utilisateur des services cloud (le responsable du traitement).

GRAPHIQUE 3

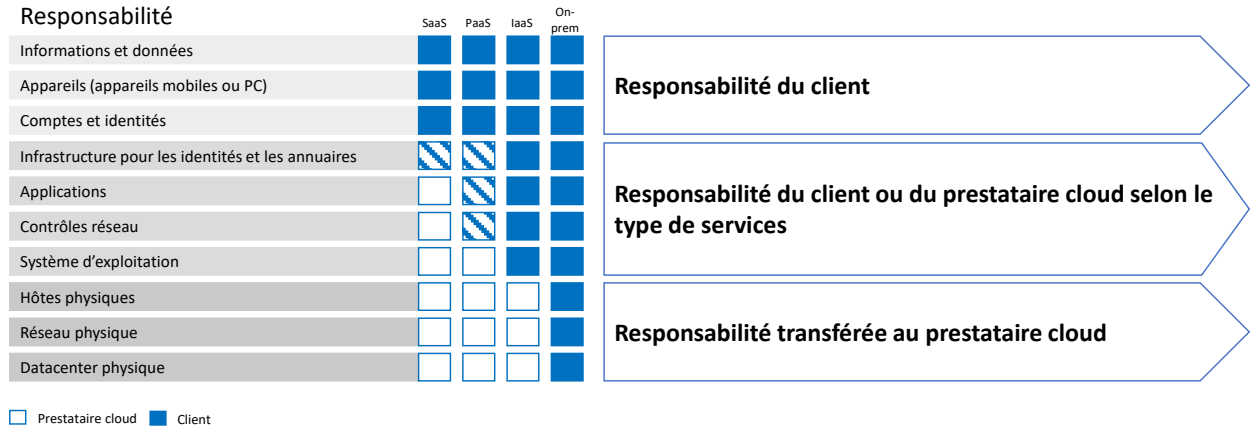
Principe de la responsabilité partagée dans les environnements SaaS et IaaS, et on-premise



Source : Microsoft, 2020

GRAPHIQUE 4

Vue synthétique du principe de la responsabilité partagée entre le prestataire et le client pour Microsoft Office 365



Source : IDC, 2020

Recommandations du prestataire cloud et bonnes pratiques

Dans son accord de service, Microsoft recommande d'utiliser une solution tierce de sauvegarde et de restauration. À l'article 6b portant sur la disponibilité des services, il est inscrit la mention suivante :

> Nous nous efforçons de maintenir les services en fonctionnement ; toutefois, tous les services en ligne font l'objet de perturbations et de pannes occasionnelles. En cas de panne ou de perturbation du service, il se peut que la récupération de votre contenu soit temporairement impossible. Nous vous recommandons de sauvegarder régulièrement votre contenu, ainsi que les données que vous stockez sur les services, ou que vous stockez en utilisant des applications et des services tiers.

Les fonctions natives d'eDiscovery et de mise en suspens juridique ne sont pas suffisantes

Les fonctions de mise en suspens juridique de Microsoft 365 sont fiables, mais elles ne remplacent pas entièrement une stratégie de sauvegarde et de restauration. Par exemple, au cours de leurs échanges avec IDC, certains clients ont souligné la nécessité de pouvoir rapidement accéder et récupérer les données afin de se conformer aux exigences de recherche de preuves électroniques (eDiscovery). Ils doivent prendre en compte le coût et les frais généraux IT liés à la restauration de données spécifiques stockées dans différents formats et sur différents appareils dans des délais susceptibles de varier. La fonction de mise en suspens juridique peut ne pas suffire, car elle ne permet pas de récupérer des données accidentellement effacées ou de garantir une restauration rapide de volumes de données importants. Une protection dédiée pour l'ensemble des données, y compris les données SaaS, peut aider les entreprises à garantir la mise en suspens de leurs données à des fins juridiques en collectant les données de toutes les applications, y compris celles d'O365, tout en maîtrisant les coûts.

Exposition aux risques

Étant donné que la responsabilité de Microsoft et les technologies associées à cette responsabilité portent essentiellement sur l'infrastructure, la sécurité logique et la disponibilité, les entreprises sont exposées aux risques suivants lorsqu'elles ne disposent pas de plans de sauvegarde tiers :

- **Perte de données, effacement accidentel et violations de sécurité.** O365 n'échappe pas aux violations de sécurité. Le produit est vulnérable aux menaces internes (p. ex., l'effacement accidentel de données, les représailles d'employés mécontents ou les accès par d'anciens employés) et aux menaces externes (p. ex., attaques par malware ou ransomware). Dans le cadre d'une enquête d'IDC de 2020 intitulée *European Multicloud Survey*, les entreprises interrogées ont indiqué que les ransomwares, la hausse des coûts et la protection des données SaaS constituaient les principaux défis à surmonter en matière de protection des données.
- **Risques liés à la rétention des données et à la conformité réglementaire.** La politique de rétention de Microsoft s'étend sur 90 jours, ce qui ne permet pas de respecter les réglementations les plus exigeantes en vigueur dans certains secteurs d'activité, tels que les services financiers, les soins de santé, le commerce de détail ou le secteur public. Grâce à une solution de sauvegarde tierce, les entreprises peuvent définir leur propre politique de rétention en fonction de leurs besoins et respecter ainsi les réglementations européennes sur les données.
- **Manque de contrôle des données dans les environnements hybrides.** La surveillance et le contrôle des données font désormais partie des priorités fixées par les conseils d'administration et constituent une première étape pour toute entreprise numérique basée sur les données. Sans sauvegarde, les entreprises ne disposent d'aucune stratégie de sortie ou marge de manœuvre face aux risques inhérents à la concentration des données SaaS.

