Mars 2021

ÉTUDE DE MARCHÉ

Sauvegarde Office 365 : état des lieux

La généralisation du travail à distance complexifie la protection des données. »

Barracuda
Your journey, secured.

Sommaire

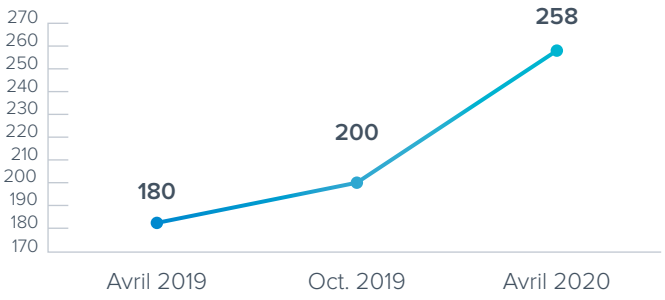
Introduction

Assurer la protection des données Office 365

On assiste à une véritable explosion des données Microsoft Office 365 et leur protection revêt un caractère urgent.

Office 365 connaît une croissance exceptionnelle, encore plus dans le contexte actuel, où le travail à distance se généralise. Selon le blog Thexyz, en mars 2020, le nombre de minutes des réunions Teams a augmenté de 380 % au cours des 19 premiers jours de la pandémie, passant ainsi de 560 millions à 2,7 milliards par jour. En avril dernier, on comptait 258 millions d'utilisateurs sous licence et 75 millions d'utilisateurs Teams actifs par jour.

Utilisateurs actifs mensuels O365 (millions)



Le nombre moyen d'utilisateurs Office 365 supplémentaires par mois a quasiment quadruplé entre octobre 2019 et avril 2020, en raison notamment de l'utilisation intensive d'outils de collaboration pendant la pandémie.

Les responsables informatiques sont conscients de la dépendance de leur entreprise à Office 365 et de la nécessité d'en assurer la protection. Toutefois, la confusion règne quant aux fonctionnalités natives de protection qui sont incluses ou non dans Office 365.

En effet, Microsoft recommande aux clients d'effectuer une sauvegarde sur une solution tierce car la société garantit uniquement la disponibilité de son service, et non la conservation des données. Étant donné que, d'origine, Microsoft inclut un certain niveau de conservation des données, les clients peuvent ne pas avoir conscience de ses limites jusqu'à ce qu'un problème survienne.

Les clients peuvent également trouver les outils natifs de Microsoft relativement basiques, rendant les tâches de restauration relativement difficiles et chronophages. Les entreprises cherchant à protéger des données de plus en plus nombreuses expriment leurs inquiétudes quant à l'exhaustivité des solutions de sauvegarde et de conservation, leur niveau de sécurité et de conformité, et, par dessus tout, la facilité à les déployer et à les utiliser.

Ce rapport se penche sur les préoccupations et les préférences des professionnels de l'informatique concernant Office 365, la sécurité des données, la sauvegarde et la restauration, les solutions SaaS (Software-as-a-Service) et les sujets connexes.

Méthodologie

En janvier 2021, Centropy, un cabinet d'études indépendant, a réalisé une enquête à la demande de Barracuda auprès des décisionnaires informatiques en charge de l'infrastructure cloud de leur entreprise. Parmi les participants figurent **1 828 décisionnaires informatiques** évoluant dans des entreprises qui comptent 50 employés ou plus, aux **États-Unis, en EMEA et en APAC**.

Résultats clés

CONSTAT N°1

Protéger les données contre les attaques et les pertes (qu'elles soient le fait d'acteurs externes ou internes) est une préoccupation majeure.

Les données doivent être protégées contre les attaques extérieures, de type ransomware par exemple, mais aussi contre les pertes internes, telles que les suppressions accidentelles ou malveillantes. Quoi qu'il en soit, dans les deux cas, les participants souhaitent vivement que les données soient protégées et sécurisées.

Les attaques par ransomware ne surviennent peut-être pas tous les jours mais elles ne restent pas moins en tête des préoccupations, ce qui est tout à fait normal étant donné les dernières tendances observées dans les actualités. Si la presse fait état des retombées et souvent des méthodes utilisées, elle ne précise cependant pas ce qui était ciblé, et ce, par crainte que cette information ne soit exploitée dans de futures attaques.

