7 raisons cruciales de sauvegarder Microsoft 365

Pourquoi les entreprises doivent protéger leurs données Microsoft 365

Introduction

Exercez-vous un contrôle sur vos données Microsoft 365 ? Avez-vous accès à tous les éléments dont vous avez besoin ? La réponse spontanée est généralement « Bien sûr » ou « Microsoft s'occupe de tout ». En y réfléchissant bien, en avez-vous la certitude ?

Microsoft s'occupe de bien des choses. Il fournit un excellent service à ses clients, en gérant l'infrastructure de Microsoft 365 et en maintenant la disponibilité pour vos utilisateurs. Mais le revers de la médaille, c'est VOUS qui êtes responsable de vos données. On pense souvent à tort que Microsoft sauvegarde automatiquement vos données. Or, une licence Microsoft 365 standard ne garantit pas une sauvegarde complète de celles-ci. En l'absence d'un changement de mentalité, il pourrait y avoir des répercussions néfastes si cette responsabilité n'est pas assumée.

En définitive, vous devez vous assurer que vous avez accès à vos données Exchange Online, SharePoint Online, OneDrive for Business et Microsoft Teams, et que vous les contrôlez. De plus, même si vous ne souhaitez pas gérer une infrastructure de sauvegarde, il existe des services de sauvegarde qui se déploient rapidement, sans aucune gestion ou maintenance manuelle continue. L'accès instantané à une protection des données personnalisable, la restauration ultrarapide et la certitude d'avoir toujours le contrôle. Maintenant, pensez à ce que vous risquez en ne les ayant pas.

Le présent rapport explore les risques auxquels vous vous exposez en ne disposant pas d'un plan de sauvegarde Microsoft 365 dans votre arsenal. Nous expliquerons dans quelle mesure les solutions de sauvegarde pour Microsoft 365, et plus particulièrement les services de sauvegarde basés sur le cloud, comblent les lacunes de la rétention et de la protection des données à long terme et sont absolument essentielles pour les entreprises modernes.

> « Sun Chemical est une entreprise véritablement mondiale : chaque jour, des employés répartis dans le monde entier utilisent les applications Microsoft 365 pour échanger des données stratégiques. Veeam Data Cloud for Microsoft 365 protège cette partie essentielle de notre environnement, en aidant nos collaborateurs à travailler de manière plus productive et en renforçant notre cyber-résilience. »

Stuart Hudson
Responsable senior de l'infrastructure IT mondiale
Programmes d'infrastructure stratégique — AP, Sun Chemical

La grande méprise au sujet de Microsoft 365

Le malentendu se situe entre la responsabilité supposée de Microsoft et la responsabilité réelle de l'utilisateur concernant la protection et la rétention à long terme de ses données Microsoft 365. Il existe souvent une différence entre la résilience et la rétention offertes par Microsoft dans une licence Microsoft 365 standard et ce dont les utilisateurs croient bénéficier. Ainsi, au-delà des mesures de précaution standard en place dans Microsoft 365, il peut être utile de réévaluer votre degré de contrôle des données et le niveau d'accès dont vous bénéficiez réellement.

Microsoft 365 offre une fonction de géo-redondance, qui est souvent confondue avec la sauvegarde. La géo-redondance protège les données contre les défaillances matérielles. Ainsi, si l'infrastructure subit un incident ou une panne, les utilisateurs ne s'en aperçoivent pas dans la plupart des cas et restent productifs. En revanche, la sauvegarde intervient lorsqu'une copie historique des données est réalisée et stockée dans un autre emplacement, distinct de l'environnement de production. Vous avez ainsi l'assurance qu'une copie de vos données existe indépendamment de ce qui se passe dans Microsoft 365, et que la restauration est toujours possible.

Les sauvegardes, plus que la géo-redondance, constituent la dernière ligne de défense d'une entreprise, mais il est tout aussi important de s'assurer que vous y avez directement accès et que vous les contrôlez. En cas de perte, de suppression accidentelle ou de manipulation malveillante de vos données, vous devez avoir la certitude de pouvoir les restaurer rapidement.

Microsoft 365 et le partage de responsabilité

La perception

Microsoft s'occupe de tout.

La réalité

Microsoft s'occupe de l'infrastructure, mais le client est responsable de ses données.

Temps de fonctionnement de Microsoft 365

Protection et rétention à long terme des données Microsoft 365

> "Quel que soit le type de déploiement dans le cloud, vous êtes propriétaire de vos données et identités."