CONSEILS POUR LES ACHETEURS DE SOLUTIONS TECHNOLOGIQUES

Si les entreprises n'étendent pas la protection des données aux environnements SaaS, tels que M365 ou O365, elles exposeront leurs données à des problèmes de conformité, à un risque de perte et à des vulnérabilités de sécurité, compromettant ainsi la continuité de leurs activités.

La sauvegarde des données des environnements SaaS – alors en pleine expansion -, telles qu'O365, n'est plus une option. Elle est devenue un impératif pour la sécurité et le contrôle des données.

La plupart des fournisseurs de solutions dédiées à la protection des données proposent des options de sauvegarde et de restauration des environnements O365 et ajoutent continuellement de nouveaux services O365 à leurs solutions. Avant d'investir dans l'une d'entre elles, les entreprises doivent s'assurer qu'elle réponde aux exigences suivantes :

- **Flexibilité et liberté de choix.** L'entreprise doit avoir la possibilité de choisir entre le on-premise ou le cloud comme destination de sauvegarde des environnements O365.
- **Fonctionnalités avancées.** La solution doit supporter les sauvegardes incrémentales, la restauration granulaire, l'automatisation et la rétention en fonction de règles définies.
- **Étendue du service.** La solution doit permettre de protéger un large éventail d'environnements de M365, y compris la gestion des courriers électroniques, Teams, SharePoint, etc.
- **Complémentarité avec O365.** Elle doit être totalement intégrée à O365 et à l'environnement de protection des données de l'entreprise.
- **Innovation.** Elle doit offrir des fonctionnalités de sécurité supplémentaires, telles que le contrôle des accès, des indicateurs d'utilisation de la solution SaaS et une authentification multifacteur permettant de renforcer la sécurité.
- **Évolutivité.** La solution de sauvegarde doit permettre une mise à l'échelle (scale-up et scale-down), sans investissement supplémentaire et en fonction des variations des activités et de la demande de données. Elle doit également suivre l'évolution du déploiement de la solution SaaS dans l'entreprise.

EN SAVOIR PLUS

Études en rapport avec le présent document

- *Western Europe Public Cloud IaaS Storage Market Forecast, 2019-2024: The COVID-19 Pandemic Keeps IaaS Storage Investments Resilient* (IDC n° EUR146999320, novembre 2020)
- *Commvault Brings Metallic SaaS Data Protection to Europe Amid Growing Demand for Cloud-Based Backup* (IDC n° IcEUR146988220, novembre 2020)
- *IDC FutureScape: Worldwide Data and Analytics 2021 Predictions* (IDC n° US46920420, octobre 2020)

En résumé

Ce document IDC Perspective présente le point de vue d'IDC sur les stratégies de protection des données pour Microsoft Office 365. Les applications SaaS rencontrent un succès croissant et l'utilisation de Microsoft Office 365 s'étend désormais à d'autres services qu'Exchange, tels que SharePoint, OneDrive et Teams. Ces services permettent d'améliorer la productivité des employés et de promouvoir le travail collaboratif dans le contexte post-pandémique actuel.

« Même si O365 devient rapidement l'une des clés de la productivité de l'entreprise, les stratégies de sauvegarde et de restauration s'inscrivent souvent dans une réflexion après-coup. Moins d'un quart des utilisateurs d'O365 disposent d'une solution de protection des données tierce dédiée à O365.

Alors que les données créées dans les environnements O365 se multiplient, les utilisateurs doivent prendre conscience qu'il leur incombe de les protéger, quel que soit l'endroit où elles se trouvent », a déclaré Archana Venkatraman, directrice de recherche, IDC European Datacenter. « Sans stratégie de sauvegarde et de restauration spécifique, les entreprises exposent leurs données O365 à de nombreux risques, tels que des attaques par ransomware, des effacements de données accidentels et des défauts de conformité, qui compromettront la résilience et la continuité de leurs activités. »

À propos d'IDC

IDC est un acteur majeur de la recherche, du conseil et de l'événementiel sur les marchés des technologies de l'information, des télécommunications et des technologies grand public. IDC aide les professionnels évoluant sur les marchés IT et les investisseurs à prendre des décisions stratégiques basées sur des données factuelles. Plus de 1 100 analystes d'IDC proposent leur expertise globale, régionale et locale sur les opportunités et les tendances technologies dans plus de 110 pays à travers le monde. Depuis plus de 50 ans, IDC propose des analyses stratégiques pour aider ses clients à atteindre leurs objectifs clés. IDC est une filiale d'IDG, leader mondial dans les domaines des médias, de la recherche et des événements liés à la technologie.

IDC Royaume-Uni

IDC R.U.
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, Royaume-Uni
Tél. : 44.208.987.7100
Twitter : @IDC
idc-community.com
www.idc.com