Bien qu'ils ignorent la nature de ce qui a été attaqué, les participants ont bien conscience qu'Office 365 peut être la cible potentielle de ransomwares. En effet, 72 % d'entre eux se disent inquiets qu'une telle attaque ne se produise. Cette inquiétude était plus marquée aux États-Unis (83 %), moins dans la région EMEA (67 %) ; la région APAC se situant entre les deux, avec 73 %.

Cela n'est sans doute pas surprenant, puisque que plus de la moitié des participants a été victime d'un ransomware. Les différences géographiques illustrent la même tendance : près des deux tiers des participants américains (64 %) ont été victimes d'un ransomware, contre 55 % en APAC et seulement 43 % dans la zone EMEA. Le désagrément qui accompagne le blocage de la messagerie ou de l'application collaborative est évident, notamment avec le travail à distance qui se généralise.

Un autre facteur qui augmente la crainte autour des ransomwares est la tendance actuelle à l'exfiltration des données : les données sont volées avant d'être bloquées et le propriétaire doit payer une rançon s'il veut les récupérer. S'il refuse de payer, alors ses données sont vendues au plus offrant sur le dark Web. Des violations de données telles que celles-ci sont potentiellement embarrassantes et souvent coûteuses.

En matière de protection des données, garantir la sécurité contre les suppressions accidentelles ou malveillantes s'avère une problématique beaucoup plus répandue et tout aussi préoccupante. Près de 80 % des personnes interrogées souhaitent disposer de plusieurs couches de contrôle d'accès basé sur les rôles, et ce, dans le but de limiter toute action potentiellement nocive, telle que la suppression et la purge de données.

J'ai peur que des ransomwares ne bloquent ou n'attaquent mes données Office 365.
72 % sont d'accord (n = 1 793)

Mon entreprise a été victime d'une attaque par ransomware.
52 % sont d'accord (n = 1 741)

Disposer d'un accès multi-couche basé sur les rôles pour les sauvegardes est important pour moi.
79 % sont d'accord (n = 1 828))

Résultats clés

CONSTAT N°2

Les entreprises souhaitent bénéficier d'un niveau de restauration plus granulaire et d'autres fonctionnalités que Microsoft ne propose pas en natif.

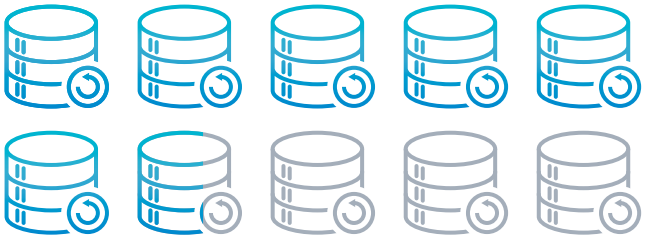
Étonnamment, seul un tiers des personnes interrogées ont déployé une solution de sauvegarde tierce ; 67 % comptent encore sur les fonctionnalités de conservation et de restauration des dossiers supprimés intégrées à Microsoft, malgré la complexité de ces politiques de conservation et l'impossibilité de restaurer les éléments de manière précise. Ce pourcentage était le plus élevé aux États-Unis, 74 % des participants se fiant uniquement à Office 365 pour leur sauvegarde. En comparaison, seuls 61 % en EMEA et 70 % dans la région APAC adoptent cette approche.

81 % des participants expliquent notamment que l'utilisation de Teams est problématique du point de vue de la conservation des données. Par exemple, au cours du premier mois plein de la pandémie, Microsoft a enregistré une augmentation de 380 % de l'utilisation de Teams.

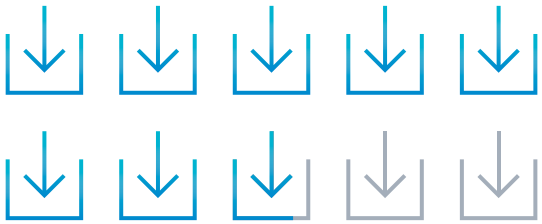
Plus de 80 % des participants souhaitent disposer d'une solution de sauvegarde qui prenne en charge Teams ainsi que les fichiers partagés. Ils souhaitent également qu'Office 365 propose un stockage illimité et avoir la possibilité de télécharger une copie des éléments récupérés.