Source : Partage des responsabilités dans le cloud,

7 raisons pour lesquelles un plan de sauvegarde Microsoft 365 est indispensable

Plateforme de logiciels à la demande (SaaS) efficace et extrêmement performante, Microsoft 365 répond parfaitement aux besoins de nombreuses entreprises. Microsoft 365 assure la disponibilité et le fonctionnement des applications afin que vos utilisateurs ne perdent jamais leur rythme. Mais une solution de sauvegarde complète peut vous protéger contre bien d'autres menaces de sécurité, vous apporter une tranquillité d'esprit et assurer une protection des données infaillible.

Vous ou votre supérieur pensez peut-être que la corbeille fera sans doute l'affaire. C'est une erreur très répandue. En effet, il s'écoule environ 140 jours entre le moment où les données sont compromises et la découverte du risque, ce qui représente un écart extrêmement important. Il est fort probable qu'un élément manquant ou disparu ne soit pas repéré à temps pour être récupéré dans la corbeille. Et c'est loin d'être le problème le plus urgent.

Source : 7 étapes vers une stratégie de sécurité holistique, Microsoft

Des échanges avec des centaines de professionnels de l'IT ayant migré vers Microsoft 365 dans le monde entier ont permis de mettre en évidence sept vulnérabilités dans la protection des données :

1. Suppression accidentelle

2. Lacunes et imprécisions dans la stratégie de rétention

3. Menaces de sécurité internes

4. Menaces de sécurité externes

5. Obligations légales et exigences de conformité

6. Gestion des déploiements de messagerie hybride et des migrations vers Microsoft 365

7. Structure des données Teams

1. Suppression accidentelle

Supposons que vous supprimiez un utilisateur. Qu'elle soit volontaire ou non, cette suppression se répercute sur l'ensemble du réseau. Le compte et la boîte aux lettres OneDrive for Business sont également supprimés. Sans aucune alternative, les corbeilles et les historiques de versions natifs de Microsoft 365 offrent une protection limitée contre les pertes de données. Ainsi, une simple tâche de sauvegarde peut devenir un problème majeur une fois que la géo-redondance de Microsoft 365 a définitivement supprimé des données ou que la période de rétention est dépassée.

Il existe deux types de suppression sur la plateforme Microsoft 365 : la suppression réversible et la suppression définitive. Vider le dossier « Éléments supprimés » est un exemple de suppression réversible. Il est également appelé « Supprimé définitivement », bien que dans ce cas, « permanent » ne soit pas strictement permanent, car l'objet se trouve encore dans le dossier « Éléments récupérables ». Une suppression définitive survient lorsqu'un objet est tagué pour être entièrement purgé de la base de données des boîtes aux lettres. Lorsque cela se produit, l'objet est irrécupérable. Mais avec une véritable solution de sauvegarde, il est impossible de perdre des données en cas de suppression accidentelle.

2. Lacunes et imprécisions dans la stratégie de rétention

À l'ère du tout numérique, le rythme soutenu de l'activité entraîne une évolution permanente des règles, notamment des stratégies de rétention difficiles à suivre et à gérer. À l'instar des suppressions réversible et définitive, Microsoft 365 comporte des règles de sauvegarde et de rétention limitées qui ne font qu'éviter de perdre des données en situation, mais ne sont pas prévues pour constituer une solution de sauvegarde universelle.

Un autre type de restauration, à savoir la restauration à un instant précis des éléments de boîte aux lettres, n'est pas inclus dans une licence Microsoft 365 standard. En cas de sinistre, une solution de sauvegarde permet de revenir à un état antérieur au problème pour éviter le drame. De plus, avec une solution de sauvegarde spécialement conçue pour Microsoft 365, les lacunes dans la stratégie de rétention et le manque de flexibilité de la restauration disparaissent. Sauvegardes à court terme ou archives à long terme, restaurations granulaires ou à un instant précis, tout se trouve toujours à portée de main pour rendre la restauration fiable, facile et rapide.

3. Menaces de sécurité internes

La notion de menace de sécurité évoque les pirates et les virus. Cependant, les entreprises sont également confrontées à des menaces venant de l'intérieur plus souvent qu'on ne l'imagine. Elles sont victimes de menaces — intentionnelles ou non — de la part de leurs propres collaborateurs. L'accès aux fichiers et aux contacts change si rapidement qu'il peut être difficile de surveiller ceux en qui vous avez la plus grande confiance.

Microsoft n'a aucun moyen de faire la différence entre un utilisateur ordinaire et un salarié sur le départ qui tenterait de supprimer des données cruciales pour l'entreprise. De plus, sans le savoir, certains utilisateurs engendrent de graves menaces en téléchargeant des fichiers infectés ou en révélant accidentellement des noms d'utilisateur et des mots de passe sur des sites qui, selon eux, sont fiables. Un autre exemple grave est la falsification de preuves par un collaborateur détruisant délibérément des e-mails ou des fichiers compromettants pour les soustraire au service juridique, aux RH ou au responsable de la conformité. Lorsque vos données Microsoft 365 sont correctement protégées, en dehors du site et dans le cloud, des couches de protection sont ajoutées pour lutter contre ces menaces internes. Ainsi, elles sont sécurisées et peuvent être restaurées.

