

# **7 RAISONS**

**pour lesquelles la sauvegarde  
d'Office 365 est indispensable**



# INTRODUCTION

Aujourd’hui, personne ne saurait se passer des différentes applications Microsoft Office 365 : Exchange, SharePoint, OneDrive et Teams. Les utilisateurs ont changé leurs comportements et concentrent sur celles-ci de nombreux documents dont la « durée de vie » doit être sécurisée et garantie : fichiers partagés sous Sharepoint et/ou Teams, qui remplacent de plus en plus les espaces partagés initialement localisés on-premise, emails à conserver obligatoirement pour des raisons de RGPD, etc.

Chez nos clients, ces applications sont ainsi devenues aussi critiques que les applications de production on-premise ou dans le Cloud... Mais ne font pas nécessairement l’objet du même niveau de sécurisation.

En effet, même si les fournisseurs de Cloud protègent le service via des contrats SLA, ce n'est généralement pas le cas pour vos données. Il existe un grand malentendu portant sur la responsabilité de Microsoft dans le domaine de la protection et de la rétention à long terme de celles-ci. Microsoft Office 365 offre la géo-redondance, qui protège uniquement contre les défaillances matérielles (par exemple si l'infrastructure subit un incident ou une panne). En revanche, les données et la sauvegarde associée sont sous la responsabilité des clients.

C'est pourquoi il est indispensable de sauvegarder ses environnements Microsoft Office 365. Aujourd’hui, 76 % des entreprises ne sont pas protégées !

Dans ce cadre, MTI vous accompagne avec son partenaire Veeam, sur la mise en œuvre de solutions efficaces et adaptées à vos besoins.

Des échanges avec des centaines de professionnels de l'IT ayant migré vers Office 365 dans le monde entier ont révélé sept vulnérabilités de 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 de conformité***



**6**

***Gestion des déploiements  
de messagerie hybride et  
migrations vers Office 365***



**7**

***Structure des  
données Teams***

# 1



## **SUPPRESSION ACCIDENTELLE**

Si vous supprimez un utilisateur, volontairement ou non, cette suppression se répercute sur l'ensemble du réseau. Son compte et sa boîte aux lettres OneDrive for Business sont également supprimés.

Les corbeilles et les historiques de versions natifs dans Microsoft 365 offrent une protection limitée contre la perte de données : une simple restauration depuis une sauvegarde peut se transformer en problème majeur dès lors que la géoredondance de Microsoft 365 a définitivement supprimé les données ou que la période de rétention est dépassée.

Il existe deux types de suppression sur la plateforme Microsoft 365 : réversible et définitive. Vider le dossier des éléments supprimés est un exemple de suppression réversible. C'est également ce que l'on appelle une « suppression permanente ». Dans ce cas, « permanente » n'est pas pris au sens strict, car l'objet se trouve encore dans le dossier des 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.

# 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. Tout comme les suppressions réversibles et définitives, Microsoft 365 comporte des règles de sauvegarde et de rétention limitées qui ne peuvent qu'amortir les pertes de données en situation, mais ne sont pas prévues pour constituer une solution de sauvegarde universelle.

Un autre type de restauration, celle des objets de boîte aux lettres à un instant précis, n'est pas couverte par Microsoft. En cas de sinistre, une solution de sauvegarde permet de revenir à un état antérieur au problème pour éviter le drame.

Avec une solution de sauvegarde de Microsoft 365, il n'y a aucune lacune dans la stratégie de rétention ni manque de souplesse dans la restauration. Sauvegardes à court terme ou archives à long terme, restaurations granulaires ou à un instant précis, tout se trouve à portée de main, si bien que la restauration devient 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 s'avérer 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 stratégiques pour l'entreprise. De plus, sans le savoir, certains utilisateurs engendrent de sérieuses menaces en téléchargeant des fichiers infectés ou en révélant accidentellement des noms d'utilisateurs et des mots de passe sur des sites auxquels ils pensent pouvoir faire confiance.

Autre exemple : 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.