Selon un rapport de l'IT Policy Compliance Group, plus des trois quarts des demandes de récupération adressées aux équipes informatiques sont dues à une suppression accidentelle. L'utilisation des processus de récupération des dossiers supprimés et de restauration assistée proposés par Microsoft s'avère chronophage, compliquée et sujette aux erreurs. Dans de nombreux cas, la restauration d'un répertoire entier pour retrouver un élément supprimé peut, par inadvertance, écraser des données plus récentes et engendrer de nouveaux problèmes.

Je me fie uniquement aux fonctionnalités intégrées à Office 365 pour sauvegarder et récupérer les données Office 365.
67 % sont d'accord (n = 1 779)



Un niveau de restauration granulaire d'Exchange, SharePoint, OneDrive et Teams est important pour moi.
77 % sont d'accord (n = 1 828)



Ce n'est donc pas étonnant que la sauvegarde des données Office 365, comprenant un niveau de restauration granulaire, soit largement réclamée.

Un pourcentage relativement similaire déclare que la possibilité de restaurer des boîtes aux lettres vers un emplacement ou un utilisateur différent est importante. Or, ce n'est pas chose aisée avec les fonctionnalités natives de Microsoft. Lorsqu'un employé quitte une entreprise, il passe au statut d'« utilisateur supprimé » au bout de 30 jours et ses données ne peuvent pas être enregistrées sur un autre emplacement ou utilisateur.

La facilité d'utilisation s'applique également à la connexion. En termes de relation entre les services Azure Active Directory (AAD) et les autres solutions déployées dans les entreprises, 76 % des personnes interrogées expliquent vouloir bénéficier de l'authentification unique via AAD.

Enfin, les trois quarts des participants souhaiteraient obtenir des rapports quotidiens sur toutes les sauvegardes, restaurations et exportations. Bien que ce point ne semble pas révolutionnaire, il est primordial de garder une trace de ses sauvegardes, et ce, pour une raison toute simple : cela peut contribuer à protéger les données en signalant rapidement toute activité suspecte dans votre système.

...il est primordial de garder une trace de ses sauvegardes, et ce, pour une raison toute simple : cela peut contribuer à protéger les données en signalant rapidement toute activité suspecte dans votre système.

Résultats clés

CONSTAT N°3

La protection des données est à la fois un enjeu de sécurité et de conformité réglementaire.

Pour de nombreuses entreprises, le lieu de stockage des données joue un rôle important, tant sur le plan de la sécurité que sur le plan réglementaire. Les données contiennent souvent des informations sensibles et doivent donc non seulement être sécurisées, mais ce niveau de sécurité doit lui-même répondre aux exigences et réglementations gouvernementales en matière de conformité. Il existe également des lois relatives à l'emplacement des données dans différents pays. Elles précisent les modalités de collecte, d'utilisation et de stockage des données de leurs citoyens ou leurs résidents. Ces exigences peuvent comporter des délais de conservation des données et l'obligation de supprimer certaines d'entre elles sur demande.

Les réglementations peuvent varier d'un pays à l'autre, si bien que les entreprises doivent se soumettre aux différentes exigences locales ; une tâche qui se révèle ardue pour les multinationales. Prenons l'exemple de l'Union Européenne : certains types de données sensibles doivent être stockés dans des emplacements physiques ou géographiques spécifiques.

Près de 7 personnes interrogées sur 10 se disent préoccupées par cette conformité, ce qui peut tout à fait se comprendre lorsque l'on sait que les amendes infligées en cas de violation peuvent atteindre 20 millions d'euros ou représenter un certain pourcentage des recettes annuelles de l'année précédente, le montant le plus élevé étant retenu.

Fait intéressant : les participants américains manifestent le plus d'inquiétude (80 %) concernant la sauvegarde de leurs données en dehors de leur zone géographique. En comparaison, 69 % des personnes interrogées en APAC et 65 % en EMEA déclarent que ce sujet les préoccupe. Ceci s'explique certainement par les différents degrés de complexité de ces exigences selon les zones géographiques. Par exemple, les exigences sont plus complètes en France et en Allemagne, mais aux États-Unis et en Inde, elles ne s'appliquent qu'à certains secteurs ou ne concernent que certains types de données. Les résultats suggèrent que dans les pays où les règles varient, les gens se révèlent plus inquiets parce qu'ils ne sont pas sûrs de s'y prendre correctement.