4. Menaces de sécurité externes

Et puis, bien sûr, il y a les menaces malveillantes externes. Les logiciels malveillants, les virus et les ransomware infligent de sérieux dommages aux entreprises du monde entier. Cela représente un risque non seulement pour la réputation de l'entreprise, mais aussi pour la confidentialité et la sécurité de ses données internes et de celles de ses clients.

Les menaces externes se glissent souvent facilement dans les e-mails et les pièces jointes. Il n'est pas toujours suffisant d'éduquer les utilisateurs sur ce à quoi ils doivent faire attention, surtout lorsque les messages infectés semblent si convaincants. Les fonctions limitées de sauvegarde et de restauration d'Exchange Online ne sont pas prévues pour combattre des attaques sérieuses. Des sauvegardes régulières, en particulier celles effectuées hors site et dans le cloud au moyen d'un service de sauvegarde, garantissent qu'une copie distincte de vos données reste intacte et peut être restaurée rapidement, dépassant largement les fonctions limitées de sauvegarde et de restauration d'Exchange Online. De plus, les meilleures solutions de sauvegarde sont intégrées à Microsoft 365 Backup Storage. La restauration rapide de grands ensembles de données après l'attaque par ransomware devient ainsi une réalité pour les entreprises.

5. Obligations légales et exigences de conformité

Parfois, vous devez récupérer de manière inattendue des e-mails, des fichiers ou d'autres types de données dans le cadre d'une action en justice. C'est une situation à laquelle vous n'imaginez peut-être pas être confronté un jour. Microsoft 365 intègre quelques filets de sécurité (tels que la rétention et la conservation pour litige), mais ils sont loin d'être une solution de sauvegarde fiable et ne protégeront pas votre société contre les ennuis juridiques.

Grâce à un service de sauvegarde fiable, si vous supprimez accidentellement des e-mails ou des documents avant la mise en œuvre d'une conservation pour litige, vous pourrez toujours les restaurer pour respecter vos obligations légales. Les obligations légales, les exigences de conformité et les réglementations d'accès varient d'un secteur d'activité à l'autre et d'un pays à l'autre. Or, les amendes, les sanctions et les litiges juridiques ne figurent pas dans votre liste de tâches.

Mieux encore, si vous ne savez pas par où commencer (car beaucoup d'entre nous n'ont tout simplement pas la bande passante suffisante pour suivre l'évolution des législations, réglementations et exigences), un service de sauvegarde s'en chargera pour vous. Grâce aux fonctionnalités de supervision et de reporting qui vous aident à respecter les exigences réglementaires et de conformité, et grâce à la vitesse et la facilité de déploiement de services de sauvegarde, vous pouvez obtenir la certitude que vous respectez ces exigences en quelques minutes seulement.

6. Gestion des déploiements de messagerie hybride et des migrations vers Microsoft 365

Les entreprises qui adoptent Microsoft 365 ont généralement besoin d'une fenêtre transitoire entre leur serveur Exchange local et Microsoft 365 Exchange Online. Ce type de configuration, dans lequel une partie du système de messagerie reste sur site et le reste est transféré vers Microsoft 365 Exchange Online, offre plus de flexibilité et de contrôle. De fait, elle est courante. Mais elle entraîne à son tour des complexités administratives supplémentaires, en particulier en ce qui concerne les sauvegardes. La gestion de plusieurs environnements nécessite une supervision minutieuse pour garantir la fluidité et la protection des données.

C'est là qu'un service de sauvegarde Microsoft 365 s'avère incontournable. Le service de sauvegarde Microsoft idéal gère efficacement les déploiements de messagerie hybride, en traitant de la même manière les données Exchange des systèmes locaux et Microsoft 365. Il rend l'emplacement source non pertinent, simplifie le processus de sauvegarde et élimine la nécessité d'administrer plusieurs systèmes distincts.

7. Structure des données Teams

Plus que jamais, les gens utilisent Teams pour la collaboration, les projets et les initiatives spéciales, le tout à un rythme de plus en plus rapide. Mais une fois que vous avez terminé un projet, il est important d'en conserver une copie pour des besoins à long terme tels que des demandes légales et de conformité. C'est là que les organisations rencontrent souvent des problèmes. Bien souvent, ces dossiers Teams sont supprimés accidentellement ou font l'objet d'une mauvaise rétention, entraînant l'indisponibilité de certains fichiers ou documents essentiels.