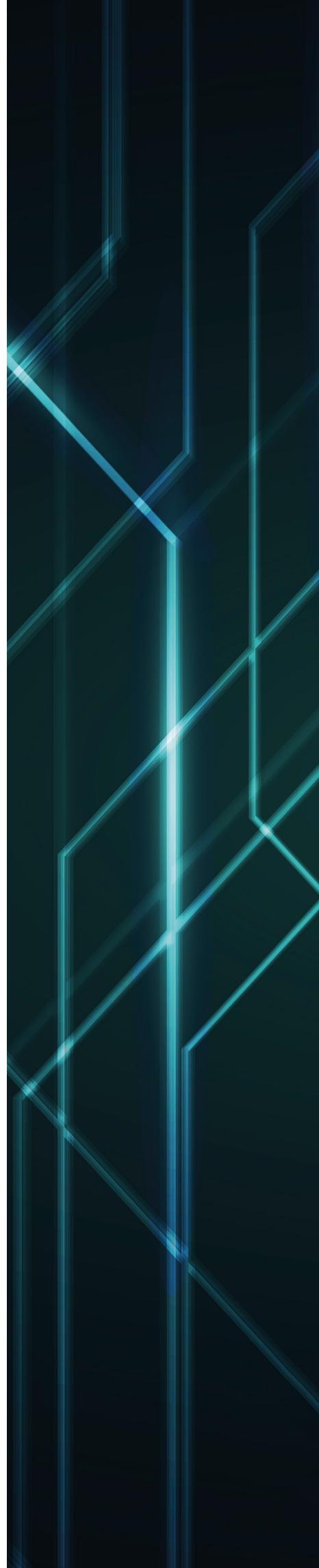
# 4



## MENACES DE SÉCURITÉ EXTERNES

Les logiciels malveillants, les virus et les ransomware infligent de sérieux dommages aux entreprises du monde entier. Ils constituent un risque non seulement pour leur réputation, mais aussi pour la confidentialité des données internes et des données des clients.

Les menaces externes peuvent se glisser dans les e-mails et les pièces jointes. Former les utilisateurs à ce qu'ils doivent surveiller ne suffit pas toujours, en particulier 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 vous permettront de vous assurer qu'une copie distincte de vos données reste intacte et que vous pouvez la restaurer rapidement.



# 5



## OBLIGATIONS LÉGALES ET DE CONFORMITÉ

Vous devez parfois récupérer le contenu de boîtes aux lettres, de fichiers ou d'autres types de données, de manière imprévue, dans le cadre d'une procédure juridique. C'est une situation à laquelle vous n'imaginez peut-être pas être confronté un jour. Microsoft a mis en place quelques filets de sécurité (tels que la conservation pour litige et la rétention). Mais là encore, ceux-ci ne constituent pas une solution de sauvegarde efficace qui saura éviter des ennuis juridiques à votre société. Par exemple, si vous supprimez accidentellement des e-mails ou des documents avant une conservation pour litige, une solution de sauvegarde vous permet de les restaurer et, de fait, de 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 n'ont pas leur place dans tout ce que vous avez à faire.

# 6



## **GESTION DES DÉPLOIEMENTS DE MESSAGERIE HYBRIDE ET MIGRATIONS VERS OFFICE 365**

Les entreprises qui adoptent Office 365 ont généralement besoin d'une période de transition entre leur serveur Exchange local et Office 365 Exchange Online. Certaines conservent même une petite partie de leur ancien système pour disposer d'une flexibilité et d'un contrôle accrues. Bien que courants, ces déploiements de messagerie hybride n'en posent pas moins des problèmes de gestion supplémentaires.

La solution de sauvegarde d'Office 365 idéale doit pouvoir gérer les déploiements de messagerie hybride et traiter de la même manière les données Exchange, faisant ainsi de l'emplacement source un élément négligeable.

Vous devriez en outre être en mesure de stocker les données dans n'importe quel emplacement de votre choix, que ce soit en local, dans un stockage objet dans le cloud (AWS S3 ou Blob Azure) ou via un fournisseur de services gérés.



# 7



## STRUCTURE DES DONNÉES TEAMS

Avec l'essor du télétravail, la plateforme Microsoft Teams fait de plus en plus d'adeptes et connaît une croissance fulgurante. Elle constitue aujourd'hui la quintessence de la productivité. Microsoft structure Teams comme une interface utilisateur qui réunit tous les services d'Office365, tels que SharePoint Online et OneDrive for Business. Une telle approche promet une collaboration et une communication en temps réel plus fluides pour les équipes.