Il en va de même pour la confidentialité des données : 85 % des participants américains admettent que le sujet les préoccupe, tandis qu'ils ne sont que 75 % en APAC et 64 % en EMEA. Cela signifie que dans les pays où le RGPD est en vigueur depuis plusieurs années, les responsables informatiques se montrent plus confiants face à la marche à suivre pour respecter les lois relatives à la confidentialité des données. En revanche, aux États-Unis, ces réglementations varient encore d'un État à l'autre. Les responsables informatiques se montrent donc moins confiants lorsqu'il s'agit de rester en phase avec tout un ensemble d'exigences changeantes.

La sauvegarde des données en dehors de ma zone géographique (emplacement géographique des données) est une source d'inquiétude pour moi.
69 % sont d'accord (n = 1 787)

Le respect des exigences en matière de confidentialité des données est une source d'inquiétude pour moi.
73 % sont d'accord (n = 1 802)

Résultats clés

CONSTAT N°4

Les entreprises préfèrent une solution SaaS facile et rapide à mettre en œuvre.

Avec Office 365, les entreprises se sont engagées de manière consciente et significative envers le SaaS et le cloud. D'une certaine manière, on peut parler de changement de mentalité : les entreprises évoluent d'une approche sur site vers des solutions cloud telles qu'Exchange Online. La croissance d'Office 365 illustre d'ailleurs que cette décision est intelligente et très répandue.

Lorsqu'ils envisagent des solutions, les responsables informatiques se montrent non seulement très intéressés par la sauvegarde en mode SaaS, mais veulent aussi obtenir satisfaction quasi immédiatement. Environ 8 personnes sur 10 souhaitent lancer leurs premières sauvegardes dès leur inscription. Parmi les autres considérations importantes relatives au SaaS, nous retrouvons l'absence de matériel ou de logiciel dont il faut assurer la maintenance : près des trois quarts des personnes ayant répondu ont déclaré qu'il s'agissait là d'une considération importante.

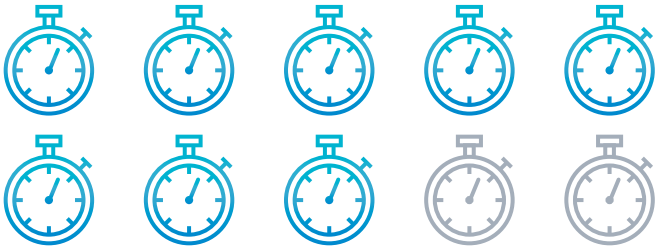
Les participants souhaitent stocker leurs données dans le cloud, et 77 % d'entre eux indiquent vouloir conserver leurs données Office 365 dans Azure, en partie pour des raisons de performance. Rien de surprenant, donc, à ce que 76 % des participants estiment qu'il est essentiel que Microsoft entretienne une relation étroite avec leur fournisseur de services de sauvegarde. Les participants américains se révèlent les plus catégoriques vis-à-vis de ces deux critères, avec respectivement 83 % et 86 % de voix favorables.

Les professionnels de l'informatique mettent également en avant les avantages qu'offre une solution tout-en-un, comparée à un certain nombre de solutions populaires qui nécessitent des licences distinctes pour la sauvegarde et le stockage dans le cloud. Outre leur coût potentiellement plus élevé, les solutions dégroupées nécessitent également une maintenance administrative plus importante, un paramètre rédhibitoire aux yeux des entreprises.

La sauvegarde en mode SaaS pour Office 365 (sans maintenance matérielle ni logicielle) est importante pour moi.
74 % sont d'accord (n = 1 772)

Disposer d'une solution avec licence tout-en-un (plutôt que différentes licences pour le stockage et le traitement informatique) est important pour moi.
79 % sont d'accord (n = 1 787)

Pouvoir m'inscrire et lancer ma sauvegarde immédiatement est important pour moi.
80 % sont d'accord (n = 1 805)



Conclusion

Les leaders mondiaux de l'informatique veulent une solution de sauvegarde SaaS cloud native pour Office 365, à la fois complète, facile d'utilisation et rapide à mettre en œuvre.

Protéger les données Office 365 est une exigence grandissante, et les entreprises veulent des solutions de sauvegarde complètes et faciles d'utilisation. La croissance des données Office 365 n'est pas seulement due à l'augmentation du nombre d'utilisateurs, mais aussi à la nature du travail à distance qui s'appuie fortement sur SharePoint, OneDrive et Teams.