Ce n'est jamais le cas avec un service de sauvegarde Microsoft 365. Vos données sont toujours là, peu importe qui ou quoi les supprime. Il peut même être utile dans des scénarios à court terme. Par exemple, si un collaborateur tient des propos inappropriés lors d'une conversation dans Teams et supprime le message, vous pouvez accéder facilement aux sauvegardes. Il suffit de quelques clics pour récupérer les données Teams et les rendre accessibles aux RH pour examen.

Plus que tout, la confiance dans vos sauvegardes est fondamentale. Le fait de savoir qu'ils existent et sont correctement protégés offre une protection contre les menaces inconnues, mais confère également divers moyens de restaurer des conversations ou canaux Teams manquants ou supprimés accidentellement. En adoptant un service de sauvegarde spécialement conçu pour Microsoft Teams, vous avez l'assurance que vos données sont toujours disponibles, quoi qu'il arrive et quand.

Raison bonus : gestion des identités et des accès

Entra ID (anciennement Azure Active Directory) constitue l'épine dorsale de Microsoft 365, assurant la connectivité de tous les services de gestion des identités et des accès, en fournissant aux comptes et groupes d'utilisateurs l'accès aux ressources qu'ils sont autorisés à utiliser. Son importance ne peut être surestimée, c'est pourquoi les acteurs malveillants reconnaissent que le moyen le plus rapide de mettre une organisation à genoux est de cibler Entra ID, avec des attaques qui s'élèvent à 600 millions chaque jour.

La nécessité de protéger Entra ID va au-delà des menaces de cybersécurité, les défis auxquels les entreprises sont confrontées reflètent ceux que nous avons vus dans les sections précédentes : exigences de conformité complexes, limites de corbeille, suppressions accidentelles et erreurs de configuration des stratégies. En définitive, c'est à vous de protéger l'identité de votre société. Pour sécuriser les données Microsoft 365, il est important de s'assurer que vous disposez d'une protection complète des utilisateurs, groupes, enregistrements d'applications et autres objets connexes Entra ID.

Source : Rapport de défense numérique Microsoft 2024

Conclusion

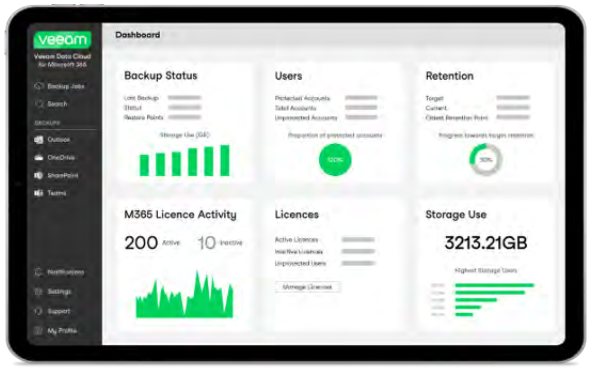
Prenez le temps d'évaluer votre posture de sécurité actuelle. Il peut y avoir des lacunes dont vous ne soupçonniez pas l'existence. Vous avez déjà pris une bonne décision en déployant Microsoft 365. Associez-le maintenant à un service de sauvegarde qui vous offre un accès et un contrôle complets de vos données pour éviter les pertes de données inutiles.

Vous n'avez plus besoin d'investir le temps, l'argent et les ressources associés à une solution logicielle. Avec **Veeam Data Cloud *for Microsoft 365***, vous pouvez tirer parti d'un service tout-en-un comprenant un stockage illimité, et choisir parmi trois plans pour atteindre vos objectifs de sauvegarde et de reprise après incident. Que vous ayez besoin de rapidité et d'évolutivité en matière de sauvegarde et de restauration, de contrôle et de flexibilité, ou d'une combinaison des deux, Veeam a établi un partenariat avec Microsoft pour garantir que vos données sont systématiquement protégées, récupérables et évolutives pour répondre aux besoins de votre entreprise.

Vous avez trouvé ce rapport utile ? N'hésitez pas à le faire suivre par e-mail : Transférez ce rapport.

Veeam Data Cloud *for Microsoft 365* :

Une protection des données résiliente et simplifiée



- Technologie de sauvegarde de Microsoft 365 fiable et leader du marché
- Service de sauvegarde tout compris avec stockage illimité
- Optimisé par le nouveau Microsoft 365 Backup Storage

→ Demander une démo

→ Contactez-nous

→ **Intéressé par la protection d'Entra ID ? Lisez le livre blanc 6 raisons *de sauvegarder Microsoft Entra ID*.**