Vous devez sécuriser vos données Teams, mais ce ne sont pas les seuls éléments à protéger. Teams offre des paramètres, des configurations et des niveaux d'adhésion qui nécessitent protection et restauration. Une solution de sauvegarde spécifiquement conçue peut non seulement protéger les données, mais aussi ces paramètres et les interconnexions applicatives associées.

Aujourd'hui plus que jamais, Teams est plébiscitée dans les projets et autres initiatives. Mais lorsque vous clôturez un projet, mieux vaut en conserver une copie (à des fins légales ou de conformité, par exemple). Bien souvent, les dossiers Teams sont supprimés accidentellement ou font l'objet d'une mauvaise rétention, entraînant l'indisponibilité de certains fichiers ou documents essentiels.

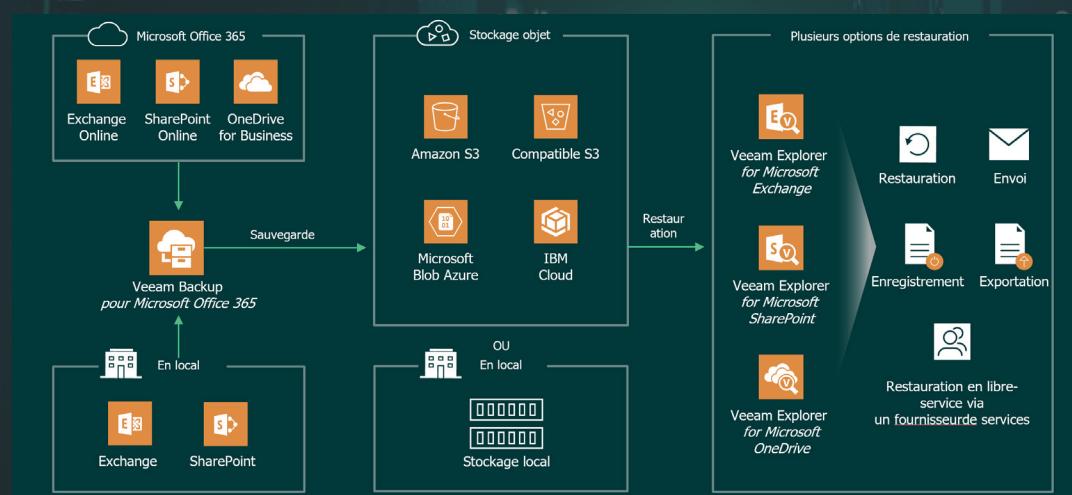
Sur le court terme également, la sauvegarde peut s'avérer utile. Par exemple, si un collaborateur tient des propos inappropriés lors d'une conversation dans Teams et supprime ensuite le message, une sauvegarde permettrait aux RH de récupérer la conversation pour l'examiner. Des fournisseurs de sauvegarde tiers proposent une protection contre les menaces inconnues et de multiples possibilités de restaurer des équipes ou des canaux qui manquent à l'appel ou ont été supprimés accidentellement.

# FAIRE LE BON CHOIX EN TERMES D'ARCHITECTURE DE SAUVEGARDE

Aujourd'hui, les entreprises ont le choix entre différents scénarios d'architectures pour leurs données O365 : on-premise, Cloud Hybride, Cloud...

Avant de mettre en œuvre son plan de sauvegarde (documents à protéger et rétentions), il est donc important de déterminer le modèle le plus adapté.

Pour cela, il est recommandé de se faire accompagner d'un spécialiste qui saura mener le projet et réaliser une étude préalable pour faire le bon choix de solution - avec la bonne stratégie de sauvegarde associée. Vous pourrez ainsi être confiant et serein afin de garantir à vos utilisateurs une protection pleine et entière des données de l'entreprise.





## MTI France

Parc Claude Monet  
3-5 allée de Giverny  
78290 Croissy-sur-Seine

Standard :  
+33 (0)1 30 09 52 00  
FRinfo@mti.com