Les entreprises encouragent l'utilisation d'applications collaboratives car elles favorisent la productivité et sont le témoin du travail effectué. En revanche, cette valeur ajoutée diminue largement en l'absence de sauvegarde, notamment parce que les capacités de conservation natives de Microsoft ne sont pas une fonction de sauvegarde. Les clients constatent souvent que les fonctions de restauration nécessaires, au même titre que des fonctionnalités classiques, font défaut.

De nombreuses entreprises découvrent que le recours à ces services de restauration natifs laisse à désirer. Les participants ont manifesté une nette préférence pour un niveau de conservation granulaire, la possibilité de récupérer des boîtes aux lettres sur un emplacement ou utilisateur différent, et différents niveaux de contrôle des accès basés sur les rôles. Plus de la moitié des personnes interrogées souhaitent bénéficier de ces fonctionnalités, mais pour autant, s'appuient toujours sur la conservation native de Microsoft, qui n'en offre aucune.

La facilité d'utilisation est une condition essentielle. La simplicité de l'obtention des licences et la rapidité du déploiement constituent autant de critères qui motivent le recours à des solutions de sauvegarde tierces et éliminent les éventuelles difficultés initiales. De plus, les questions de confidentialité des données et de conformité constituent des motivations supplémentaires qui incitent à adopter une solution de protection des données adaptée.

Enfin, disposer d'une plateforme capable de s'adapter à leur infrastructure Microsoft existante est une autre exigence clé aux yeux des professionnels de l'informatique. Ils sont nombreux à avoir renoncé à un environnement Microsoft sur site après avoir découvert les avantages qu'offre une plateforme SaaS cloud native : la possibilité de stocker les données dans le cloud pendant tout la durée de leur cycle de vie, de meilleures performances, un coût total de possession plus avantageux et zéro maintenance ; autant d'éléments qui sont la preuve de la prise de conscience des avantages liés au cloud.

La facilité d'utilisation est une condition essentielle. La simplicité de l'obtention des licences et la rapidité du déploiement constituent autant de critères qui motivent le recours à des solutions de sauvegarde tierces et éliminent les éventuelles difficultés initiales.

Annexe

CONSTAT N°1

Protéger les données contre les attaques et les pertes (qu'elles soient le fait d'acteurs externes ou internes) est une préoccupation majeure.

Je connais une entreprise qui a été victime d'une attaque par ransomware et qui a du mal à récupérer ses données.
66 % sont d'accord (n = 1 758)

CONSTAT N°2

Les entreprises veulent une solution de sauvegarde complète qui soit également facile à utiliser.

Une solution de sauvegarde avec un espace de stockage illimité est importante pour moi.
84 % sont d'accord (n = 1 794)

La possibilité d'effectuer une restauration des boîtes aux lettres vers un emplacement ou un utilisateur différent est important pour moi.
79 % sont d'accord (n = 1 828)

La possibilité de télécharger une copie des éléments récupérés est importante pour moi.
84 % sont d'accord (n = 1 792)

L'authentification unique avec des services d'annuaire pour gérer ma solution de sauvegarde est importante pour moi.
76 % sont d'accord (n = 1 797)

Je souhaiterais obtenir des rapports quotidiens sur toutes mes sauvegardes, restaurations et exportations.
75 % sont d'accord (n = 1 828)

CONSTAT N°4

Les entreprises préfèrent une solution SaaS qui corresponde à l'infrastructure qu'elles utilisent déjà pour Office 365.

Une solution de sauvegarde qui prend en charge Azure et stocke les données Office 365 dans Azure est importante pour moi.
75 % sont d'accord (n = 1 828)

Une relation étroite entre Microsoft et mon fournisseur de services de sauvegarde est importante pour moi.
76 % sont d'accord (n = 1 793)

Barracuda en quelques mots

Rendre le monde plus sûr est notre objectif chez Barracuda.

Nous pensons que chaque entreprise doit se doter de solutions cloud, faciles à acquérir, à déployer et à utiliser, tout en gardant leur niveau de sécurité. Nous protégeons les e-mails, les réseaux, les données et les applications avec des solutions innovantes et évolutives, qui s'adaptent à la croissance de nos clients.

Plus de 200 000 entreprises à travers le monde font confiance à Barracuda pour les protéger – elles restent sereines face aux risques qui sont toujours là – et peuvent se concentrer sur le développement de leur business.

Pour en savoir plus, rendez-vous sur barracuda.com.

Barracuda
Your journey, secured.